

# IPsec VPN ?? ???

Published  
2025-07-28

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

*IPsec VPN* ??? ???

Copyright © 2025 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

## YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

## END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://support.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.



?? ?? | xviii

1

## IPsec ?? |

### Internet Key Exchange | 2

IKE(Internet Key Exchange) ?? | 2

IKE(Internet Key Exchange) ?? | 3

IKE? IPsec ?? ?? | 3

IKEv1 ??? | 3

IKE(Internet Key Exchange) ?? ?? 1?? | 4

IKE(Internet Key Exchange) ?? ?? 2?? | 5

IKEv2 ??? | 6

??? ID | 8

??? | 8

IKE(Internet Key Exchange) ??(?? ?? ? ? ???? ?? ??) | 8

???? ?? ??-??(NAT-T) | 9

Suite B ? PRIME ??? | 10

### IPsec ?? ?? | 11

IPsec ?? | 11

IPsec ? ?? | 12

IPsec ?? ???? | 14

IPsec ?? ?? | 16

???? IPsec ? IKE(Internet Key Exchange) ?? | 16

???? IPsec ?? ?? | 18

?? ???? | 19

## Junos OS IPsec VPN

### IPsec VPN IKE(Internet Key Exchange) | 21

IKE(Internet Key Exchange) IPsec | 22

Junos OS IKE(Internet Key Exchange) | 27

IKE(Internet Key Exchange) | 32

IKE(Internet Key Exchange) | 32

| 33

IKE(Internet Key Exchange) ( ) | 34

IKE IPsec SA | 37

| 37

| 37

| 38

| 38

| 49

IKEv2 | 59

(DDoS) IKE | 61

IKE(Internet Key Exchange) (DDoS) | 63

IKE(Internet Key Exchange) SA IKE | 64

IKE(Internet Key Exchange) SA IKE | 66

IKE(Internet Key Exchange) | 67

: | 70

| 70

| 70

| 71

| 79

IKE IPsec SA | 80

IKEv2 | 82

CA IKE(Internet Key Exchange) | 83

IKE Establish-Tunnel Responder-only | 85

IKEv2 | 86

## IPSec VPN | 88

SRX IPsec VPN | 89

VPN VPN VPN | 89

VPN VPN VPN VPN | 91

VPN-VPN st0 | 92

IKE(Internet Key Exchange) IPsec | 94

SPU IKE(Internet Key Exchange) IPsec | 97

SPC(Services Processing Card) VPN | 98

iked IPsec VPN | 99

VPN | 101

IPSec VPN | 101

Anti-Replay | 101

VPN VPN | 102

IPsec VPN | 103

VPN | 105

## IPsec | 111

## VPN

## IPsec VPN | 118

IKE(Internet Key Exchange) IPsec VPN | 118

IP VPN VPN | 119

IP VPN VPN VPN VPN | 121

VPN VPN IPsec VPN | 122

IKE ID | 124

VPN VPN IKE ID | 125

SRX VPN VPN VPN(OSPF) OSPFv3 | 126

2: SRX 2220 222022 22 22 22(OSPF) 222222 22 IPsec 22 22 | 127

22 22 | 128

22 | 128

22 | 129

22 | 132

VPN 2222 2222 IPsec VPN 22 | 133

2: 22 2 2222 VPN 22 | 134

22 22 | 134

22 | 135

22 | 145

22 | 175

22 22 VPN 2 22 22 VPN 22 | 183

22 2222 HA 22 22 2222 | 185

22 22 IPsec VPN | 188

22 22 22 | 188

Junos Key Manager 22 | 189

Quantum Safe IPsec VPN 2 2222 22 | 189

22 2 22(Quantum Key Distribution) | 189

Junos Key Manager 2 22 22 2 2222 22 | 191

2: 2222 2 VPN 2 22 22 2 2222 22 | 193

22 22 22 22 | 193

22222 22 | 194

22 22 | 194

22222 22 | 197

22222 22 | 198

SRX 2222 2222 222222 2222 22 | 198

22 | 201

22 1 : 22 2222 22 22 22 | 206

22 2 : DUT 22 22 22 | 208

2: AutoVPN 22 22 2 2222 22 | 217

22 22 22 22 | 217

|                      |     |
|----------------------|-----|
| ?? ?? ?              | 218 |
| ?? ?                 | 219 |
| ???? ?               | 222 |
| ???? ?               | 224 |
| ???? ? ?             | 224 |
| ?? ? ? ? ? ?         | 227 |
| ??                   | 230 |
| ?? 1 : ? ? ? ? ? ? ? | 239 |
| ?? 2 : DUT ? ? ? ? ? | 243 |

|                                                     |     |
|-----------------------------------------------------|-----|
| Junos Key Manager ? ? Quantum Key Manager ? ? ? ? ? | 255 |
|-----------------------------------------------------|-----|

|                                             |     |
|---------------------------------------------|-----|
| ? : ? ? ? ? IPsec VPN ? ? ? ? ? ? ? ? ? ? ? | 259 |
|---------------------------------------------|-----|

|                         |     |
|-------------------------|-----|
| ?? ? ? ? ?              | 260 |
| ???? ?                  | 260 |
| ?? ?                    | 261 |
| ???? ?                  | 264 |
| ???? ?                  | 265 |
| SRX ? ? ? ? ? ? ? ? ? ? | 265 |
| ??                      | 268 |
| ?? 1 : ? ? ? ? ? ? ?    | 273 |
| ?? 2 : DUT ? ? ? ? ?    | 275 |

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| ? : Quantum Key Manager ? ? ? ? ? ? ? ? ? ? IPsec AutoVPN ? ? ? ? ? | 284 |
|---------------------------------------------------------------------|-----|

|                      |     |
|----------------------|-----|
| ?? ? ? ? ?           | 284 |
| ???? ?               | 285 |
| ?? ?                 | 286 |
| ???? ?               | 290 |
| ???? ?               | 292 |
| ???? ? ? ?           | 292 |
| ?? ? ? ? ? ? ? ?     | 296 |
| ??                   | 299 |
| ?? 1 : ? ? ? ? ? ? ? | 308 |
| ?? 2 : DUT ? ? ? ? ? | 313 |

## ?? ? VPN

|                 |     |
|-----------------|-----|
| ?? ? IPsec VPNs | 327 |
|-----------------|-----|

|                  |     |
|------------------|-----|
| ?? ? IPsec VPN ? | 327 |
|------------------|-----|

## 2. 2.2.2 VPN 2.2 | 328

2.2.2 | 328

2.2 | 328

2.2 | 332

2.2 | 345

## 2.2.2 VPN 2.2.2 VPN 2.2.2.2.2.2 | 351

## 2.2.2.2.2.2 IPsec VPN 2.2 | 355

2.2.2.2.2.2 | 355

2.2.2.2.2.2 | 356

2.2.2.2.2.2 | 359

2.2.2.2.2.2 | 370

IKE, PKI 2.2 IPsec 2.2.2.2.2 | 377

## 2.2.2.2.2.2.2.2 OCSP 2.2.2.2.2.2 IPsec VPN 2.2 | 387

2.2.2.2.2.2.2.2 | 388

2.2.2.2.2.2.2.2 | 388

2.2.2.2.2.2.2.2 | 391

2.2.2.2.2.2.2.2 | 402

## IPv6 IPsec VPN | 409

IPv6 2.2.2.2.2 VPN 2.2.2.2.2 | 409

IPv6 IKE 2.2 IPsec 2.2.2.2.2.2.2.2 | 414

IPv6 IPsec 2.2.2.2.2.2.2.2 | 421

2.2.2.2.2.2.2.2 IPv6 IPsec 2.2.2.2.2.2.2.2 VPN 2.2.2.2.2.2.2.2 | 421

2.2.2.2.2.2.2.2 | 422

2.2.2.2.2.2.2.2 | 422

2.2.2.2.2.2.2.2 | 422

2.2.2.2.2.2.2.2 | 425

2.2.2.2.2.2.2.2 IPv6 2.2.2.2.2 IKE(Internet Key Exchange) 2.2.2.2.2.2.2.2 VPN 2.2.2.2.2.2.2.2 | 425

2.2.2.2.2.2.2.2 | 426

2.2.2.2.2.2.2.2 | 426



?? | 431

?? | 445

???? IPv6 ?? ?? | 449

## ?? ?? VPN

?? ?? IPsec VPN | 452

?? ?? IPSec VPN ?? | 452

?: ?? ?? VPN ?? | 453

?? ?? | 453

?? | 453

?? | 457

?? | 471

IKEv2 ???? ?? ?? VPN | 478

?: IKEv2 ?? ?? ?? VPN ?? | 479

?? ?? | 479

?? | 479

?? | 483

?? | 497

?: IKEv2 ?? ???? ???? Pico ? ???? ???? SRX ??? ? | 503

?? ?? | 503

?? | 504

?? | 509

?? | 529

??? ? ?? CA? IKE(Internet Key Exchange) ?? | 535

?? ???? ?? ?? ???? | 537

?? ?? VPN? ?? ?? ???? ?? ?? | 537

?: ?? ???? st0 ???? ?? | 538

?? ?? | 539

?? | 539

?? | 542

?? | 548

?? ???? ???? ?? ?? ?? ?? | 549

VPN 22 22 22 | 549

2: 22 22 22 22 22 22 22 22 | 553

22 22 | 553

22 | 553

22 | 557

22 | 563

22 22 22 22 IPsec VPN 22 | 567

22 22 22-22 IPsec VPN 22 22 22 22 | 567

2: 22 22 22 22 22 22 22 22 | 569

22 22 | 569

22 | 569

22 | 572

22 | 576

22 22 VPN 22 22 22 | 578

22 22 VPN 22 22 22 22 22 | 578

2: 22 22 VPN 22 22 22 22 | 584

22 22 | 584

22 | 585

22 | 586

22 | 600

6

22 22 22 VPN

CoS 22 IPsec VPN | 606

22 IPsec SA 22 22 22 CoS 22 IPsec VPN 22 | 606

22 22 22 22 CoS 22 IPsec VPN 22 | 609

2: CoS 22 IPsec VPN 22 | 611

22 22 | 611

22 | 612

22 | 616

22 | 636

st0 22 22 22 22 CoS 22 22 | 640

22 22 CoS 22 IPsec VPN 22 | 642

## 7

## NAT-T

NAT-T ? ? ? ? ? ? ? ? ? ? VPN | 645

NAT-T ? ? ? ? ? | 645

? . ? ? ? ? ? ? ? ? (NAT) ? ? ? ? ? ? ? ? ? ? ? ? ? ? VPN ? ? | 646

? ? ? ? ? | 646

? ? | 646

? ? | 652

? ? | 671

? . ? ? ? ? ? ? ? ? (NAT) ? ? ? ? ? ? ? ? ? ? ? ? ? ? VPN ? ? | 681

? ? ? ? ? | 682

? ? | 682

? ? | 689

? ? | 718

? . ? ? ? ? ? ? ? ? VPN ? ? ? ? NAT-T ? ? | 727

? ? ? ? ? | 727

? ? | 728

? ? | 730

? ? | 746

IPsec VPN ? ? ? ? ? ? ? ? NAT-T | 750

## 8

## ?? VPN

?? VPNv1 | 752

?? VPNv1 ? ? | 752

?? VPNv1 ? ? ? ? | 760

?? VPNv1 ? IKE 1 ? ? ? ? ? ? | 761

?? VPNv1 ? ? IPsec SA ? ? ? ? | 762

?? VPNv1 ? ? ? ? ? ? | 762

?? VPNv1 ? ? Antireplay ? ? ? ? | 763

? . ? ? VPNv1 ? ? ? ? ? ? ? ? | 763

? ? ? ? ? | 764

|                                                   |     |
|---------------------------------------------------|-----|
| ??                                                | 764 |
| ??                                                | 765 |
| ??                                                | 781 |
| 2. ??? ?? ? ? ? ? ? ? ? ? VPNv1 ??-?? ? ? ? ?     | 784 |
| ?? ??                                             | 784 |
| ??                                                | 785 |
| ??                                                | 785 |
| ??                                                | 786 |
| 2. ??? ?? ? ? ? ? ? ? ? ? VPNv1 ??-?? ? ? ? ?     | 786 |
| ?? ??                                             | 786 |
| ??                                                | 787 |
| ??                                                | 787 |
| ??                                                | 789 |
| 2. ?? ?? ? ? ? ? ? ? ? ? VPNv1 ??                 | 789 |
| ?? ??                                             | 790 |
| ??                                                | 790 |
| ??                                                | 791 |
| ??                                                | 800 |
| ?? VPNv2                                          | 802 |
| ?? VPNv2 ??                                       | 803 |
| ?? VPNv2 ?? ??                                    | 807 |
| ?? VPNv2? ?? IKE(Internet Key Exchange) 1?? ? ? ? | 808 |
| ?? VPNv2? ?? IPsec SA ?? ? ? ? ?                  | 809 |
| ?? VPNv2 ??? ? ? ? ? ? ? ? ? ?                    | 809 |
| ?? VPNv2 ?? ? ? ? ? ? ? ? ? ? ?                   | 811 |
| ?? VPNv2 ? ? ? ? ? ? ? ? ? ?                      | 811 |
| 2. ?? VPNv2 ?? ? ? ? ? ? ?                        | 812 |
| ?? ??                                             | 812 |
| ??                                                | 813 |
| ??                                                | 814 |
| ??                                                | 849 |

2: 22222 2 222 2222 22 22 VPNv2 22-22 22 22 | 858

22 22 | 858

22 | 858

22 | 859

22 | 859

22 VPNv2 22 2222 | 860

22 VPNv2 22 2222 2222 | 860

22 VPNv2 22 2222 22 22 2222 | 864

22 VPNv2 22 2222 222 2222 | 865

22 VPNv2 22 22222 22 22 2222 | 867

222 22 VPNv2 222 22 VPNv2 22 22222 222222 | 870

2: 22 VPNv2 22 2222 2 222 22 | 871

22 22 | 872

22 | 872

22 | 874

22 | 942

22 22 222

22 22 VPN | 957

22 22 VPN 22 | 957

22 22 222 222 222 222 22 | 963

2: 22 22 VPN 22 222 22 2222 222 222 22 | 965

22 22 | 966

22 | 966

22 | 970

22 | 994

2: IPv6 2222 22 OSPFv3 2222 ADVPN 22 | 1017

22 22 | 1018

22 | 1018

22 | 1021

22 | 1050

ADVPN ? ? ? ? ? OSPF ? ? ? ? ? ? ? ? ? ? | 1053

ADVPN ? ? ? ? ? ? ? ? ? ? | 1054

## AutoVPN

? ? ? ? ? ? ? ? ? ? AutoVPN | 1057

AutoVPN ? ? | 1058

AutoVPN ? ? ? ? ? ? ? ? ? ? | 1063

AutoVPN ? ? ? ? | 1066

? : iBGP ? ? ? ? ? ? AutoVPN ? ? | 1067

? ? ? ? | 1067

? ? | 1067

? ? | 1071

? ? | 1099

? : IPv6 ? ? ? ? ? ? iBGP ? ? ? ? ? ? AutoVPN ? ? | 1103

? ? ? ? | 1103

? ? | 1103

? ? | 1107

? ? | 1136

? : iBGP ? ECMP ? ? ? ? ? ? AutoVPN ? ? | 1140

? ? ? ? | 1140

? ? | 1140

? ? | 1143

? ? | 1167

? : iBGP ? Active-Backup ? ? ? ? ? ? AutoVPN ? ? | 1172

? ? ? ? | 1172

? ? | 1173

? ? | 1177

? ? | 1201

? : OSPF ? ? ? ? ? ? AutoVPN ? ? | 1208

? ? ? ? | 1209

? ? | 1209

? ? | 1213

?? | 1238

?: IPv6 ???? ?? OSPFv3? ???? AutoVPN ?? | 1241

?? ?? | 1241

?? | 1242

?? | 1245

?? | 1274

?: ???? ???? ???? AutoVPN ??? ?? ???? ?? | 1277

?? ?? | 1278

?? | 1278

?? | 1281

?? | 1294

?: AutoVPN ? ??? ???? ?? VPN ?? ???? ?? | 1298

?? ?? | 1299

?? | 1299

?? | 1302

?? | 1323

?: ?? ?? ?? ???? AutoVPN ?? | 1326

P2MP ???? ???? ?? ?? | 1330

???? AutoVPN ?? | 1332

11

?? ??? VPN

Juniper Secure Connect | 1335

12

VPN ???? ?

VPN ???? ? | 1339

VPN ???? ? | 1340

IPsec ??? ?? ? | 1341

Dead Peer Detection(?? ?? ??) | 1342

VPN ?? ???? | 1345

Dead Peer Detection ?? | 1346

VPN ?? ???? ? | 1347

VPN 1348

## VPN 1349

VPN 1350

VPN 1351

VPN 1352

1353

1353

1353

1353

1354

1354

1355

1355

1355

1358

13

## VPN 1360

VPN 1360

VPN 1361

IPsec VPN 1364

IPsec 1365

VPN 1366

VPN 1367

## PowerMode IPsec 1368

PowerMode IPsec 1368

1373

1374

1374

1375



?? | 1378

?: vSRX ?? ???? ???? ???? PMI?? ?? ??(Behavioral Aggregate) ??? ?? | 1379

?? ?? | 1379

?? | 1379

?? | 1380

?? | 1384

?: PMI?? ?? ?? ???? ???? ???? ???? ???? | 1385

?? ?? | 1386

?? | 1386

?? | 1386

?? | 1391

?: PMI? ?? ???? ???? ???? ???? ???? ???? | 1392

?? ?? | 1392

?? | 1393

?? | 1393

?? | 1396

PMI?? IPsec ESP ?? ?? ?? ?? | 1397

???? PMI ?? | 1398

?? ???? ?? | 1399

14

?? ??

??? VPN ?? ?? ?? | 1403

?? ???? ???? ???? ???? VPN ?? ?? | 1405

??? VPN ?? ?? ?? | 1410

IKE(Internet Key Exchange) 2?? VPN ?? ???? ?? ?? | 1412

15

?? ???? ? ?? ??

Junos CLI ?? ?? | 1418

# 第 1 章 网络基础

1.1 网络基础 Junos OS 1.1.1 IPsec VPN 1.1.2 网络基础 1.1.3 网络基础 1.1.4 WAN 1.1.5 网络基础 1.1.6 网络基础 1.1.7 网络基础.

1.1 网络基础

1.1.1 IPsec VPN 1.1.1.1 网络基础

1.1.1.2 网络基础 1.1.1.3 网络基础 1.1.1.4 网络基础

IPsec 1.1.1.1.1 网络基础 GRE 1.1.1.1.2 MPLS 1.1.1.1.3 SRX 1.1.1.1.4

# 1

CHAPTER LABEL COVER PAGE

## IPsec ?? ??

---

### in this chapter

- Internet Key Exchange | 2
  - IPsec ?? ?? | 11
-

# Internet Key Exchange

## summary

IKE is IPsec's main component that negotiates and manages the IPsec security associations.

## in this section

- IKE(Internet Key Exchange) is | 2
- IKE(Internet Key Exchange) is | 3
- IKE/IPsec is | 3
- IKEv1 is | 3
- IKE(Internet Key Exchange) is | 4
- IKE(Internet Key Exchange) is | 5
- IKEv2 is | 6
- ID is | 8
- ID is | 8
- IKE(Internet Key Exchange) is | 8
- NAT-T is | 9
- Suite B is | 10

## IKE(Internet Key Exchange) is

IKE(Internet Key Exchange) is a protocol that negotiates and manages the IPsec security associations.

IKE(Internet Key Exchange) is a protocol that negotiates and manages the IPsec security associations.

- IKE is IPsec's main component that negotiates and manages the IPsec security associations.
- IKE is a protocol that negotiates and manages the IPsec security associations.
- IKE is a protocol that negotiates and manages the IPsec security associations.
- ID is a protocol that negotiates and manages the IPsec security associations.
- Diffie-Hellman is a protocol that negotiates and manages the IPsec security associations.

## IKE(Internet Key Exchange) 介绍

介绍 IKE(Internet Key Exchange) 协议及其作用。

- IKE 版本 1 - RFC 2409 定义了 IKE 协议。
- IKE 版本 2 - IKEv2(IKEv2) RFC 7296 定义了 IKE 协议。

IKEv2(Internet Key Exchange version 2) RFC 7296 定义了 IKE(Internet Key Exchange) 协议。VPN 使用 IKEv1 和 IKEv2 协议。IKEv2 协议比 IKEv1 协议更安全、更高效。IKEv1 协议使用 MD5 和 DES 算法，而 IKEv2 协议使用 SHA-256 和 AES 算法。

IKEv1 和 IKEv2 协议的主要区别如下：

- 802.11 无线网络使用 IKEv2 协议。
- IPsec SA 使用 IKEv2 协议。
- DOS 攻击使用 IKEv2 协议。
- 使用 IKEv2 协议，可以实现快速建立和拆除 IPsec SA。
- 使用 IKEv2 协议，可以实现快速建立和拆除 IPsec SA。

## IKE 与 IPsec 的关系

IPsec 使用 IKE 协议建立和拆除 IPsec SA。

- IKE(Internet Key Exchange) 协议 - IPsec 使用 IKE 协议建立和拆除 IPsec SA。IKE 协议使用 MD5 和 DES 算法，而 IPsec 使用 SHA-256 和 AES 算法。
- IKE 和 IPsec 协议共同使用 IKEv2 协议。

## IKEv1 介绍

IKE(Internet Key Exchange) 协议使用 MD5 和 DES 算法。

- 1998 年，RFC 2409 定义了 IKE 协议。
- 2005 年，RFC 7296 定义了 IPsec 协议。



- **???** - **???(SA)??**, DH **???**, **??** IKE(Internet Key Exchange) ID? **???**.

1?? ?? ? ? ???? ???? ???? ? ? , DH ??? ? ? ???? ? ? ???? DH ??? ?????? . ? 4? ? ? ? ?  
? ?????.

- $\varphi: \mathbb{R}^n \rightarrow \mathbb{R}^n$  -  $\varphi(x) = Ax + b$ ,  $A \in \mathbb{R}^{n \times n}$ ,  $b \in \mathbb{R}^n$ ,  $\det A \neq 0$ ,  $\varphi$  is a linear transformation.
- $\varphi: \mathbb{R}^n \rightarrow \mathbb{R}^n$  -  $\varphi(x) = Ax$ ,  $A \in \mathbb{R}^{n \times n}$ ,  $\det A = 1$ ,  $\varphi$  is a linear transformation.

???? ID? ????? ?????(?? ? ??????), ????? ID ??? ????? ????.

?? ? ???? ??? IKEv1 ?????? ??????. IKEv2 ?????? ?? ? ????? ???? ????? ?????? ??????.

## SEE ALSO

VPNv1 IKE 1?? ?? ?? | 761

## IKE(Internet Key Exchange) ?? ?? 2??

in this section

- ?? ID | 6
- PFS(Perfect Forward Secrecy) | 6
- ?? ?? | 6

???? ???? ??? ??? ? ???? IPsec ??? ?? ??? ???? ???? ?? ?? ??(SA)? ???? 2??? ?? ?????.

[illegible]

1???? ???? ??? ????? 2???? ?? ?? ???? ????? ? ?? ????? ????? ? ?????.





IKE ? ? 2? IKEv1 ???? ? ?????. ? ? VPN ???? ? ? ? ? VPN ? ? ? ? ???? ???? ???? IPsec SA(Security Association)? ? ? ? ? ? ? ????.

IKEv2 IKEv1 1 2, IPsec IKEv2 4. IKEv2.   
.

- IPsec **???** **????** **??** **??** **????** **??????**. **????** **???** **????**/**??????** Diffie-Hellman **???** **???** **??????**.
- **?** **???** IPsec **???** **????** **??** **???** ID? **??????** **??????**.
- **??** - **??** **??** **??** **??** **???** **????**.
- **????** **????** **??**, SA **??** **??** **?** **??** **????** **????** **??????**.

IKEv2 ☐☐ ☐☐☐☐

?? ????? ?????? ?????? ?????? ??? ????? ?? ????? IKEv2 ??????. IKEv2 ?? ?????? ?? ?? VPN???? ??????

RFC 5996, [?] ? [?] [??] [?] 2(IKEv2)? [?] [?] [?] [?] [?] 15[?] [?] [?] [?] [?].

## IKEv2 ? ? ? ? ? ? ? ?

IKEv2[?] ? [?] [?] [?] [?][?][?].

? ???? IKE SA(?? ??)? ?? ? ?? ???? ??? ID ???? ???????? ??? ??????? ?????

```

00000000 VPN 0000 00 00 0000 00 0000 0000 00000000. 000000 IKE SA 0 00 SA0 00 0 00 000000. 00 00 IKE SA 00
00 SA0 0 00000 0 00 00000 00000. 0 IKE 0 00 SA0 00000 00 IKE 0 00 SA0 000000.

```

IKEv2 22222 222222 2222222 22222. 222 22 22 122 100 222 2222 2222 222222 222222. 222 222 2222 2222 22 2  
 2222 IKE 2 222 222222. 22 22, 222 222 222 12 22 IKE 2 2222 22 222 2222 222222. 222 222 222 222 22 22  
 IKE 2 22222 22222 222222. 222 222 222 322 2 22 IKE 2 222 222 2222 222222.

IKEv2 ???

?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? IKEv2 ? ? MTU? ? ? ? ? ? , IKE ? ? ? ? ? MTU? ? ? ? ?  
IP ? ? ? ? ? ? ? ? ? ? NAT ? ? ? ? ? ? ? ? IP ? ? ? ? ? ? ? ? IPsec ? ? ? ? ? ? ? ? .

[illegible]

## IKEv2 配置

IKE 和 IKEv2 是 Internet Key Exchange (Internet Key Exchange) 协议，用于在两个设备之间建立安全连接。IKEv2 是 IKE 的升级版，支持更多的加密算法和认证方式。IKEv2 通常用于建立 VPN 连接，提供安全的网络通信。

## 配置 ID

配置 ID 是指 IKE(Internet Key Exchange) Virtual Private Network(VPN) 的配置 ID。配置 ID 用于标识不同的 VPN 配置。配置 ID 通常由 IP 地址和子网掩码组成。配置 ID 用于标识不同的 VPN 配置。

## 配置

配置 ID 是指 IKE(Internet Key Exchange) Virtual Private Network(VPN) 的配置 ID。配置 ID 用于标识不同的 VPN 配置。配置 ID 通常由 IP 地址和子网掩码组成。配置 ID 用于标识不同的 VPN 配置。

## IKE(Internet Key Exchange) 配置

IKE 是 Internet Key Exchange (Internet Key Exchange) 协议，用于在两个设备之间建立安全连接。IKE 通常用于建立 VPN 连接，提供安全的网络通信。

|           |           |
|-----------|-----------|
| 配置 ID     | 配置 ID     |
| VPN 配置 ID | VPN 配置 ID |

(Continued)

| ?? ?? ? ??                                                                                                                                                                                                                                                                                       | ???? ?? ??                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>?? ?? ?? ? ??? ????? ??? ??????. ? ??? ??, ?? ?? ?? ??? ?? ?????, ??? ????? ??? ?? ?????.</li> <li>?? ?? ?? ??, ?? ? ????? ?? ??? ??? ????? ?? 8?(12? ?? ??)? ????? ? ?? ??? ?? ??? ?????? ?? ????? ???.</li> <li>?? ?? ?? ?? ??? ??? ? ?????.</li> </ul> | <p>???? ?? ?? ?? ?? ????? ?? ??(CA)? ???? ?? ????? ?? ? ?????.</p>                |
| <p>???? ?? ??? ?? Diffie-Hellman ????? ?? ??? ?? ?? ?????? ?? ?????.</p>                                                                                                                                                                                                                         | <p>???? ????? ????? ??? ? ?? CA? ?? ?????? ? ?????.</p>                           |
| <p>?? ?? ?? ?????? ?? ?? ? ?? ?? ?? ?? ??? ? IPsec VPN? ?????.</p>                                                                                                                                                                                                                               | <p>???? ?? ?? ?? ?? ?? ?? ?????? ??? ?? ??? ?? ?? ?? ?? ?? ?????? ?? ? ??????</p> |

## ???? ?? -??(NAT-T)

NAT-T(???? ?? ??-Traversal)? IPsec? ?? ????? ????? ?? ??? ?? ????? ?? ??(NAT) ?????? ??? ? ????? IP ?? ? ? ??? ????? ?????.

NAT? ??? ?????? ?? ????? IKE(Internet Key Exchange)? ??? ??????. 1?? ?? ? ??? ??? ?? ?? ??? ?????? ?? ?? (NAT) ?????? ??? ? , NAT-T? IPsec ??? UDP(User Datagram Protocol) ????? ?????? ?????? ?? ??? ?? ?? ? ?? ?? ?????. NAT-T? ?? ? ?? ?? ??? ?????? ?? 4500? ?? UDP ??? IKE? ESP ??? ??? ???????. ????? ?? ??(NAT) ?????? ?? UDP ??? ?????? ?? ? keepalive ????? ?????.

???? ?? ??(NAT) ?????? ??? ??? ?? ? ?????.

- IKEv1 ?? IKEv2 ?????? ????? ?? ??(NAT) ?????? ?? ?????. ?? ????? ??? ????? ?? ??(NAT) ????? ?? ?? ? ?? ??, ????? ?? ?? ????? ?? ??(NAT) ?????? ?? ????? ??? ? ?????.
- IKEv1 ?? IKEv2 ?????? ?????? ?? ??(NAT) ?????? ?? ?????.
- IKEv1 ?? IKEv2 ?????? ?????? ?? ?????? ?? ??(NAT) ?????? ?? ?????.



# IPsec

## summary

IPsec ? ??, ?? ?????, ?? ??, IPsec ? IKE ??? ? ???? ?  
? ??? ?????.

in this section

- IPsec **??** | **11**
- IPsec **??** | **12**
- IPsec **??** **???** | **14**
- IPsec **??** **??** | **16**
- **???** IPsec **?** IKE(Internet Key Exchange) **?**  
**?** | **16**
- **???** IPsec **??** **??** | **18**
- **??** **???** **??** | **19**

☐? ?☒?☒☒?☒??☒?☒?☒?☒?☒?☒?

???? ???? ???? "???? Isec ?? ??" ??? 18 ???? ?????.

??? ??? ??? "?? ????" ??? 19 ??????.

## IPsec ??

in this section

- ?? ?? | 12

IPsec? IP ?? ???? ???? ???? ???? ?? ?? ???? ?????. IPsec? ?? ??(SA) ? ? ??? ?? ? ?? ?? ??? ?????.  
 ?? ??(DOI)? ?? ?? ???? ?????. IPsec DOI? ???? VPN ?? ??? ?? ?? ??, ? SA? IKE ??? ?? ?? ?? ?  
 ??? ?????. ??? ??? RFC 2407 ? RFC 2408? ??????.

IPsec **??** **????** **????** **??** **SA** **????**. **SA** **?** **????** IPsec **??** **??** **????** **???** **?** **???** **??** **????**. IPsec **?** **?** **???** **SA** **????**. **??** **?** **??**.

IPsec(?? ? ? ? ? ? ?)(?? ? ? ? ? ? ?)? ? ? ? ? ?.



?? ? ? ?? VPN? ????? ? ? ? ????, Junos OS? ? ? ? ? ? ? ???? VPN ??? ???? ? IPsec ???  
????.

- **?? ?**
- **?? ?? ?(PSK) ?? ???? ???? ? ? IKE(Internet Key Exchange)**

1?? ? 2?? ?? ?? ?? ? ?? ???? (?? ??????? ?) ? ??? ? ?????. "Internet Key Exchange" ??? 2? ??????.

?? ?

?? ?? ????? ?? ?? ?? ????? ?? ?? ?? ??? ?????, ?? ?? ? ??, ?? ?? ? ??? ??? ?? ??? ?? ????? ??? ?????, ?  
?? ?? ? ??? ? ??? ????? ????? ?? ??? ?????, ?? ?? ????? ????? ? ??? ?? ??? ?? ?? ?? ????? ????? ??  
??? ? ?????, ?? ?? ????? ? ??? ?? ??? ?? ??? ?? ??? ?????.

## ?? ? IKE(Internet Key Exchange)

[illegible]

- [illegible]

## Diffie-Hellman ??

[illegible]









- RFC 2410, *NULL* [\[1\]](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [\[5\]](#) [\[6\]](#) [\[7\]](#) [\[8\]](#) [\[9\]](#) [\[10\]](#) [\[11\]](#) [\[12\]](#) [\[13\]](#) [\[14\]](#) [\[15\]](#) [\[16\]](#) [\[17\]](#) [\[18\]](#) [\[19\]](#) [\[20\]](#) [\[21\]](#) [\[22\]](#) [\[23\]](#) [\[24\]](#) [\[25\]](#) [\[26\]](#) [\[27\]](#) [\[28\]](#) [\[29\]](#) [\[30\]](#) [\[31\]](#) [\[32\]](#) [\[33\]](#) [\[34\]](#) [\[35\]](#) [\[36\]](#) [\[37\]](#) [\[38\]](#) [\[39\]](#) [\[40\]](#) [\[41\]](#) [\[42\]](#) [\[43\]](#) [\[44\]](#) [\[45\]](#) [\[46\]](#) [\[47\]](#) [\[48\]](#) [\[49\]](#) [\[50\]](#) [\[51\]](#) [\[52\]](#) [\[53\]](#) [\[54\]](#) [\[55\]](#) [\[56\]](#) [\[57\]](#) [\[58\]](#) [\[59\]](#) [\[60\]](#) [\[61\]](#) [\[62\]](#) [\[63\]](#) [\[64\]](#) [\[65\]](#) [\[66\]](#) [\[67\]](#) [\[68\]](#) [\[69\]](#) [\[70\]](#) [\[71\]](#) [\[72\]](#) [\[73\]](#) [\[74\]](#) [\[75\]](#) [\[76\]](#) [\[77\]](#) [\[78\]](#) [\[79\]](#) [\[80\]](#) [\[81\]](#) [\[82\]](#) [\[83\]](#) [\[84\]](#) [\[85\]](#) [\[86\]](#) [\[87\]](#) [\[88\]](#) [\[89\]](#) [\[90\]](#) [\[91\]](#) [\[92\]](#) [\[93\]](#) [\[94\]](#) [\[95\]](#) [\[96\]](#) [\[97\]](#) [\[98\]](#) [\[99\]](#) [\[100\]](#) [\[101\]](#) [\[102\]](#) [\[103\]](#) [\[104\]](#) [\[105\]](#) [\[106\]](#) [\[107\]](#) [\[108\]](#) [\[109\]](#) [\[110\]](#) [\[111\]](#) [\[112\]](#) [\[113\]](#) [\[114\]](#) [\[115\]](#) [\[116\]](#) [\[117\]](#) [\[118\]](#) [\[119\]](#) [\[120\]](#) [\[121\]](#) [\[122\]](#) [\[123\]](#) [\[124\]](#) [\[125\]](#) [\[126\]](#) [\[127\]](#) [\[128\]](#) [\[129\]](#) [\[130\]](#) [\[131\]](#) [\[132\]](#) [\[133\]](#) [\[134\]](#) [\[135\]](#) [\[136\]](#) [\[137\]](#) [\[138\]](#) [\[139\]](#) [\[140\]](#) [\[141\]](#) [\[142\]](#) [\[143\]](#) [\[144\]](#) [\[145\]](#) [\[146\]](#) [\[147\]](#) [\[148\]](#) [\[149\]](#) [\[150\]](#) [\[151\]](#) [\[152\]](#) [\[153\]](#) [\[154\]](#) [\[155\]](#) [\[156\]](#) [\[157\]](#) [\[158\]](#) [\[159\]](#) [\[160\]](#) [\[161\]](#) [\[162\]](#) [\[163\]](#) [\[164\]](#) [\[165\]](#) [\[166\]](#) [\[167\]](#) [\[168\]](#) [\[169\]](#) [\[170\]](#) [\[171\]](#) [\[172\]](#) [\[173\]](#) [\[174\]](#) [\[175\]](#) [\[176\]](#) [\[177\]](#) [\[178\]](#) [\[179\]](#) [\[180\]](#) [\[181\]](#) [\[182\]](#) [\[183\]](#) [\[184\]](#) [\[185\]](#) [\[186\]](#) [\[187\]](#) [\[188\]](#) [\[189\]](#) [\[190\]](#) [\[191\]](#) [\[192\]](#) [\[193\]](#) [\[194\]](#) [\[195\]](#) [\[196\]](#) [\[197\]](#) [\[198\]](#) [\[199\]](#) [\[200\]](#) [\[201\]](#) [\[202\]](#) [\[203\]](#) [\[204\]](#) [\[205\]](#) [\[206\]](#) [\[207\]](#) [\[208\]](#) [\[209\]](#) [\[210\]](#) [\[211\]](#) [\[212\]](#) [\[213\]](#) [\[214\]](#) [\[215\]](#) [\[216\]](#) [\[217\]](#) [\[218\]](#) [\[219\]](#) [\[220\]](#) [\[221\]](#) [\[222\]](#) [\[223\]](#) [\[224\]](#) [\[225\]](#) [\[226\]](#) [\[227\]](#) [\[228\]](#) [\[229\]](#) [\[230\]](#) [\[231\]](#) [\[232\]](#) [\[233\]](#) [\[234\]](#) [\[235\]](#) [\[236\]](#) [\[237\]](#) [\[238\]](#) [\[239\]](#) [\[240\]](#) [\[241\]](#) [\[242\]](#) [\[243\]](#) [\[244\]](#) [\[245\]](#) [\[246\]](#) [\[247\]](#) [\[248\]](#) [\[249\]](#) [\[250\]](#) [\[251\]](#) [\[252\]](#) [\[253\]](#) [\[254\]](#) [\[255\]](#) [\[256\]](#) [\[257\]](#) [\[258\]](#) [\[259\]](#) [\[260\]](#) [\[261\]](#) [\[262\]](#) [\[263\]](#) [\[264\]](#) [\[265\]](#) [\[266\]](#) [\[267\]](#) [\[268\]](#) [\[269\]](#) [\[270\]](#) [\[271\]](#) [\[272\]](#) [\[273\]](#) [\[274\]](#) [\[275\]](#) [\[276\]](#) [\[277\]](#) [\[278\]](#) [\[279\]](#) [\[280\]](#) [\[281\]](#) [\[282\]](#) [\[283\]](#) [\[284\]](#) [\[285\]](#) [\[286\]](#) [\[287\]](#) [\[288\]](#) [\[289\]](#) [\[290\]](#) [\[291\]](#) [\[292\]](#) [\[293\]](#) [\[294\]](#) [\[295\]](#) [\[296\]](#) [\[297\]](#) [\[298\]](#) [\[299\]](#) [\[300\]](#) [\[301\]](#) [\[302\]](#) [\[303\]](#) [\[304\]](#) [\[305\]](#) [\[306\]](#) [\[307\]](#) [\[308\]](#) [\[309\]](#) [\[310\]](#) [\[311\]](#) [\[312\]](#) [\[313\]](#) [\[314\]](#) [\[315\]](#) [\[316\]](#) [\[317\]](#) [\[318\]](#) [\[319\]](#) [\[320\]](#) [\[321\]](#) [\[322\]](#) [\[323\]](#) [\[324\]](#) [\[325\]](#) [\[326\]](#) [\[327\]](#) [\[328\]](#) [\[329\]](#) [\[330\]](#) [\[331\]](#) [\[332\]](#) [\[333\]](#) [\[334\]](#) [\[335\]](#) [\[336\]](#) [\[337\]](#) [\[338\]](#) [\[339\]](#) [\[340\]](#) [\[341\]](#) [\[342\]](#) [\[343\]](#) [\[344\]](#) [\[345\]](#) [\[346\]](#) [\[347\]](#) [\[348\]](#) [\[349\]](#) [\[350\]](#) [\[351\]](#) [\[352\]](#) [\[353\]](#) [\[354\]](#) [\[355\]](#) [\[356\]](#) [\[357\]](#) [\[358\]](#) [\[359\]](#) [\[360\]](#) [\[361\]](#) [\[362\]](#) [\[363\]](#) [\[364\]](#) [\[365\]](#) [\[366\]](#) [\[367\]](#) [\[368\]](#) [\[369\]](#) [\[370\]](#) [\[371\]](#) [\[372\]](#) [\[373\]](#) [\[374\]](#) [\[375\]](#) [\[376\]](#) [\[377\]](#) [\[378\]](#) [\[379\]](#) [\[380\]](#) [\[381\]](#) [\[382\]](#) [\[383\]](#) [\[384\]](#) [\[385\]](#) [\[386\]](#) [\[387\]](#) [\[388\]](#) [\[389\]](#) [\[390\]](#) [\[391\]](#) [\[392\]](#) [\[393\]](#) [\[394\]](#) [\[395\]](#) [\[396\]](#) [\[397\]](#) [\[398\]](#) [\[399\]](#) [\[400\]](#) [\[401\]](#) [\[402\]](#) [\[403\]](#) [\[404\]](#) [\[405\]](#) [\[406\]](#) [\[407\]](#) [\[408\]](#) [\[409\]](#) [\[410\]](#) [\[411\]](#) [\[412\]](#) [\[413\]](#) [\[414\]](#) [\[415\]](#) [\[416\]](#) [\[417\]](#) [\[418\]](#) [\[419\]](#) [\[420\]](#) [\[421\]](#) [\[422\]](#) [\[423\]](#) [\[424\]](#) [\[425\]](#) [\[426\]](#) [\[427\]](#) [\[428\]](#) [\[429\]](#) [\[430\]](#) [\[431\]](#) [\[432\]](#) [\[433\]](#) [\[434\]](#) [\[435\]](#) [\[436\]](#) [\[437\]](#) [\[438\]](#) [\[439\]](#) [\[440\]](#) [\[441\]](#) [\[442\]](#) [\[443\]](#) [\[444\]](#) [\[445\]](#) [\[446\]](#) [\[447\]](#) [\[448\]](#) [\[449\]](#) [\[450\]](#) [\[451\]](#) [\[452\]](#) [\[453\]](#) [\[454\]](#) [\[455\]](#) [\[456\]](#) [\[457\]](#) [\[458\]](#) [\[459\]](#) [\[460\]](#) [\[461\]](#) [\[462\]](#) [\[463\]](#) [\[464\]](#) [\[465\]](#) [\[466\]](#) [\[467\]](#) [\[468\]](#) [\[469\]](#) [\[470\]](#) [\[471\]](#) [\[472\]](#) [\[473\]](#) [\[474\]](#) [\[475\]](#) [\[476\]](#) [\[477\]](#) [\[478\]](#) [\[479\]](#) [\[480\]](#) [\[481\]](#) [\[482\]](#) [\[483\]](#) [\[484\]](#) [\[485\]](#) [\[486\]](#) [\[487\]](#) [\[488\]](#) [\[489\]](#) [\[490\]](#) [\[491\]](#) [\[492\]](#) [\[493\]](#) [\[494\]](#) [\[495\]](#) [\[496\]](#) [\[497\]](#) [\[498\]](#) [\[499\]](#) [\[500\]](#) [\[501\]](#) [\[502\]](#) [\[503\]](#) [\[504\]](#) [\[505\]](#) [\[506\]](#) [\[507\]](#) [\[508\]](#) [\[509\]](#) [\[510\]](#) [\[511\]](#) [\[512\]](#) [\[513\]](#) [\[514\]](#) [\[515\]](#) [\[516\]](#) [\[517\]](#) [\[518\]](#) [\[519\]](#) [\[520\]](#) [\[521\]](#) [\[522\]](#) [\[523\]](#) [\[524\]](#) [\[525\]](#) [\[526\]](#) [\[527\]](#) [\[528\]](#) [\[529\]](#) [\[530\]](#) [\[531\]](#) [\[532\]](#) [\[533\]](#) [\[534\]](#) [\[535\]](#) [\[536\]](#) [\[537\]](#) [\[538\]](#) [\[539\]](#) [\[540\]](#) [\[541\]](#) [\[542\]](#) [\[543\]](#) [\[544\]](#) [\[545\]](#) [\[546\]](#) [\[547\]](#) [\[548\]](#) [\[549\]](#) [\[550\]](#) [\[551\]](#) [\[552\]](#) [\[553\]](#) [\[554\]](#) [\[555\]](#) [\[556\]](#) [\[557\]](#) [\[558\]](#) [\[559\]](#) [\[560\]](#) [\[561\]](#) [\[562\]](#) [\[563\]](#) [\[564\]](#) [\[565\]](#) [\[566\]](#) [\[567\]](#) [\[568\]](#) [\[569\]](#) [\[570\]](#) [\[571\]](#) [\[572\]](#) [\[573\]](#) [\[574\]](#) [\[575\]](#) [\[576\]](#) [\[577\]](#) [\[578\]](#) [\[579\]](#) [\[580\]](#) [\[581\]](#) [\[582\]](#) [\[583\]](#) [\[584\]](#) [\[585\]](#) [\[586\]](#) [\[587\]](#) [\[588\]](#) [\[589\]](#) [\[590\]](#) [\[591\]](#) [\[592\]](#) [\[593\]](#) [\[594\]](#) [\[595\]](#) [\[596\]](#) [\[597\]](#) [\[598\]](#) [\[599\]](#) [\[600\]](#) [\[601\]](#) [\[602\]](#) [\[603\]](#) [\[604\]](#) [\[605\]](#) [\[606\]](#) [\[607\]](#) [\[608\]](#) [\[609\]](#) [\[610\]](#) [\[611\]](#) [\[612\]](#) [\[613\]](#) [\[614\]](#) [\[615\]](#) [\[616\]](#) [\[617\]](#) [\[618\]](#) [\[619\]](#) [\[620\]](#) [\[621\]](#) [\[622\]](#) [\[623\]](#) [\[624\]](#) [\[625\]](#) [\[626\]](#) [\[627\]](#) [\[628\]](#) [\[629\]](#) [\[630\]](#) [\[631\]](#) [\[632\]](#) [\[633\]](#) [\[634\]](#) [\[635\]](#) [\[636\]](#) [\[637\]](#) [\[638\]](#) [\[639\]](#) [\[640\]](#) [\[641\]](#) [\[642\]](#) [\[643\]](#) [\[644\]](#) [\[645\]](#) [\[646\]](#) [\[647\]](#) [\[648\]](#) [\[649\]](#) [\[650\]](#) [\[651\]](#) [\[652\]](#) [\[653\]](#) [\[654\]](#) [\[655\]](#) [\[656\]](#) [\[657\]](#) [\[658\]](#) [\[659\]](#) [\[660\]](#) [\[661\]](#) [\[662\]](#) [\[663\]](#) [\[664\]](#) [\[665\]](#) [\[666\]](#) [\[667\]](#) [\[668\]](#) [\[669\]](#) [\[670\]](#) [\[671\]](#) [\[672\]](#) [\[673\]](#) [\[674\]](#) [\[675\]](#) [\[676\]](#) [\[677\]](#) [\[678\]](#) [\[679\]](#) [\[680\]](#) [\[681\]](#) [\[682\]](#) [\[683\]](#) [\[684\]](#) [\[685\]](#) [\[686\]](#) [\[687\]](#) [\[688\]](#) [\[689\]](#) [\[690\]](#) [\[691\]](#) [\[692\]](#) [\[693\]](#) [\[694\]](#) [\[695\]](#) [\[696\]](#) [\[697\]](#) [\[698\]](#) [\[699\]](#) [\[700\]](#) [\[701\]](#) [\[702\]](#) [\[703\]](#) [\[704\]](#) [\[705\]](#) [\[706\]](#) [\[707\]](#) [\[708\]](#) [\[709\]](#) [\[710\]](#) [\[711\]](#) [\[712\]](#) [\[713\]](#) [\[714\]](#) [\[715\]](#) [\[716\]](#) [\[717\]](#) [\[718\]](#) [\[719\]](#) [\[720\]](#) [\[721\]](#) [\[722\]](#) [\[723\]](#) [\[724\]](#) [\[725\]](#) [\[726\]](#) [\[727\]](#) [\[728\]](#) [\[729\]](#) [\[730\]](#) [\[731\]](#) [\[732\]](#) [\[733\]](#) [\[734\]](#) [\[735\]](#) [\[736\]](#) [\[737\]](#) [\[738\]](#) [\[739\]](#) [\[740\]](#) [\[741\]](#) [\[742\]](#) [\[743\]](#) [\[744\]](#) [\[745\]](#) [\[746\]](#) [\[747\]](#) [\[748\]](#) [\[749\]](#) [\[750\]](#) [\[751\]](#) [\[752\]](#) [\[753\]](#) [\[754\]](#) [\[755\]](#) [\[756\]](#) [\[757\]](#) [\[758\]](#) [\[759\]](#) [\[760\]](#) [\[761\]](#) [\[762\]](#) [\[763\]](#) [\[764\]](#) [\[765\]](#) [\[766\]](#) [\[767\]](#) [\[768\]](#) [\[769\]](#) [\[770\]](#) [\[771\]](#) [\[772\]](#) [\[773\]](#) [\[774\]](#) [\[775\]](#) [\[776\]](#) [\[777\]](#) [\[778\]](#) [\[779\]](#) [\[780\]](#) [\[781\]](#) [\[782\]](#) [\[783\]](#) [\[784\]](#) [\[785\]](#) [\[786\]](#) [\[787\]](#) [\[788\]](#) [\[789\]](#) [\[790\]](#) [\[791\]](#) [\[792\]](#) [\[793\]](#) [\[794\]](#) [\[795\]](#) [\[796\]](#) [\[797\]](#) [\[798\]](#) [\[799\]](#) [\[800\]](#) [\[801\]](#) [\[802\]](#) [\[803\]](#) [\[804\]](#) [\[805\]](#) [\[806\]](#) [\[807\]](#) [\[808\]](#) [\[809\]](#) [\[810\]](#) [\[811\]](#) [\[812\]](#) [\[813\]](#) [\[814\]](#) [\[815\]](#) [\[816\]](#) [\[817\]](#) [\[818\]](#) [\[819\]](#) [\[820\]](#) [\[821\]](#) [\[822\]](#) [\[823\]](#) [\[824\]](#) [\[825\]](#) [\[826\]](#) [\[827\]](#) [\[828\]](#) [\[829\]](#) [\[830\]](#) [\[831\]](#) [\[832\]](#) [\[833\]](#) [\[834\]](#) [\[835\]](#) [\[836\]](#) [\[837\]](#) [\[838\]](#) [\[839\]](#) [\[840\]](#) [\[841\]](#) [\[842\]](#) [\[843\]](#) [\[844\]](#) [\[845\]](#) [\[846\]](#) [\[847\]](#) [\[848\]](#) [\[849\]](#) [\[850\]](#) [\[851\]](#) [\[852\]](#) [\[853\]](#) [\[854\]](#) [\[855\]](#) [\[856\]](#) [\[857\]](#) [\[858\]](#) [\[859\]](#) [\[860\]](#) [\[861\]](#) [\[862\]](#) [\[863\]](#) [\[864\]](#) [\[865\]](#) [\[866\]](#) [\[867\]](#) [\[868\]](#) [\[869\]](#) [\[870\]](#) [\[871\]](#) [\[872\]](#) [\[873\]](#) [\[874\]](#) [\[875\]](#) [\[876\]](#) [\[877\]](#) [\[878\]](#) [\[879\]](#) [\[880\]](#) [\[881\]](#) [\[882\]](#) [\[883\]](#) [\[884\]](#) [\[885\]](#) [\[886\]](#) [\[887\]](#) [\[888\]](#) [\[889\]](#) [\[890\]](#) [\[891\]](#) [\[892\]](#) [\[893\]](#) [\[894\]](#) [\[895\]](#) [\[896\]](#) [\[897\]](#) [\[898\]](#) [\[899\]](#) [\[900\]](#) [\[901\]](#) [\[902\]](#) [\[903\]](#) [\[904\]](#) [\[905\]](#) [\[906\]](#) [\[907\]](#) [\[908\]](#) [\[909\]](#) [\[910\]](#) [\[911\]](#) [\[912\]](#) [\[913\]](#) [\[914\]](#) [\[915\]](#) [\[916\]](#) [\[917\]](#) [\[918\]](#) [\[919\]](#) [\[920\]](#) [\[921\]](#) [\[922\]](#) [\[923\]](#) [\[924\]](#) [\[925\]](#) [\[926\]](#) [\[927\]](#) [\[928\]](#) [\[929\]](#) [\[930\]](#) [\[931\]](#) [\[932\]](#) [\[933\]](#) [\[934\]](#) [\[935\]](#) [\[936\]](#) [\[937\]](#) [\[938\]](#) [\[939\]](#) [\[940\]](#) [\[941\]](#) [\[942\]](#) [\[943\]](#) [\[944\]](#) [\[945\]](#) [\[946\]](#) [\[947\]](#) [\[948\]](#) [\[949\]](#) [\[950\]](#) [\[951\]](#) [\[952\]](#) [\[953\]](#) [\[954\]](#) [\[955\]](#) [\[956\]](#) [\[957\]](#) [\[958\]](#) [\[959\]](#) [\[960\]](#) [\[961\]](#) [\[962\]](#) [\[963\]](#) [\[964\]](#) [\[965\]](#) [\[966\]](#) [\[967\]](#) [\[968\]](#) [\[969\]](#) [\[970\]](#) [\[971\]](#) [\[972\]](#) [\[973\]](#) [\[974\]](#) [\[975\]](#) [\[976\]](#) [\[977\]](#) [\[978\]](#) [\[979\]](#) [\[980\]](#) [\[981\]](#) [\[982\]](#) [\[983\]](#) [\[984\]](#) [\[985\]](#) [\[986\]](#) [\[987\]](#) [\[988\]](#) [\[989\]](#) [\[990\]](#) [\[991\]](#) [\[992\]](#) [\[993\]](#) [\[994\]](#) [\[995\]](#) [\[996\]](#) [\[997\]](#) [\[998\]](#) [\[999\]](#) [\[1000\]](#) [\[1001\]](#) [\[1002\]](#) [\[1003\]](#) [\[1004\]](#) [\[1005\]](#) [\[1006\]](#) [\[1007\]](#) [\[1008\]](#) [\[1009\]](#) [\[1010\]](#) [\[1011\]](#) [\[1012\]](#) [\[1013\]](#) [\[1014\]](#) [\[1015\]](#) [\[1016\]](#) [\[1017\]](#) [\[1018\]](#) [\[1019\]](#) [\[1020\]](#) [\[1021\]](#) [\[1022\]](#) [\[1023\]](#) [\[1024\]](#) [\[1025\]](#) [\[1026\]](#) [\[1027\]](#) [\[1028\]](#) [\[1029\]](#) [\[1030\]](#) [\[1031\]](#) [\[1032\]](#) [\[1033\]](#) [\[1034\]](#) [\[1035\]](#) [\[1036\]](#) [\[1037\]](#) [\[1038\]](#) [\[1039\]](#) [\[1040\]](#) [\[1041\]](#) [\[1042\]](#) [\[1043\]](#) [\[1044\]](#) [\[1045\]](#) [\[1046\]](#) [\[1047\]](#) [\[1048\]](#) [\[1049\]](#) [\[1050\]](#) [\[1051\]](#) [\[1052\]](#) [\[1053\]](#) [\[1054\]](#) [\[1055\]](#) [\[1056\]](#) [\[1057\]](#) [\[1058\]](#) [\[1059\]](#) [\[1060\]](#) [\[1061\]](#) [\[1062\]](#) [\[1063\]](#) [\[1064\]](#) [\[1065\]](#) [\[1066\]](#) [\[1067\]](#) [\[1068\]](#) [\[1069\]](#) [\[1070\]](#) [\[1071\]](#) [\[1072\]](#) [\[1073\]](#) [\[1074\]](#) [\[1075\]](#) [\[1076\]](#) [\[1077\]](#) [\[1078\]](#) [\[1079\]](#) [\[1080\]](#) [\[1081\]](#) [\[1082\]](#) [\[1083\]](#) [\[1084\]](#) [\[1085\]](#) [\[1086\]](#) [\[1087\]](#) [\[1088\]](#) [\[1089\]](#) [\[1090\]](#) [\[1091\]](#) [\[1092\]](#) [\[1093\]](#) [\[1094\]](#) [\[1095\]](#) [\[1096\]](#) [\[1097\]](#) [\[1098\]](#) [\[1099\]](#) [\[1100\]](#) [\[1101\]](#) [\[1102\]](#) [\[1103\]](#) [\[1104\]](#) [\[1105\]](#) [\[1106\]](#) [\[1107\]](#) [\[1108\]](#) [\[1109\]](#) [\[1110\]](#) [\[1111\]](#) [\[1112\]](#) [\[1113\]](#) [\[1114\]](#) [\[1115\]](#) [\[1116\]](#) [\[1117\]](#) [\[11](#)

- RFC 3526, *IKE(Internet Key Exchange)* *MODP(More Modular Exponential) Diffie-Hellman*
  - RFC 5114, *IETF Diffie-Hellman*
  - RFC 5903, *IKE IKEv2 ECP(Elliptic Curve Groups modulo a Prime)*
- RFC "IPsec, IKE". IETF "IPsec".
- RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*
  - RFC 2412, *OAKLEY*
  - RFC 3706, *IKE(Internet Key Exchange)*
  - draft-eastlake-sha2-02.txt, *(SHA HMAC-SHA)(2006 7)*

SEE ALSO

- [IPsec](#)
- [MX 5G](#)
- [IPsec](#)

IPsec

IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.

IPsec is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet in a communication session.

2: IPsec

| SRX | IPsec                                                                                                                             |
|-----|-----------------------------------------------------------------------------------------------------------------------------------|
|     | <ul style="list-style-type: none"><li>• IPsec VPN SRX5400, SRX5600 SRX5800:</li><li>• Junos OS SPU</li><li>• SPU ESP AH</li></ul> |

?? ???? ??

?? ???? ???? ? ???? ? ???? ? ???? ? ???? ?????. ?? ???? ???? ? ????.

3: ?? ???? ??

|                         |                                                            |                    |                                                                |                               |                                           |
|-------------------------|------------------------------------------------------------|--------------------|----------------------------------------------------------------|-------------------------------|-------------------------------------------|
| ??                      | SRX300<br>SRX320<br>SRX340<br>SRX345<br>SRX380<br>SRX550HM | SRX1500<br>SRX1600 | SRX2300<br>SRX4100<br>SRX4200<br>SRX4300<br>SRX4600<br>SRX4700 | SRX5400<br>SRX5600<br>SRX5800 | vSRX ?? ???                               |
| DH ?? 15,<br>16 ? 21 ?? | ???                                                        | ?                  | ?                                                              | ?                             | vSRX 3.0(??? ?<br>? junos-ike )? ?<br>? ? |

?? ?? ?

?? ??? ?? ? ???? ???? ? ?????. [Feature Explorer](#) ? ???? ???? ???? ?????.

|                                           |                                                                                                                                        |
|-------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| release heading<br>in release-<br>history | desc heading in release-history                                                                                                        |
| 24.2R1                                    | Junos OS ??? 24.2R1? SRX1600, SRX2300, SRX4300, SRX4600, SRX5400, SRX5600,<br>SRX5800 ? vSRX 3.0? ChaCha20-Poly1305 ???? ? ???? ?????. |
| 20.3R1                                    | Junos OS ??? 20.3R1?? vSRX ?? ???? DH ?? 15, 16 ? 21? ????.                                                                            |
| 19.1R1                                    | Junos OS ??? 19.1R1?? SRX ??? ???? DH ?? 15, 16 ? 21? ????.                                                                            |

# 2

CHAPTER LABEL COVER PAGE

## Junos OS<sup>®</sup> IPsec VPN

---

### in this chapter

- IPsec VPN<sup>®</sup> IKE(Internet Key Exchange) | 21
  - IPsec VPN <sup>??</sup> | 88
  - <sup>???</sup> IPsec | 111
-

# IPsec VPN IKE(Internet Key Exchange)

summary

IPsec VPN IKEv2 Junos OS

in this section

- IKE(Internet Key Exchange) IPsec | 22
- Junos OS IKE(Internet Key Exchange) | 27
- IKE(Internet Key Exchange) | 32
- IKE(Internet Key Exchange) | 32
- | 33
- IKE(Internet Key Exchange) (IKE) | 34
- IKE IPsec SA | 37
- IKEv2 | 59
- (DDoS) IKE | 61
- IKE(Internet Key Exchange) (DDoS) | 63
- : IKE | 70
- IKEv2 | 82
- CA IKE(Internet Key Exchange) | 83
- IKE Establish-Tunnel Responder-only | 85
- IKEv2 | 86

IKEv2(Internet Key Exchange version 2) IPsec IKEv2 VPN VPN IPsec SA(Security Association)

IKE

"IKEv2" 86

- IKE(Internet Key Exchange) ?? ?? | 22
- IPsec ?? ?? | 25

## IKE(Internet Key Exchange) ?? ??

???, ?? ???? ???? ?? ?????. ???? ? ?? ??? ??? ???? IKE ??? ???? Junos OS? ??? ??? ?? ?? ??? ?  
?? ?? IPsec? ???? ????.





- 0002 - SA `?? ????? 1?? ?? 2?? SA? ?? ??? ????? ?????`.
  - 0004 - `?? ????? 1?? ?? 2?? ??? ? ?????`.
  - 0008—`?? ????? SA ?????? ?????? ?? ?????? ????????`.
  - 0010—KE(Key Exchange) `??????? DH ?? ?? ?? ? ??? ????? ? ??? ??? ????? ?????`.
  - 0020—`?(IDx) ?????`.
    - `1????, IDi? ??? ID? ?????, IDir? ??? ID? ?????`.
    - `2???? IDui? ??? ?????? IDur? ??? ?????? ??????`.
- ID? FQDN, U-FQDN, IP ?? ? ASN.1\_DN? ?? IKE ID ?????.
- 0040 - `?(CERT) ?????`.
  - 0080—`??? ??(CERT_REQ) ?????`.
  - 0100 - `?(HASH) ?????? ?? ?? ??? ?????? ??? ??????`.
  - 0200 - `?(SIG) ?????? ??? ??? ????? ?????`.
  - 0400 - Nonce(Nx) `?????? ??? ??? ?? ?? ?? ??? ????? ?????`.
  - 0800 - `???? ??`.
  - 1000 - ISAKMP `???? ??`.
  - 2000 - VID(Vendor ID) `????? 1?? ??? ?? ??? ??? ? ?????`. Junos OS? NAT-T? ?? ??? ????? ?? ?? ??????

? ISAKMP `????? ? ??? ?? 2 ??? 24?? ??? ?? ??? ??????`.

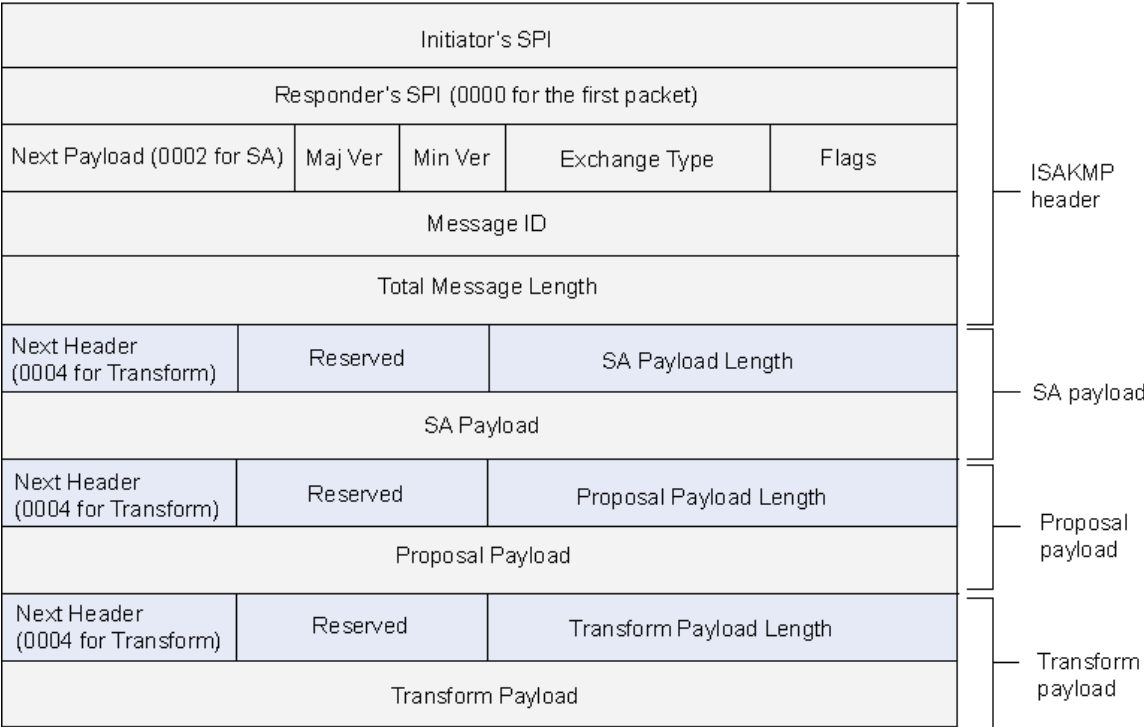
## ?? 2: ?? ISAKMP ????? ??

| Next Header | Reserved | Transform Payload Length (in bytes) |
|-------------|----------|-------------------------------------|
| Payload     |          |                                     |

gd30616

?? ISAKMP `????? ?? ??? ? ???, ? ?? ????? ??? ?? ?? ??? ??? ??????`. ? **0000** ? ??? ISAKMP `????? ?????`  
 ?. ?? ??? ?(?) `???????? ?? 3 ??? 25`.

3: ISAKMP ISAKMP

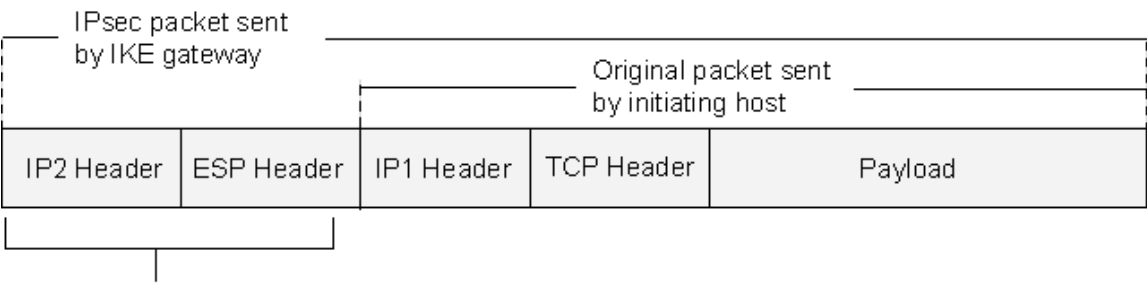


g030617

IPsec

IKE IKE IKE 1 IKE SA IKE SA, 2 SA  
ESP(Encapsulating Security Protocol) 4 25  
4 25, TCP IP(IP1)

4: IPsec-ESP



The local gateway adds these headers to the packet

g030618



6: IP (IP1) TCP

Inner IP Header (IP1)

|                                      |                      |                 |                                |   |         |                 |
|--------------------------------------|----------------------|-----------------|--------------------------------|---|---------|-----------------|
| Version                              | Header               | Type of Service | Total Packet Length (in Bytes) |   |         |                 |
| Identification                       |                      |                 | O                              | D | M       | Fragment Offset |
| Time to Live (TTL)                   | Protocol (6 for TCP) |                 | Header Checksum                |   |         |                 |
| Source Address (Installing Host)     |                      |                 |                                |   |         |                 |
| Destination Address (Receiving Host) |                      |                 |                                |   |         |                 |
| IP Options (if any)                  |                      |                 |                                |   | Padding |                 |
| Payload                              |                      |                 |                                |   |         |                 |

TCP Header

|                        |          |     |     |      |       |     |                  |             |  |         |  |  |  |
|------------------------|----------|-----|-----|------|-------|-----|------------------|-------------|--|---------|--|--|--|
| Source Port            |          |     |     |      |       |     | Destination Port |             |  |         |  |  |  |
| Sequence Number        |          |     |     |      |       |     |                  |             |  |         |  |  |  |
| Acknowledgement Number |          |     |     |      |       |     |                  |             |  |         |  |  |  |
| Header Length          | Reserved | URG | ACK | PUSH | RESET | SYN | FIN              | Window Size |  |         |  |  |  |
| Checksum               |          |     |     |      |       |     | Urgent Pointer   |             |  |         |  |  |  |
| IP Options (if any)    |          |     |     |      |       |     |                  |             |  | Padding |  |  |  |
| Data                   |          |     |     |      |       |     |                  |             |  |         |  |  |  |

00000000

Junos OS IKE(Internet Key Exchange)

in this section

- Junos OS IKEv2 | 28



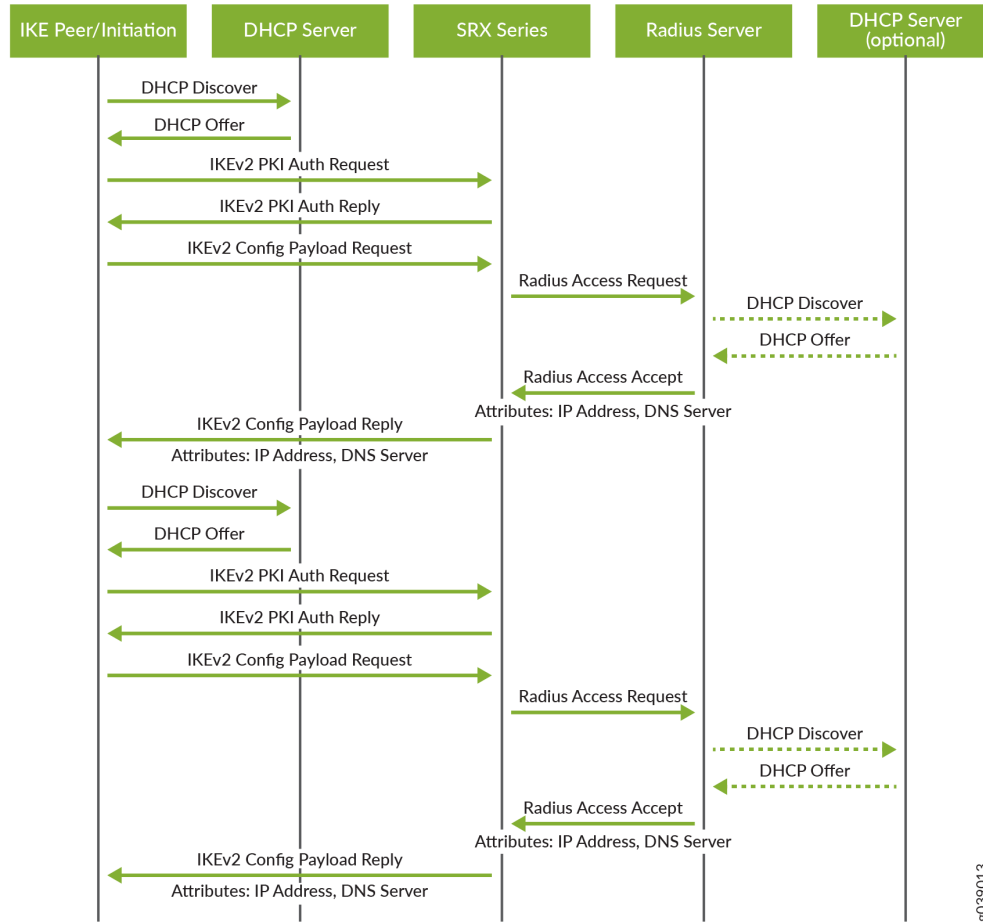
IKE(Internet Key Exchange) ?????? ??? ?????. RADIUS ??? ?? ??? ???? ??? ???? ???.

RADIUS ??? ?? DHCP ????? ?????? ??? ??? ?? ?????. RADIUS ????? ??? ???? ?? ??? ???? ??? ???.





## Figure 7: IKEv2 and DHCP Interaction



IKEv2 peer (st0) initiates IKEv2 authentication and configuration requests. The SRX Series receives these requests and interacts with the Radius Server for authentication and configuration. The DHCP Server provides IP address and DNS server information to the SRX Series. The optional DHCP Server is also shown interacting with the main DHCP Server.

## Pico SRX Series

IKEv2 peer (st0) initiates IKEv2 authentication and configuration requests. The SRX Series receives these requests and interacts with the Radius Server for authentication and configuration. The DHCP Server provides IP address and DNS server information to the SRX Series. The optional DHCP Server is also shown interacting with the main DHCP Server.

The SRX Series initiates IKEv2 authentication and configuration requests. The SRX Series receives these requests and interacts with the Radius Server for authentication and configuration. The DHCP Server provides IP address and DNS server information to the SRX Series. The optional DHCP Server is also shown interacting with the main DHCP Server.

### 1. SRX Series - pico SRX Series

- SRX Series initiates IKEv2 authentication and configuration requests.
- SRX Series receives these requests and interacts with the Radius Server for authentication and configuration.

- [ ] [ ] [ ] [ ] [ ] [ ] FQDN([ ] [ ] [ ])

?? ?? ???? DHCP ???? IKE ??? ???? ???? ?????. ?? ?? ? ??? ???? SRX ??? ???? ? ? ???? ? ? ? ? ? ? ? ?  
 ?. OAM(Operation, Administration, and Management) ???? ? ? ? ? DHCP ??? ? ? ? ? ? ? ? ? ? ? ? ? ? ?  
 ? ? ? ? ? ? ? ?.

- [illegible]

## SEE ALSO

?: ?? ???? VPN? ??? NAT-T ?? | 727

## IKE(Internet Key Exchange) ??

IKE (Internet Key Exchange) is a protocol used for establishing and managing security associations (SAs) between two communicating entities. It is part of the IPsec suite of protocols. IKE is used to negotiate the parameters of the SAs, such as the encryption and authentication algorithms, key lengths, and the lifetime of the SAs. It also handles the exchange of keys for the SAs. IKE is typically used in conjunction with the Internet Security Association and Key Management Protocol (ISAKMP) and the Internet Security Protocol (IPsec).

IKE(Internet Key Exchange) [\[\[1\]\]](#) [\[\[2\]\]](#) [\[\[3\]\]](#) [\[\[4\]\]](#) [\[\[5\]\]](#) proposal [edit security\_ike] [\[\[6\]\]](#) [\[\[7\]\]](#) [\[\[8\]\]](#) [\[\[9\]\]](#) [\[\[10\]\]](#).

## IKE(Internet Key Exchange) ??

IKE [redacted] IKE [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] (IKE [redacted]) [redacted] [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted] [redacted], [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]  
[redacted] [redacted] [redacted] [redacted] [redacted] PSK([redacted] [redacted] [redacted]) [redacted]. IKE [redacted] [redacted] IKE? [redacted] [redacted] [redacted] [redacted] [redacted] [redacted], [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]  
[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]  
([redacted] [redacted]) [redacted] [redacted] [redacted] [redacted] [redacted], [redacted] PSK [redacted] [redacted] [redacted] [redacted] [redacted].

?? ?? ??? IKE(Internet Key Exchange) ??? ??????. ?? ?? ??? ??? IKE(Internet Key Exchange) ??? ??????

IKE(Internet Key Exchange)      policy [edit security ike]      .

**?   ? ? ?   ?   ? ? ?**

in this section

-   
-   
-   

??

```

IKEv2???? ? ????? ????? ??? ??????????. ? ????? IKE SA(?? ??)? ?? ? ?? ????? ??? ID ????? ???????? ??? ?????
? ?????, ????? VPN ??? ?? ?? ??? ?? ??? ??? ?????? ??????. ????? IKE SA ? ?? SA? ?? ? ?? ?????, ?? ??
IKE SA ?? ?? SA? ? ????? ? ?? ????? ?????, ? IKE ? ?? SA? ????? ?? IKE ? ?? SA? ??????.

```

IKEv2 ???? ?????? ?????? ???. ??? ?? ?? 1?? 100 ??? ????? ????? ?????? ??????. ??? ??? ????? ????? ?? ?  
 ??? IKE ? ??? ?????. ?? ??, ??? ??? ??? 1? ?? IKE ? ????? ?? ??? ????? ??????. ??? ??? ??? 2?? ?? ??  
 IKE ? ?????? ????? ??????, ??? ??? ??? 3?? ? ?? IKE ? ??? ??? ????? ??????.

```
[edit security ike policy policy-name] ?? ??? ? ???? reauth-frequency ??? ??? ??????. ??? ??? O(???)?? ?????
???? ????????. ??? ??? ??? ? ???? ??, ? ??? ??? ??? ? ? ? ? ? ????.
```

□□□□ □□

IKEv2 [?] [?] [?] [?] [?] [?].

- IKEv2 (???) ?? ???
- DPD(Dead Peer Detection)
- ?? ??? ? ?? ????? ?? ??(st0) ?????
- ????? ?? ?? ??(NAT-T)
- SRX5400, SRX5600 ? SRX5800 ?????? ?? ???-??? ? ???-??? ??? ?? ?????
- SRX5400, SRX5600 ? SRX5800 ?????? ISSU(In-Service Software Upgrade)
- ISHU(In-Service Hardware Upgrade) ??? ????? ? SPU(Services Processing Unit)? ?????? ?? ??

??

IKEv2 配置 2 个 IKE 策略。

- NAT-T 配置 2 个 IKE(Internet Key Exchange) SA 和 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。
- NAT-T 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 NAT 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 NAT 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 NAT-T keepalive 配置 DPD 配置。 AutoVPN 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。
- 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 EAP(Extensible Authentication Protocol) 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。 EAP 配置 2 个 IKE(Internet Key Exchange) SA 的 NAT-T 配置。

## IKE(Internet Key Exchange) 配置(配置 2 个 IKE 策略)

in this section

- [配置 2 个 IKE 策略](#) | 34

### 配置 2 个 IKE 策略

配置 2 个 IKE 策略。 SRX 配置 2 个 IKE 策略。 CA(配置 2 个 IKE 策略) 配置 2 个 IKE 策略。 EE(End Entity) 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。

配置 2 个 IKE 策略。 2 个 IKE 策略。 EE 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 IKE 配置 2 个 IKE 策略。 EE 配置 2 个 IKE 策略。

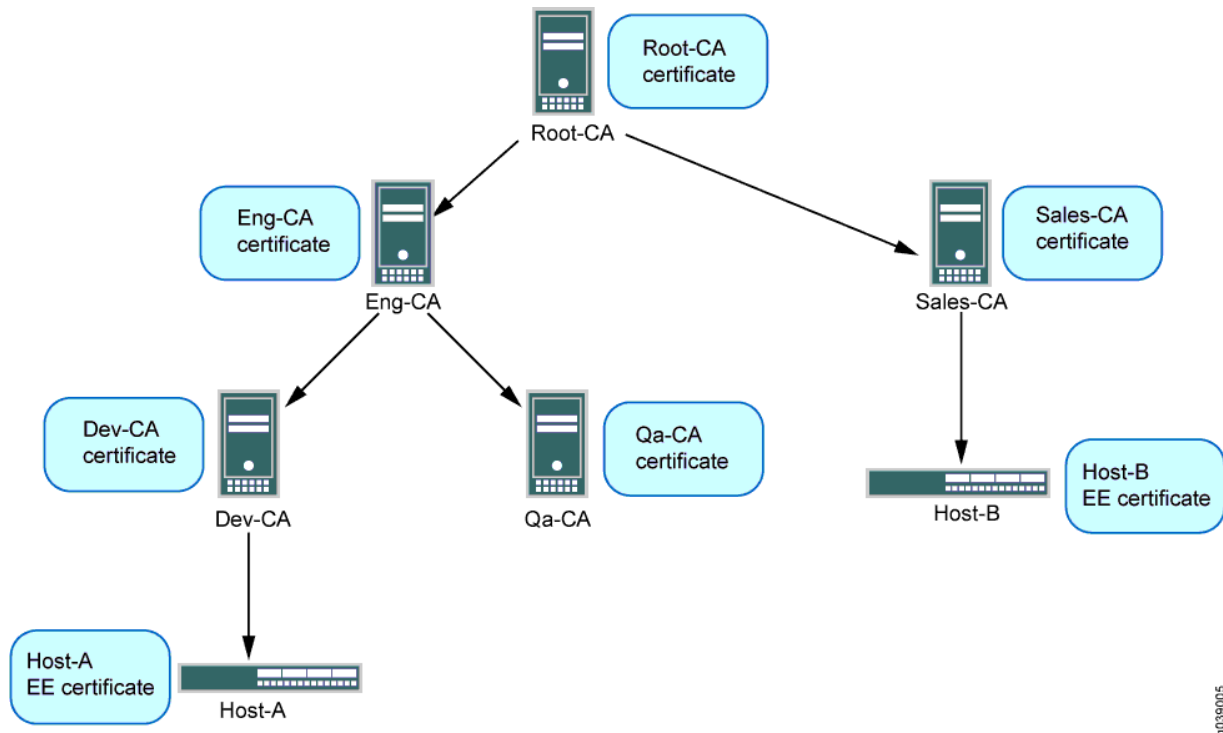
2 个 IKE 策略。 2 个 IKE 策略。 EE 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 EE 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。

配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 EE 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 10 个 IKE 策略。

配置 2 个 IKE 策略。 V2 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 2 个 IKE 策略。 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 IKE 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。 CA 配置 2 个 IKE 策略。

? ? 8 ? 35?? CA ?? Root-CA? ???? ? ???? ? ? ? ? CA???. Root-CA? ?? Eng-CA  
 ? Sales-CA? ???? ? ? CA? CA ???? ?????. Eng-CA? ?? Dev-CA ? Qa-CA? ???? ? ? ? ? CA?  
 CA ???? ?????. Host-A? Dev-CA??? EE ???? ? Host-B? Sales-CA??? EE ???? ????.

## 8: Multilevel Hierarchy



? ?? ????? ? ? CA ???? ? ?????. Host-A?? Root-CA, Eng-CA ? Dev-CA ???? ???? ?????. Sales-CA  
 ? Qa-CA ???? ???? ?????. Host-B?? Root-CA ? Sales-CA ???? ???? ?????. ???? ???? ???? ???? ???? SCEP(?  
 ? ??? ? ? ???? ? ???? ? ? ?????.

? ?? ????? ??? ??? ? CA? ?? CA ???? ?????? ???. ?? ??? Host-A? ??? CA ???? ??????.

```
admin@host-A# show security
pki {
  ca-profile Root-CA {
    ca-identity Root-CA;
    enrollment {
      url "www.example.net/scep/Root/";
    }
  }
  ca-profile Eng-CA {
    ca-identity Eng-CA;
```

```

    enrollment {
        url "www.example.net/scep/Eng/";
    }
}
ca-profile Dev-CA {
    ca-identity Dev-CA;
    enrollment {
        url "www.example.net/scep/Dev/";
    }
}
}

```

?? ???? Host-B? ???? CA ???? ?????.

```

admin@host-B# show security
pki {
    ca-profile Root-CA {
        ca-identity Root-CA;
        enrollment {
            url "www.example.net/scep/Root/";
        }
    }
    ca-profile Sales-CA {
        ca-identity Sales-CA;
        enrollment {
            url "www.example.net/scep/Sales/";
        }
    }
}

```

## SEE ALSO

[Junos OS?? PKI? ?? ??](#)

[?? ?? ???? ??](#)

## Configuring IKE and IPsec SA

### summary

This section describes how to configure IKE and IPsec SA.

### in this section

- [IKE and IPsec SA](#) | 37
- [IKE and IPsec SA](#) | 37
- [IKE and IPsec SA](#) | 38
- [IKE and IPsec SA](#) | 38
- [IKE and IPsec SA](#) | 49

This section describes how to configure IKE and IPsec SA.

Junos OS 22.4R1 introduces IKE(Internet Key Exchange) certificates authentication-method. To configure IKE and IPsec SA, use the following commands:

Use the following command to show the configuration of the IKE and IPsec SA:

Use the following command to request the configuration of the IKE and IPsec SA:

### Configuring IKE

Use the following command:

- Use the following command to configure the IKE and IPsec SA:

Use the following command to request the configuration of the IKE and IPsec SA:

- IKE and IPsec SA: Use the following command to show the version of the IKE and IPsec SA.

Use the following command to request the configuration of the IKE and IPsec SA:

### Configuring IPsec SA

Use the following command to configure the IPsec SA:

Use the following command to request the configuration of the IPsec SA:

5: SRX\_A SRX\_B

|       |          | IKE(Internet Key Exchange) | IKE(Internet Key Exchange) |
|-------|----------|----------------------------|----------------------------|
| SRX_A | ge-0/0/0 | 192.168.1.2                | 192.168.1.1                |
| SRX_B | ge-0/0/0 | 192.168.1.1                | 192.168.1.2                |

9 38

9:



in this section

- SRX\_A | 39
- SRX\_B | 44





```
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN establish-tunnels on-traffic
```

?? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? CLI ?? ?? ??? ?????.

IKE(Internet Key Exchange) ? IPsec SA? ???? ? ? ???? ???? ?????.

1. ??? ???? show security pki local-certificate certificate-id *certificate-name* detail ???? ? ? ????.

??? ???? ???? ? ? ? ? ???? ?????. ??? ??? ??? ????.

2. ???? ????.

```
user@srxa# set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.1/24
user@srxa# set interfaces ge-0/0/1 unit 0 family inet address 172.16.1.1/24
user@srxa# set interfaces st0 unit 1 family inet
```

3. ?? ??? ? ? ? ? ?.

```
user@srxa# set security zones security-zone trust host-inbound-traffic system-services all
user@srxa# set security zones security-zone trust host-inbound-traffic protocols all
user@srxa# set security zones security-zone trust interfaces ge-0/0/1
user@srxa# set security zones security-zone untrust host-inbound-traffic system-services ike
user@srxa# set security zones security-zone untrust interfaces ge-0/0/0
user@srxa# set security zones security-zone VPN interfaces st0.1
user@srxa# set security policies from-zone VPN to-zone trust policy 1 match source-address
any
user@srxa# set security policies from-zone VPN to-zone trust policy 1 match destination-
address any
user@srxa# set security policies from-zone VPN to-zone trust policy 1 match application any
user@srxa# set security policies from-zone VPN to-zone trust policy 1 then permit
user@srxa# set security policies from-zone trust to-zone VPN policy 1 match source-address
any
user@srxa# set security policies from-zone trust to-zone VPN policy 1 match destination-
address any
user@srxa# set security policies from-zone trust to-zone VPN policy 1 match application any
user@srxa# set security policies from-zone trust to-zone VPN policy 1 then permit
user@srxa# set security policies default-policy deny-all
```

#### 4. IKE(Internet Key Exchange) `???` `??????`.

```
[edit]
user@srxa# set security ike proposal IKE_PROP authentication-method certificates
user@srxa# set security ike proposal IKE_PROP dh-group group5
user@srxa# set security ike proposal IKE_PROP authentication-algorithm sha-256
user@srxa# set security ike proposal IKE_PROP encryption-algorithm aes-128-cbc
```

#### 5. IKE(Internet Key Exchange) `???` `??????`.

```
[edit]
user@srxa# set security ike policy IKE_POL proposals IKE_PROP
user@srxa# set security ike policy IKE_POL certificate local-certificate r0_rsa.crt
```

#### 6. IKE(Internet Key Exchange) `??????` `??????`.

```
[edit]
user@srxa# set security ike gateway IKE_GW ike-policy IKE_POL
user@srxa# set security ike gateway IKE_GW address 192.168.1.2
user@srxa# set security ike gateway IKE_GW external-interface ge-0/0/0
user@srxa# set security ike gateway IKE_GW local-address 192.168.1.1
user@srxa# set security ike gateway IKE_GW version v2-only
```

#### 7. IPsec `???` `??????`.

```
[edit]
user@srxa# set security ipsec proposal IPSEC_PROP protocol esp
user@srxa# set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srxa# set security ipsec proposal IPSEC_PROP encryption-algorithm aes-192-cbc
```

#### 8. IPsec `???` `??????`.

```
[edit]
user@srxa# set security ipsec policy IPSEC_POL proposals IPSEC_PROP
```

## 9. IPsec VPN `???`.

```
[edit]
user@srxa# set security ipsec vpn IPSEC_VPN bind-interface st0.1
user@srxa# set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
user@srxa# set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
user@srxa# set security ipsec vpn IPSEC_VPN establish-tunnels on-traffic
```

`??`

`?? ???? , show security ike ? show security ipsec ??? ???? show interfaces??? ?????. ??? ???? ???? ???? , ?  
?? ?? ???? ???? ????.`

```
[edit]
user@srxa# show interfaces
ge-0/0/0 {
  description untrust;
  unit 0 {
    family inet {
      address 192.168.1.1/24;
    }
  }
}
ge-0/0/1 {
  description trust;
  unit 0 {
    family inet {
      address 172.16.1.1/24;
    }
  }
}
st0 {
  unit 1 {
    family inet;
  }
}

[edit]
user@srxa# show security ike
proposal IKE_PROP {
  authentication-method certificates;
```

```

    dh-group group5;
    authentication-algorithm sha-256;
    encryption-algorithm aes-128-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate r0.crt_rsa;
    }
}
gateway IKE_GW {
    ike-policy IKE_POL;
    address 192.168.1.2;
    external-interface ge-0/0/0;
    local-address 192.168.1.1;
    version v2-only;
}

[edit]
user@srxa# show security ipsec
    proposal IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-192-cbc;
    }
    policy IPSEC_POL {
        proposals IPSEC_PROP;
    }
    vpn IPSEC_VPN {
        bind-interface st0.1;
        ike {
            gateway IKE_GW;
            ipsec-policy IPSEC_POL;
        }
        establish-tunnels on-traffic;
    }

```

```

?? ?? ?? ?? commit?(?) ??.

```



```
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN establish-tunnels on-traffic
```

?? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? CLI ?? ?? ???? ?????.

IKE(Internet Key Exchange) ? IPsec SA? ???? ? ? ???? ???? ?????.

1. ??? ???? request security pki local-certificate certificate-id *certificate-name* detail ???? ???? ????.

??? ???? ???? ? ? ? ? ???? ?????. ??? ???? ??? ????.

2. ???? ????.

```
user@srxb# set interfaces ge-0/0/0 unit 0 family inet address 192.168.1.2/24
user@srxb# set interfaces ge-0/0/1 unit 0 family inet address 172.18.1.2/24
user@srxb# set interfaces st0 unit 1 family inet
```

3. ?? ??? ? ? ? ? ?.

```
user@srxb# set security zones security-zone trust host-inbound-traffic system-services all
user@srxb# set security zones security-zone trust host-inbound-traffic protocols all
user@srxb# set security zones security-zone trust interfaces ge-0/0/1
user@srxb# set security zones security-zone untrust host-inbound-traffic system-services ike
user@srxb# set security zones security-zone untrust interfaces ge-0/0/0
user@srxb# set security zones security-zone VPN interfaces st0.1
user@srxb# set security policies from-zone VPN to-zone trust policy 1 match source-address
any
user@srxb# set security policies from-zone VPN to-zone trust policy 1 match destination-
address any
user@srxb# set security policies from-zone VPN to-zone trust policy 1 match application any
user@srxb# set security policies from-zone VPN to-zone trust policy 1 then permit
user@srxb# set security policies from-zone trust to-zone VPN policy 1 match source-address
any
user@srxb# set security policies from-zone trust to-zone VPN policy 1 match destination-
address any
user@srxb# set security policies from-zone trust to-zone VPN policy 1 match application any
user@srxb# set security policies from-zone trust to-zone VPN policy 1 then permit
user@srxb# set security policies default-policy deny-all
```

#### 4. IKE(Internet Key Exchange) `???` `??????`.

```
[edit]
user@srxb# set security ike proposal IKE_PROP authentication-method certificates
user@srxb# set security ike proposal IKE_PROP dh-group group5
user@srxb# set security ike proposal IKE_PROP authentication-algorithm sha-256
user@srxb# set security ike proposal IKE_PROP encryption-algorithm aes-128-cbc
```

#### 5. IKE(Internet Key Exchange) `???` `??????`.

```
[edit]
user@srxb# set security ike policy IKE_POL proposals IKE_PROP
user@srxb# set security ike policy IKE_POL certificate local-certificate r1.crt_ecdsa384
```

#### 6. IKE(Internet Key Exchange) `??????` `??????`.

```
[edit]
user@srxb# set security ike gateway IKE_GW ike-policy IKE_POL
user@srxb# set security ike gateway IKE_GW address 192.168.1.1
user@srxb# set security ike gateway IKE_GW external-interface ge-0/0/0
user@srxb# set security ike gateway IKE_GW local-address 192.168.1.2
user@srxb# set security ike gateway IKE_GW version v2-only
```

#### 7. IPsec `???` `??????`.

```
[edit]
user@srxb# set security ipsec proposal IPSEC_PROP protocol esp
user@srxb# set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srxb# set security ipsec proposal IPSEC_PROP encryption-algorithm aes-192-cbc
```

#### 8. IPsec `???` `??????`.

```
[edit]
user@srxb# set security ipsec policy IPSEC_POL proposals IPSEC_PROP
```



## 9. IPsec VPN `???`.

```
[edit]
user@srxb# set security ipsec vpn IPSEC_VPN bind-interface st0.1
user@srxb# set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
user@srxb# set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
user@srxb# set security ipsec vpn IPSEC_VPN establish-tunnels immediately
```

`??`

`?? ???? , show security ike ? show security ipsec ??? ???? show interfaces??? ?????. ??? ???? ???? ???? , ?  
?? ?? ???? ???? ????.`

```
[edit]
user@srxb# show interfaces
ge-0/0/0 {
  description untrust;
  unit 0 {
    family inet {
      address 192.168.1.2/24;
    }
  }
}
ge-0/0/1 {
  description trust;
  unit 0 {
    family inet {
      address 172.18.1.2/24;
    }
  }
}
st0 {
  unit 1 {
    family inet;
  }
}

[edit]
user@srxb# show security ike
proposal IKE_PROP {
  authentication-method certificates;
```

```

    dh-group group5;
    authentication-algorithm sha-256;
    encryption-algorithm aes-128-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate r1.crt_ecdsa384;
    }
}
gateway IKE_GW {
    ike-policy IKE_POL;
    address 192.168.1.1;
    external-interface ge-0/0/0;
    local-address 192.168.1.2;
    version v2-only;
}

[edit]
user@srxb# show security ipsec
    proposal IPSEC_PROP {
        protocol esp;
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-192-cbc;
    }
    policy IPSEC_POL {
        proposals IPSEC_PROP;
    }
    vpn IPSEC_VPN {
        bind-interface st0.1;
        ike {
            gateway IKE_GW;
            ipsec-policy IPSEC_POL;
        }
        establish-tunnels immediately;
    }

```

```

?? ?? ?? ?? commit?(?) ??.

```

??

in this section

SRX\_A ?? | 49

SRX\_B ?? | 54

??? ???? ???? ???? ????.

SRX\_A ??

??? ?? ??? SRX-A? ????.

??

IPsec 2?? ???? ????.

??

?? ???? show security ike security-associations ??? ????.

```
user@srxa> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
32      UP    6723643250f0f357 f6295f11b0d7c8ab IKEv2 192.168.1.2
```

?? ???? show security ipsec security-associations ??? ????.

```
user@srxa> show security ipsec security-associations
Total active tunnels: 1    Total IPsec sas: 1
ID      Algorithm      SPI      Life:sec/kb Mon lsys Port Gateway
<500033 ESP:aes-cbc-192/sha256 0x5f156c1b 2750/ unlim - root 500 192.168.1.2
>500033 ESP:aes-cbc-192/sha256 0x7ea065e7 2750/ unlim - root 500 192.168.1.2
```

?? ???? show security ike security-associations detail ??? ????.

```
user@srxa> show security ike security-associations detail
IKE peer 192.168.1.2, Index 32, Gateway Name: IKE_GW
```

```

Role: Responder, State: UP
Initiator cookie: 6723643250f0f357, Responder cookie: f6295f11b0d7c8ab
Exchange type: IKEv2, Authentication method: RSA-signatures
Local gateway interface: ge-0/0/0.0
Routing instance: default
Local: 192.168.1.1:500, Remote: 192.168.1.2:500
Lifetime: Expires in 28165 seconds
Reauth Lifetime: Disabled
IKE Fragmentation: Enabled, Size: 576
Remote Access Client Info: Unknown Client
Peer ike-id: 192.168.1.2
AAA assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha256-128
  Encryption          : aes128-cbc
  Pseudo random function: hmac-sha256
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input  bytes :           1346
  Output bytes :           1887
  Input  packets:           3
  Output packets:           4
  Input  fragmented packets: 2
  Output fragmented packets: 3
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1
IPSec Tunnel IDs: 500033

```

```

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 192.168.1.1:500, Remote: 192.168.1.2:500
Local identity: 192.168.1.1
Remote identity: 192.168.1.2
Flags: IKE SA is created

```

```
IPsec SA Rekey CREATE_CHILD_SA exchange stats:
```

|                           |                          |
|---------------------------|--------------------------|
| Initiator stats:          | Responder stats:         |
| Request Out : 0           | Request In :             |
| 0                         |                          |
| Response In : 0           | Response Out :           |
| 0                         |                          |
| No Proposal Chosen In : 0 | No Proposal Chosen Out : |
| 0                         |                          |
| Invalid KE In : 0         | Invalid KE Out :         |

```

0
    TS Unacceptable In      : 0                TS Unacceptable Out      :
0
    Res DH Compute Key Fail : 0                Res DH Compute Key Fail:
0
    Res Verify SA Fail      : 0
    Res Verify DH Group Fail: 0
    Res Verify TS Fail      : 0

```

?? ???? show security ipsec security-associations detail ??? ????.

```

user@srxa> show security ipsec security-associations detail
ID: 500033 Virtual-system: root, VPN Name: IPSEC_VPN
Local Gateway: 192.168.1.1, Remote Gateway: 192.168.1.2
Local Identity: ipv4(0.0.0.0-255.255.255.255)
Remote Identity: ipv4(0.0.0.0-255.255.255.255)
TS Type: proxy-id
Version: IKEv2
PFS group: N/A
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Tunnel MTU: 0, Policy-name:
IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
Tunnel events:
  Thu Mar 09 2023 22:41:36: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 1
Distribution-Profile: default-profile
Direction: inbound, SPI: 0x5f156c1b, AUX-SPI: 0
              , VPN Monitoring: -
  Hard lifetime: Expires in 2895 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2286 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (192 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
  Extended-Sequence-Number: Disabled
  tunnel-establishment: establish-tunnels-on-traffic
  IKE SA Index: 32
Direction: outbound, SPI: 0x7ea065e7, AUX-SPI: 0
              , VPN Monitoring: -
  Hard lifetime: Expires in 2895 seconds

```

```

Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2286 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (192 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-on-traffic
IKE SA Index: 32

```

?? ???? show security pki local-certificate certificate-id r0\_rsa\_cr detail ??? ?????.

```

user@srxa> show security pki local-certificate certificate-id r0_rsa_cr detail
LSYS: root-logical-system
Certificate identifier: r0_rsa_cr
Certificate version: 3

Serial number:
  hexadecimal: 0x0186a62478ae8f0cdd766eb38dbd53
  decimal: 7923302907757301847007106226306387
Issuer:
  Organization: juniper, Country: India, Common name: Root-CA
Subject:
  Organization: juniper, Organizational unit: marketing, State: california, Locality:
sunnyvale, Common name: r0, Domain component: juniper
Subject string:
  DC=juniper, CN=r0, OU=marketing, O=juniper, L=sunnyvale, ST=california, C=us
Alternate subject: "r0@juniper.net", r0.juniper.net, 192.168.1.1
Cert-Chain: Root-CA
Validity:
  Not before: 03- 3-2023 05:54 UTC
  Not after: 06- 6-2027 12:36 UTC
Public key algorithm: rsaEncryption(2048 bits)
30:82:01:0a:02:82:01:01:00:b0:e5:53:8d:7e:20:fa:6b:21:c2:d1
2b:48:8f:af:c3:eb:8b:23:4a:f7:c5:1f:cf:2c:6a:b3:2e:8a:ef:1b
f7:97:aa:fd:1d:ab:1c:76:9b:40:a3:ac:bb:49:f6:93:f9:e1:4e:62
df:3d:ca:e5:d2:95:9c:a0:f4:2b:d7:7e:1d:20:94:69:a8:e4:cf:dc
15:90:4c:be:1d:d8:1c:52:08:3a:d1:05:a3:bb:2f:8f:31:0c:6b:21
ef:76:c3:c7:fb:be:4a:cb:da:cc:8d:04:3a:75:0c:eb:5d:e2:f6:13
50:fe:39:67:c0:77:2f:32:b0:5e:38:6f:9c:79:b3:5d:f3:57:f4:f8
42:f5:22:5b:6c:58:67:90:4e:1e:ec:6a:03:e2:c0:87:65:02:ca:da
6f:95:0a:8c:2a:fd:45:4f:3a:b5:ef:18:05:1c:54:e6:fe:45:bb:73
53:81:b2:c6:b7:36:36:57:6d:9c:d3:d9:80:e7:d6:85:92:74:32:88

```

```

16:01:03:27:57:76:8e:5e:d6:73:ac:bf:68:fd:6d:a1:2a:8f:f5:3a
29:b0:c9:44:9b:c8:46:c1:bf:c0:52:2a:f0:51:be:b5:f6:e1:f5:3e
96:1d:3a:42:29:28:d3:cf:60:b9:eb:24:04:47:d3:f1:3f:5e:38:fc
7f:33:f6:94:9d:02:03:01:00:01
Signature algorithm: sha256WithRSAEncryption
Fingerprint:
  4d:f6:89:c5:d6:3c:74:73:db:3e:f6:4b:1e:26:6c:c1:1c:1d:a7:4d (sha1)
  6b:1c:a8:1f:de:5a:9b:3e:d5:c4:85:29:af:3f:82:f2 (md5)

6b:7a:b5:d1:57:cf:75:9d:1f:63:b9:f6:49:e4:4e:b3:13:2c:83:f1:f7:25:44:6f:45:2f:0d:2f:ae:a8:80:85
(sh256)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

?? ???? show security pki ca-certificate ca-profile Root-CA detail ??? ????.

```

user@srxa> show security pki ca-certificate ca-profile Root-CA detail
LSYS: root-logical-system
CA profile: Root-CA
Certificate identifier: Root-CA
Certificate version: 3

Serial number:
  hexadecimal: 0x00000440
  decimal: 1088
Issuer:
  Organization: juniper, Country: India, Common name: Root-CA
Subject:
  Organization: juniper, Country: India, Common name: Root-CA
Subject string:
  C=India, O=juniper, CN=Root-CA
Validity:
  Not before: 06- 7-2022 12:36 UTC
  Not after: 06- 6-2027 12:36 UTC
Public key algorithm: rsaEncryption(2048 bits)
30:82:01:0a:02:82:01:01:00:cd:9c:e6:9f:62:6c:49:15:c2:da:eb
8e:e6:e5:a1:88:40:d8:b5:2e:5b:1a:0e:de:96:d7:0b:19:f9:03:44
98:49:d5:cc:a8:90:2b:7f:1b:58:7b:1f:26:92:18:4c:2d:37:65:5c
9f:0f:6e:10:b5:34:6f:2d:b5:9c:27:3b:a6:b1:b5:a0:e2:a6:92:3d
e4:68:fe:5d:71:06:6f:ce:e6:0f:0f:e3:94:2a:23:57:98:a0:6a:9c
e0:52:a2:47:ff:ce:b0:47:bd:36:95:80:a7:af:d2:49:b1:5d:2a:3d

```

```

28:e4:95:06:b8:b3:d9:07:11:3c:13:af:c6:e2:51:08:22:82:2d:ec
4f:26:40:b0:b0:55:2d:6e:c0:c8:19:34:a7:99:5a:bc:58:98:69:ae
04:d6:6d:ec:4a:c9:55:a5:ff:00:cb:3b:02:85:fa:02:a1:5c:c1:9d
6d:44:b8:95:8f:77:c0:53:fc:7f:a4:09:a3:25:1c:4a:e2:9d:0c:81
08:b4:c8:b8:0d:bc:94:75:54:75:57:4f:d3:a4:17:0d:5d:1a:f3:c1
1d:5d:73:2f:fe:8b:cb:fc:1f:93:87:72:d6:be:df:86:d7:e6:d1:c7
0d:00:1a:6e:58:db:6a:1c:2f:1d:17:46:9a:f2:69:b4:21:db:08:5d
8d:ab:30:7d:7f:02:03:01:00:01
Signature algorithm: sha256WithRSAEncryption
Distribution CRL:
    http://10.102.40.55:8080/crl-as-der/currentcrl-11.crl?id=11
Use for key: CRL signing, Certificate signing, Key encipherment, Digital signature
Fingerprint:
    8b:84:60:2a:58:5b:80:f0:b9:ae:25:9f:67:3d:d6:81:ee:43:6c:d4 (sha1)
    ab:ec:4d:fe:d4:04:9c:c9:79:1d:9a:33:4e:6d:78:f6 (md5)

9d:f0:c0:a0:93:74:11:53:d3:4d:2d:75:d3:60:37:5f:fb:b7:a9:67:42:cd:7c:3c:0e:0f:9b:58:36:3c:14:f5
(sh256)

```

**SRX\_B**

SRX-B.

IPsec.

show security ike security-associations.

```

user@srxb> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
56042   UP    6723643250f0f357 f6295f11b0d7c8ab IKEv2 192.168.1.1

```

show security ipsec security-associations.

```

user@srxb> show security ipsec security-associations
Total active tunnels: 1      Total IPsec sas: 1
ID      Algorithm SPI      Life:sec/kb Mon lsys Port Gateway

```



```
<500230 ESP:aes-cbc-192/sha256 0x7ea065e7 2638/ unlim - root 500 192.168.1.1
>500230 ESP:aes-cbc-192/sha256 0x5f156c1b 2638/ unlim - root 500 192.168.1.1
```

?? ???? show security ike security-associations detail ??? ????.

```
user@srxb> show security ike security-associations detail
IKE peer 192.168.1.1, Index 56042, Gateway Name: IKE_GW
Role: Responder, State: UP
Initiator cookie: 6723643250f0f357, Responder cookie: f6295f11b0d7c8ab
Exchange type: IKEv2, Authentication method: ECDSA-384-signatures
Local gateway interface: ge-0/0/0.0
Routing instance: default
Local: 192.168.1.2:500, Remote: 192.168.1.1:500
Lifetime: Expires in 18995 seconds
Reauth Lifetime: Disabled
IKE Fragmentation: Enabled, Size: 576
Remote Access Client Info: Unknown Client
Peer ike-id: 192.168.1.1
AAA assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha256-128
  Encryption          : aes128-cbc
  Pseudo random function: hmac-sha256
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes  : 2934
  Output bytes : 2379
  Input packets: 10
  Output packets: 9
  Input fragmented packets: 3
  Output fragmented packets: 2
IPSec security associations: 8 created, 3 deleted
Phase 2 negotiations in progress: 1
IPSec Tunnel IDs: 500230

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 192.168.1.2:500, Remote: 192.168.1.1:500
Local identity: 192.168.1.2
Remote identity: 192.168.1.1
Flags: IKE SA is created

IPsec SA Rekey CREATE_CHILD_SA exchange stats:
```

| Initiator stats:         |     | Responder stats:         |   |
|--------------------------|-----|--------------------------|---|
| Request Out              | : 1 | Request In               | : |
| Response In              | : 1 | Response Out             | : |
| No Proposal Chosen In    | : 0 | No Proposal Chosen Out   | : |
| Invalid KE In            | : 0 | Invalid KE Out           | : |
| TS Unacceptable In       | : 0 | TS Unacceptable Out      | : |
| Res DH Compute Key Fail  | : 0 | Res DH Compute Key Fail: |   |
| Res Verify SA Fail       | : 0 |                          |   |
| Res Verify DH Group Fail | : 0 |                          |   |
| Res Verify TS Fail       | : 0 |                          |   |

?? ???? show security ipsec security-associations detail ??? ?????.

```

user@srxb> show security ipsec security-associations detail
ID: 500230 Virtual-system: root, VPN Name: IPSEC_VPN
Local Gateway: 192.168.1.2, Remote Gateway: 192.168.1.1
Local Identity: ipv4(0.0.0.0-255.255.255.255)
Remote Identity: ipv4(0.0.0.0-255.255.255.255)
TS Type: proxy-id
Version: IKEv2
PFS group: N/A
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Tunnel MTU: 0, Policy-name:
IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
Tunnel events:
  Thu Mar 02 2023 22:26:16: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 1
Distribution-Profile: default-profile
Direction: inbound, SPI: 0x7ea065e7, AUX-SPI: 0
              , VPN Monitoring: -
Hard lifetime: Expires in 2633 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2002 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed

```

```

Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (192 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-on-traffic
IKE SA Index: 56042
Direction: outbound, SPI: 0x5f156c1b, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 2633 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2002 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (192 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-on-traffic
IKE SA Index: 56042

```

?? ???? show security pki local-certificate certificate-id r1.crt\_ecdsa384 detail ??? ?????.

```

user@srxb> show security pki local-certificate certificate-id r1.crt_ecdsa384 detail
LSYS: root-logical-system
Certificate identifier: r1.crt_ecdsa384
Certificate version: 3

Serial number:
  hexadecimal: 0x0186a6254347a38063946d08595a55
  decimal: 7923303152683216740296668848151125
Issuer:
  Organization: juniper, Country: India, Common name: root-ecdsa-384
Subject:
  Organization: juniper, Organizational unit: marketing, State: california, Locality:
sunnyvale, Common name: r1_spk1, Domain component: juniper
Subject string:
  DC=juniper, CN=r1_spk1, OU=marketing, O=juniper, L=sunnyvale, ST=california, C=us
Alternate subject: "r1_spk1@juniper.net", r1_spk1.juniper.net, 192.168.2
Cert-Chain: root-ecdsa-384
Validity:
  Not before: 03- 3-2023 05:55 UTC
  Not after: 06- 6-2027 13:21 UTC
Public key algorithm: ecdsaEncryption(384 bits)
  04:c2:ba:19:dc:0d:62:a7:94:7b:9b:1d:4d:ff:a1:e1:44:b5:57:a7
  cb:7d:33:6b:35:87:b8:e4:ca:44:b1:6c:6d:63:ae:6f:3c:31:7c:7e

```

```

65:99:b3:2d:a3:76:30:23:e5:0e:34:e1:28:54:d6:3e:d3:8b:de:b6
b9:45:05:82:6f:1d:20:b7:6f:3c:ce:a2:13:a2:b4:37:0b:db:35:1e
20:54:b5:06:9d:f8:7f:19:7b:c5:d7:7b:57:8b:28:31:d3
Signature algorithm: ecdsa-with-SHA384
Fingerprint:
  9b:cb:5a:57:a8:60:a0:ee:5c:be:59:4c:db:35:39:d3:b7:29:ef:b1 (sha1)
  ef:b5:e3:be:35:1b:6e:02:0b:61:11:a5:53:07:b4:89 (md5)

8f:86:d0:12:ea:bc:a8:81:a8:17:3a:f9:03:e4:91:57:20:9c:11:bc:a4:dd:d1:7f:d1:48:3f:5b:d9:fb:93:32
(sh256)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

S

?? ???? show security pki ca-certificate ca-profile Root-CA detail ??? ??????.

```

user@srxb> show security pki ca-certificate ca-profile Root-CA detail
LSYS: root-logical-system
CA profile: Root-CA
Certificate identifier: Root-CA
Certificate version: 3

Serial number:
  hexadecimal: 0x00000440
  decimal: 1088
Issuer:
  Organization: juniper, Country: India, Common name: Root-CA
Subject:
  Organization: juniper, Country: India, Common name: Root-CA
Subject string:
  C=India, O=juniper, CN=Root-CA
Validity:
  Not before: 06- 7-2022 12:36 UTC
  Not after: 06- 6-2027 12:36 UTC
Public key algorithm: rsaEncryption(2048 bits)
30:82:01:0a:02:82:01:01:00:cd:9c:e6:9f:62:6c:49:15:c2:da:eb
8e:e6:e5:a1:88:40:d8:b5:2e:5b:1a:0e:de:96:d7:0b:19:f9:03:44
98:49:d5:cc:a8:90:2b:7f:1b:58:7b:1f:26:92:18:4c:2d:37:65:5c
9f:0f:6e:10:b5:34:6f:2d:b5:9c:27:3b:a6:b1:b5:a0:e2:a6:92:3d
e4:68:fe:5d:71:06:6f:ce:e6:0f:0f:e3:94:2a:23:57:98:a0:6a:9c

```

```
e0:52:a2:47:ff:ce:b0:47:bd:36:95:80:a7:af:d2:49:b1:5d:2a:3d
28:e4:95:06:b8:b3:d9:07:11:3c:13:af:c6:e2:51:08:22:82:2d:ec
4f:26:40:b0:b0:55:2d:6e:c0:c8:19:34:a7:99:5a:bc:58:98:69:ae
04:d6:6d:ec:4a:c9:55:a5:ff:00:cb:3b:02:85:fa:02:a1:5c:c1:9d
6d:44:b8:95:8f:77:c0:53:fc:7f:a4:09:a3:25:1c:4a:e2:9d:0c:81
08:b4:c8:b8:0d:bc:94:75:54:75:57:4f:d3:a4:17:0d:5d:1a:f3:c1
1d:5d:73:2f:fe:8b:cb:fc:1f:93:87:72:d6:be:df:86:d7:e6:d1:c7
0d:00:1a:6e:58:db:6a:1c:2f:1d:17:46:9a:f2:69:b4:21:db:08:5d
8d:ab:30:7d:7f:02:03:01:00:01
Signature algorithm: sha256WithRSAEncryption
Distribution CRL:
    http://10.102.40.55:8080/crl-as-der/currentcrl-11.crl?id=11
Use for key: CRL signing, Certificate signing, Key encipherment, Digital signature
Fingerprint:
    8b:84:60:2a:58:5b:80:f0:b9:ae:25:9f:67:3d:d6:81:ee:43:6c:d4 (sha1)
    ab:ec:4d:fe:d4:04:9c:c9:79:1d:9a:33:4e:6d:78:f6 (md5)

9d:f0:c0:a0:93:74:11:53:d3:4d:2d:75:d3:60:37:5f:fb:b7:a9:67:42:cd:7c:3c:0e:0f:9b:58:36:3c:14:f5
 sha256)
```

## IKEv2

summary

IKEv2 is a protocol used for establishing secure connections between devices. It is commonly used in Junos OS for configuring VPNs.

in this section

- IKEv2 configuration | 60
- | 60

IKEv2(Internet Key Exchange version 2) is a protocol used for establishing secure connections between devices. It is commonly used in Junos OS for configuring VPNs. IKEv2 is a protocol used for establishing secure connections between devices. It is commonly used in Junos OS for configuring VPNs. IKEv2 is a protocol used for establishing secure connections between devices. It is commonly used in Junos OS for configuring VPNs.

RFC 7427 is a standard for IKEv2. It defines the protocol and its implementation. RFC 7427 is a standard for IKEv2. It defines the protocol and its implementation. RFC 7427 is a standard for IKEv2. It defines the protocol and its implementation.



# ???(DDoS) ????? IKE ??

in this section

- IKE ????(DDoS) ?? | 61
- ??:???(DDoS) ?? | 62
- ???(DDoS) ?? | 63

☐ ☐☐☐ ☐☐ DDoS ☐☐☐☐☐ IPsec VPN IKE ☐☐ ☐☐ ☐☐☐☐ ☐☐ ☐☐☐

DoS(Denial of service)? ???? ?? IPsec VPN ?????? ?? ????? ??? ? ?????. DoS ??? ????? ????? ?? ???  
 ??? ??? ?? ??? ????? ??? ? ?? ??? ?? ??? ?????. CYber???? ????? ????? ?? ? ??? ?????.

DoS [ ] [ ] [ ]

???? ? ? ???? ???? ???? ???? ???? ???? ???? ? CPU? ? ???? ???? ? ? ???? ??.  
?? ? ???? ???? ???? ???? ? ? ? ???? ???? ?? DDoS(Distributed DoS) ????? ??

## IKE ??? ???(DDoS) ?? ???

?? ??(???)? SA\_INIT ????? ????? ?? ??(???)? ????? ??? ??? ?? ????? ??????. IKE\_AUTH ????? ????? ??? ???  
 ????? ??? ?? ?? IKE ?????? ???, ??? IKE(Internet Key Exchange) ?? ??(SA)? ????? ??? ??? ?? IKE(Internet  
 Key Exchange) ??? ??? .

IKEv2 DDoS [REDACTED] IKE SA[REDACTED]

- `0000 00 00 IKE 00 00 0000 00 0 00 0000SA_INIT 0000(IKE_AUTH 0000 00)0 00000. 0 00 00 00 000000 00000 0 000 00000 00000000.`
- `00000 00000 00 0000 SPI_i0 SPI_r 00 00 00 00 IKE_AUTH 0000 00000. 0000 0000 00000 00 000000 00000 0000000.`
- `SA_INIT 0000 000000 000000. 00000 0000 00 00 000000 00000 00 000000 00000 000000.`
- `0000 00 00 IKE(Internet Key Exchange) 00 00 00 00 00 0 0000 0000 00000.`
- `0000 0000 ID(0000)0 00000 00 00 00000 00000. 000000 00000 00 IKE 00000 0000000 00000 000000.`

IKE(Internet Key Exchange) ??? ???? ??

```

##### IKEv1 0 IKEv2 ##### ?? ??(DDoS) ??? ????? ?????? 0 ?? ??? ????? ??????. ##### IPsec VPN ##### ??
##### iked #####junos-ike ??? 0 IKE ??? ?? ??????? ??? 0 ??????.

```



2: IKEv2? ???(DDoS) ??? ?? ??? ??? RFC 8019, ?? ??? ?? ?????? IKEv2(Internet Key Exchange Protocol Version 2) ?? ??? ??????.???? iked ????? ????? IPsec VPN ????? ?? ? IKEv1? ?? ??? ??? ?????, RFC? ????? ?????? ?? ????? ????? ?????.

???:???(DDoS) ?? ??

IKE(Internet Key Exchange) ?? ?? ???? ?(DDoS) ??? ? ? ? ???? ???? ? ?????. ??? ?????? ?  
 ? ??? IKE(Internet Key Exchange) SA? ?? ?? ? ? ???? ???? ? ???? ???? ? ? ? ? ? ? ? ? ? ?  
 IKE(Internet Key Exchange) SA? ?? ??(DDoS) ?????? ???? ? ? ? ? ? ? ? ? ? ?.

- [illegible]

??? ???? ???? ???? ?? ???? ???? "IKE(Internet Key Exchange) DDoS ??? ?? ?? ??" ??? 63 ??????.

□□□ □□□□ □□□□



- kmd `???` `???` IPsec VPN `???` `??` `???`(DDoS) `??` `??`.
- `???` `???` `???` `???` `???` `??` `??` URL `???` `???` `???` `???`.

## ???(DDoS) ?? ???? ??

???(DDoS) `???` `???` `???` `???` `??` `???` `??` `???` `???`.

- show security ike security-associations `???` `???` `??` `??` `???` `??` IKE `??` `???` `???`, `???` `???` `??` `ike` `??` `??` `???` `???`.
- show security ike stats `???` `???` `??` `?`, `??`, `??` `???` `??` IPsec VPN `???` `???` IKE `???` `???` `???`, `???` `???` `??` `ike` `??` `???` `???`.
- show security ike active-peer `???` `???` `??` `???` `???` IKE(Internet Key Exchange) `???` `??` `??` `???` `???`. `???` `???` `??` `ike` `active-peer` `???` `???`.
- show security ike peers in-progress `???` `???` `???` `??` IKE(Internet Key Exchange) SA `???` `???` `??` `??` IKE(Internet Key Exchange) SA `??` `???` `???`. `???` `???` `?` `???` `???` *show security ike peers.* `??` `?` `???` `??` `??`, `??` `?` `???` `???` `??` `???` `?` `???`.
- clear security ike peers `???` `???` `???`, `??`, `??` `??` `??` `??` IKE(Internet Key Exchange) `???` `???`. `???` `???` `???` `???` *clear security ike peers.*
- `??` `???` `???` `??` `???` `??` IKE `??` `???` `???` `???` `???` `???` `clear security ike security-associations.` `???` `???` `??` `ike` `??` `??` `???` `???`.
- iked system log(syslog) `???` `IKE_GATEWAY_PEER_BLOCKED`, `IKE_GATEWAY_PEER_BACKOFF` `IKE_GATEWAY_PEER_FAILED` `??` `???` `??`, `???` `?` `???` IKE `???` `??` `??` `???` `??` `???`.
- `??` `???` `??` Junos OS `???`, `??` `?` `?` `???` `??` `??` `???` `???` `???` `???` `???` `???` `???` `???` `???`. `???` `???` `[]` `?` `???` `show firewall` `??` `?` `ids-option` `??` edit security screen ids-option *screen-name* `???` `???`.

## IKE(Internet Key Exchange) ???? (DDoS) ???? ?? ?? ??

### summary

IKE(Internet Key Exchange) `???` `???` `???`(DDoS) `??` `?` `??` `???` `???` `???` `?` `???` `???`.

### in this section

`???` `??` IKE(Internet Key Exchange) SA `??` `ike` `??` `??` | 64





- `set security ike session half-open discard-duplicate` discards duplicate IKE SA requests.

[edit]

```
user@host# set security ike session half-open discard-duplicate
```

`set security ike session half-open discard-duplicate` discards duplicate IKE SA requests. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

- `set security ike session half-open backoff-timeouts` sets the backoff-timeouts.

`set security ike session half-open backoff-timeouts` sets the backoff-timeouts. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

- `set security ike session half-open backoff-timeouts auth-phase-failure` sets the backoff-timeouts for the auth-phase-failure. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

[edit]

```
user@host# set security ike session half-open backoff-timeouts auth-phase-failure 150
```

`set security ike session half-open backoff-timeouts auth-phase-failure` sets the backoff-timeouts for the auth-phase-failure. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

- `set security ike session half-open backoff-timeouts init-phase-failure` sets the backoff-timeouts for the init-phase-failure. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

[edit]

```
user@host# set security ike session half-open backoff-timeouts init-phase-failure 160
```

`set security ike session half-open backoff-timeouts init-phase-failure` sets the backoff-timeouts for the init-phase-failure. The command is useful in environments where multiple IKE SAs are established between the same two peers. The command is useful in environments where multiple IKE SAs are established between the same two peers.

## IKE(Internet Key Exchange) SA

### in this section

• [IKE\(Internet Key Exchange\) SA](#) | 67

• [IKE\(Internet Key Exchange\) SA](#) | 67







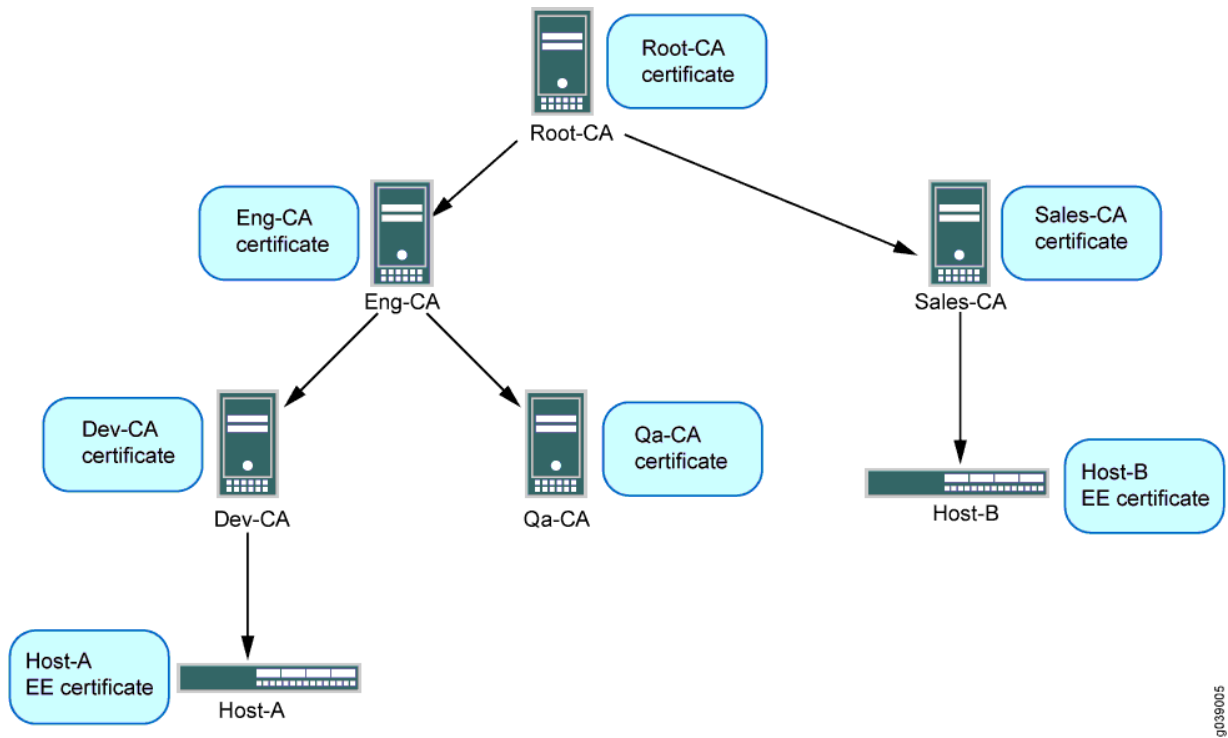




???

? ???? ? ??? ? 10 ??? 71?? Host-A? ?? ? ?? ? ?? ??. Host-A? Sales-CA?? CRL? ?????? Host-B ?  
??? ? ? ? ? ? ? ? ? Host-A? ?? CA ???? ???? ?????.

?? 10: ??? ?? ?



1?? ? 2?? ??? ?? IPsec VPN ??? ? ??? Host-A? ?? ??????. ?? ?????(Host-B)? 1?? ? 2?? ??? ?????? ????? ?  
? ??(SA)? ?????? ????? ?????? ???. VPN? ?? ?? ????? ? ? ? "?? ? VPN? ?? ?? IKE ID ??? " ??? 125 ??????  
?.

??

#### in this section

- CA ??? ?? | 72
- ??? ?? | 74
- IPsec VPN ?? ?? | 77



### 3. Dev-CA? ?? CA ???? ????.

```
[edit security pki]
user@host# set ca-profile Dev-CA ca-identity Dev-CA
user@host# set ca-profile Dev-CA enrollment url http://198.51.100.230:8080/scep/Dev/
user@host# set ca-profile Dev-CA revocation-check crl
```

??

?? ???? show security pki ??? ???? ???? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show security pki
ca-profile Root-CA {
  ca-identity Root-CA;
  enrollment {
    url "http://198.51.100.230:8080/scep/Root/";
  }
  revocation-check {
    crl ;
  }
}
ca-profile Eng-CA {
  ca-identity Eng-CA;
  enrollment {
    url "http://198.51.100.230:8080/scep/Eng/";
  }
  revocation-check {
    crl ;
  }
}
ca-profile Dev-CA {
  ca-identity Dev-CA;
  enrollment {
    url "http://198.51.100.230:8080/scep/Dev/";
  }
  revocation-check {
    crl ;
  }
}
```

???? ???? ???? ?? ???? commit?(?) ?????.

??? ??

??? ??

??? ?????:

## 1. CA ????? ?????.

```
user@host> request security pki ca-certificate enroll ca-profile Root-CA
```

```
user@host> request security pki ca-certificate enroll ca-profile Eng-CA
```

```
user@host> request security pki ca-certificate enroll ca-profile Dev-CA
```

????? ???? **yes** CA ????? ?????.

## 2. CA ????? ?????? ????? ???? ?????.

```
user@host> show security pki ca-certificate ca-profile Root-CA
Certificate identifier: Root-CA
    Issued to: Root-CA, Issued by: C = us, O = example, CN = Root-CA
    Validity:
        Not before: 08-14-2012 22:19
        Not after: 08-13-2017 22:19
    Public key algorithm: rsaEncryption(2048 bits)
```

```
user@host> show security pki ca-certificate ca-profile Eng-CA
Certificate identifier: Eng-CA
    Issued to: Eng-CA, Issued by: C = us, O = example, CN = Root-CA
    Validity:
        Not before: 08-15-2012 01:02
```

```
Not after: 08-13-2017 22:19
Public key algorithm: rsaEncryption(2048 bits)
```

```
user@host> show security pki ca-certificate ca-profile Dev-CA
Certificate identifier: Dev-CA
Issued to: Dev-CA, Issued by: C = us, O = example, CN = Eng-CA
Validity:
  Not before: 08-15-2012 17:41
  Not after: 08-13-2017 22:19
Public key algorithm: rsaEncryption(2048 bits)
```

3. `show security pki ca-certificate ca-profile Root-CA`.

```
user@host> request security pki ca-certificate verify ca-profile Root-CA
CA certificate Root-CA verified successfully
```

```
user@host> request security pki ca-certificate verify ca-profile Eng-CA
CA certificate Eng-CA verified successfully
```

```
user@host> request security pki ca-certificate verify ca-profile Dev-CA
CA certificate Dev-CA verified successfully
```

4. `request security pki generate-key-pair certificate-id Host-A type rsa size 1024`.

```
user@host> request security pki generate-key-pair certificate-id Host-A type rsa size 1024
```

5. `request security pki local-certificate enroll certificate-id Host-A ca-profile Dev-CA challenge-password example domain-name host-a.example.net email host-a@example.net subject DC=example,CN=Host-A, OU=DEV,O=PKI,L=Sunnyvale,ST=CA,C=US`.

```
user@host> request security pki local-certificate enroll certificate-id Host-A ca-
profile Dev-CA challenge-password example domain-name host-a.example.net email host-
a@example.net subject DC=example,CN=Host-A, OU=DEV,O=PKI,L=Sunnyvale,ST=CA,C=US
```

- 6.**

```
user@host> show security pki local-certificate
Issued to: Host-A, Issued by: C = us, O = example, CN = Dev-CA
Validity:
    Not before: 09-17-2012 22:22
    Not after: 08-13-2017 22:19
Public key algorithm: rsaEncryption(1024 bits)
```

- [illegible]

```
user@host> request security pki local-certificate verify certificate-id Host-A
Local certificate Host-A verification success
```

8.  CA   CRL  .

```
user@host> show security pki crl

CA profile: Root-CA
  CRL version: V00000001
  CRL issuer: C = us, O = example, CN = Root-CA
  Effective date: 09- 9-2012 13:08
  Next update: 09-21-2012 02:55

CA profile: Eng-CA
  CRL version: V00000001
  CRL issuer: C = us, O = example, CN = Eng-CA
  Effective date: 08-22-2012 17:46
  Next update: 10-24-2015 03:33

CA profile: Dev-CA
  CRL version: V00000001
  CRL issuer: C = us, O = example, CN = Dev-CA
  Effective date: 09-14-2012 21:15
  Next update: 09-26-2012 11:02
```

## IPsec VPN 配置

### CLI 配置

在配置模式下，使用 `set` 命令配置 IPsec 策略。配置完成后，使用 `commit` 命令提交配置。

```
set security ike proposal ike_cert_prop_01 authentication-method rsa-signatures
set security ike proposal ike_cert_prop_01 dh-group group5
set security ike proposal ike_cert_prop_01 authentication-algorithm sha1
set security ike proposal ike_cert_prop_01 encryption-algorithm aes-256-cbc
set security ike policy ike_cert_pol_01 mode main
set security ike policy ike_cert_pol_01 proposals ike_cert_prop_01
set security ike policy ike_cert_pol_01 certificate local-certificate Host-A
set security ike gateway ike_cert_gw_01 ike-policy ike_cert_pol_01
set security ike gateway ike_cert_gw_01 address 192.0.2.51
set security ike gateway ike_cert_gw_01 external-interface ge-0/0/1.0
set security ike gateway ike_cert_gw_01 local-identity 192.0.2.31
set security ipsec proposal ipsec_prop_01 protocol esp
set security ipsec proposal ipsec_prop_01 authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_prop_01 encryption-algorithm 3des-cbc
set security ipsec proposal ipsec_prop_01 lifetime-seconds 300
set security ipsec policy ipsec_pol_01 proposals ipsec_prop_01
set security ipsec vpn ipsec_cert_vpn_01 bind-interface st0.1
set security ipsec vpn ipsec_cert_vpn_01 ike gateway ike_cert_gw_01
set security ipsec vpn ipsec_cert_vpn_01 ike ipsec-policy ipsec_pol_01
```

配置完成。

在配置模式下，使用 `set` 命令配置 IPsec 策略。配置完成后，使用 `commit` 命令提交配置。

IPsec VPN 配置完成。

#### 1. 配置 IPsec 策略。

```
[edit security ike proposal ike_cert_prop_01]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy ike_cert_pol_01]
```

```

user@host# set mode main
user@host# set proposals ike_cert_prop_01
user@host# set certificate local-certificate Host-A
[edit security ike gateway ike_cert_gw_01]
user@host# set ike-policy ike_cert_pol_01
user@host# set address 192.0.2.51
user@host# set external-interface ge-0/0/1.0
user@host# set local-identity 192.0.2.31

```

## 2. 2?? ??? ?????.

```

[edit security ipsec proposal ipsec_prop_01]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm 3des-cbc
user@host# set lifetime-seconds 300
[edit security ipsec policy ipsec_pol_01]
user@host# set proposals ipsec_prop_01
[edit security ipsec vpn ipsec_cert_vpn_01]
user@host# set bind-interface st0.1
user@host# set ike gateway ike_cert_gw_01
user@host# set ike ipsec-policy ipsec_pol_01

```

??

?? ????? show security ike ? show security ipsec ??? ?????? ??? ??????, ??? ??? ??? ?????, ? ?? ?? ??? ???  
 ? ??????

```

[edit]
user@host# show security ike
proposal ike_cert_prop_01 {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy ike_cert_pol_01 {
    mode main;
    proposals ike_cert_prop_01;
    certificate {

```



```

        local-certificate Host-A;
    }
}
gateway ike_cert_gw_01 {
    ike-policy ike_cert_pol_01;
    address 192.0.2.51;
    external-interface ge-0/0/1.0;
}
[edit]
user@host# show security ipsec
proposal ipsec_prop_01 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 300;
}
policy ipsec_pol_01 {
    proposals ipsec_prop_01;
}
vpn ipsec_cert_vpn_01 {
    bind-interface st0.1;
    ike {
        gateway ike_cert_gw_01;
        ipsec-policy ipsec_pol_01;
    }
}

```

?? ?? ?? ?? ?? commit?(?) ????.

??

#### in this section

- [IKE\(Internet Key Exchange\) 1?? ?? ?? | 80](#)
- [IPsec 2?? ?? ?? | 80](#)

?? ????? ?? IKE ?? ?? ??? ??? IKE ? IPsec SA(Security Association)? ?? ?????.

???? ???? IKE(Internet Key Exchange) SA? ?? ?????. ???? ???? IKE SA? DOWN?? IPSEC SA? ?? ?????

?? ??? ???? ???? ?????

IKE(Internet Key Exchange) 1?? ? ? ?

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

show security ike security-associations ?? ????? ?? ? ?????.

```
user@host> show security ike security-associations
      Index   State Initiator cookie Responder cookie Mode      Remote Address
      2090205 DOWN      285feacb50824495  59fca3f72b64da10 Main      192.0.2.51
```

IPsec 2?? ? ? ?

??

IPsec 2?? ??? ?????.

??

show security ipsec security-associations ?? ????? ?? ?????.

```
user@host> show security ipsec security-associations
Total active tunnels: 1
      ID      Algorithm      SPI      Life:sec/kb Mon vsys Port Gateway
      <131073 ESP:3des/sha1 a4756de9 207/ unlim - root 500 192.0.2.51
      >131073 ESP:3des/sha1 353bacd3 207/ unlim - root 500 192.0.2.51
```

??? ????? ? ? IKE ? IPsec SA ??







1. CA `ca1` CA `ca2` `ca3`.

```
[edit]
user@host# set security pki ca-profile root-ca ca-identity root-ca
```

2. IKE(Internet Key Exchange) `ike1` IKE(Internet Key Exchange) `ike2` `ike3`.

```
[edit]
user@host# set security ike proposal ike_prop authentication-method rsa-signatures
```

3. IKE(Internet Key Exchange) `ike1` Diffie-Hellman `dh1`, `dh2`, `dh3`.

```
[edit]
user@host# set security ike proposal ike_prop dh-group group2
user@host# set security ike proposal ike_prop authentication-algorithm sha-256
user@host# set security ike proposal ike_prop encryption-algorithm aes-256-cbc
```

4. IKE(Internet Key Exchange) `ike1` IKE(Internet Key Exchange) `ike2`.

```
[edit]
user@host# set security ike policy ike_policy proposals ike_prop
```

5. IKE(Internet Key Exchange) `ike1` `ike2` `ike3`.

```
[edit]
user@host# set security ike policy ike_policy certificate local-certificate SPOKE
```

6. IKE(Internet Key Exchange) `ike1` CA `ca1`.

```
[edit]
user@host# set security ike policy ike_policy certificate trusted-ca ca-profile root-ca
```

`ca1` CA `ca2` `ca3` show security pki .

```
user@host# show security ike
proposal ike_prop {
  authentication-method rsa-signatures;
  dh-group group2;
```

## SEE ALSO

## IKE?? Establish-Tunnel Responder-only ??

IKE?? establish-tunnel responder-only ????:

















- `vpn vpn1 {`  
`bind-interface st0.0;`  
`ike {`  
`gateway gw1;`  
`ipsec-policy ipsec_pol;`  
`}`  
`traffic-selector ts1 {`  
`local-ip 192.168.2.0/24;`  
`remote-ip 10.0.2.0/24;`  
`}`  
`}`
- `vpn vpn2 {`  
`bind-interface st0.0;`  
`ike {`  
`gateway gw2;`  
`ipsec-policy ipsec_pol;`  
`}`  
`}`

??

IPsec VPN? ??? ?? point-to-point st0 ?????? ??? ? ????

- `vpn vpn1 {`  
`bind-interface st0.0;`  
`ike {`  
`gateway gw1;`  
`ipsec-policy ipsec_pol;`  
`}`  
`traffic-selector ts1 {`  
`local-ip 192.168.2.0/24;`  
`remote-ip 10.0.2.0/24;`  
`}`  
`}`
- `vpn vpn2 {`  
`bind-interface st0.0;`  
`ike {`  
`gateway gw2;`  
`ipsec-policy ipsec_pol;`  
`}`  
`}`

?? ??

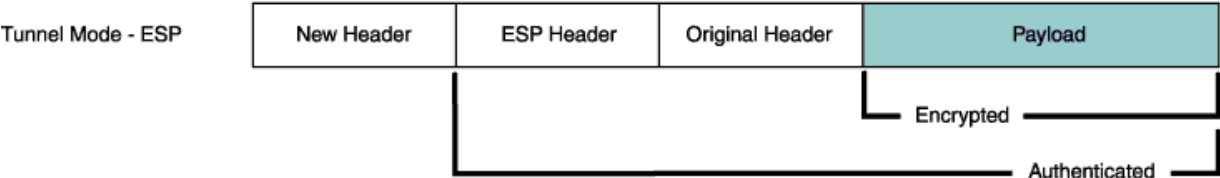
?? IPsec VPN ?????? st0 ?????? ??? ? ????. ??? st0 ?????? ??? ? ?? ?? ?? IPsec VPN ??? ????? ?  
 ?? ?? IKE ?????? ??? ? ????

```
[edit security ipsec]
user@host# show
vpn vpn1 {
  bind-interface st0.0;
  ike {
    gateway gw1;
    ipsec-policy ipsec_pol;
  }
  traffic-selector ts1 {
    local-ip 192.168.2.0/24;
    remote-ip 10.0.2.0/24;
  }
}
vpn vpn2 {
  bind-interface st0.0;
  ike {
    gateway gw2;
    ipsec-policy ipsec_pol;
  }
}
```



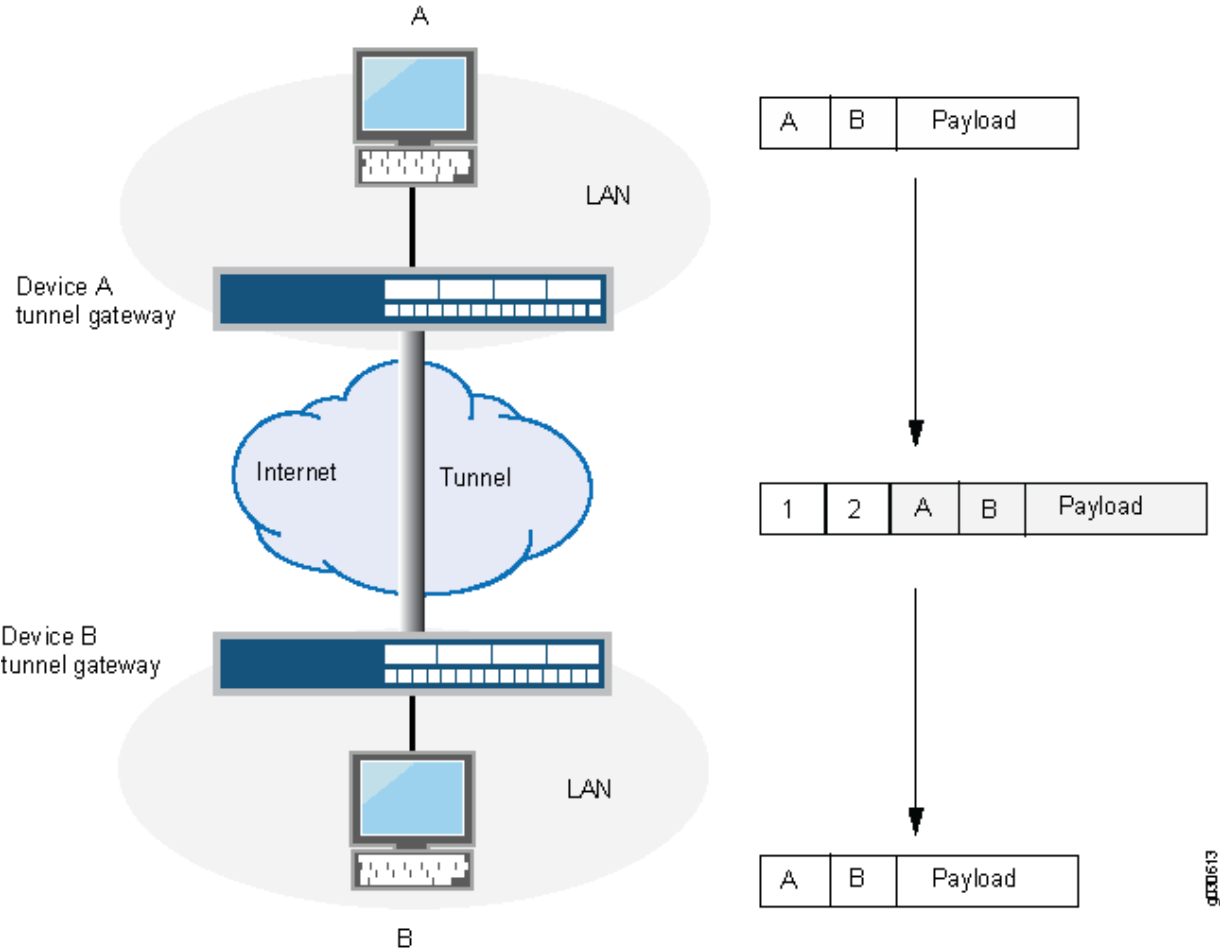


11: Tunnel Mode - ESP



VPN IP 12 95(2) .

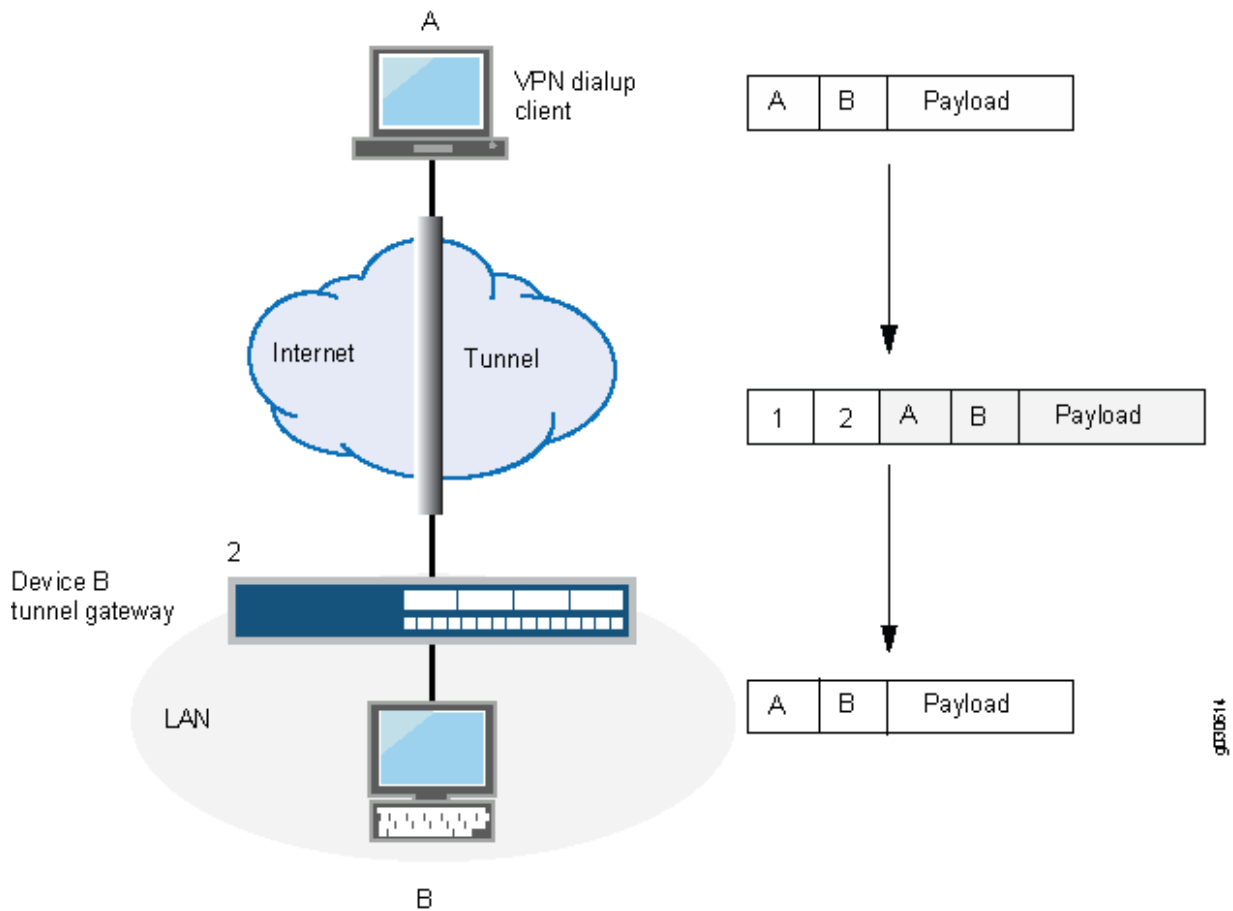
12: VPN



?? VPN?? ?? VPN ?? ?? ?????? ?? ?? ?????? ???. ??? ?????? ????? ?? ??????. (?? 13 ??? 96 ??) ? ??  
 ?? ?? ?????????? ?? ?????? ??? ?????? ?? ?? ??? ?? ?? IP ??? ??????. ??????? ?????????.

Netscreen-Remote? ?? ?? VPN ??????? ?? ?? IP ??("?? ??"???? ?) ? ??????. Netscre-Remote?? ?? IP ??? ?  
 ?? ? ??????. ??? ?? ?? ?? IP ??? ?????????? ?????? ????? ?? ?? ?????? ?? IP ?????, ISP? ????? ??? ?? ?? ???????  
 IP ??? ?? ?????? ?? IP ??????

### ?? 13: ?? ????? ?? ?? VPN



### SEE ALSO

[?: ?? ?? VPN ?? | 328](#)

[?? ?? IPsec VPN | 452](#)

## SPU? IKE(Internet Key Exchange)? IPsec ?? ??

???? ???? ???? "???? SPU VPN ?? ??" ??? 104 ?????????.

SRX ??? ????? IKE? IPsec? ?? ?? ??? ????? ?? ????? ??????. IKE? ????? ? IPsec ??? ????? ?? Diffie-Hellman(DH) ? ??? ??????. IKE?? ??? IPsec ??? ??, ??, IP ????? ????? ?? ?? ???? ??????.

VPN? ????? ?? ??? ?? ??(SPU)? ? IKE ? IPsec ????? ??? ????? ??????. ??? ? ??? ?? ?? ?? ??? ?? SPU? ?? SPU? ??????. ?? SPU? ??? ?? ?? ??? ??? ?? ?? ? ?? ??? ?? SPU? ??? ? ??????. ??, ??? ??? ? ?????? ? ? SPU? ??? ?? ?? VPN ?? ?? ??????. ?? ??? ?? ?? ??? ?? ??? ?? ?????? ????? SPU? ??????.

IPsec?? ????? IKE? ????? ?? ??? ?????? ?? ??????. ??? VPN ?? ?? ??? ? ?? 2?? SA? ?? SPU? ?????? ??? ? ???, 2?? SA? ?? ?? IPsec ??? IPsec ??? ?? SA? ??? SPU? ??????.

?? IPsec ??(2?? SA)? ?? ??? IKE ????? ??? ? ??????. IPsec ??? ????? ?? ??? SPU? ?? IKE ??? ????? SPU? ?? ?? ?? ?????. ??? ?? IKE ??????? ?? ????? ?? IPsec ??? ??? SPU? ?? ?????? ?? SPU? ?? ?? ??? ?? ?????.

[? 9](#) [???](#) [97](#)(?) 3?? IKE ??????? 7?? IPsec ??? ????? 3?? SPU? ?? ????? ??????.

### ? 9: SPU? IKE(Internet Key Exchange)? IPsec ?? ??

| SPU  | IKE(Internet Key Exchange) ??<br>??? | IPsec ?? |
|------|--------------------------------------|----------|
| SPU0 | IKE-1                                | IPsec-1  |
|      |                                      | IPsec-2  |
|      |                                      | IPsec-3  |
| SPU1 | IKE-2                                | IPsec-4  |
|      |                                      | IPsec-5  |
|      |                                      | IPsec-6  |
| SPU2 | IKE-3                                | IPsec-7  |

SPU 3?? ? IKE ????? 1?? ??? ??? ??????. ??? IKE ?????? ??? SPU0, SPU1, ?? SPU2? ????? IKE ??? ?? ? IPsec ??? ? ?????.

?? IPsec ??? ???? ???? ?? ?? IKE ???? ?? IPsec ??? ???? ???? ????.

SPU ? ??? ?? ?? ?? ?? ???? show ??? ?????. show security ike tunnel-map.

? ?????? ?? ????? ?? ?? ???? summary ??? ?????. show security ike tunnel-map summary.

## SPC(Services Processing Card) ??? ?? VPN ??

?? SRX ??? ???? ?? ?? ?? ???? ???? ???? ?????. ??? ?? ??? ?????. SPC(Services Processing Card) ?? ?? ???? ? SPC? ???? ???? ?? ???? ???? ? ????.

???? ?? ???? "???? SRX5000 ?? SPC ??" ??? 104 ??? ????.

??? ??? "SRX5000 ??? cmd ? iked ????? ? ? ??" ??? 105 ??? ????.

?? SRX ??? ?? ???? ?? IKE ?? IPsec VPN ??? ???? ???? ???? ? ???? SPC? ??? ? ????.

SPC3 ?? SPC2 ??? SPC3 ??? ??? ?? ??? ???? ? ?????. ??? ?? SPC3 ???? ? ???? ???? ? ????.

??? ?? ??? ??? SPC?? SPU(Service Processing Units)? ?? ??? ??? ? ?????. ? SPU? ??? ??? ??? ? ??? ?? ??? ??? ? ?????. ??? ??? ??? ??? ? SPC?? ???? ? ? ????.

??? ? ??? ?? ??? ???? ???? ?? ?? SPU? ?????. ?? ??? ???? ? SPU? ???? ??? ?? ?? ?????. ??? ? ? ? ???? IP ??? ??? ??? SPU?? ???? ? ???? RT ???? ???? SPU? ?????. ??? ?? ?? SPU? ?? SPU? ?? ??? ? SPU? ?? ?? SPU?? ???? ???? RT ??? ?? ?????. ? SPU?? ???? ???? RT ??? ?? SPU ??? ?? ????.

?? ??? = SPU? ??? ?? ? / SPU?? ???? ???? RT ???? ? ??

?? ??? ??? ??(round-robin) ???? ???? ?? ?? SPU? ?????. ??? ??? ? ???? ? SPC? ???? ? ? ????.

SPC2 ? SPC3 ??? ?? ??? ??, show security ipsec tunnel-distribution ??? ???? ? SPU?? ?? ??? ??? ? ????.

show security ike tunnel-map ??? ???? SPC2 ??? ??? ?? SPU?? ?? ??? ??? ? ?????. show security ike tunnel-map ??? SPC2 ? SPC3 ??? ??? ???? ???? ????.

SPC3 ?? ?? : ?? ? ?? ??:

- ?? ?????? ?? ? ??? 1?? SPC3 ??? ?? ?? ??? 2?? SPC3 ??? ?? ??, 1?? SPC3 ??? ?? ??? ?? ????? ??? ? ????.
- ?? ??? ?? ?? SPC3?? ?? ??? ?? ??? SPC3 ?? SPC2? ???? ????.
- SPC3 ISHU? ????? ? SPC3 ??? ?? ?? ??? ???? ????.
- ??? SPC3 Hot removal? ????? ????.

## SEE ALSO

`show security ike tunnel-map`

## iked [IKEv2](#) IPsec VPN

### in this section

- iked [IKEv2](#) IPsec VPN [IKEv2](#) | 100

iked [IKEv2](#) ikemd, [IKEv2](#) [IKEv2](#) SRX [IKEv2](#) IPsec VPN [IKEv2](#). iked [IKEv2](#) ikemd [IKEv2](#) SRX [IKEv2](#) junos-ike [IKEv2](#) [IKEv2](#).

junos-ike [IKEv2](#) [IKEv2](#) iked [IKEv2](#) IPsec VPN [IKEv2](#). SRX [IKEv2](#) junos-ike [IKEv2](#) [IKEv2](#).

[IKEv2](#) [IKEv2](#) "[IKEv2](#) [IKEv2](#) junos-ike[IKEv2](#) [IKEv2](#)" [IKEv2](#) 105 [IKEv2](#).

[IKEv2](#) [IKEv2](#) iked [IKEv2](#) ikemd [IKEv2](#) junos-ike [IKEv2](#) [IKEv2](#) [IKEv2](#).

SRX [IKEv2](#) junos-ike [IKEv2](#) [IKEv2](#) [IKEv2](#).

```
user@host> request system software add optional://junos-ike.tgz
```

```
Verified junos-ike signed by PackageProductionECP256_2022 method ECDSA256+SHA256
```

```
Rebuilding schema and Activating configuration...
```

```
mgd: commit complete
```

```
Restarting MGD ...
```

```
WARNING: cli has been replaced by an updated version:
```

```
CLI release 20220208.163814_builder.r1239105 built by builder on 2022-02-08 17:07:55 UTC
```

```
Restart cli using the new version ? [yes,no] (yes)
```

[IKEv2](#) [IKEv2](#) ikemd [IKEv2](#) restart ike-config-management [IKEv2](#).

[IKEv2](#) [IKEv2](#) iked [IKEv2](#) restart ike-key-management [IKEv2](#).



?: junos-ike???? ???? ? ???? Junos OS ??? ???? ???? ???? ? ???? ???? ???? ? ? ? ????.

SRX ??? ????? ??? kmd ????? ???? IPsec VPN ??? ????? request system software delete junos-ike ??? ???  
? ????? ?????.

??? junos-ike ???? ????? ? ???? ???? ????.

```
user@host> show version | grep ike

JUNOS ike [20190617.180318_builder_junos_182_x41]
JUNOS ike [20190617.180318_builder_junos_182_x41]

{primary:node0}
```

iked ?????? ???? ? IPsec VPN ??

? ????? SRX ??? ????? ? IPsec VPN ??? ????.

[? 10](#) [100](#)?? iked ????? ???? ? vSRX ?? ? ? SRX ??? ????? ? IPsec VPN ??? ???? ? ????.

**? 10: SRX** ??? ????? ? IPsec VPN ??

| ??                                                                       | ?? ???                     |
|--------------------------------------------------------------------------|----------------------------|
| AutoVPN PIM(Protocol Independent Multicast) P2MP(Point-to-multipoint) ?? | ???, ??? vSRX 3.0??? ????. |
| IPsec VPN?? ??? ?? ?                                                     | ???                        |
| ?? VPN                                                                   | ???                        |
| IPsec datapath ??? ?? ?? ??                                              | ???                        |
| ?? ?? IPsec VPN                                                          | ???                        |

???

??? ?? ?? ?? "???? ???? ???? ??" ??? 103 ??? ?????.

??? ???? "??? ???? ???? ?? ?? ???? ??" ???? 105 ???? ??????.

Junos OS? [REDACTED] SRX [REDACTED] DH, RSA, ECDSA [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED].

```

junos-ike [redacted] [redacted] [redacted] iked [redacted] [redacted] IPsec VPN [redacted] [redacted], [redacted] [redacted] IPsec VPN [redacted] [redacted] [redacted] [redacted]
[redacted] [redacted] [redacted] [redacted] [redacted] iked [redacted] [redacted], junos-ike [redacted] [redacted], [redacted] [redacted] IPsec [redacted] [redacted] [redacted](kmd) [redacted] [redacted] [redacted]
iked [redacted] ikemd [redacted] [redacted].

```

□□□□ □□□ □□□□ □□ □□□□ □□□□ □□□□□.

## SEE ALSO

```
?? ipsec ?? ?? ??
```

```
?? ipsec ?? ?? ??
```

## IPSec VPN [?] [?] [?] [?] [?] [?]

105 18 107, 19 108, 20 108, 21 109 22 109  
 23 110,

Junos OS SRX IPsec VPN SPC3 MX IPsec VPN SPC3 MX. kmd iked OSPF, BGP, PIM, RIP BFD.

- IP   : IPv4  IPv6
- st0     : P2P(Point-to-Point)  P2MP(Point-to-multipoint)

## Anti-Replay

???? ???? ???? "???? ?????? ? ??" ??? 105 ????? ??????.

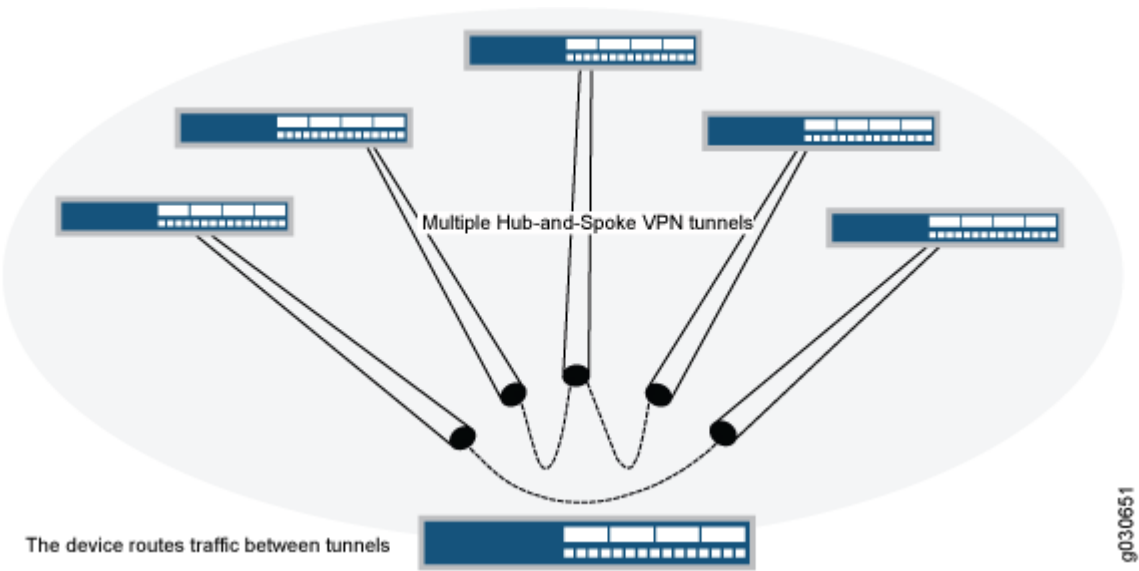
SRX ??? ?????? ?????? ??? ?? ?? 64? ?????? ?????? anti-replay-window.

[?] [??] [??] [??] [??] [?] anti-replay-window-size [??] [??] [??] [??] [?] anti-replay-window-size [?] [?] [??] [?] [??] [??]





Figure 14: Configuring VPN tunnels



SEE ALSO

[Configuring VPN tunnels](#) | 134

IPsec VPN

in this section

- [Configuring SPU VPN tunnels](#) | 104
- [Configuring SRX5000 SPC SPC](#) | 104
- [Configuring VPN tunnels](#) | 105
- [Configuring VPN tunnels](#) | 105

For more information, see [Configuring VPN tunnels](#).

For more information, see [Configuring VPN tunnels](#) 105.

For more information, see [Configuring VPN tunnels](#).

## 配置 SPU VPN 配置

### 图 11: 配置 SPU

| 配置项    | 配置内容                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| SRX 配置 | <ul style="list-style-type: none"> <li>SPU 配置 SRX5000 配置 SPU 配置 IKE 配置 IPsec 配置。"SPU 配置 IKE(Internet Key Exchange) 配置 IPsec 配置" 配置 97 配置。</li> </ul> |

## 配置 SRX5000 配置 SPC 配置

### 图 12: 配置 SPC

| 配置项    | 配置内容                                                                                                                                                                                                                                                                                                                                              |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SRX 配置 | <ul style="list-style-type: none"> <li>SPC 配置 SRX5000 配置:             <ul style="list-style-type: none"> <li>配置 SPC 配置。</li> <li>SPC3 配置 IPsec 配置。</li> <li>SRX5K-SPC-4-15-320(SPC2) 配置 SPC3 配置 IPsec 配置。SRX5K-SPC3 配置 IPsec VPN 配置。配置 "SPC(Services Processing Card) 配置 VPN 配置" 配置 98 配置。</li> <li>配置 SRX5800 配置 SPC3 配置。</li> </ul> </li> </ul> |





**Table 17: SRX Series SRX Series (Continued)**

| SRX Series           | SRX150<br>0<br>(SRX150) | SRX150<br>0<br>(iked) | SRX410<br>0<br>SRX420<br>0<br>(SRX420) | SRX410<br>0<br>SRX420<br>0<br>(iked) | SRX460<br>0<br>(SRX460) | SRX460<br>0<br>(iked) | SPC300<br>SRX500<br>0 SRX500<br>(iked) | vSRX<br>3.0<br>(SRX300) | vSRX<br>3.0<br>(iked) |
|----------------------|-------------------------|-----------------------|----------------------------------------|--------------------------------------|-------------------------|-----------------------|----------------------------------------|-------------------------|-----------------------|
| DH 21                | SRX150                  | SRX150                | SRX410                                 | SRX410                               | SRX460                  | SRX460                | SPC300                                 | SRX300                  | SRX300                |
| DH 24                | SRX150                  | SRX150                | SRX410                                 | SRX410                               | SRX460                  | SRX460                | SPC300                                 | SRX300                  | SRX300                |
| RSA                  | SRX150                  | SRX150                | SRX410                                 | SRX410                               | SRX460                  | SRX460                | SPC300                                 | SRX300                  | SRX300                |
| ECDSA(256, 384, 521) | SRX150                  | SRX150                | SRX410                                 | SRX410                               | SRX460                  | SRX460                | SPC300                                 | SRX300                  | SRX300                |

**Table 18: IPsec VPN SRX Series (OSPF) SRX Series**

| IPsec VPN SRX Series | SRX300<br>SRX320<br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC300<br>SRX500<br>0 SRX500<br>0 SRX500<br>0 SPC2 | SRX500<br>0 SRX500<br>(SPC3+S<br>PC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|----------------------|------------------------------------------------|--------------|-------------|-------------------------------------------|----------------------------------------------------|---------------------------------------|-------------|-------------|
| P2P st0              | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |
| IPv4                 | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |
| IPv6                 | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |
| P2MP st0             | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |
| IPv4                 | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |
| IPv6                 | SRX300                                         | SRX550       | SRX150      | SRX410                                    | SPC300                                             | SRX500                                | SRX300      | SRX300      |

### 19: IPsec VPN OSPFv3

| IPsec VPN OSPFv3 |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|------------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
| P2P<br>st0       | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|                  | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |
| P2MP<br>st0      | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|                  | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |

### 20: IPsec VPN BGP

| IPsec VPN BGP |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|---------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
| P2P<br>st0    | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |
| P2MP<br>st0   | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |

## 21: IPsec VPN PIM

| IPsec VPN PIM |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|---------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
| P2P<br>st0    | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |
| P2MP<br>st0   | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |

## 22: IPsec VPN RIP

| IPsec VPN RIP |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|---------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
| P2P<br>st0    | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |
| P2MP<br>st0   | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |

## Table 22: IPsec VPN RIP (Continued)

| IPsec VPN RIP |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|---------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |

## Table 23: IPsec VPN BFD

| IPsec VPN BFD |      | SRX300<br>SRX320<br><br>SRX340<br>SRX345<br>SRX380 | SRX550<br>HM | SRX150<br>0 | SRX410<br>0<br>SRX420<br>0<br>SRX460<br>0 | SPC3<br>SRX500<br>0<br>SRX500<br>0<br>SPC2 | SRX500<br>0<br>(SPC3+<br>SPC2) | vSRX<br>3.0 | MX-<br>SPC3 |
|---------------|------|----------------------------------------------------|--------------|-------------|-------------------------------------------|--------------------------------------------|--------------------------------|-------------|-------------|
| P2P<br>st0    | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |
| P2MP<br>st0   | IPv4 |                                                    |              |             |                                           |                                            |                                |             |             |
|               | IPv6 |                                                    |              |             |                                           |                                            |                                |             |             |

Table 24: IPsec VPN





- ?? | 112
- ??? IPsec? ?? ?? | 113
- ??? IPsec? ?? ?? ?? | 115

??

100% IPsec 100% CPU 100% 100% 100% 100% Junos OS 100%. 1 100 100 100 100  
 ASIC 100% IPsec 100% 100% 100%. 1 100 100 CPU 1 QAT(Quick Assist Technology) 1 100%  
 PMI(PowerMode IPsec) 100 IPsec VPN 100%.

?? IPsec? ??? CPU?? IPsec ??? ???, Intel QAT? ? ???? ? ? PMI? ? ???? ???? ? ?  
 ??. ?? IPsec? ? SRX ??? ???? ? ? ? ? ASIC? ???? IPsec ??? ? ? ??. IPsec ??? ? ???? ASIC?  
 ?????? ???? ?????. ?? IPsec? ??? ? ? ? ? ? ? CPU? ?????.

- **PSK(PSK)** **IKEv2(Internet Key Exchange version 2)**
- **PPK**
- **PKI(Public-Key Infrastructure)**
- **IPsec**

????? ??? IPsec ??? ?????? ??? ?????? ??????. ? ?????? ?????? ? ??? ?????? ?????? ??????.

??

- VPN 22: 2222 2 2222 ASIC 222222 22 222 2222 2 22 2222 22222.
- CPU 222: ASIC 22 222 2222 CPU 2222 222222 CPU 2 22 222 222 222 2 222 22 2222 222 222 222222.
- VPN 22: 2222 2222 222 AES-GCM(Advanced Encryption Standard–Galois/Counter Mode) 222 22222 2222 222 2222 22 22 22 222 222 222 22222.
- 22: 222 22 22 IPsec 222 2222 222 222 22222.
- 222: 22 222 22 222 2 22 222 2222 222 22222.

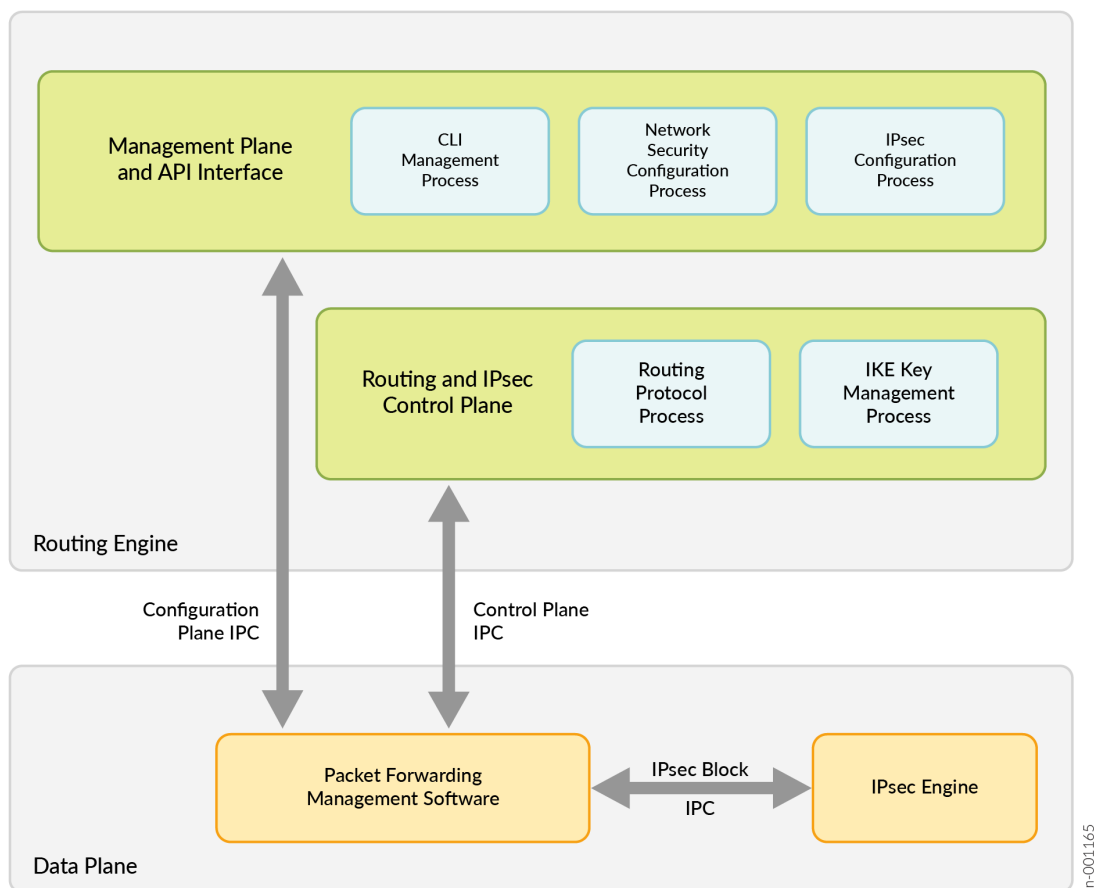
## 配置 IPsec 策略

图 15-114 展示了 IPsec 策略的配置。在 IPsec 策略配置窗口中，配置 IPsec 策略的名称、IPsec 策略的 ID、IPsec 策略的本地地址、IPsec 策略的远端地址、IPsec 策略的本地子网、IPsec 策略的远端子网、IPsec 策略的本地端口、IPsec 策略的远端端口、IPsec 策略的本地认证方式、IPsec 策略的远端认证方式、IPsec 策略的本地认证密钥、IPsec 策略的远端认证密钥、IPsec 策略的本地认证期限、IPsec 策略的远端认证期限、IPsec 策略的本地认证算法、IPsec 策略的远端认证算法、IPsec 策略的本地认证密钥长度、IPsec 策略的远端认证密钥长度、IPsec 策略的本地认证期限单位、IPsec 策略的远端认证期限单位、IPsec 策略的本地认证算法名称、IPsec 策略的远端认证算法名称、IPsec 策略的本地认证密钥名称、IPsec 策略的远端认证密钥名称、IPsec 策略的本地认证期限名称、IPsec 策略的远端认证期限名称、IPsec 策略的本地认证算法名称、IPsec 策略的远端认证算法名称、IPsec 策略的本地认证密钥名称、IPsec 策略的远端认证密钥名称、IPsec 策略的本地认证期限名称、IPsec 策略的远端认证期限名称。

SRX 设备支持 IPsec 策略配置。

- IPsec 策略配置，请参考图 15-114。
- 配置 IPsec 策略的 ASIC 表项 IPsec ESP(Encapsulating Security Payload) 表项。
- 配置 IPsec 策略的 IKE(Internet Key Exchange) 表项 CPU 表项。
- IKE 策略配置，请参考图 15-115。
- 配置 IPsec 策略的 IKE 策略表项。
- IPv4 和 IPv6 策略配置，请参考图 15-116。
- IKEv1 和 IKEv2 策略配置，请参考图 15-117。

## ?? 15: ??? IPsec ???



??? IPsec? ????? ?????? ?? ??? ??? ? ????

- `iked` ????? ?? ????? ?????? ??? IPsec ??? ??????. ? ??? ????? IPsec ??? ? ?? ?? CPU ? ??? ? ????
- `?? show security ipsec security association ? ??? ?? ??????`
  - Hardware Offloaded: Yes - `??? IPsec VPN ??? ??`.
  - Hardware Offloaded: No CPU? ??? ??? ?.
- `flowd` ????? IPsec VPN ??? flow? ?? ?? ? ?? ??? ??????

?? ??? ?? ASIC?? IPsec ?? ??? ?? IPsec ????? ?????? ?????? ??????????

- `??? set security ipsec hw-offload-disable?????`

? ????? ?????? ??? ?? ??? ?? ASIC ?? CPU?? ?? IPsec ??? ??????. [ipsec\(?\)?](#) ????????



?? ??

| ?? ipsec ?? ?? ?? ??

# 3

CHAPTER LABEL COVER PAGE

## VPN ?? ??

---

### in this chapter

- IPsec VPN ?? ?? | **118**
  - ?? ?? VPN ?? ?? VPN ?? | **183**
  - ?? ???? HA ?? ?? ??? | **185**
  - ?? ?? IPsec VPN | **188**
-

# IPsec VPN **?? ??**

## summary

Junos OS? VPN **???** **??** **??????** **?** **???** **??????**.

## in this section

- [?? ? IKE\(Internet Key Exchange\)? \*\*???\*\* IPsec VPN \*\*?? ??\*\* | 118](#)
- [?? IP \*\*???\*\* \*\*?????\*\* \*\*???\*\* \*\*?\*\* VPN? \*\*?????\*\* \*\*?? ??\*\* | 119](#)
- [?? IP \*\*???\*\* \*\*?????\*\* \*\*???\*\* \*\*?\*\* \*\*?? ??\*\* VPN? \*\*?????\*\* \*\*?? ??\*\* | 121](#)
- [?? \*\*???????\*\* \*\*??\*\* IPsec VPN \*\*??\*\* | 122](#)
- [IKE ID \*\*?? ??\*\* | 124](#)
- [???? \*\*?\*\* VPN? \*\*?? ??\*\* IKE ID \*\*??\*\* | 125](#)
- [SRX \*\*???\*\* \*\*??????\*\* \*\*?????\*\* \*\*?? ??\*\* \*\*??\*\*\(OSPF\) \*\*?\*\* OSPFv3 \*\*??\*\* \*\*?????\*\* | 126](#)
- [?: SRX \*\*???\*\* \*\*??????\*\* \*\*?? ??\*\* \*\*??\*\*\(OSPF\) \*\*???????\*\* \*\*??\*\* IPsec \*\*?? ??\*\* | 127](#)
- [VPN \*\*?????\*\* \*\*?????\*\* IPsec VPN \*\*??\*\* | 133](#)
- [?: \*\*?? ?\*\* \*\*????\*\* VPN \*\*??\*\* | 134](#)

VPN **????** **?** LAN(??? VPN) **?? ??** **????** **??** **?????** LAN? **????** **?** **?????**. **?** **?** **????** **????** **?????** **??** WAN? **?????** **????**, **??** **?** **??** **??** **?????** **????** **??** **?????** **???????**. **?** **????** **?????** **????** IPsec **????** **?????** VPN **????** **???????**.

## **?? ? IKE(Internet Key Exchange)? **???** IPsec VPN **?? ??****

IPsec VPN **????** **?** **????** **???????**. 1**?????** **?????** IPsec **?? ??**(SA)? **????** **??** **????** **???????**. 2**?????** **?????** **????** **??** **????** **??** **?????** **??** IPsec SA? **???????**.

**?** **????** **??** **?** IKE(**??** **????** **?** **??** **????**)? **?????** **??** **??** **??** **??** IPsec VPN? **?????** **??** **????** **??** **???????**.

**??** **?** IKE(Internet Key Exchange)? **????** **??** **??** **??** **??** **??** IPsec VPN? **???????** **????** **???????**.

1. **??????**, **??** **??** **?** **??** **?** **????** **???????**.

(**??** **??** VPN? **??**) **??** **??** st0.x **???????** **???????**. **???????** **?????** **???????**.

2. IPsec VPN **????** 1**????** **???????**.



- a) (?? ??) ??? ?? IKE(Internet Key Exchange) 1?? ??? ??????. ?? ??? IKE(Internet Key Exchange) 1?? ???(??, ?? ?? ??)? ??? ? ??? ? ??? ?? ??????.
  - b) ??? ?? IKE(Internet Key Exchange) 1?? ?? ?? ?? ??? IKE 1?? ?? ??? ????? IKE ??? ??????. ?? ? IKE(Internet Key Exchange) ?? ?? ? ?? ??? ??? ??????. 1?? ??? ?? ??(? ?? ???)? ??????.
  - c) IKE(Internet Key Exchange) ??? ????? IKE ?????? ??????. ?? ? ?? ?????? IKE(Internet Key Exchange) ?? ?? ???(IDS)? ??????. ?? ?????? IP ??? ????? ? ? ?? ?? ????? ? ? ?? ??????
3. IPSec VPN ??? ?????????.
- a) (?? ??) ??? ?? IPsec 2?? ??? ??????. ?? ??? IPsec 2?? ?? ??(??, ?? ?? ??)? ??? ? ????? ? ??? ?? ?? ???.
  - b) ??? ?? IPsec 2?? ?? ?? ?? ??? IPsec 2?? ?? ??? ????? IPsec ??? ??????. ??? ??? ??(PFS) ?? ??????.
  - c) IKE(Internet Key Exchange) ?????? ? IPsec ?? ??? ????? IPsec VPN ??? ??????. 2?? ????? ??? ID? ??????.
- (?? ?? VPN? ??) ?? ?? ????? st0.x? IPsec VPN ??? ??????.
4. ?? ????? ?? ????? ?????? ?????? ?? ??? ??????.
- (?? ?? VPN? ??) ????? IPsec VPN ??? ??? ??? ?? ?? tunnel ipsec-vpn?(?) ??????.
5. ??? VPN ??? ????????

## SEE ALSO

?? ?? IPSec VPN ?? | 452

IPsec VPN | 327

?? IP ??? ???? ??? ? VPN? ????? ?? ??

[25](#) [119](#) IP [VPN](#). [VPN](#).

**25: IP 192.168.1.1 VPN 192.168.1.1**

?? ??      ???

*IKE(Internet Key Exchange) ?? ??:*

## 25: IPsec VPN (Continued)

| IPsec                               | IPsec                                                                                                                                                                             |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec                               | IPsec IPsec IPsec IPsec.                                                                                                                                                          |
| RSA DSA                             | RSA DSA IPsec IPsec IPsec IPsec, IPsec IPsec IPsec(PKCS7 X.509) IPsec IPsec.                                                                                                      |
| DH(Diffe-Hellman) 14                | DH 14 DH 1, 2 5 IPsec IPsec IPsec IPsec.                                                                                                                                          |
| AES(AES)                            | AES IPsec IPsec IPsec IPsec(DES) IPsec DES(3DES) IPsec IPsec IPsec IPsec.<br>FIPS(Federal Information Processing Standards) IPsec IPsec EAL4 IPsec IPsec IPsec IPsec IPsec IPsec. |
| SHA-256                             | SHA-256 SHA-1 MD5 IPsec IPsec IPsec IPsec IPsec.                                                                                                                                  |
| IPsec:                              |                                                                                                                                                                                   |
| PFS(Perfect Forward Secrecy) DH 14  | PFS DH 14 IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec.                                                                                                |
| ESP(Encapsulating Security Payload) | ESP IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec.                                                                                                      |
| AES                                 | AES IPsec IPsec IPsec IPsec DES 3DES IPsec IPsec IPsec IPsec IPsec IPsec. FIPS IPsec IPsec EAL4 IPsec IPsec IPsec IPsec IPsec IPsec.                                              |
| SHA-256                             | SHA-256 SHA-1 MD5 IPsec IPsec IPsec IPsec IPsec.                                                                                                                                  |
| IPsec                               | IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec IPsec.                                                                                                          |

## SEE ALSO

IPsec | 11

?? IP ??? ????? ? ? ? ? ? ? ? ? ? ? VPN? ????? ?? ??

26 121 IP VPN .

**? 26: ?? IP ??? ????? ? ?? ?? ?? VPN? ?? ?? ??**

?? ??

*IKE(Internet Key Exchange) ?? ??:*

|                             |                                                                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| ?? ??                       | ???? ?? ?????.                                                                                                                                  |
| 2048?? ??                   | RSA ?? DSA ????? ?? ? ?????. ?? ?????? ?? ?????. ??? ??? ?(PKCS7 ?? X.509)? ??????.                                                             |
| DH(Difie-Hellman) ?? 14     | DH ?? 14? DH ?? 1, 2 ?? 5?? ? ?? ??? ?????.                                                                                                     |
| ?? ??? ?(AES) ???           | AES? ? ??? ?? ? ??? ??? ?(DES)? ??? DES(3DES)?? ? ??? ?????. FIPS(Federal Information Processing Standards) ? ?? ? EAL4 ??? ?? ??? ??? ? ?????. |
| ?? ?? ????? 256(SHA-256) ?? | SHA-256? SHA-1 ?? MD5(Message Digest 5)? ? ??? ??? ??? ?????.                                                                                   |

IPsec  :

|                                        |                                         |
|----------------------------------------|-----------------------------------------|
| PFS(Perfect Forward Secrecy)<br>DH 14  | PFS DH 14 DH IPsec IPsec<br>DH 14.      |
| ESP(Encapsulating Security<br>Payload) | ESP IP ESP ESP ESP ESP ESP ESP ESP ESP. |
| AES                                    | AES DES 3DES FIPS EAL4<br>AES.          |
| SHA-256                                | SHA-256 SHA-1 MD5<br>SHA-256.           |

26: IP VPN (Continued)

|  |  |
|--|--|
|  |  |
|  |  |

SEE ALSO

IPsec | 11

IPsec VPN

in this section

- | 122
- IKE(Internet Key Exchange) ID | 123
- IKEv1 | 123
- IKE | 123
- NAT | 123
- IKE ID | 123

IPsec VPN VPN IP IP, DHCP(Dynamic Host Configuration Protocol) IP IP. NAT IP VPN SRX, IKEv1 IKEv2 VPN SRX VPN IPv4 SRX VPN IPv6.

IPv6 AutoVPN.

VPN



## IKE ID `?? ??`

### in this section

- [IKE ID `??` | 124](#)
- [IKE ID `??` VPN | 125](#)
- [IKE ID `??` VPN | 125](#)
- [SRX `???` IKE ID | 125](#)

IKE ID(IKE ID) `?` IKE `??` VPN `??` `??????` `?????` `??` `??????`. SRX `???` `?????` `??` `??????` `?????` IKE(Internet Key Exchange) ID `?` IPv4 `??` IPv6 `??`, `????` `??`, `????` `????` (FQDN), `????` FQDN(UFQDN) `??` `??` `??` (DN) `?` `?` `????`. `??` `????` `????` IKE ID `?` SRX `???` `?????` `?????` `??` `?????` `????`. `????` `????` IKE ID `????` `????` `?????` VPN `??` `????` `?????`.

### IKE ID `??`

SRX `???` `?????` `??` `????` `??` `????` `??` `????` IKE ID `??????`.

- IPv4 `??` IPv6 `????` `??????` `??` `????` `??` IP `????` `????` `????` `?` VPN `??` `??????`.
- `????` `????` `??` `??` `?????` `?????` `????????`. `????` IP `????` `?????` FQDN `?` `?????`. `??` `??` `??` `?????` `?????` `??` IKE `????` `??` `?` `??` `?????` `??` FQDN `??` `?????`.  
  
IP `??` `??` `????` `????` `????` `??` `????` `??` `?` `??` `??` `????` `??` `????` IP `????` `?????` `????`. `??` `????` IP `????` `?????` `????` `?` `??` `????` `?` `?????`.
- UFQDN `?` `user@example.com` `?(?)` `??` `????` `????` `????` `????` `????` `????????`.
- DN `?` `?????` `?????` `?????` `??` `????` `?????` `??` `?????` `????????`. `??` `??`, DN `?` `"CN=user, DC=messages, DC=com"` `?` `?????`. `??????` container `?????` `?????` DN `?` `??` `????` `??` `????` DN `?` `????` `??????` `???????`, wildcard `?????` `?????` DN `?` `??` `??` `?????` `?????` `??` `????` `??` `????` `?????` `?` `?????`.  
  
`??` [edit security ike gateway *gateway\_name* dynamic distinguished-name] `????` container-string `?` wildcard-string `?` `????` `??` DN `????` `????` `?` `?????`. `?` `??` `????` `????` `?` `?` `??` `????` `???????` `??` `?` `??` `????` `?` `??` `?????` `?????`. `???????` `???????` `??` `??` `?` `????` `??` `????` `??` `????` `?????` `?????` `?????`.
- SRX `???` `??????` `????` VPN `????????` `?????` `??` `????` `??` `??` AutoVPN `?` `??` `????` VPN `??` IKE `????` `????` `????` `?` `?????`. `??` IKE ID `?` `???????` ike-user-type group-ike-id `?(?)`, `??` IKE ID `?` `???????` ike-user-type shared-ike-id `?(?)` `?` `?????`.







- OSPF `??` OSPFv3 `?????? ??` [edit protocols ospf area *area-id* interface *interface-name*] `??` [edit protocols ospf3 area *area-id* interface *interface-name*] `??` `???` ipsec-sa *name*`??` `??????`. OSPF `??` OSPFv3 `????????` IPsec SA `???` `???` `???` `?` `???`, `??` `??` OSPF/OSPFv3 `??????????` `???` IPsec SA`?` `???` `?` `?????`.
- OSPF `??` OSPFv3 `??` `????` `??` [edit protocols ospf area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*] `??` [edit protocols ospf3 area *area-id* virtual-link neighbor-id *router-id* transit-area *area-id*] `??` `???` ipsec-sa *name*`??` `??????`. `??` `??????` `???` `???` `??` `???` `??` `???` IPsec SA`?` `????` `???`.

SRX ??? ????? OSPF ?? OSPFv3? ?? IPsec ????? ???? ?? ???? ??????.

- [edit security ipsec vpn *vpn-name* manual] `??` `????` `???` `??` VPN `???` IPsec `??` `?` `????` `????` `??` OSPF `??` OSPFv3 `????` `??` `??` `???` `???` `?` `????`.
- `????` `???` `??` `?` `??` `???` `????` `???` `??` IPsec VPN `??` `??` `??` OSPF `??` OSPFv3 `???` `??` IPsec `???` `?` `????`.
- `??` `??` st0 `????????` OSPF `??` OSPFv3 `???` `??` IPsec `?` `????` `????`.
- `??` `??` `?` `????` `????` `????`.
- `??` IKE(Internet Key Exchange) SA `????` `????`.
- IPsec `??` `???` `??????`. `??` `??????` IP `???` `?????`(`?????` `???`)`?` `???????` `???????` `?` `???`. `??` `???` `?????` `?????`.
- `???` `??` SA `??????` `??` OSPFv3 `???` `???` IPsec SA `?????` `???`. [edit security ipsec] `??` `?????` `??` `???` SA `?` `?????`.
- `??` `??????` `???` `???` `??` `???` `??` `???` IPsec SA `?????` `???`.

## SEE ALSO

IPsec ?? | 11

**?: SRX ??? ????? ?? ?? ??(OSPF) ?????? ?? IPsec ?? ??**

in this section

- 
- ?? ?? | 128
- ?? | 128
- ?? | 129
- ?? | 132

在配置 SA(Security Association)和 OSPF 时，需要配置以下参数。

配置参数

配置参数：

- 配置 SA(Security Association)。
- OSPF 配置。
- OSPF 配置。
- 配置 OSPF 配置。
- 配置 OSPF 配置。

配置

OSPF 和 OSPFv3 配置 IPsec 配置。配置 SA 和 OSPF 配置。27 128(?) 配置 SA 和 OSPF 配置。

27: IPsec OSPF 配置 SA

| 配置参数  | 配置                      |
|-------|-------------------------|
| SA 配置 | sa1                     |
| 配置    | 配置                      |
| 配置    | 配置                      |
| 配置    | AH                      |
| SPI   | 256                     |
| 配置 配置 | hmac-md5-96             |
| key   | (ASCII) 123456789012abc |
| 配置 配置 | des                     |
| key   | (ASCII) cba210987654321 |

in this section

- ?? SA ?? | 129
- OSPF ?????? ?? IPsec ?? ?? | 131

**?? SA ??**

CLI

OSPF [REDACTED] IPsec [REDACTED] SA [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED], [REDACTED] [REDACTED], [REDACTED] [REDACTED] [REDACTED]  
[REDACTED] [REDACTED] [REDACTED] [REDACTED], [REDACTED] [REDACTED] [edit] [REDACTED] CLI [REDACTED], [REDACTED] commit[REDACTED] [REDACTED].

```
[edit]
set security ipsec security-association sa1
set security ipsec security-association sa1 mode transport
set security ipsec security-association sa1 manual direction bidirectional
set security ipsec security-association sa1 manual direction bidirectional protocol ah
set security ipsec security-association sa1 manual direction bidirectional spi 256
set security ipsec security-association sa1 manual direction bidirectional authentication
algorithm hmac-md5-96 key ascii-text 123456789012abc
set security ipsec security-association sa1 manual direction bidirectional encryption algorithm
des key ascii-text cba210987654321
```

???

?? ?? ?? ???? ??? ??? ???? ?????. ?? ???? ??? ? ???? CLI ??? ??? /?? /??? CLI ??? ??? ?????.

?? SA? ?????,

1. SA? ? ? ? ? ? ? ?.

```
[edit]
user@host# edit security ipsec security-association sa1
```





OSPFv3 `???` `[edit protocols]??` `ospf3??` `???`.

```
[edit]
user@host# edit protocols ospf area 0.0.0.0
```

## 2. `???` `???`.

```
[edit protocols ospf area 0.0.0.0]
user@host# edit interface so-0/2/0
```

## 3. IPsec `??` SA `???`.

```
[edit protocols ospf area 0.0.0.0 interface so-0/2/0.0]
user@host# set ipsec-sa sa1
```

`??`

**show ospf interface detail** `???` `???` `???` `???`. `??` `???` `???` `???` `???` `???` `??` `???` `???` `???` `???`.

OSPFv3 `???` `???` **show protocols ospf3** `???` `???`.

```
[edit]
user@host# show protocols ospf
area 0.0.0.0 {
  interface so-0/2/0.0 {
    ipsec-sa sa1;
  }
}
```

`???` `???` `???` `??` `???` **commit**`?(?)` `???`.

`??`

### in this section

- [IPsec `??` `??` `??` `??` | 133](#)
- [OSPF `???` `???` `???` `??` | 133](#)

?? ???? ???? ???? ?????.

**IPsec** ?? ?? ?? ??

??

??? IPsec ?? ?? ???? ?????. ?? ??? ?????.

- ?? ?? ???? ???? ???? ???? ????.
- SPI ???? ???? ????.
- ?? ??? ???? ????.
- ?? ???? ???? ???? ????.

??

?? ???? **show ospf interface detail** ??? ????.

**OSPF** ???? IPsec ?? ?? ??

??

??? IPsec ?? ??? OSPF ???? ???? ?????. IPsec SA ?? ??? IPsec ?? ??? ???? ????.

??

?? ???? OSPF? ?? **show ospf interface detail** ??? ???? OSPFv3? ?? **show ospf3 interface detail** ??? ??  
???

## SEE ALSO

| [?? VPNv1? ?? IPsec SA ?? ??](#) | [762](#)

## VPN ???? ???? IPsec VPN ??

VPN ???? ???? 1?? ? 2??? ?? ??? ?? IPsec VPN? ??? ? ?????. ?? ??? J-Web ???? ?? CLI? ?????.  
? ??? SRX300, SRX320, SRX340, SRX345, SRX550HM ???? ????.

- SSG140



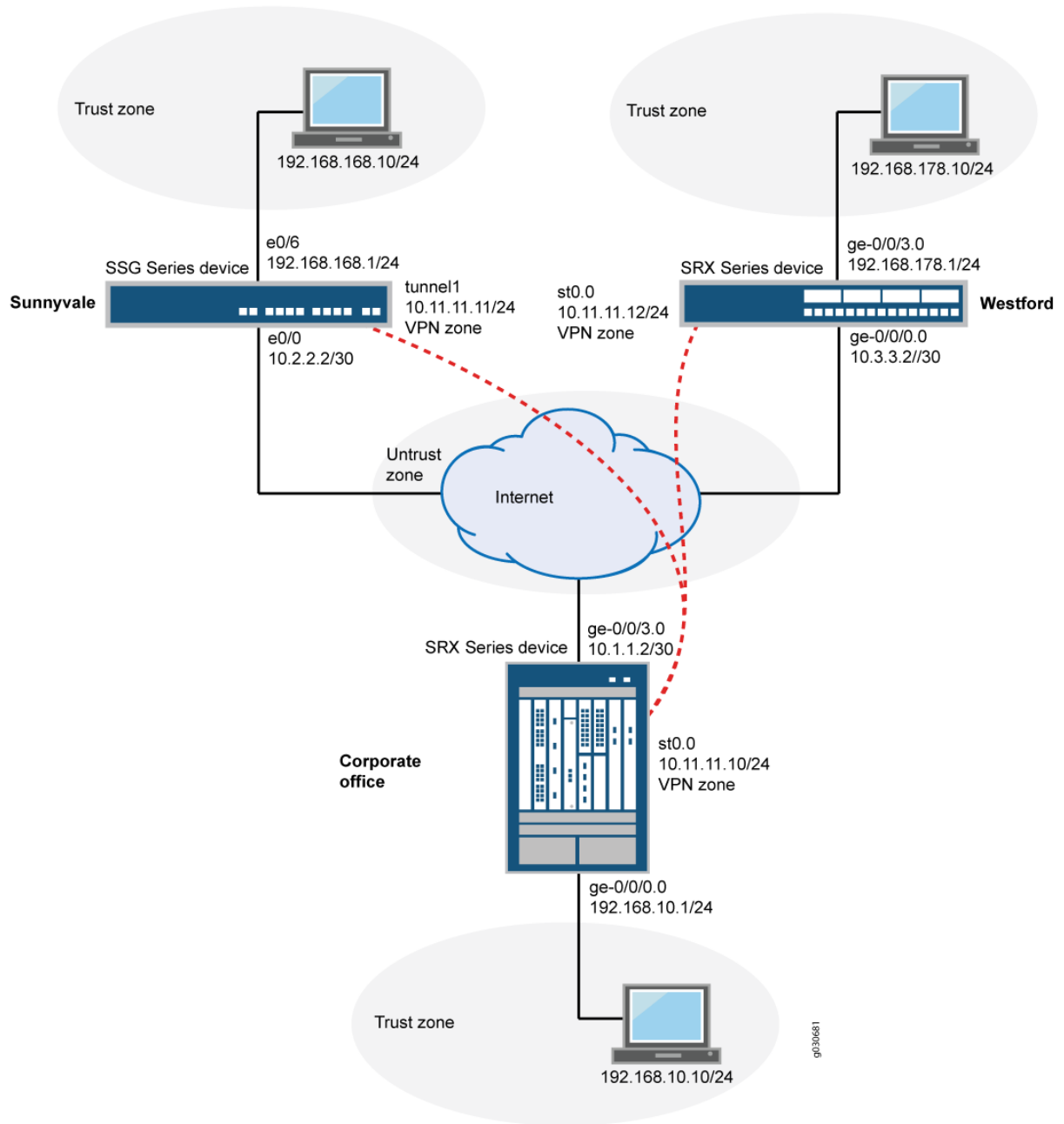
???? ?? "IPsec ??" ??? 11?(?) ??????.

??

我 想 知 道 你 們 有 沒 有 用 過 VPN? 有 沒 有 用 過 過 境 網 站, 有 沒 有 用 過 過 境 網 站, 有 沒 有 用 過 過 境 網 站  
 有 沒 有 用 過 過 境 網 站, 有 沒 有 用 過 過 境 網 站, 有 沒 有 用 過 過 境 網 站, 有 沒 有 用 過 過 境 網 站.

16 136 VPN SRX5800 SRX  
Westford SSG140 Sunnyvale

# ?? 16: ?? ? ??? VPN ????



? ???? ? ? , ???? ? , ???? ???? ???? . ? ???? , IPv4 ? ? ? ? ? , ? ? , ???? ???? . ? ?  
 IKE(Internet Key Exchange) 1??? IPsec 2?? ? ???? , st0.0 ???? IPsec VPN? ???? . ????  
 st0.0? ???? ???? ? NHTB ???? ???? . ???? , ? ? ? TCP-MSS ? ???? . ? ???? ? ? ?  
 ? ? ? ? ? 28 ? 137~? 32 ? 144?(?) ???? .

图 28: ???? , ? ? ? ? ?

| ?? ? ? ? | ??   | ??         | ?? ? ?                                                                                                                                |
|----------|------|------------|---------------------------------------------------------------------------------------------------------------------------------------|
| ??       | ???? | ge-0/0/0.0 | 192.168.10.1/24                                                                                                                       |
|          |      | ge-0/0/3.0 | 10.1.1.2/30                                                                                                                           |
|          |      | st0        | 10.11.11.10/24                                                                                                                        |
| ???      | ???? | ge-0/0/0.0 | 10.3.3.2/30                                                                                                                           |
|          |      | ge-0/0/3.0 | 192.168.178.1/24                                                                                                                      |
|          |      | st0        | 10.11.11.12/24                                                                                                                        |
| ??       | ?? ? | ??         | <ul style="list-style-type: none"> <li>?? ???? ???? .</li> <li>ge-0/0/0.0 ???? ? ? ? ? ? ? .</li> </ul>                               |
|          |      | untrust    | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange)? ???? ???? ???? .</li> <li>ge-0/0/3.0 ???? ? ? ? ? ? ? .</li> </ul> |
|          |      | VPN        | st0.0 ???? ? ? ? ? ? .                                                                                                                |

Figure 28: Configuration, (Continued)

| Configuration | Device        | Configuration | Configuration                                                                                                                |
|---------------|---------------|---------------|------------------------------------------------------------------------------------------------------------------------------|
| Configuration | Device        | Configuration | <ul style="list-style-type: none"> <li>Configuration</li> <li>ge-0/0/3.0 Configuration</li> </ul>                            |
|               |               | untrust       | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) Configuration</li> <li>ge-0/0/0.0 Configuration</li> </ul> |
|               |               | VPN           | st0.0 Configuration                                                                                                          |
| Configuration | Configuration | local-net     | <ul style="list-style-type: none"> <li>Configuration</li> <li>Configuration 192.168.10.0/24</li> </ul>                       |
|               |               | sunnyvale-net | <ul style="list-style-type: none"> <li>Configuration vpn Configuration</li> <li>Configuration 192.168.168.0/24</li> </ul>    |
|               |               | westford-net  | <ul style="list-style-type: none"> <li>Configuration vpn Configuration</li> <li>Configuration 192.168.178.0/24</li> </ul>    |



## 29: IKE(Internet Key Exchange) 1 (Continued)

| ?? ?? | ??   | ??                  | ?? ??                                                                                                                                                           |
|-------|------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | ??   | ike-phase1-policy   | <ul style="list-style-type: none"> <li>??: main</li> <li>?? ??: ike-phase1-proposal</li> <li>IKE(Internet Key Exchange) 1: pre-shared-key ascii-text</li> </ul> |
|       | ???? | gw-westford         | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: ike-phase1-policy</li> <li>?? ??: ge-0/0/3.0</li> <li>?? ??: 10.3.3.2</li> </ul>       |
|       |      | gw-sunnyvale        | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: ike-phase1-policy</li> <li>?? ??: ge-0/0/3.0</li> <li>?? ??: 10.2.2.2</li> </ul>       |
| ???   | ??   | ike-phase1-proposal | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> <li>Diffie-Hellman ??: group2</li> <li>?? ??: sha1</li> <li>?? ??: aes-128-cbc</li> </ul>    |

## 29: IKE(Internet Key Exchange) 1 (Continued)

| ?? ? ? ? ? | ??     | ??                | ?? ? ? ? ?                                                                                                                                                                 |
|------------|--------|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|            | ??     | ike-phase1-policy | <ul style="list-style-type: none"> <li>??: main</li> <li>?? ??: ike-phase1-proposal</li> <li>IKE(Internet Key Exchange) 1 ? ? ? ? ? : pre-shared-key ascii-text</li> </ul> |
|            | ?????? | gw-corporate      | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ? ? ??: ike-phase1-policy</li> <li>?? ?????: ge-0/0/0.0</li> <li>?????? ??: 10.1.1.2</li> </ul>          |

## 30: IPsec 2 ? ? ? ? ?

| ?? ? ? ? ? | ??  | ??                    | ?? ? ? ? ?                                                                                                                                                              |
|------------|-----|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??         | ??  | ipsec-phase2-proposal | <ul style="list-style-type: none"> <li>?????: esp</li> <li>?? ?????: hmac-sha1-96</li> <li>???? ?????: aes-128-cbc</li> </ul>                                           |
|            | ??  | ipsec-phase2-policy   | <ul style="list-style-type: none"> <li>?? ??: ipsec-phase2-proposal</li> <li>PFS: Diffie-Hellman group2</li> </ul>                                                      |
|            | VPN | vpn-sunnyvale         | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ???? ??: gw-sunnyvale</li> <li>IPsec ? ? ??: ipsec-phase2-policy</li> <li>?????? ??: st0.0</li> </ul> |

### Figure 30: IPsec 200 200 200 (Continued)

| 200 200 200 | 200 | 200                   | 200 200 200                                                                                                                                                                                    |
|-------------|-----|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|             |     | vpn-westford          | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) 200200 200: gw-westford</li> <li>• IPsec 200 200: ipsec-phase2-policy</li> <li>• 200200200 200200: st0.0</li> </ul>        |
| 200200      | 200 | ipsec-phase2-proposal | <ul style="list-style-type: none"> <li>• 200200200: esp</li> <li>• 200 200200200: hmac-sha1-96</li> <li>• 200200 200200200: aes-128-cbc</li> </ul>                                             |
|             | 200 | ipsec-phase2-policy   | <ul style="list-style-type: none"> <li>• 200 200: ipsec-phase2-proposal</li> <li>• PFS: Diffie-Hellman group2</li> </ul>                                                                       |
|             | VPN | vpn-corporate         | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) 200200200 200: gw-corporate</li> <li>• IPsec 200 200: ipsec-phase2-policy</li> <li>• 200200200200 200200: st0.0</li> </ul> |



### 31: ? ? ? ? ? ? ? ?

| ??<br>??<br>??<br>? | ??                                        | ??                  | ?? ?? ??                                                                                                                                                                                          |
|---------------------|-------------------------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??<br>?             | ?? ???? ???? ???? VPN ???? ????<br>?????. | local-to-<br>spokes | <ul style="list-style-type: none"> <li>?? ??:</li> <li>source-address local-net</li> <li>destination-address sunnyvale-net</li> <li>destination-address westford-net</li> <li>?? ?????</li> </ul> |
|                     | ?? ???? VPN ???? ???? ???? ????<br>?????. | spokes-to-<br>local | <p>?? ??:</p> <ul style="list-style-type: none"> <li>source-address sunnyvale-net</li> <li>source-address westford-net</li> <li>destination-address local-net</li> <li>?? ?????</li> </ul>        |
|                     | ?? ???? intrazone ???? ????.              | spoke-to-<br>spoke  | <p>?? ??:</p> <ul style="list-style-type: none"> <li>?? source-address</li> <li>?? destination-address</li> <li>?? ?????</li> </ul>                                                               |
| ??<br>?             | ?? ???? ???? ???? VPN ???? ????<br>?????. | to-corp             | <ul style="list-style-type: none"> <li>?? ??:</li> <li>source-address local-net</li> <li>destination-address corp-net</li> <li>destination-address sunnyvale-net</li> <li>?? ?????</li> </ul>     |





```
set security address-book book2 address sunnyvale-net 192.168.168.0/24
set security address-book book2 address westford-net 192.168.178.0/24
set security address-book book2 attach zone vpn
```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

??? ?? ???? , ?? ?? ? ???? ?? ?? ??:

1. ??? ???? ???? ????.

```
[edit]
user@hub# set interfaces ge-0/0/0 unit 0 family inet address 192.168.10.1/24
user@hub# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/30
user@hub# set interfaces st0 unit 0 family inet address 10.11.11.10/24
```

2. ?? ?? ???? ????.

```
[edit]
user@hub# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
user@hub# set routing-options static route 192.168.168.0/24 next-hop 10.11.11.11
user@hub# set routing-options static route 192.168.178.0/24 next-hop 10.11.11.12
```

3. ?????(untrust) ?? ??? ????.

```
[edit ]
user@hub# set security zones security-zone untrust
```

4. ????? ???? (untrust) ?? ??? ????.

```
[edit security zones security-zone untrust]
user@hub# set interfaces ge-0/0/3.0
```

5. `set security zones security-zone untrust set host-inbound-traffic system-services ike`

```
[edit security zones security-zone untrust]
user@hub# set host-inbound-traffic system-services ike
```

6. `set security zones security-zone trust`

```
[edit]
user@hub# edit security zones security-zone trust
```

7. `set security zones security-zone trust set interfaces ge-0/0/0.0`

```
[edit security zones security-zone trust]
user@hub# set interfaces ge-0/0/0.0
```

8. `set security zones security-zone trust set host-inbound-traffic system-services all`

```
[edit security zones security-zone trust]
user@hub# set host-inbound-traffic system-services all
```

9. `set security address-book book1 set address local-net 10.10.10.0/24 set attach zone trust`

```
[edit security address-book book1]
user@hub# set address local-net 10.10.10.0/24
user@hub# set attach zone trust
```

10. `set security zones security-zone vpn`

```
[edit]
user@hub# edit security zones security-zone vpn
```

11. `set security zones security-zone vpn set interfaces st0.0`

```
[edit security zones security-zone vpn]
user@hub# set interfaces st0.0
```



```

route 0.0.0.0/0 next-hop 10.1.1.1;
route 192.168.168.0/24 next-hop 10.11.11.11;
route 192.168.178.0/24 next-hop 10.11.11.12;
}

```

```

[edit]
user@hub# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    host-inbound-traffic {
    }
    interfaces {
        st0.0;
    }
}
[edit]
user@hub# show security address-book
book1 {
    address local-net 10.10.10.0/24;
    attach {
        zone trust;
    }
}

```

```

}
book2 {
    address sunnyvale-net 192.168.168.0/24;
    address westford-net 192.168.178.0/24;
    attach {
        zone vpn;
    }
}

```

?? ?? ?? ?? commit?(?) ?????.

## ?? IKE(Internet Key Exchange) ??

### CLI ?? ??

? ?? ?? ?????, ?? ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
 ? ???? ???? CLI? ??? ?? ?? ??, ?? ???? commit?(?) ?????.

```

set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy mode main
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text "$ABC123"
set security ike gateway gw-westford external-interface ge-0/0/3.0
set security ike gateway gw-westford ike-policy ike-phase1-policy
set security ike gateway gw-westford address 10.3.3.2
set security ike gateway gw-sunnyvale external-interface ge-0/0/3.0
set security ike gateway gw-sunnyvale ike-policy ike-phase1-policy
set security ike gateway gw-sunnyvale address 10.2.2.2

```

??? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?? IKE(Internet Key Exchange) ?? ??:



1. IKE(Internet Key Exchange) 1?? ???? ????.

```
[edit security ike]
user@hub# set proposal ike-phase1-proposal
```

2. IKE(Internet Key Exchange) ?? ?? ??? ????.

```
[edit security ike proposal ike-phase1-proposal]
user@hub# set authentication-method pre-shared-keys
```

3. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ????.

```
[edit security ike proposal ike-phase1-proposal]
user@hub# set dh-group group2
```

4. IKE(Internet Key Exchange) ?? ?? ????? ????.

```
[edit security ike proposal ike-phase1-proposal]
user@hub# set authentication-algorithm sha1
```

5. IKE(Internet Key Exchange) ?? ??? ????? ????.

```
[edit security ike proposal ike-phase1-proposal]
user@hub# set encryption-algorithm aes-128-cbc
```

6. IKE(Internet Key Exchange) 1?? ??? ????.

```
[edit security ike]
user@hub# set policy ike-phase1-policy
```

7. IKE(Internet Key Exchange) 1?? ?? ??? ????.

```
[edit security ike policy ike-phase1-policy]
user@hub# set mode main
```

8. IKE(Internet Key Exchange) 100 100 100 10000.

```
[edit security ike policy ike-phase1-policy]
user@hub# set proposals ike-phase1-proposal
```

9. IKE(Internet Key Exchange) 100 100 100 1000 100000.

```
[edit security ike policy ike-phase1-policy]
user@hub# set pre-shared-key ascii-text "$ABC123"
```

10. IKE(Internet Key Exchange) 100 1000000 10000 100 1000000 100000.

```
[edit security ike]
user@hub# set gateway gw-westford external-interface ge-0/0/3.0
```

11. IKE(Internet Key Exchange) 100 100 1000 100000.

```
[edit security ike]
user@hub# set gateway gw-westford ike-policy ike-phase1-policy
```

12. IKE(Internet Key Exchange) 100 100000 1000 100000.

```
[edit security ike]
user@hub# set gateway gw-westford address 10.3.3.2
```

13. IKE(Internet Key Exchange) 100 1000000 10000 100 1000000 100000.

```
[edit security ike]
user@hub# set gateway gw-sunnyvale external-interface ge-0/0/3.0
```

14. IKE(Internet Key Exchange) 100 100 1000 100000.

```
[edit security ike gateway]
user@hub# set gateway gw-sunnyvale ike-policy ike-phase1-policy
```

## 15. IKE(Internet Key Exchange) 1?? ???? ? ????.

```
[edit security ike gateway]
user@hub# set gateway gw-sunnyvale address 10.2.2.2
```

??

?? ???? show security ike ??? ???? ? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ?????.

```
[edit]
user@hub# show security ike
proposal ike-phase1-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-phase1-policy {
    mode main;
    proposals ike-phase1-proposal;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway gw-sunnyvale {
    ike-policy ike-phase1-policy;
    address 10.2.2.2;
    external-interface ge-0/0/3.0;
}
gateway gw-westford {
    ike-policy ike-phase1-policy;
    address 10.3.3.2;
    external-interface ge-0/0/3.0;
}
```

???? ?? ???? ? ???? commit?(?) ?????.

## ?? IPsec ??

### CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
set security ipsec vpn vpn-westford ike gateway gw-westford
set security ipsec vpn vpn-westford ike ipsec-policy ipsec-phase2-policy
set security ipsec vpn vpn-westford bind-interface st0.0
set security ipsec vpn vpn-sunnyvale ike gateway gw-sunnyvale
set security ipsec vpn vpn-sunnyvale ike ipsec-policy ipsec-phase2-policy
set security ipsec vpn vpn-sunnyvale bind-interface st0.0
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.11 ipsec-vpn vpn-sunnyvale
set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.12 ipsec-vpn vpn-westford
```

### ??? ??

?? ?? ?? ????? ??? ??? ??? ??????. ?? ????? ??? ?? ??? CLI ??? ????? ?? ????? CLI ??? ?? ??????.

??? IPsec ?? ??:

1. IPsec 2?? ??? ?????.

```
[edit]
user@hub# set security ipsec proposal ipsec-phase2-proposal
```

2. IPsec 2?? ?? ?????? ??????.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@hub# set protocol esp
```

3. IPsec 2?? ?? ?? ?????? ??????.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@hub# set authentication-algorithm hmac-sha1-96
```

4. IPsec 2?? ?? ??? ?????? ??????.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@hub# set encryption-algorithm aes-128-cbc
```

5. IPsec 2?? ??? ??????.

```
[edit security ipsec]
user@hub# set policy ipsec-phase2-policy
```

6. IPsec 2?? ?? ??? ??????.

```
[edit security ipsec policy ipsec-phase2-policy]
user@hub# set proposals ipsec-phase2-proposal
```

7. Diffie-Hellman ?? 2? ??? ? ??? IPsec 2?? PFS? ??????.

```
[edit security ipsec policy ipsec-phase2-policy]
user@host# set perfect-forward-secrecy keys group2
```

8. IKE(Internet Key Exchange) ?????? ??????.

```
[edit security ipsec]
user@hub# set vpn vpn-westford ike gateway gw-westford
user@hub# set vpn vpn-sunnyvale ike gateway gw-sunnyvale
```



```

        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
vpn vpn-sunnyvale {
    bind-interface st0.0;
    ike {
        gateway gw-sunnyvale;
        ipsec-policy ipsec-phase2-policy;
    }
}
vpn vpn-westford {
    bind-interface st0.0;
    ike {
        gateway gw-westford;
        ipsec-policy ipsec-phase2-policy;
    }
}

```

?? ?? ?? ?? commit?(?) ????.

?? ?? ?? ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ?????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set security policies from-zone trust to-zone vpn policy local-to-spokes match source-address
local-net
set security policies from-zone trust to-zone vpn policy local-to-spokes match destination-
address sunnyvale-net
set security policies from-zone trust to-zone vpn policy local-to-spokes match destination-
address westford-net
set security policies from-zone trust to-zone vpn policy local-to-spokes match application any
set security policies from-zone trust to-zone vpn policy local-to-spokes then permit
set security policies from-zone vpn to-zone trust policy spokes-to-local match source-address
sunnyvale-net
set security policies from-zone vpn to-zone trust policy spokes-to-local match source-address
westford-net
set security policies from-zone vpn to-zone trust policy spokes-to-local match destination-
address local-net

```

```

set security policies from-zone vpn to-zone trust policy spokes-to-local match application any
set security policies from-zone vpn to-zone trust policy spokes-to-local then permit
set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match source-address any
set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match destination-address
any
set security policies from-zone vpn to-zone vpn policy spoke-to-spoke match application any
set security policies from-zone vpn to-zone vpn policy spoke-to-spoke then permit

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

??? ?? ?? ?? ??:

1. ??? ???? VPN ???? ???? ???? ?? ??? ????.

```

[edit security policies from-zone trust to-zone vpn]
user@hub# set policy local-to-spokes match source-address local-net
user@hub# set policy local-to-spokes match destination-address sunnyvale-net
user@hub# set policy local-to-spokes match destination-address westford-net
user@hub# set policy local-to-spokes match application any
user@hub# set policy local-to-spokes then permit

```

2. VPN ???? ???? ???? ???? ???? ?? ??? ????.

```

[edit security policies from-zone vpn to-zone trust]
user@hub# set policy spokes-to-local match source-address sunnyvale-net
user@hub# set policy spokes-to-local match source-address westford-net
user@hub# set policy spokes-to-local match destination-address local-net
user@hub# set policy spokes-to-local match application any
user@hub# set policy spokes-to-local then permit

```

3. intrazone ???? ???? ?? ??? ????.

```

[edit security policies from-zone vpn to-zone vpn]
user@hub# set policy spoke-to-spoke match source-address any
user@hub# set policy spoke-to-spoke match destination-address any
user@hub# set policy spoke-to-spoke match application any
user@hub# set policy spoke-to-spoke then permit

```



??

?? ???? show security policies ??? ???? ???? ??????, ??? ??? ???? ????? ???, ? ?? ?? ???? ????? ??????.

```
[edit]
user@hub# show security policies
from-zone trust to-zone vpn {
  policy local-to-spokes {
    match {
      source-address local-net;
      destination-address [ sunnyvale-net westford-net ];
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone vpn to-zone trust {
  policy spokes-to-local {
    match {
      source-address [ sunnyvale-net westford-net ];
      destination-address local-net;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone vpn to-zone vpn {
  policy spoke-to-spoke {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
```

```
}
}
```

```
?? ?? ?? ?? commit?(?) ?????.
```

??? TCP-MSS ??

CLI ?? ??

```
? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ???? ????? ?????, ????? ??? ??? ? ?? ? ???? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.
```

```
set security flow tcp-mss ipsec-vpn mss 1350
```

??? ??

??? TCP-MSS ?? ?? ??:

1. TCP-MSS ??? ?????.

```
[edit]
user@hub# set security flow tcp-mss ipsec-vpn mss 1350
```

??

```
?? ????? show security flow ??? ????? ?. ?? ?? ?? ?????, ? ?? ? ???? ?????.
```

```
[edit]
user@hub# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```

```
???? ?? ?? ?? commit?(?) ?????.
```

????? ???? ?? ?????, ?? ?? ? ??? ?? ??

CLI    

```
? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? CLI? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? .
```

```
set interfaces ge-0/0/0 unit 0 family inet address 10.3.3.2/30
set interfaces ge-0/0/3 unit 0 family inet address 192.168.178.1/24
set interfaces st0 unit 0 family inet address 10.11.11.12/24
set routing-options static route 0.0.0.0/0 next-hop 10.3.3.1
set routing-options static route 10.10.10.0/24 next-hop 10.11.11.10
set routing-options static route 192.168.168.0/24 next-hop 10.11.11.10
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone trust interfaces ge-0/0/3.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone vpn interfaces st0.0
set security address-book book1 address local-net 192.168.178.0/24
set security address-book book1 attach zone trust
set security address-book book2 address corp-net 10.10.10.0/24
set security address-book book2 address sunnyvale-net 192.168.168.0/24
set security address-book book2 attach zone vpn
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ??/ ???? CLI ???/ ???/ ?????.

□□□□□ □□□□ □□ □□□□, □□ □□ □ □□□ □□ □□ □□:

- 1.**                        .

```
[edit]
user@spoke# set interfaces ge-0/0/0 unit 0 family inet address 10.3.3.2/30
user@spoke# set interfaces ge-0/0/3 unit 0 family inet address 192.168.178.1/24
user@spoke# set interfaces st0 unit 0 family inet address 10.11.11.12/24
```

2. `?? ?? ??? ?????.`

```
[edit]
user@spoke# set routing-options static route 0.0.0.0/0 next-hop 10.3.3.1
user@spoke# set routing-options static route 10.10.10.0/24 next-hop 10.11.11.10
user@spoke# set routing-options static route 192.168.168.0/24 next-hop 10.11.11.10
```

3. `?????(untrust) ?? ??? ?????.`

```
[edit]
user@spoke# set security zones security-zone untrust
```

4. `?????? ?? ??? ?????.`

```
[edit security zones security-zone untrust]
user@spoke# set interfaces ge-0/0/0.0
```

5. `?????(untrust) ?? ??? ??? ???? ???? ?????.`

```
[edit security zones security-zone untrust]
user@spoke# set host-inbound-traffic system-services ike
```

6. `???? ?? ??? ?????.`

```
[edit]
user@spoke# edit security zones security-zone trust
```

7. `?????? ????? ?? ??? ?????.`

```
[edit security zones security-zone trust]
user@spoke# set interfaces ge-0/0/3.0
```

8. `set security zones security-zone trust`.

```
[edit security zones security-zone trust]
user@spoke# set host-inbound-traffic system-services all
```

9. `vpn`.

```
[edit]
user@spoke# edit security zones security-zone vpn
```

10. `vpn`.

```
[edit security zones security-zone vpn]
user@spoke# set interfaces st0.0
```

11. `set security address-book book1`.

```
[edit security address-book book1]
user@spoke# set address local-net 192.168.178.0/24
user@spoke# set attach zone trust
```

12. `set security address-book book2`.

```
[edit security address-book book2]
user@spoke# set address corp-net 10.10.10.0/24
user@spoke# set address sunnyvale-net 192.168.168.0/24
user@spoke# set attach zone vpn
```

??

?? `show interfaces, show routing-options, show security zones` ? `show security address-book` ???  
 ??? ???? ???? ???? ???? ???? ? ? ? ? ???? ???? ????.

```
[edit]
user@spoke# show interfaces
ge-0/0/0 {
  unit 0 {
```

```

        family inet {
            address 10.3.3.2/30;
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family inet {
            address 192.168.178.1/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.11.11.10/24;
        }
    }
}
}

```

```

[edit]
user@spoke# show routing-options
static {
    route 0.0.0.0/0 next-hop 10.3.3.1;
    route 192.168.168.0/24 next-hop 10.11.11.10;
    route 10.10.10.0/24 next-hop 10.11.11.10;
}

```

```

[edit]
user@spoke# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
}

```

```

security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
  }
  interfaces {
    ge-0/0/3.0;
  }
}
security-zone vpn {
  interfaces {
    st0.0;
  }
}
[edit]
user@spoke# show security address-book
book1 {
  address corp-net 10.10.10.0/24;
  attach {
    zone trust;
  }
}
book2 {
  address local-net 192.168.178.0/24;
  address sunnyvale-net 192.168.168.0/24;
  attach {
    zone vpn;
  }
}

```

```

?? ?? ?? ?? commit?(?) ?????.

```

???? ???? IKE(Internet Key Exchange) ??

CLI ?? ??

```

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?
? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```

```

set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2

```

```

set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy mode main
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text "$ABC123"
set security ike gateway gw-corporate external-interface ge-0/0/0.0
set security ike gateway gw-corporate ike-policy ike-phase1-policy
set security ike gateway gw-corporate address 10.1.1.2

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

????? ???? IKE(Internet Key Exchange) ?? ??:

1. IKE(Internet Key Exchange) 1??? ???? ????.

```

[edit security ike]
user@spoke# set proposal ike-phase1-proposal

```

2. IKE(Internet Key Exchange) ?? ?? ???? ????.

```

[edit security ike proposal ike-phase1-proposal]
user@spoke# set authentication-method pre-shared-keys

```

3. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ????.

```

[edit security ike proposal ike-phase1-proposal]
user@spoke# set dh-group group2

```

4. IKE(Internet Key Exchange) ?? ?? ???? ????.

```

[edit security ike proposal ike-phase1-proposal]
user@spoke# set authentication-algorithm sha1

```



5. IKE(Internet Key Exchange) 100 100 10000 100000.

```
[edit security ike proposal ike-phase1-proposal]
user@spoke# set encryption-algorithm aes-128-cbc
```

6. IKE(Internet Key Exchange) 100 100 100000.

```
[edit security ike]
user@spoke# set policy ike-phase1-policy
```

7. IKE(Internet Key Exchange) 100 10 100 100000.

```
[edit security ike policy ike-phase1-policy]
user@spoke# set mode main
```

8. IKE(Internet Key Exchange) 100 10 100 100000.

```
[edit security ike policy ike-phase1-policy]
user@spoke# set proposals ike-phase1-proposal
```

9. IKE(Internet Key Exchange) 100 10 10 100 100000.

```
[edit security ike policy ike-phase1-policy]
user@spoke# set pre-shared-key ascii-text "$ABC123"
```

10. IKE(Internet Key Exchange) 100 1000000 10000 10 1000000 100000.

```
[edit security ike]
user@spoke# set gateway gw-corporate external-interface ge-0/0/0.0
```

11. IKE(Internet Key Exchange) 100 10 100 100000.

```
[edit security ike]
user@spoke# set gateway gw-corporate ike-policy ike-phase1-policy
```

## 12. IKE(Internet Key Exchange) 1?? ???? ???? ????.

```
[edit security ike]
user@spoke# set gateway gw-corporate address 10.1.1.2
```

??

?? ???? show security ike ??? ???? ???? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@spoke# show security ike
proposal ike-phase1-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-phase1-policy {
    mode main;
    proposals ike-phase1-proposal;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway gw-corporate {
    ike-policy ike-phase1-policy;
    address 10.1.1.2;
    external-interface ge-0/0/0.0;
}
```

???? ???? ???? ???? ???? commit?(?) ?????.

???? ???? IPsec ??

### CLI ?? ??

? ?? ???? ?????. ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????. ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
? ???? ???? CLI? ??? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
```

```

set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
set security ipsec vpn vpn-corporate ike gateway gw-corporate
set security ipsec vpn vpn-corporate ike ipsec-policy ipsec-phase2-policy
set security ipsec vpn vpn-corporate bind-interface st0.0

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

???? IPsec ?? ??:

1. IPsec 2?? ???? ????.

```

[edit]
user@spoke# set security ipsec proposal ipsec-phase2-proposal

```

2. IPsec 2?? ?? ???? ????.

```

[edit security ipsec proposal ipsec-phase2-proposal]
user@spoke# set protocol esp

```

3. IPsec 2?? ?? ?? ???? ????.

```

[edit security ipsec proposal ipsec-phase2-proposal]
user@spoke# set authentication-algorithm hmac-sha1-96

```

4. IPsec 2?? ?? ?? ???? ????.

```

[edit security ipsec proposal ipsec-phase2-proposal]
user@spoke# set encryption-algorithm aes-128-cbc

```

5. IPsec 2?? ??? ????.

```

[edit security ipsec]
user@spoke# set policy ipsec-phase2-policy

```

## 6. IPsec 2?? ?? ???? ?????.

```
[edit security ipsec policy ipsec-phase2-policy]
user@spoke# set proposals ipsec-phase2-proposal
```

## 7. Diffie-Hellman ?? 2? ??? ? ??? IPsec 2?? PFS? ?????.

```
[edit security ipsec policy ipsec-phase2-policy]
user@host# set perfect-forward-secrecy keys group2
```

## 8. IKE(Internet Key Exchange) ???? ????.

```
[edit security ipsec]
user@spoke# set vpn vpn-corporate ike gateway gw-corporate
```

## 9. IPsec 2?? ??? ????.

```
[edit security ipsec]
user@spoke# set vpn vpn-corporate ike ipsec-policy ipsec-phase2-policy
```

## 10. ???? ???? ????.

```
[edit security ipsec]
user@spoke# set vpn vpn-corporate bind-interface st0.0
```

??

?? ???? show security ipsec ??? ???? ???? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ??? ???? ????.

```
[edit]
user@spoke# show security ipsec
proposal ipsec-phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy ipsec-phase2-policy {
```

```

    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
vpn vpn-corporate {
    bind-interface st0.0;
    ike {
        gateway gw-corporate;
        ipsec-policy ipsec-phase2-policy;
    }
}

```

```

?? ?? ?? ?? ?? commit?(?) ?????.

```

```

???? ???? ?? ?? ??

```

## CLI ?? ??

```

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

```

set security policies from-zone trust to-zone vpn policy to-corporate match source-address local-
net
set security policies from-zone trust to-zone vpn policy to-corporate match destination-address
corp-net
set security policies from-zone trust to-zone vpn policy to-corporate match destination-address
sunnyvale-net
set security policies from-zone trust to-zone vpn policy to-corporate application any
set security policies from-zone trust to-zone vpn policy to-corporate then permit
set security policies from-zone vpn to-zone trust policy from-corporate match source-address
corp-net
set security policies from-zone vpn to-zone trust policy from-corporate match source-address
sunnyvale-net
set security policies from-zone vpn to-zone trust policy from-corporate match destination-
address local-net
set security policies from-zone vpn to-zone trust policy from-corporate application any
set security policies from-zone vpn to-zone trust policy from-corporate then permit

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

????? ???? ? ? ? ? ?:

1. ???? ???? VPN ???? ???? ???? ? ? ? ? ?.

```
[edit security policies from-zone trust to-zone vpn]
user@spoke# set policy to-corp match source-address local-net
user@spoke# set policy to-corp match destination-address corp-net
user@spoke# set policy to-corp match destination-address sunnyvale-net
user@spoke# set policy to-corp match application any
user@spoke# set policy to-corp then permit
```

2. VPN ???? ???? ???? ???? ???? ? ? ? ? ?.

```
[edit security policies from-zone vpn to-zone trust]
user@spoke# set policy spokes-to-local match source-address corp-net
user@spoke# set policy spokes-to-local match source-address sunnyvale-net
user@spoke# set policy spokes-to-local match destination-address local-net
user@spoke# set policy spokes-to-local match application any
user@spoke# set policy spokes-to-local then permit
```

??

?? ???? show security policies ??? ???? ???? ?????. ??? ???? ???? ???? ??, ? ? ? ? ? ???? ????.

```
[edit]
user@spoke# show security policies
from-zone trust to-zone vpn {
  policy to-corp {
    match {
      source-address local-net;
      destination-address [ sunnyvale-net westford-net ];
      application any;
    }
    then {
      permit;
    }
  }
}
```

```

    }
}
from-zone vpn to-zone trust {
    policy spokes-to-local {
        match {
            source-address [ sunnyvale-net westford-net ];
            destination-address local-net;
            application any;
        }
        then {
            permit;
        }
    }
}
}

```

?? ?? ?? ?? commit?(?) ????.

???? TCP-MSS ??

CLI ?? ??

? ?? ??, ?? ?? ?? ?? ?? ?? ?? ??, ??? ?? ?? ?? [edit] ?  
 ? ??? CLI? ?? ?? ??, ?? ??? commit?(?) ????.

```
set security flow tcp-mss ipsec-vpn mss 1350
```

?? ??

???? TCP-MSS ?? ??:

1. TCP-MSS ??? ????.

```

[edit]
user@spoke# set security flow tcp-mss ipsec-vpn mss 1350

```

??

?? ???? show security flow ??? ???? ???? ?????. ??? ??? ??? ???? ???? , ? ?? ?? ??? ???? ?????.

```
[edit]
user@spoke# show security flow
tcp-mss {
  ipsec-vpn {
    mss 1350;
  }
}
```

???? ???? ???? ???? commit?(?) ?????.

???? ???? ??

## CLI ?? ??

? ??? ???? ???? SSG ??? ???? ?????. ??? SSG ??? ???? ??? ?????. SSG ??? ???? ???? [https://www.juniper.net/documentation/? Concepts and Examples ScreenOS Reference Guide?\(?\) ?????](https://www.juniper.net/documentation/? Concepts and Examples ScreenOS Reference Guide?(?) ?????).

? ?? ??? ???? ?????. ?? ??? ???? ???? ???? ?? ?? ?? ???? ???? ???? , ????? ??? ???? ???? ???? ?? ??? ???? ???? ???? ???? [edit] ???? ???? CLI? ?? ?? ?? , ?? ???? commit?(?) ?????.

```
set zone name "VPN"
set interface ethernet0/6 zone "Trust"
set interface "tunnel.1" zone "VPN"
set interface ethernet0/6 ip 192.168.168.1/24
set interface ethernet0/6 route
set interface ethernet0/0 ip 10.2.2.2/30
set interface ethernet0/0 route
set interface tunnel.1 ip 10.11.11.11/24
set flow tcp-mss 1350
set address "Trust" "sunnyvale-net" 192.168.168.0 255.255.255.0
set address "VPN" "corp-net" 10.10.10.0 255.255.255.0
set address "VPN" "westford-net" 192.168.178.0 255.255.255.0
set ike gateway "corp-ike" address 10.1.1.2 Main outgoing-interface ethernet0/0 preshare
"395psksecr3t" sec-level standard
set vpn corp-vpn monitor optimized rekey
set vpn "corp-vpn" bind interface tunnel.1
set vpn "corp-vpn" gateway "corp-ike" replay tunnel idletime 0 sec-level standard
```



```
set policy id 1 from "Trust" to "Untrust" "ANY" "ANY" "ANY" nat src permit
set policy id 2 from "Trust" to "VPN" "sunnyvale-net" "corp-net" "ANY" permit
set policy id 2
exit
set dst-address "westford-net"
exit
set policy id 3 from "VPN" to "Trust" "corp-net" "sunnyvale-net" "ANY" permit
set policy id 3
set src-address "westford-net"
exit
set route 10.10.10.0/24 interface tunnel.1
set route 192.168.178.0/24 interface tunnel.1
set route 0.0.0.0/0 interface ethernet0/0 gateway 10.2.2.1
```

??

in this section

IKE(Internet Key Exchange) 1?? ?? ?? | 175

IPsec 2?? ?? ?? | 177

Next-Hop ?? ??? ?? | 179

?? ?? ?? LAN? ?? ?? ?? ?? | 180

IPsec ?? ??? ?? ?? ? ?? ?? | 181

VPN ??? ??? ??? ??? | 181

??? ??? ?????? ?????? ??? ??? ???????:

IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ??? ??????

??

?? ?????? ?????? ?? ??? ?????? 192.168.10/24 ?????? ?????? 192.168.168/24 ? 192.168.178/24 ?????? ??  
?? ?????? ?????? ?????? ?? ?? VPN? ??, SRX ??? ?????? ??? ?????? ??? ?? ?? ? ??????. IPsec ??? ?????? ? VPN? ?

[?] [?] [?] [?] [?] [?] VPN [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?]. [?] [?], 192.168.10.10[?]  
 192.168.168.10[?] ping [?] [?] [?] [?].

[?] [?] [?] [?] show security ike security-associations [?] [?] [?] [?]. [?] [?] [?] [?] [?] [?] show security ike security-associations index *index\_number* detail [?] [?] [?] [?] [?].

```
user@hub> show security ike security-associations
```

| Index | Remote Address | State | Initiator cookie | Responder cookie | Mode |
|-------|----------------|-------|------------------|------------------|------|
| 6     | 10.3.3.2       | UP    | 94906ae2263bbd8e | 1c35e4c3fc54d6d3 | Main |
| 7     | 10.2.2.2       | UP    | 7e7a1c0367dfe73c | f284221c656a5fbc | Main |

```
user@hub> show security ike security-associations index 6 detail
```

```
IKE peer 10.3.3.2, Index 6,
  Role: Responder, State: UP
  Initiator cookie: 94906ae2263bbd8e,, Responder cookie: 1c35e4c3fc54d6d3
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.1.2:500, Remote: 10.3.3.2:500
  Lifetime: Expires in 3571 seconds
  Algorithms:
    Authentication      : sha1
    Encryption          : aes-cbc (128 bits)
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes      :          1128
    Output bytes     :          988
    Input packets    :           6
    Output packets   :           5
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 1
    Negotiation type: Quick mode, Role: Responder, Message ID: 1350777248
    Local: 10.1.1.2:500, Remote: 10.3.3.2:500
    Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
    Flags: Caller notification sent, Waiting for done
```

??

```
show security ike security-associations [?] [?] [?] IKE(Internet Key Exchange) 1[?] SA? [????]. SA? [????] [?]
[?] [?], 1[?] [??] [??] [?] [????]. [???] IKE(Internet Key Exchange) ?? [?] [?] ? [?] [????] [??] [????].
```



??

?? ???? show security ipsec security-associations ??? ?????. ???? ???? ???? ? show security ipsec security-associations index *index\_number* detail ??? ?????.

```
user@hub> show security ipsec security-associations
total configured sa: 4
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<16384  10.2.2.2        500   ESP:aes-128/sha1 b2fc36f8 3364/ unlim - 0
>16384  10.2.2.2        500   ESP:aes-128/sha1 5d73929e 3364/ unlim - 0
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<16385  10.3.3.2        500   ESP:3des/sha1   70f789c6 28756/unlim - 0
>16385  10.3.3.2        500   ESP:3des/sha1   80f4126d 28756/unlim - 0
```

```
user@hub> show security ipsec security-associations index 16385 detail
Virtual-system: Root
Local Gateway: 10.1.1.2, Remote Gateway: 10.3.3.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/24)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
DF-bit: clear
Direction: inbound, SPI: 1895270854, AUX-SPI: 0
Hard lifetime: Expires in 28729 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 28136 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
Anti-replay service: enabled, Replay window size: 32

Direction: outbound, SPI: 2163479149, AUX-SPI: 0
Hard lifetime: Expires in 28729 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 28136 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
Anti-replay service: enabled, Replay window size: 32
```

??

show security ipsec security-associations ??? ???? ???? ?????.







??

SRX ??? ????? ping ??? ????? ? ???? PC?? ??? ????? ????? ? ?????, ?? ??? ????? ?? ?? ? ???? ? ???? ?????  
? ?? ??????? ??????? ????.

?? ????? ping ??? ???????.

```
user@hub> ping 192.168.168.10 interface ge-0/0/0 count 5
PING 192.168.168.10 (192.168.168.10): 56 data bytes
64 bytes from 192.168.168.10: icmp_seq=0 ttl=127 time=8.287 ms
64 bytes from 192.168.168.10: icmp_seq=1 ttl=127 time=4.119 ms
64 bytes from 192.168.168.10: icmp_seq=2 ttl=127 time=5.399 ms
64 bytes from 192.168.168.10: icmp_seq=3 ttl=127 time=4.361 ms
64 bytes from 192.168.168.10: icmp_seq=4 ttl=127 time=5.137 ms

--- 192.168.168.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.119/5.461/8.287/1.490 ms
```

?? SSG ??? ?????? ping ??? ??? ? ?????.

```
user@hub> ping 192.168.10.10 from ethernet0/6
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 1 seconds from ethernet0/6
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=4/4/5 ms
```

```
ssg-> ping 192.168.178.10 from ethernet0/6
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 192.168.178.10, timeout is 1 seconds from
ethernet0/6
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=8/8/10 ms
```

??

SRX ??? ?? SSG ??? ?????? ping ??? ??? ?, ???, ?? ??, ?? ??? ?? ESP ??? ????? ????? ?? ? ?????.







**33: ?? ?? VPN? ?? ?? VPN? ??? (Continued)**

|                                                                                                                                                                                                                                                                                                     |                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <p>?? ?? VPN</p> <p>?? ?????? ??? ?????? ?? ?????? ?????? ?? ??????? ?? ?<br/>         ? ?? ??? ????? ? ?? VPN ??? ?????? ?? ?? ??????(st0)<br/>         ? ?? ??? ?????.</p> <p>?? ?? VPN ??? ? ? ??? ??? ?? ?????? ??? ? ???, ??<br/>         ? ?? ??? ????? ?????? ?????? ?????? ??? ? ?????.</p> | <p>?? ?? VPN</p> <p>?? ?? VPN ??? ? ? ??? ?? ??? ??? ??? ? ?????.</p> |
| <p>?? ?? VPN? st0 ??????? ?? NAT? ??????</p>                                                                                                                                                                                                                                                        | <p>????? ????? NAT? ??? ?? ?? ?? VPN? ??? ? ?????.</p>                |

[illegible]

?? ??

🔗: 📄 📄 VPN 📄 | 453

?: ?? ?? VPN ?? | 328

?? ???? HA ?? ?? ???

?? O? ?? 1? ?? ?? ??? ??????. ?? O? ?? 1?? ??? ?? ?? ??? ??????, ??? ???? ? ?? ??? ?????? ?? ??? ?????  
?.

SRX

1. `?? ?????? ????? ? ????? 1?? ?? ?? ??? ??? ?? HA ?? ????? ?????? ?? ? ????????. ?? ? ??? ?? ????? 1?`  
`node0 ? node1 HA ?? ??? ????? ????? ???.`

[edit]

```
user@host# set groups node0 security ike proposal HA authentication-method pre-shared-keys
user@host# set groups node0 security ike proposal HA dh-group group20
user@host# set groups node0 security ike proposal HA authentication-algorithm sha-256
user@host# set groups node0 security ike proposal HA encryption-algorithm aes-256-cbc
```

```

user@host# set groups node0 security ike policy HA proposals HA
user@host# prompt groups node0 security ike policy HA pre-shared-key ascii-text
This Should Be A Strong And Secure Key
Retype This Should Be A Strong And Secure Key
user@host# set groups node0 security ike gateway HA ike-policy HA
user@host# set groups node0 security ike gateway HA version v2-only
user@host# set groups node0 security ipsec proposal HA protocol esp
user@host# set groups node0 security ipsec proposal HA authentication-algorithm hmac-sha1-96
user@host# set groups node0 security ipsec proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node0 security ipsec policy HA perfect-forward-secrecy keys group20
user@host# set groups node0 security ipsec policy HA proposal HA
user@host# set groups node0 security ipsec vpn HA ha-link-encryption
user@host# set groups node0 security ipsec vpn HA ike gateway HA
user@host# set groups node0 security ipsec vpn HA ike ipsec-policy HA
user@host# set groups node1 security ike proposal HA authentication-method pre-shared-keys
user@host# set groups node1 security ike proposal HA dh-group group20
user@host# set groups node1 security ike proposal HA authentication-algorithm sha-256
user@host# set groups node1 security ike proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy HA proposals HA
user@host# prompt groups node1 security ike policy HA pre-shared-key ascii-text
New ascii-text(secret): juniper
Retype This Should Be A Strong And Secure Key
user@host# set groups node1 security ike gateway HA ike-policy HA
user@host# set groups node1 security ike gateway HA version v2-only
user@host# set groups node1 security ipsec proposal HA protocol esp
user@host# set groups node1 security ipsec proposal HA authentication-algorithm hmac-sha1-96
user@host# set groups node1 security ipsec proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node1 security ipsec policy HA perfect-forward-secrecy keys group20
user@host# set groups node1 security ipsec policy HA proposals HA
user@host# set groups node1 security ipsec vpn HA ha-link-encryption
user@host# set groups node1 security ipsec vpn HA ike gateway HA
user@host# set groups node1 security ipsec vpn HA ike ipsec-policy HA
user@host# commit
user@host> request system reboot

```

2. `set groups node0 security ike policy HA proposals HA`  
`set groups node0 security ike gateway HA ike-policy HA`  
`set groups node0 security ike gateway HA version v2-only`  
`set groups node0 security ipsec proposal HA protocol esp`  
`set groups node0 security ipsec proposal HA authentication-algorithm hmac-sha1-96`  
`set groups node0 security ipsec proposal HA encryption-algorithm aes-256-cbc`  
`set groups node0 security ipsec policy HA perfect-forward-secrecy keys group20`  
`set groups node0 security ipsec policy HA proposals HA`  
`set groups node0 security ipsec vpn HA ha-link-encryption`  
`set groups node0 security ipsec vpn HA ike gateway HA`  
`set groups node0 security ipsec vpn HA ike ipsec-policy HA`  
`commit`  
`request system reboot`
3. `set groups node1 security ike proposal HA authentication-method pre-shared-keys`  
`set groups node1 security ike proposal HA dh-group group20`  
`set groups node1 security ike proposal HA authentication-algorithm sha-256`  
`set groups node1 security ike proposal HA encryption-algorithm aes-256-cbc`  
`set groups node1 security ike policy HA proposals HA`  
`set groups node1 security ipsec proposal HA protocol esp`  
`set groups node1 security ipsec proposal HA authentication-algorithm hmac-sha1-96`  
`set groups node1 security ipsec proposal HA encryption-algorithm aes-256-cbc`  
`set groups node1 security ipsec policy HA perfect-forward-secrecy keys group20`  
`set groups node1 security ipsec policy HA proposals HA`  
`set groups node1 security ipsec vpn HA ha-link-encryption`  
`set groups node1 security ipsec vpn HA ike gateway HA`  
`set groups node1 security ipsec vpn HA ike ipsec-policy HA`  
`commit`  
`request system reboot`

[edit]

```

user@host# set groups node0 security ike proposal HA authentication-method pre-shared-keys

```

```

user@host# set groups node0 security ike proposal HA dh-group group20
user@host# set groups node0 security ike proposal HA authentication-algorithm sha-256
user@host# set groups node0 security ike proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node0 security ike policy HA proposals HA
user@host# prompt groups node0 security ike policy HA pre-shared-key ascii-text
This Should Be A Strong And Secure Key
Retype This Should Be A Strong And Secure Key
user@host# set groups node0 security ike gateway HA ike-policy HA
user@host# set groups node0 security ike gateway HA version v2-only
user@host# set groups node0 security ipsec proposal HA protocol esp
user@host# set groups node0 security ipsec proposal HA authentication-algorithm hmac-sha1-96
user@host# set groups node0 security ipsec proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node0 security ipsec policy HA perfect-forward-secrecy keys group20
user@host# set groups node0 security ipsec policy HA proposal HA
user@host# set groups node0 security ipsec vpn HA ha-link-encryption
user@host# set groups node0 security ipsec vpn HA ike gateway HA
user@host# set groups node0 security ipsec vpn HA ike ipsec-policy HA
user@host# set groups node1 security ike proposal HA authentication-method pre-shared-keys
user@host# set groups node1 security ike proposal HA dh-group group20
user@host# set groups node1 security ike proposal HA authentication-algorithm sha-256
user@host# set groups node1 security ike proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node1 security ike policy HA proposals HA
user@host# prompt groups node1 security ike policy HA pre-shared-key ascii-text
New ascii-text(secret): juniper
Retype This Should Be A Strong And Secure Key
user@host# set groups node1 security ike gateway HA ike-policy HA
user@host# set groups node1 security ike gateway HA version v2-only
user@host# set groups node1 security ipsec proposal HA protocol esp
user@host# set groups node1 security ipsec proposal HA authentication-algorithm hmac-sha1-96
user@host# set groups node1 security ipsec proposal HA encryption-algorithm aes-256-cbc
user@host# set groups node1 security ipsec policy HA perfect-forward-secrecy keys group20
user@host# set groups node1 security ipsec policy HA proposals HA
user@host# set groups node1 security ipsec vpn HA ha-link-encryption
user@host# set groups node1 security ipsec vpn HA ike gateway HA
user@host# set groups node1 security ipsec vpn HA ike ipsec-policy HA
user@host# commit
user@host> request system reboot

```



?: 3???? node1?? HA ?? ????? ?????? ??? ????? ?? ?? ??? ?? ????? ???, ??? ? ????? ???  
 ? ????? ??, ??? ??? node1 ????? HA ?? ????? ????? ??? 3???? ?? ????? ???.

# IPsec VPN

## summary

IKE(Internet Key Exchange) IPsec SA  
 IKED  
 .

## in this section

- | 188
- Junos Key Manager | 189
- Quantum Safe IPsec VPN | 189
- (Quantum Key Distribution) | 189
- Junos Key Manager | 191
- : VPN | 193
- : AutoVPN | 217
- Junos Key Manager Quantum Key Manager | 255
- : IPsec VPN | 259
- : Quantum Key Manager IPsec AutoVPN | 284

## IPsec

IPsec IKE(Internet Key Exchange) IKE(Internet Key Exchange)  
 .

DH(Diffie Hellman) ECDH(Elliptic Curve Diffie Hellman)  
 .

RFC8784 . PPK(Pre-Shared Key).

- IKEv2 PPK.
- PPK IPsec SA ik IPsec SA SA .
- PPK .







## Junos Key Manager

### in this section

-   | 191
-   | 191
-   | 191
-   | 191

 Junos             IPsec            

### 

1.   —  SRX1500          vSRX   (vSRX3.0).
2.  —Junos OS  22.4R1  ( JUNOS Key Manager   JUNOS ike).

### 

       ID     IPsec VPN          IKE(Internet Key Exchange) SA     ID .

### 

Junos     .

```
user@host# set security key-manager profiles km_profile_1 static key-id ascii-text test-ppk-id
user@host# set security key-manager profiles km_profile_1 static key ascii-text
qjwbdip139u5mcy89m28pcgowerefnkjsdg
```

### 

###

?? ? ??? ? ?? ?????.

??

?? ????? ?(?) request security key-manager profiles get profile-keys name km\_profile\_1 ) ????? ?? ? ????? ?? ?????  
?.

```
user@host> request security key-manager profiles get profile-keys name km_profile_1
```

```
- Response:
  - Status: SUCCESS
  - Name: km_profile_1
  - Type: Static
  - Key-size: 280 bits
  - Key-count: 1
  - Key-ids:
    - test-ppk-id
  - Keys:
    - 716a776264697031333975356d637938396d32387063676f77657265666e6b6a736467
```

?? ????? ?(?) show security key-manager profiles name km\_profile\_1 detail ) ????? ?? ? ??? ?? ??? ?????.

```
user@host> show security key-manager profiles name km_profile_1 detail
```

```
Name: km_profile_1, Index: 1, Type: Static
Configured-at: 10.09.23 (20:16:34)
Time-elapsed: 0 hrs 2 mins 21 secs
Request stats:
  Received: 1
  In-progress: 0
  Success: 1
  Failed: 0
```

??

?? request security key-manager profiles get profile-keys name km\_profile\_1 , ?? ? ??? ??, ??, ? ??, ? ID ? ?? ??  
???

?? show security key-manager profiles name km\_profile\_1 detail ?? ? ??? ??, ?? ? ?? ??? ?????.

?: **VPN**

summary

IPsec Site-to-Site VPN

in this section

- 193
- 194
- 194
- 197
- 198
- SRX 198
- 201
- 206
- 208

IPsec Site-to-Site VPN

SRX1 SRX2 IPsec VPN QKD QKD



?:  
34:

|  |  |
|--|--|
|  |  |
|  |  |

35:

|  |                          |
|--|--------------------------|
|  | ® SRX1500 vSRX (vSRX3.0) |
|--|--------------------------|

|             |                         |
|-------------|-------------------------|
| ????? ?? ?? | Junos OS ??? 22.4R1 ??. |
|-------------|-------------------------|

???? ??

? 36: ??, ??? ? ?? ??

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??        | <ul style="list-style-type: none"><li>?? ??<br/>?? ?? ????? QKD ????? ?? ?? ?? ????? ??? ? ?????, ?? ?? ?? ??? ????? ?????? ??? ? ?<br/>???</li><li>?? ??<br/>?? ?? ?? ?? ????? ?? VPN ??? ?? ??? ? ????? ? ?????, ?? IPsec VPN ????? ??? ?<br/>??.</li><li>??? ??? ??<br/>RFC 8784 ?? ??? ????? ??? ????? ?? ????? ?? ?? ??? ? ?? ??? ?????, ?? ?? ??? ?<br/>?? ?? ????? ?? ????? ?????.</li><li>?? ??? ??<br/><a href="#">ETSI QKD Rest API</a> ? ????? ?? QKD ?????? ??? ? ?????.</li></ul> |
| ??? ??    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ??? ????? | <ul style="list-style-type: none"><li><a href="#">IPsec VPN</a></li><li><a href="#">?? ?? IPsec VPN</a></li></ul>                                                                                                                                                                                                                                                                                                                                                                              |
| ?? ??     | <a href="#">vLAB ????</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ??? ??    | <a href="#">RFC 8784 - ??? ?? ??? ?? Internet Key Exchange ????? ?? 2(IKEv2)</a> ?? ?? ?? ? ??                                                                                                                                                                                                                                                                                                                                                                                                 |

?? ??

? 37: ?? ? ??? ?? ??





|          |                                       |
|----------|---------------------------------------|
| ??       | ??? ??? ???? ?????                    |
| untrust  | ?? ?? ??? ???? ?????                  |
| VPN      | SRX1 ? SRX2 ???? ? ? ???? ???? ?????. |
| ?? ?? ?? | ??? IKE ? IPsec SA? ?? ???? ?????.    |

???? ??

???? SRX1? CLI ?? ?? ?? ???? SRX2? ?? ?? IPsec ??? ??? ?????. SRX2? ?? ?? SRX1? ID? ???? ? ??? ?  
??? ??? ?? IPsec VPN? ?????. ??? ???? Host1? Host2 ??? ??? ???? ???? IPsec ??? ??? ????.

图 38: ???? ???? ??, ?? ? ??

| ??? ?? | ??/?                           | ??                                                                                                                |
|--------|--------------------------------|-------------------------------------------------------------------------------------------------------------------|
| SRX1   | IPsec ??? ??? ? ?? SRX ??? ??? | IKE ?? IPsec SA ??? ???? SRX1? ??<br>? ?? ?? ???? SRX2? ?? ?? IPsec ??<br>? ????.                                 |
| SRX2   | IPsec ??? ??? ? ?? SRX ??? ??? | SRX1? ?? ??? IKE(Internet Key<br>Exchange) ?? IPsec SA ??? ????<br>SRX2? ??? ?? ?? ???? ??? ?? IPsec<br>??? ????. |
| ???1   | SRX1? ??? ? ?? ?? ?? LAN ? ??? | Host2? ?? ???? ? ???? ????.                                                                                       |
| ???2   | SRX2? ??? ? ?? ?? ?? LAN ? ??? | Host1? ???? ? ???? ??                                                                                             |





## 2. key-id `test-key-id` static `test-key-id`.

```
[edit security key-manager profiles]
user@srx# set km_profile_1 static key-id ascii-text test-key-id
user@srx# set km_profile_1 static key ascii-text qjwbdip139u5mcy89m28pcgowerefnkjsdg
```

## 3. `test-key-id`.

```
[edit security zones]
user@srx# set security-zone untrust host-inbound-traffic system-services ike
user@srx# set security-zone untrust interfaces ge-0/0/0.0
user@srx# set security-zone vpn interfaces st0.1
user@srx# set security-zone trust host-inbound-traffic system-services ping
user@srx# set security-zone trust interfaces ge-0/0/1.0
```

```
[edit security policies]
user@srx# set from-zone trust to-zone vpn policy vpn_out match source-address any
user@srx# set from-zone trust to-zone vpn policy vpn_out match destination-address any
user@srx# set from-zone trust to-zone vpn policy vpn_out match application any
user@srx# set from-zone trust to-zone vpn policy vpn_out then permit
user@srx# set from-zone vpn to-zone trust policy vpn_in match source-address any
user@srx# set from-zone vpn to-zone trust policy vpn_in match destination-address any
user@srx# set from-zone vpn to-zone trust policy vpn_in match application any
user@srx# set from-zone vpn to-zone trust policy vpn_in then permit
```

```
[edit security ike proposal]
user@srx# set IKE_PROP authentication-method pre-shared-keys
user@srx# set IKE_PROP dh-group group14
user@srx# set IKE_PROP authentication-algorithm sha-256
```

```
user@srx# set IKE_PROP encryption-algorithm aes-256-cbc
user@srx# set IKE_PROP lifetime-seconds 3600
```

```
[edit security ike policy]
user@srx# set IKE_POL proposals IKE_PROP
user@srx# set IKE_POL pre-shared-key ascii-text ipsec-test
```

```
[edit security ike gateway]
user@srx# set IKE_GW ike-policy IKE_POL
user@srx# set IKE_GW address 172.18.10.2
user@srx# set IKE_GW external-interface ge-0/0/0.0
user@srx# set IKE_GW local-address 172.18.10.1
user@srx# set IKE_GW version v2-only
user@srx# set IKE_GW ppk-profile km_profile_1
```

```
[edit security ipsec proposal]
user@srx# set IPSEC_PROP protocol esp
user@srx# set IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srx# set IPSEC_PROP encryption-algorithm aes-256-cbc
user@srx# set IPSEC_PROP lifetime-seconds 2400
```

```
[edit security ipsec policy]
user@srx# set IPSEC_POL proposals IPSEC_PROP
```

```
[edit security ipsec vpn]
user@srx# set IPSEC_VPN bind-interface st0.1
user@srx# set IPSEC_VPN ike gateway IKE_GW
user@srx# set IPSEC_VPN ike ipsec-policy IPSEC_POL
user@srx# set IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
user@srx# set IPSEC_VPN traffic-selector ts1 remote-ip 192.168.80.0/24
user@srx# set IPSEC_VPN establish-tunnels immediately
```

??

in this section

IKE(Internet Key Exchange) SA ?? | 201

IPsec SA ?? | 203

IPsec ?? ?? | 204

? ??? ????? ?? | 205

HOST 1?? HOST 2? ping | 205

? ?????? ? ??? ???? ????? ? ??? ? ?? show ?? ??? ?????.

? 39: ??? ?? ??

| ???                                       | ?? ??                                                    |
|-------------------------------------------|----------------------------------------------------------|
| ?? ike ?? ?? ?? ?? ??                     | "IKE(Internet Key Exchange) SA? ??????? ??????." ??? 201 |
| ?? ipsec ?? ?? ?? ?? ??                   | "IPsec SA? ??????? ??????." ??? 203                      |
| ?? ipsec ?? ??                            | "IPsec ??? ? ??? ??? ??????." ??? 204                    |
| ?? ? ??? ????? ?? ?? ??                   | "? ??? ??? ??????." ??? 205                              |
| ping 192.168.80.20 ?? 192.168.90.20 ??? 4 | "HOST1?? HOST2? ?? ? ??? ping???" ??? 205                |

IKE(Internet Key Exchange) SA ??

??

IKE(Internet Key Exchange) SA ??

??

?? ???? ?? ???? show security ike security-associations detail IKE(Internet Key Exchange) SA? ?????.

```

user@srx> show security ike security-associations detail IKE peer 172.18.10.2, Index 1, Gateway
Name: IKE_GW
Role: Initiator, State: UP
Initiator cookie: dee592254e808a2b, Responder cookie: 51f6b1d4a8618332 Exchange type: IKEv2,
Authentication method: Pre-shared-keys
Local gateway interface: ge-0/0/2.0 Routing instance: default
Local: 172.18.10.1:500, Remote: 172.18.10.2:500
Lifetime: Expires in 1286 seconds Reauth Lifetime: Disabled
IKE Fragmentation: Enabled, Size: 576 SRG ID: 0
Remote Access Client Info: Unknown Client Peer ike-id: 172.18.10.2
AAA assigned IP: 0.0.0.0
PPK-profile: km_profile_1 Optional: No
State      : Used
Algorithms:
Authentication      : hmac-sha256-128
Encryption          : aes256-cbc Pseudo random function: hmac-sha256 Diffie-Hellman group : DH-group-14
Traffic statistics:
Input bytes :      1058
Output bytes :      1074
Input packets:      4
Output packets:      4
Input fragmented packets:      0
Output fragmented packets:      0
IPsec security associations: 4 created, 1 deleted Phase 2 negotiations in progress: 1
IPsec Tunnel IDs: 500002
Negotiation type: Quick mode, Role: Initiator, Message ID: 0 Local: 172.18.10.1:500, Remote:
172.18.10.2:500
Local identity: 172.18.10.1
Remote identity: 172.18.10.2 Flags: IKE SA is created
IPsec SA Rekey CREATE_CHILD_SA exchange stats:
Initiator stats:      Responder stats:
Request Out      : 0      Request In      : 1
Response In      : 0      Response Out     : 1
No Proposal Chosen In      : 0      No Proposal Chosen Out : 0

Invalid KE In      : 0      Invalid KE Out      : 0

```

```

TS Unacceptable In      : 0    TS Unacceptable Out      : 0
Res DH Compute Key Fail : 0    Res DH Compute Key Fail: 0 Res Verify SA Fail    : 0
Res Verify DH Group Fail: 0 Res Verify TS Fail      : 0

```

??

,, PPK-profile: km\_profile\_1 Optional: NoIPSec security associations: 4 createdFlags: IKE SA is created ? ????  
 Role: Initiator, State: UPIKE SA? ???? ???? ????.

**IPsec SA ??**

??

**IPsec SA ??**

??

?? ???? ???? show security ipsec security-associations detail **IPsec SA? ????.**

```

user@srx> show security ipsec security-associations detail

```

```

ID: 500002 Virtual-system: root, VPN Name: IPSEC_VPN Local Gateway: 172.18.10.1, Remote Gateway:
172.18.10.2 Traffic Selector Name: ts1
Local Identity: ipv4(192.168.90.0-192.168.90.255)
Remote Identity: ipv4(192.168.80.0-192.168.80.255) TS Type: traffic-selector
Version: IKEv2 Quantum Secured: Yes PFS group: N/A
SRG ID: 0
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: IPSEC_POL Port:
500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0 Tunnel events:
Thu Mar 30 2023 23:43:42: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0, KMD-Instance 0
Anchorship: Thread 1
Distribution-Profile: default-profile Direction: inbound, SPI: 0x983a0221, AUX-SPI: 0
, VPN Monitoring: - Hard lifetime: Expires in 1330 seconds Lifesize Remaining: Unlimited
Soft lifetime: Expires in 662 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits) Anti-replay
service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled

```

```

tunnel-establishment: establish-tunnels-immediately IKE SA Index: 1
Direction: outbound, SPI: 0x4112746b, AUX-SPI: 0
, VPN Monitoring: - Hard lifetime: Expires in 1330 seconds Lifesize Remaining: Unlimited
Soft lifetime: Expires in 662 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits) Anti-replay
service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-immediately IKE SA Index: 1

```

??

? tunnel-establishment: establish-tunnels-immediately IKE SA Index: 1 ??? Version: IKEv2 Quantum Secured: Yes  
IPsec SA? ?????? ??????? ??????.

?? ??? IPsec SA? ??????.

**IPsec** ?? ??

??

IPsec ??? ??????.

??

?? ????? ??? ????? show security ipsec statistics IPsec ??? ??????.

```

user@srx> show security ipsec statistics
ESP Statistics:
Encrypted bytes:    624
Decrypted bytes:    624
Encrypted packets:   4
Decrypted packets:   4
AH Statistics:
Input bytes:        0
Output bytes:       0
Input packets:      0
Output packets:     0

```

Errors:

AH authentication failures: 0, Replay errors: 0

ESP authentication failures: 0, ESP decryption failures: 0 Bad headers: 0, Bad trailers: 0

Invalid SPI: 0, TS check fail: 0 Exceeds tunnel MTU: 0

Discarded: 0

??

? AH Statistics ???? ESP Statistics IPsec ??? ?????.

? ??? ????? ??

??

? ??? ????? ?????.

??

?? ????? ?? ??? ????? show security key-manager profiles ? ??? ????? ?????.

```
user@srx> show security key-manager profiles detail
```

Name: km\_profile\_1, Index: 1, Type: Static

Configured-at: 30.03.23 (23:22:43)

Time-elapsed: 1 hrs 16 mins 3 secs Request stats:

Received: 1

In-progress: 0

Success: 1

Failed: 0

??

? Type: Static ????? ? ??? ????? Name: km\_profile\_1 ?????.

**HOST 1?? HOST 2? ping**

??

HOST 1?? HOST 2?? ??? ?????.

??

?? ping 192.168.80.20 source 192.168.90.20 count 4? HOST 1?? HOST 2?? ???

```
user@HOST1# ping 192.168.80.20 source 192.168.90.20 count 4
PING 192.168.80.20 (192.168.80.20): 56 data bytes
64 bytes from 192.168.80.1: icmp_seq=0 ttl=64 time=2.151 ms
64 bytes from 192.168.80.1: icmp_seq=1 ttl=64 time=1.710 ms
64 bytes from 192.168.80.1: icmp_seq=2 ttl=64 time=1.349 ms
64 bytes from 192.168.80.1: icmp_seq=3 ttl=64 time=1.597 ms
--- 192.168.80.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max/stddev =
1.349/1.702/2.151/0.290 ms
Data traffic is successfully flowing between the HOSTs
```

??

HOST PING 192.168.80.20 (192.168.80.20): 56 data bytes 1?? HOST 2?? ???

?? 1 : ?? ??? ?? ??

?? ??? ?? ??

**SRX1**?? ??

```
set security key-manager profiles km_profile_1 static key-id ascii-text test-key-id
set security key-manager profiles km_profile_1 static key ascii-text
qjwbdip139u5mcy89m28pcgowerefnkjsdg
set interfaces ge-0/0/0 unit 0 family inet address 172.18.10.1/24
set interfaces st0 unit 1 family inet
set interfaces ge-0/0/1 unit 0 family inet address 192.168.90.1/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
```



```

set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group14
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 3600
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text ipsec-test
set security ike gateway IKE_GW ike-policy IKE_POL
set security ike gateway IKE_GW address 172.18.10.2
set security ike gateway IKE_GW external-interface ge-0/0/0.0
set security ike gateway IKE_GW local-address 172.18.10.1
set security ike gateway IKE_GW version v2-only
set security ike gateway IKE_GW ppk-profile km_profile_1
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal IPSEC_PROP lifetime-seconds 2400
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN bind-interface st0.1
set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
set security ipsec vpn IPSEC_VPN traffic-selector ts1 remote-ip 192.168.80.0/24
set security ipsec vpn IPSEC_VPN establish-tunnels immediately

```

## SRX2 ?? ??

```

set security key-manager profiles km_profile_1 static key-id ascii-text test-key-id
set security key-manager profiles km_profile_1 static key ascii-text
qjwbdip139u5mcy89m28pcgowerefnkjsdg
set interfaces ge-0/0/0 unit 0 family inet address 172.18.10.2/24
set interfaces st0 unit 1 family inet
set interfaces ge-0/0/1 unit 0 family inet address 192.168.80.1/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0

```

```

set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group14
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 3600
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text "ipsec-test"
set security ike gateway IKE_GW ike-policy IKE_POL
set security ike gateway IKE_GW address 172.18.10.1
set security ike gateway IKE_GW external-interface ge-0/0/0.0
set security ike gateway IKE_GW local-address 172.18.10.2
set security ike gateway IKE_GW version v2-only
set security ike gateway IKE_GW ppk-profile km_profile_1
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal IPSEC_PROP lifetime-seconds 2400
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN bind-interface st0.1
set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
set security ipsec vpn IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set security ipsec vpn IPSEC_VPN establish-tunnels immediately

```

## 2 : DUT

### in this section

- SRX1 | 209
- SRX2 | 213

**SRX1**

```

?? ???? , show security key-manager, , show security zonesshow interfaces, show security ike gateway IKE_GWshow
security ipsec vpn IPSEC_VPNshow security policiesshow security ipsec policy IPSEC_POLshow security ike proposal
IKE_PROPShow security ipsec proposal IPSEC_PROPShow security ike policy IKE_POL? ???? ???? show security key-
manager profiles???? ?????. ??? ???? ???? ???? ???? , ? ?? ???? ???? ???? ?????.

```

```

user@srx1# show security key-manager profiles
km_profile_1 {
  static {
    key-id ascii-text "$9$.mz6pu1hyKBI8X-boajHqmF/hcylK836"; ## SECRET-DATA
    key ascii-text "$9$5Q6AhclXNbtuIcyeXxGDikfT369A0Bn/
vWLNy2aZUjPQAp0BEcFnyleMXxGDi.mT9CuhSeIElMLXwsaZUikPpu1hSen/ew8XbwJGD"; ## SECRET-DATA
  }
}

```

```

user@srx1# show security key-manager
profiles {
  km_profile_1 {
    static {
      key-id ascii-text "$9$.mz6pu1hyKBI8X-boajHqmF/hcylK836"; ## SECRET-DATA
      key ascii-text "$9$5Q6AhclXNbtuIcyeXxGDikfT369A0Bn/
vWLNy2aZUjPQAp0BEcFnyleMXxGDi.mT9CuhSeIElMLXwsaZUikPpu1hSen/ew8XbwJGD"; ## SECRET-DATA
    }
  }
}

```

```

user@srx1# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 172.18.10.2/24;
      address 172.18.10.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {

```

```

        address 192.168.80.1/24;
        address 192.168.90.1/24;
    }
    family mpls;
}
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
}

```

```

user@srx1# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    interfaces {
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

```

    }
}

```

```

user@srx1# show security policies
from-zone trust to-zone vpn {
  policy vpn_out {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone vpn to-zone trust {
  policy vpn_in {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}

```

```

user@srx1# show security ike proposal IKE_PROP
authentication-method pre-shared-keys;
dh-group group14;
authentication-algorithm sha-256;

```

```

encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@srx1# show security ike policy IKE_POL
proposals IKE_PROP;
pre-shared-key ascii-text "$9$z0C63/tp0Icrvz39p0Ihcs24aZjqmTn9p"; ## SECRET-DATA

```

```

user@srx1# show security ike gateway IKE_GW
ike-policy IKE_POL;
address [ 172.18.10.1 172.18.10.2 ];
external-interface ge-0/0/0.0;
local-address 172.18.10.1;
version v2-only;
ppk-profile km_profile_1;

```

```

user@srx1# show security ipsec proposal IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;
lifetime-seconds 2400;

```

```

user@srx1# show security ipsec policy IPSEC_POL
proposals IPSEC_PROP;

```

```

user@srx1# show security ipsec vpn IPSEC_VPN
bind-interface st0.1;
ike {
    gateway IKE_GW;
    ipsec-policy IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.90.0/24;
    remote-ip 192.168.80.0/24;
}

```

```
}
establish-tunnels immediately;
```

## SRX2

?? ???? , show security key-manager, , show security zonesshow interfaces, show security ike gateway IKE\_GWshow security ipsec vpn IPSEC\_VPNshow security policiesshow security ipsec policy IPSEC\_POLshow security ike proposal IKE\_PROPShow security ipsec proposal IPSEC\_PROPShow security ike policy IKE\_POL? ??? ???? show security key-manager profiles???? ?????. ??? ??? ???? ???? ???? , ? ? ? ? ???? ???? ????.

```
user@srx2# show security key-manager profiles
km_profile_1 {
    static {
        key-id ascii-text "$9$Hk5FCA0IhruOvWx-2gGDikT3IRhSrvQF"; ## SECRET-DATA
        key ascii-text "$9$zDD33CuyrvNVY0BhreMN-jHqmQF/Ctu1R9A8X7V4oGDikT3u01RSr69evMLN-
jHqf5FtpBylMhSvL7N2gGDiqmTOBEylM9AMXxNY2UjH"; ## SECRET-DATA
    }
}
```

```
user@srx2# show security key-manager
profiles {
    km_profile_1 {
        static {
            key-id ascii-text "$9$Hk5FCA0IhruOvWx-2gGDikT3IRhSrvQF"; ## SECRET-DATA
            key ascii-text "$9$zDD33CuyrvNVY0BhreMN-jHqmQF/Ctu1R9A8X7V4oGDikT3u01RSr69evMLN-
jHqf5FtpBylMhSvL7N2gGDiqmTOBEylM9AMXxNY2UjH"; ## SECRET-DATA
        }
    }
}
```

```
user@srx2# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}
```

```

ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
        }
        family mpls;
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
}

```

```

user@srx2# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    interfaces {
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
}

```



```

    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

```

user@srx2# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}

```

```

user@srx2# show security ike proposal IKE_PROP
authentication-method pre-shared-keys;
dh-group group14;
authentication-algorithm sha-256;

```

```

encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@srx2# show security ike policy IKE_POL
proposals IKE_PROP;
pre-shared-key ascii-text "$9$zTi03/tp0Icrvz39p0Ihcs24aZjqmTn9p"; ## SECRET-DATA

```

```

user@srx2# show security ike gateway IKE_GW
ike-policy IKE_POL;
address 172.18.10.1;
external-interface ge-0/0/0.0;
local-address 172.18.10.2;
version v2-only;
ppk-profile km_profile_1;

```

```

user@srx2# show security ipsec proposal IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;
lifetime-seconds 2400;

```

```

user@srx2# show security ipsec policy IPSEC_POL
proposals IPSEC_PROP;

```

[edit]

```

user@srx2# show security ipsec vpn IPSEC_VPN
bind-interface st0.1;
ike {
    gateway IKE_GW;
    ipsec-policy IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.80.0/24;
    remote-ip 192.168.90.0/24;
}
establish-tunnels immediately;

```

?: AutoVPN? ?? ?? ? ???? ??

summary

? ?? ???? ?? ? ???? ???? IPsec AutoVPN ???? ????  
??.

in this section

- ?? ?? ?? ?? | 217
- ???? ?? | 218
- ?? ?? | 219
- ???? ?? | 222
- ???? ?? | 224
- ???? ???? ?? | 224
- ??? ?????? ???? ?? | 227
- ?? | 230
- ?? 1 : ?? ???? ?? ?? ?? | 239
- ?? 2 : DUT? ?? ?? ?? | 243

?? ? ???? ???? IPsec AutoVPN ???? ???? ? ????.

? ?? ???? ??, ??? 1, ??? 2? ?? ? ???? ???? IPsec VPN?? QKD ?? ?????. QKD ?? ???? ???? ?? ???? ????  
? ???? ? ????.



?:

? 40: ?? ???

|       |         |
|-------|---------|
| ?? ?? | ? ?? ?? |
| ?? ?? | ? ?? ?? |

?? ?? ?? ??

? 41: ?? ??





|              |                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>?? ??</p> | <p>IPsec SA? ?? ??? ??? ??? ??? ? ????.</p> <ul style="list-style-type: none"><li>• VPN-OUT—TRUST ??? VPN ????? ????. ?? ? ? ? ? ? ? ? ? ? ?.</li><li>• ?? ??: HOST-1-?</li><li>• ?? ??: HOST-2-?</li><li>• ??: ??</li><li>• VPN-IN—VPN ??? ? ? ???? ???? ?????. ?? ? ? ? ? ? ? ? ? ? ?.</li><li>• ?? ??: HOST-2-?</li><li>• ?? ??: HOST-1-?</li><li>• ??: ??</li></ul> |
| <p>???</p>   |                                                                                                                                                                                                                                                                                                                                                                         |





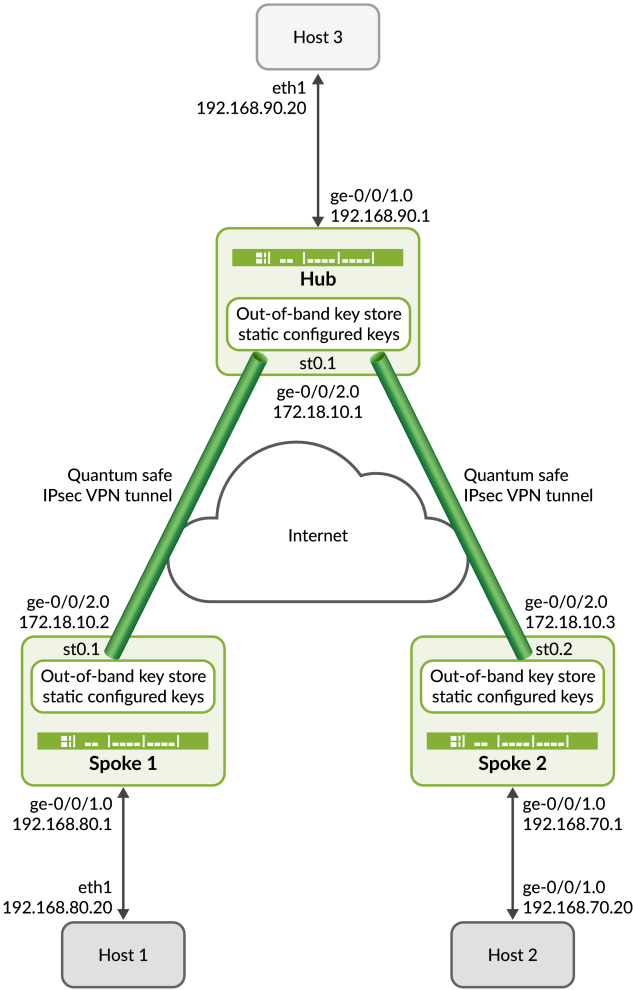


Table 44: Network Configuration, (Continued)

| Device   | IP Address                      | Subnet         |
|----------|---------------------------------|----------------|
| Device 1 | 192.168.1.1 LAN 192.168.1.1     | 192.168.1.0/24 |
| Device 2 | 192.168.2.1 LAN 192.168.2.1     | 192.168.2.0/24 |
| Device 3 | HUB 192.168.3.1 LAN 192.168.3.1 | 192.168.3.0/24 |

?? ??

?? 19: ?? VPN? ???? ? ?



jn-000642

???? ? ?

?: DUT? ?? ?? ? ???? ???? ?????.

- "???? ? ?" ??? 239

? ??? ? ???? ?????. ????? ? ???? ???? ????.

1. `set ge-0/0/2 unit 0 family inet address 172.18.10.1/24`

```
[edit interfaces]
user@hub# set ge-0/0/2 unit 0 family inet address 172.18.10.1/24
user@hub# set ge-0/0/1 unit 0 family inet address 192.168.90.1/24
user@hub# set st0 unit 1 family inet
```

2. CA(certification authority) `set ca-profile Root-CA ca-identity Root-CA`

```
[edit security pki]
user@hub# set ca-profile Root-CA ca-identity Root-CA
user@hub# set ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/mscep.dll
user@hub# set ca-profile Root-CA revocation-check disable
```

3. `request security pki ca-certificate enroll ca-profile Root-CA`

```
user@hub> request security pki ca-certificate enroll ca-profile Root-CA
user@hub> request security pki generate-key-pair certificate-id HUB_CERT size 2048 type rsa
user@hub> request security pki local-certificate enroll certificate-id HUB_CERT challenge-
password <different> domain-name hub.juniper.net email hub@juniper.net subject
DC=juniper,CN=hub.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-profile
Root-CA
```

4. `set HUB_KM_PROFILE_1 static key-id ascii-text test-key-id`

```
[edit security key-manager profiles]
user@hub# set HUB_KM_PROFILE_1 static key-id ascii-text test-key-id
user@hub# set HUB_KM_PROFILE_1 static key ascii-text qjwbdip139u5mcy89m28pcgowerefnkjsdg
```

5. IPsec VPN `set HUB_IKE_PROP authentication-method rsa-signatures`

```
[edit security ike proposal]
user@hub# set HUB_IKE_PROP authentication-method rsa-signatures
user@hub# set HUB_IKE_PROP dh-group group14
user@hub# set HUB_IKE_PROP authentication-algorithm sha-256
```

```
user@hub# set HUB_IKE_PROP encryption-algorithm aes-256-cbc
user@hub# set HUB_IKE_PROP lifetime-seconds 3600
```

```
[edit security ike policy]
user@hub# set HUB_IKE_POL proposals HUB_IKE_PROP
user@hub# set HUB_IKE_POL certificate local-certificate HUB_CRT
```

```
[edit security ike gateway]
user@hub# set HUB_IKE_GW local-address 172.18.10.1
user@hub# set HUB_IKE_GW ike-policy HUB_IKE_POL
user@hub# set HUB_IKE_GW external-interface ge-0/0/2.0
user@hub# set HUB_IKE_GW local-identity distinguished-name
user@hub# set HUB_IKE_GW dynamic ike-user-type group-ike-id
user@hub# set HUB_IKE_GW dynamic distinguished-name wildcard C=us,DC=juniper
user@hub# set HUB_IKE_GW ppk-profile HUB_KM_PROFILE_1
user@hub# set HUB_IKE_GW version v2-only
```

```
[edit security ipsec proposal]
user@hub# set HUB_IPSEC_PROP protocol esp
user@hub# set HUB_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@hub# set HUB_IPSEC_PROP encryption-algorithm aes-256-cbc
```

```
[edit security ipsec policy]
user@hub# set HUB_IPSEC_POL proposals HUB_IPSEC_PROP
```

```
[edit security ipsec vpn]
user@hub# set HUB_IPSEC_VPN bind-interface st0.1
user@hub# set HUB_IPSEC_VPN ike gateway HUB_IKE_GW
user@hub# set HUB_IPSEC_VPN ike ipsec-policy HUB_IPSEC_POL
user@hub# set HUB_IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
user@hub# set HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0
```

```
[edit security zones]
user@hub# set security-zone untrust host-inbound-traffic system-services ike
user@hub# set security-zone untrust interfaces ge-0/0/2.0
```



```
user@spoke# set SPOKE_1_IKE_PROP encryption-algorithm aes-256-cbc
user@spoke# set SPOKE_1_IKE_PROP lifetime-seconds 3600
```

```
[edit security ike policy]
user@spoke# set SPOKE_1_IKE_POL proposals SPOKE_1_IKE_PROP
user@spoke# set SPOKE_1_IKE_POL certificate local-certificate SPOKE_1_CRT
```

```
[edit security ike gateway]
user@spoke# set SPOKE_1_IKE_GW address 172.18.10.1
user@spoke# set SPOKE_1_IKE_GW local-address 172.18.10.2
user@spoke# set SPOKE_1_IKE_GW ike-policy SPOKE_1_IKE_POL
user@spoke# set SPOKE_1_IKE_GW external-interface ge-0/0/2.0
user@spoke# set SPOKE_1_IKE_GW local-identity distinguished-name
user@spoke# set SPOKE_1_IKE_GW remote-identity distinguished-name
user@spoke# set SPOKE_1_IKE_GW ppk-profile SPOKE_1_KM_PROFILE_1
user@spoke# set SPOKE_1_IKE_GW version v2-only
```

```
[edit security ipsec proposal]
user@spoke# set SPOKE_1_IPSEC_PROP protocol esp
user@spoke# set SPOKE_1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@spoke# set SPOKE_1_IPSEC_PROP encryption-algorithm aes-256-cbc
```

```
[edit security ipsec policy]
user@spoke# set SPOKE_1_IPSEC_POL proposals SPOKE_1_IPSEC_PROP
```

```
[edit security ipsec vpn]
user@spoke# set SPOKE_1_IPSEC_VPN bind-interface st0.1
user@spoke# set SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW
user@spoke# set SPOKE_1_IPSEC_VPN ike ipsec-policy SPOKE_1_IPSEC_POL
user@spoke# set SPOKE_1_IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
user@spoke# set SPOKE_1_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
```

```
[edit security zones]
user@spoke# set security-zone untrust host-inbound-traffic system-services ike
user@spoke# set security-zone untrust interfaces ge-0/0/2.0
```

```

user@spoke# set security-zone vpn interfaces st0.1
user@spoke# set security-zone trust host-inbound-traffic system-services ping
user@spoke# set security-zone trust interfaces ge-0/0/1.0

```

```

[edit security policies]
user@spoke# set from-zone trust to-zone vpn policy vpn_out match source-address any
user@spoke# set from-zone trust to-zone vpn policy vpn_out match destination-address any
user@spoke# set from-zone trust to-zone vpn policy vpn_out match application any
user@spoke# set from-zone trust to-zone vpn policy vpn_out then permit
user@spoke# set from-zone vpn to-zone trust policy vpn_in match source-address any
user@spoke# set from-zone vpn to-zone trust policy vpn_in match destination-address any
user@spoke# set from-zone vpn to-zone trust policy vpn_in match application any
user@spoke# set from-zone vpn to-zone trust policy vpn_in then permit

```

```

[edit security pki ]
user@spoke# set ca-profile Root-CA ca-identity Root-CA
user@spoke# set ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
user@spoke# set ca-profile Root-CA revocation-check disable

```

```

user@spoke> request security pki ca-certificate enroll ca-profile Root-CA
user@spoke> request security pki generate-key-pair certificate-id SPOKE_1_CRT size 2048 type
rsa
user@spoke> request security pki local-certificate enroll certificate-id SPOKE_1_CRT
challenge-password <different> domain-name spoke_1.juniper.net email spoke_1@juniper.net
subject
DC=juniper,CN=spoke_1.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA

```

### 3. `?? ? ??? ???? ?????.`

```

[edit security key-manager profiles]
user@spoke# set SPOKE_1_KM_PROFILE_1 static key-id ascii-text test-key-id
user@spoke# set SPOKE_1_KM_PROFILE_1 static key ascii-text qjwb dip139u5mcy89m28pcgowerefnkjsdg

```

??

in this section

IKE(Internet Key Exchange) SA ?? | 230

IPsec SA ?? | 234

IPsec ?? ?? | 236

? ??? ????? ?? | 237

??? 1?? ??? 3?? ?? ? ??? ping | 238

??? 2?? ??? 3?? ?? ? ??? ping | 238

? ?????? ? ??? ??? ????? ? ??? ? ?? show ?? ??? ?????.

| ???                                                 | ?? ??                                                  |
|-----------------------------------------------------|--------------------------------------------------------|
| ?? ike ?? ?? ?? ??<br>??                            | "IKE(Internet Key Exchange) SA? ?????? ??????" ??? 234 |
| ?? ipsec ?? ?? ??<br>?? ??                          | "IPsec SA? ?????? ??????" ??? 230                      |
| ?? ipsec ?? ??                                      | "IPsec ??? ? ??? ??? ??????" ??? 236                   |
| ?? ? ??? ??? ?? ?<br>? ??                           | "? ??? ??? ??????" ??? 237                             |
| ping<br>192.168.90.20 ??<br>192.168.80.20 ??<br>? 4 | "??? 1?? ??? 3?? ?? ? ??? ping???" ??? 238             |

IKE(Internet Key Exchange) SA ??

??

IKE(Internet Key Exchange) SA? ?????.



??

?? ???? ???? show security ike security-associations detail IKE(Internet Key Exchange) SA? ????.

```
user@hub> show security ike security-associations detail
```

```
IKE peer 172.18.10.2, Index 2123, Gateway Name: HUB_IKE_GW
```

```
Role: Responder, State: UP
```

```
Initiator cookie: 0e40ccdcee1b54bd, Responder cookie: 43964f5cc4d4491c
```

```
Exchange type: IKEv2, Authentication method: RSA-signatures
```

```
Local gateway interface: ge-0/0/2.0
```

```
Routing instance: default
```

```
Local: 172.18.10.1:500, Remote: 172.18.10.2:500
```

```
Lifetime: Expires in 2840 seconds
```

```
Reauth Lifetime: Disabled
```

```
IKE Fragmentation: Enabled, Size: 576
```

```
Remote Access Client Info: Unknown Client
```

```
Peer ike-id: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke.juniper.net
```

```
AAA assigned IP: 0.0.0.0
```

```
PPK-profile: HUB_KM_PROFILE_1
```

```
Optional: No
```

```
State : Used
```

```
Algorithms:
```

```
Authentication : hmac-sha256-128
```

```
Encryption : aes256-cbc
```

```
Pseudo random function: hmac-sha256
```

```
Diffie-Hellman group : DH-group-14
```

```
Traffic statistics:
```

```
Input bytes : 2610
```

```
Output bytes : 2571
```

```
Input packets: 5
```

```
Output packets: 5
```

```
Input fragmented packets: 4
```

```
Output fragmented packets: 4
```

```
IPSec security associations: 2 created, 0 deleted
```

```
Phase 2 negotiations in progress: 1
```

```
IPSec Tunnel IDs: 500440
```

```
Negotiation type: Quick mode, Role: Responder, Message ID: 0
```

```
Local: 172.18.10.1:500, Remote: 172.18.10.2:500
```

```
Local identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,
```

CN=hub.juniper.net

Remote identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke.juniper.net

Flags: IKE SA is created

IPsec SA Rekey CREATE\_CHILD\_SA exchange stats:

| Initiator stats:          |     | Responder stats:         |   |
|---------------------------|-----|--------------------------|---|
| Request Out               | : 0 | Request In               | : |
| 0                         |     |                          |   |
| Response In               | : 0 | Response Out             | : |
| 0                         |     |                          |   |
| No Proposal Chosen In     | : 0 | No Proposal Chosen Out   | : |
| 0                         |     |                          |   |
| Invalid KE In             | : 0 | Invalid KE Out           | : |
| 0                         |     |                          |   |
| TS Unacceptable In        | : 0 | TS Unacceptable Out      | : |
| 0                         |     |                          |   |
| Res DH Compute Key Fail   | : 0 | Res DH Compute Key Fail: |   |
| 0                         |     |                          |   |
| Res Verify SA Fail        | : 0 |                          |   |
| Res Verify DH Group Fail: | 0   |                          |   |
| Res Verify TS Fail        | : 0 |                          |   |

IKE peer 172.18.10.3, Index 2124, Gateway Name: HUB\_IKE\_GW

Role: Responder, State: UP

Initiator cookie: 651bf4a52a9375ec, Responder cookie: d9a9c95c27e3f929

Exchange type: IKEv2, Authentication method: RSA-signatures

Local gateway interface: ge-0/0/2.0

Routing instance: default

Local: 172.18.10.1:500, Remote: 172.18.10.3:500

Lifetime: Expires in 2901 seconds

Reauth Lifetime: Disabled

IKE Fragmentation: Enabled, Size: 576

Remote Access Client Info: Unknown Client

Peer ike-id: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke\_2.juniper.net

AAA assigned IP: 0.0.0.0

PPK-profile: HUB\_KM\_PROFILE\_1

Optional: No

State : Used

Algorithms:

Authentication : hmac-sha256-128

Encryption : aes256-cbc

Pseudo random function: hmac-sha256

Diffie-Hellman group : DH-group-14

Traffic statistics:

Input bytes : 2610

Output bytes : 2571

Input packets: 5

Output packets: 5

Input fragmented packets: 4

Output fragmented packets: 4

IPSec security associations: 2 created, 0 deleted

Phase 2 negotiations in progress: 1

IPSec Tunnel IDs: 500441

Negotiation type: Quick mode, Role: Responder, Message ID: 0

Local: 172.18.10.1:500, Remote: 172.18.10.3:500

Local identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=hub.juniper.net

Remote identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke\_2.juniper.net

Flags: IKE SA is created

IPsec SA Rekey CREATE\_CHILD\_SA exchange stats:

Initiator stats:

Request Out : 0  
0

Response In : 0  
0

No Proposal Chosen In : 0  
0

Invalid KE In : 0  
0

TS Unacceptable In : 0  
0

Res DH Compute Key Fail : 0  
0

Res Verify SA Fail : 0

Res Verify DH Group Fail: 0

Res Verify TS Fail : 0

Responder stats:

Request In :

Response Out :

No Proposal Chosen Out :

Invalid KE Out :

TS Unacceptable Out :

Res DH Compute Key Fail:

??

,, PPK-profile: HUB\_KM\_PROFILE\_1IPsec security associations: 2 created, 0 deletedFlags: IKE SA is created ? ???  
Role: Responder, State: UPIKE SA? ???? ???? ????.

## IPsec SA ??

??

IPsec SA? ????.

??

?? ???? ???? show security ipsec security-associations detail IPsec SA? ????.

```
user@hub> show security ipsec security-associations detail
```

```
ID: 500440 Virtual-system: root, VPN Name: HUB_IPSEC_VPN
Local Gateway: 172.18.10.1, Remote Gateway: 172.18.10.2
Traffic Selector Name: ts1
Local Identity: ipv4(192.168.90.0-192.168.90.255)
Remote Identity: ipv4(192.168.80.0-192.168.80.255)
TS Type: traffic-selector
Version: IKEv2
Quantum Secured: Yes
PFS group: N/A
Passive mode tunneling: Disabled
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: HUB_IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
Tunnel events:
  Thu Jul 20 2023 10:44:19: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0
Anchorship: Thread 1
Distribution-Profile: default-profile
Direction: inbound, SPI: 0x649d371f, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 2840 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2183 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```

Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2123
Direction: outbound, SPI: 0xd5ef611e, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 2840 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2183 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2123

ID: 500441 Virtual-system: root, VPN Name: HUB_IPSEC_VPN
Local Gateway: 172.18.10.1, Remote Gateway: 172.18.10.3
Traffic Selector Name: ts1
Local Identity: ipv4(192.168.90.0-192.168.90.255)
Remote Identity: ipv4(192.168.70.0-192.168.70.255)
TS Type: traffic-selector
Version: IKEv2
Quantum Secured: Yes
PFS group: N/A
Passive mode tunneling: Disabled
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: HUB_IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
Tunnel events:
  Thu Jul 20 2023 10:45:19: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0
Anchorship: Thread 1
Distribution-Profile: default-profile
Direction: inbound, SPI: 0xa0d3ba32, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 2901 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2258 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64

```

```

Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2124
Direction: outbound, SPI: 0xe54414e3, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 2901 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2258 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2124

```

??

, Passive mode tunneling: Disabled, Policy-name: HUB\_IPSEC\_POLIPsec SA negotiation succeeds (1 times) ? ???? Quantum Secured: YesIPsec SA? ?????? ??????? ??????.

**IPsec ?? ??**

??

IPsec ??? ?????.

??

?? ????? ??? ????? show security ipsec statistics IPsec ??? ?????.

```
user@hub> show security ipsec statistics
```

ESP Statistics:

Encrypted bytes: 1248

Decrypted bytes: 1248

Encrypted packets: 8

Decrypted packets: 8

AH Statistics:

Input bytes: 0

Output bytes: 0

Input packets: 0

```

Output packets:          0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
  Invalid SPI: 0, TS check fail: 0
  Exceeds tunnel MTU: 0
  Discarded: 0

```

??

? AH Statistics ???? ESP Statistics IPsec ??? ????.

? ??? ???? ??

??

? ??? ???? ????.

??

?? ???? ???? show security key-manager profiles detail ? ??? ???? ????.

```

user@hub> show security key-manager profiles detail

```

```

Name: HUB_KM_PROFILE_1, Index: 4, Type: Static
Configured-at: 20.07.23 (09:59:06)
Time-elapsed: 1 hrs 2 mins 7 secs
Request stats:
  Received: 2
  In-progress: 0
  Success: 2
  Failed: 0

```

??

? Type: Static ??? Name: HUB\_KM\_PROFILE\_1 ? ??? ???? ????.

192.168.80.20 192.168.90.20 3 ping

??

192.168.80.20 192.168.90.20 3 ping.

??

192.168.80.20 192.168.90.20 ping 192.168.90.20 source 192.168.80.20 count 4 Host 192.168.80.20 Host 192.168.90.20.

```
user@HOST1# ping 192.168.90.20 source 192.168.80.20 count 4
PING 192.168.90.20 (192.168.90.20): 56 data bytes
64 bytes from 192.168.90.20: icmp_seq=0 ttl=64 time=2.151 ms
64 bytes from 192.168.90.20: icmp_seq=1 ttl=64 time=1.710 ms
64 bytes from 192.168.90.20: icmp_seq=2 ttl=64 time=1.349 ms
64 bytes from 192.168.90.20: icmp_seq=3 ttl=64 time=1.597 ms
--- 192.168.90.20 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.349/1.702/2.151/0.290 ms
```

Data traffic is successfully flowing between the HOSTs

??

HOST PING 192.168.80.20 (192.168.80.20): 56 data bytes 192.168.80.20 HOST 192.168.90.20.

192.168.80.20 192.168.90.20 3 ping

??

192.168.80.20 192.168.90.20 3 ping.

??

192.168.80.20 192.168.90.20 ping 192.168.90.20 source 192.168.80.20 count 4 ) 192.168.80.20 Host 192.168.90.20 Host 192.168.90.20.

```
user@HOST1# ping 192.168.90.20 source 192.168.70.20 count 4
PING 192.168.90.20 (192.168.90.20): 56 data bytes
64 bytes from 192.168.90.20: icmp_seq=0 ttl=64 time=2.151 ms
64 bytes from 192.168.90.20: icmp_seq=1 ttl=64 time=1.710 ms
```



```

64 bytes from 192.168.90.20: icmp_seq=2 ttl=64 time=1.349 ms
64 bytes from 192.168.90.20: icmp_seq=3 ttl=64 time=1.597 ms
--- 192.168.90.20 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.349/1.702/2.151/0.290 ms

```

Data traffic is successfully flowing between the HOSTs

??

HOST PING 192.168.80.20 (192.168.80.20): 56 data bytes 2?? HOST 3??? ??? ?????.

?? 1: ?? ??? ?? ?? ??

?? ????? ?? ??? ?????.

???? ?? ??

```

set security ike proposal HUB_IKE_PROP dh-group group14
set security ike proposal HUB_IKE_PROP authentication-algorithm sha-256
set security ike proposal HUB_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal HUB_IKE_PROP lifetime-seconds 3600
set security ike policy HUB_IKE_POL proposals HUB_IKE_PROP
set security ike policy HUB_IKE_POL certificate local-certificate HUB_CRT
set security ike gateway HUB_IKE_GW local-address 172.18.10.1
set security ike gateway HUB_IKE_GW ike-policy HUB_IKE_POL
set security ike gateway HUB_IKE_GW external-interface ge-0/0/2.0
set security ike gateway HUB_IKE_GW local-identity distinguished-name
set security ike gateway HUB_IKE_GW dynamic ike-user-type group-ike-id
set security ike gateway HUB_IKE_GW dynamic distinguished-name wildcard C=us,DC=juniper
set security ike gateway HUB_IKE_GW ppk-profile HUB_KM_PROFILE_1
set security ike gateway HUB_IKE_GW version v2-only
set security ipsec proposal HUB_IPSEC_PROP protocol esp
set security ipsec proposal HUB_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal HUB_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy HUB_IPSEC_POL proposals HUB_IPSEC_PROP
set security ipsec vpn HUB_IPSEC_VPN bind-interface st0.1
set security ipsec vpn HUB_IPSEC_VPN ike gateway HUB_IKE_GW
set security ipsec vpn HUB_IPSEC_VPN ike ipsec-policy HUB_IPSEC_POL
set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0

```

```

set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.1/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.90.1/24
set interfaces st0 unit 1 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```

?? 1?? ?? ??

```

set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
set security pki ca-profile Root-CA revocation-check disable
request security pki ca-certificate enroll ca-profile Root-CA
request security pki generate-key-pair certificate-id SPOKE_1_CRT size 2048 type rsa
request security pki local-certificate enroll certificate-id SPOKE_1_CRT challenge-password
<different> domain-name spoke_1.juniper.net email spoke_1@juniper.net subject
DC=juniper,CN=spoke_1.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA
set security key-manager profiles SPOKE_1_KM_PROFILE_1 static key-id ascii-text test-key-id
set security key-manager profiles SPOKE_1_KM_PROFILE_1 static key ascii-text
qjwbdipl39u5mcy89m28pcgowerefnkjsdg
set security ike proposal SPOKE_1_IKE_PROP authentication-method rsa-signatures
set security ike proposal SPOKE_1_IKE_PROP dh-group group14
set security ike proposal SPOKE_1_IKE_PROP authentication-algorithm sha-256
set security ike proposal SPOKE_1_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SPOKE_1_IKE_PROP lifetime-seconds 3600
set security ike policy SPOKE_1_IKE_POL proposals SPOKE_1_IKE_PROP
set security ike policy SPOKE_1_IKE_POL certificate local-certificate SPOKE_1_CRT
set security ike gateway SPOKE_1_IKE_GW address 172.18.10.1
set security ike gateway SPOKE_1_IKE_GW local-address 172.18.10.2

```

```

set security ike gateway SPOKE_1_IKE_GW ike-policy SPOKE_1_IKE_POL
set security ike gateway SPOKE_1_IKE_GW external-interface ge-0/0/2.0
set security ike gateway SPOKE_1_IKE_GW local-identity distinguished-name
set security ike gateway SPOKE_1_IKE_GW remote-identity distinguished-name
set security ike gateway SPOKE_1_IKE_GW ppk-profile SPOKE_1_KM_PROFILE_1
set security ike gateway SPOKE_1_IKE_GW version v2-only
set security ipsec proposal SPOKE_1_IPSEC_PROP protocol esp
set security ipsec proposal SPOKE_1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SPOKE_1_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy SPOKE_1_IPSEC_POL proposals SPOKE_1_IPSEC_PROP
set security ipsec vpn SPOKE_1_IPSEC_VPN bind-interface st0.1
set security ipsec vpn SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW
set security ipsec vpn SPOKE_1_IPSEC_VPN ike ipsec-policy SPOKE_1_IPSEC_POL
set security ipsec vpn SPOKE_1_IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
set security ipsec vpn SPOKE_1_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.2/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.80.1/24
set interfaces st0 unit 1 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```

?? 2?? ?? ??

```

set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
set security pki ca-profile Root-CA revocation-check disable
request security pki ca-certificate enroll ca-profile Root-CA
request security pki generate-key-pair certificate-id SPOKE_2_CRT size 2048 type rsa
request security pki local-certificate enroll certificate-id SPOKE_2_CRT challenge-password

```

```

<different> domain-name spoke_2.juniper.net email spoke_2@juniper.net subject
DC=juniper,CN=spoke_2.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA
set security key-manager profiles SPOKE_2_KM_PROFILE_1 static key-id ascii-text test-key-id
set security key-manager profiles SPOKE_2_KM_PROFILE_1 static key ascii-text
qjwbdip139u5mcy89m28pcgowerefnkjsdg
set security ike proposal SPOKE_2_IKE_PROP authentication-method rsa-signatures
set security ike proposal SPOKE_2_IKE_PROP dh-group group14
set security ike proposal SPOKE_2_IKE_PROP authentication-algorithm sha-256
set security ike proposal SPOKE_2_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SPOKE_2_IKE_PROP lifetime-seconds 3600
set security ike policy SPOKE_2_IKE_POL proposals SPOKE_IKE_PROP
set security ike policy SPOKE_2_IKE_POL certificate local-certificate SPOKE_2_CRT
set security ike gateway SPOKE_2_IKE_GW address 172.18.10.1
set security ike gateway SPOKE_2_IKE_GW local-address 172.18.10.3
set security ike gateway SPOKE_2_IKE_GW ike-policy SPOKE_2_IKE_POL
set security ike gateway SPOKE_2_IKE_GW external-interface ge-0/0/2.0
set security ike gateway SPOKE_2_IKE_GW local-identity distinguished-name
set security ike gateway SPOKE_2_IKE_GW remote-identity distinguished-name
set security ike gateway SPOKE_2_IKE_GW ppk-profile SPOKE_2_KM_PROFILE_1
set security ike gateway SPOKE_2_IKE_GW version v2-only
set security ipsec proposal SPOKE_2_IPSEC_PROP protocol esp
set security ipsec proposal SPOKE_2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SPOKE_2_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy SPOKE_2_IPSEC_POL proposals SPOKE_2_IPSEC_PROP
set security ipsec vpn SPOKE_2_IPSEC_VPN bind-interface st0.2
set security ipsec vpn SPOKE_2_IPSEC_VPN ike gateway SPOKE_2_IKE_GW
set security ipsec vpn SPOKE_2_IPSEC_VPN ike ipsec-policy SPOKE_2_IPSEC_POL
set security ipsec vpn SPOKE_2_IPSEC_VPN traffic-selector ts1 local-ip 192.168.70.0/24
set security ipsec vpn SPOKE_2_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.3/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.70.1/24
set interfaces st0 unit 2 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.2
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any

```

```

set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```

## 2 : DUT

### in this section

- | 243
- 1 | 247
- 2 | 251

, show security ike policy HUB\_IKE\_POL,, show security ipsec proposal HUB\_IPSEC\_PROPS show security ike gateway HUB\_IKE\_GW, show security ipsec policy HUB\_IPSEC\_POL, show security ipsec vpn HUB\_IPSEC\_VPN, show interfaces, show security zonesshow security policies show security ike proposal HUB\_IKE\_PROP. .

```

user@hub# show security ike proposal HUB_IKE_PROP
dh-group group14;
authentication-algorithm sha-256;
encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@hub# show security ike policy HUB_IKE_POL
proposals HUB_IKE_PROP;
certificate {
    local-certificate HUB_CRT;
}

```

```

user@hub# show security ike gateway HUB_IKE_GW
ike-policy HUB_IKE_POL;
dynamic {
    distinguished-name {
        wildcard C=us,DC=juniper;
    }
}

```

```

    }
    ike-user-type group-ike-id;
}
local-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.1;
version v2-only;
ppk-profile HUB_KM_PROFILE_1;

```

```

user@hub# show security ipsec proposal HUB_IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;

```

```

user@hub# show security ipsec policy HUB_IPSEC_POL
proposals HUB_IPSEC_PROP;

```

```

user@hub# show security ipsec vpn HUB_IPSEC_VPN
bind-interface st0.1;
ike {
    gateway HUB_IKE_GW;
    ipsec-policy HUB_IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.90.0/24;
    remote-ip 0.0.0.0/0;
}

```

```

user@hub# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}

```

```

ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
        }
        family mpls;
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
}

```

```

user@hub# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
        ge-0/0/2.0;
    }
}
security-zone vpn {
    interfaces {

```

```

        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

```

user@hub# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

```





```

    local-certificate SPOKE_1_CRT;
}

```

```

user@spoke1# show security ike gateway SPOKE_1_IKE_GW
ike-policy SPOKE_1_IKE_POL;
address 172.18.10.1;
local-identity distinguished-name;
remote-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.2;
version v2-only;
ppk-profile SPOKE_1_KM_PROFILE_1;

```

```

user@spoke1# show security ipsec proposal SPOKE_1_IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;

```

```

user@spoke1# show security ipsec policy SPOKE_1_IPSEC_POL
proposals SPOKE_1_IPSEC_PROP;

```

```

user@spoke1# show security ipsec vpn SPOKE_1_IPSEC_VPN
bind-interface st0.1;
ike {
    gateway SPOKE_1_IKE_GW;
    ipsec-policy SPOKE_1_IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.80.0/24;
    remote-ip 192.168.90.0/24;
}

```

```

user@spoke1# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {

```

```

        address 172.18.10.1/24;
        address 172.18.10.2/24;
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
        }
        family mpls;
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
}

```

```

user@spoke1# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
}
interfaces {

```

```

        ge-0/0/2.0;
    }
}
security-zone vpn {
    interfaces {
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
}

```

```

user@spoke1# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

```

**???** 2

```
user@spoke2# show security pki
ca-profile Root-CA {
  ca-identity Root-CA;
  enrollment {
    url https://ca-server.juniper.net/certsrv/mscep/mscep.dll;
  }
  revocation-check {
    disable;
  }
}
```

```
user@spoke2# show security key-manager
profiles {
    SPOKE_2_KM_PROFILE_1 {
        static {
            key-id ascii-text "$9$C4Y8ABELeWx-wM8goGjPf369A1hx7-VwgIE"; ## SECRET-DATA
            key ascii-text "$9$15SRyKdVYGjqvW7Vw2GUUn/CtBIcylK8XSr4aZjPfz3690RKm8X-VhSwY2oGUUn/
```

```

Cu0IleWdb27-YoZG.mz36Ct0MWxdb2Sr2aJGq.Fn/"; ## SECRET-DATA
    }
}
}

```

```

user@spoke2# show security ike proposal SPOKE_2_IKE_PROP
authentication-method rsa-signatures;
dh-group group14;
authentication-algorithm sha-256;
encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@spoke2# show security ike policy SPOKE_2_IKE_POL
proposals SPOKE_IKE_PROP;
certificate {
    local-certificate SPOKE_2_CRT;
}

```

```

user@spoke2# show security ike gateway SPOKE_2_IKE_GW
ike-policy SPOKE_2_IKE_POL;
address 172.18.10.1;
local-identity distinguished-name;
remote-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.3;
version v2-only;
ppk-profile SPOKE_2_KM_PROFILE_1;

```

```

user@spoke2# show security ipsec proposal SPOKE_2_IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;

```

```

user@spoke2# show security ipsec vpn SPOKE_2_IPSEC_VPN
bind-interface st0.2;
ike {

```

```

    gateway SPOKE_2_IKE_GW;
    ipsec-policy SPOKE_2_IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.70.0/24;
    remote-ip 192.168.90.0/24;
}

```

```

user@spoke2# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
            address 192.168.70.1/24;
        }
        family mpls;
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
            address 172.18.10.3/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}

```

```

st0 {
    unit 1 {
        family inet;
    }
    unit 2 {
        family inet;
    }
}

```

```

user@spoke2# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
security-zone vpn {
    interfaces {
        st0.2;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

```

user@spoke2# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {

```



```

        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}
```

?? ??

1. ???? ?? ?? —??? ????® SRX1500 ??? ? ? ?? ???? ???? ?? ?? ???? ????® vSRX ?? ???(vSRX3.0).
2. ???? ???? —Junos OS ??? 22.4R1 ??( JUNOS Key Manager ??? JUNOS ike).
3. ??? ???? ETSI ?? ? ??(QKD) Rest API ??? ???? ???? QKD ???? ????.
4. ???? ???? ???? ?????. ???? ???? ???? ???? ????.

??

SRX ??? ???? IPsec VPN? ???? ???? ???? ?????. IPsec VPN?? ? ? ???? ? ???? ???? ???? IKE(Internet Key Exchange) SA? ? ? ? ????.

? ? ???? ? ???? QKD ??? ? ? ? ???? ???? ???? ???? ?????. ???? ? ????.

??

1. CA ???? ????.

```
user@host# set security pki ca-profile Root-CA ca-identity Root-CA
user@host# set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile Root-CA revocation-check disable
```

2. CA ???? ????.

```
user@host> request security pki local-certificate load certificate-id SAE_A filename
SAE_A.cert key SAE_A.key
```

3. CA ???? ????.

```
user@host> request security pki ca-certificate enroll ca-profile Root-CA
```

4. ?? ? ???? ????.

```
user@host# set security key-manager profiles KM_PROFILE_1 quantum-key-manager url https://
kme.juniper.net
user@host# set security key-manager profiles KM_PROFILE_1 quantum-key-manager local-sae-id
```

```
SAE_A
user@host# set security key-manager profiles KM_PROFILE_1 quantum-key-manager local-
certificate-id SAE_A_CERT
user@host# set security key-manager profiles KM_PROFILE_1 quantum-key-manager trusted-cas
Root-CA
```

??

??

?? ? ???? ? ???? ? ?? ?????.

??

?? ????? ?(?) show security pki ca-certificate ca-profile Root-CA ) ????? CA ??? ? CA ????? ?????.

```
user@host> show security pki ca-certificate ca-profile Root-CA
LSYS: root-logical-system
  CA profile: Root-CA
Certificate identifier: Root-CA
  Issued to: Root-CA, Issued by: C = IN, ST = WestBengal, O = JuniperNetworks, CN = Root-CA
  Validity:
    Not before: 09-11-2023 09:03 UTC
    Not after: 03-24-2044 09:03 UTC
  Public key algorithm: rsaEncryption(4096 bits)
  Keypair Location: Keypair generated locally
```

?? ????? ?(?) show security pki local-certificate certificate-id SAE\_A\_CERT ) ????? PKI ?? ????? ?????.

```
user@host> show security pki local-certificate certificate-id SAE_A_CERT
LSYS: root-logical-system
Certificate identifier: SAE_A_CERT
  Issued to: SAE_A, Issued by: C = IN, ST = WestBengal, O = JuniperNetworks, CN = ROOT_CA
  Validity:
    Not before: 08-28-2023 04:54 UTC
    Not after: 03-10-2044 04:54 UTC
  Public key algorithm: rsaEncryption(2048 bits)
  Keypair Location: Keypair generated locally
```

```
?? ???? ?(?) request security key-manager profiles get profile-keys name km_profile_1 peer-sae-id SAE_B ) ???? ?
???? ? ???? ???? ? ? ? ????.
```

```
user@host> request security key-manager profiles get profile-keys name km_profile_1 peer-sae-id
SAE_B
```

```
- Response:
- Status: SUCCESS
- Name: km_profile_1
- Type: quantum-key-manager
- Key-size: 256 bits
- Key-count: 1
- Key-ids:
  - 002420bd-7a03-4725-9c41-6969d8e1815a
- Keys:
  - 728d21c4a05fe2f73c7b2f58d1e3631dc68fcfaca16be12ca3fc7715079db0f9
```

```
?? ???? ?(?) show security key-manager profiles name KM_PROFILE_1 detail ) ???? ? ???? ???? ????.
```

```
user@host> show security key-manager profiles name KM_PROFILE_1 detail
```

```
Name: KM_PROFILE_1, Index: 2, Type: quantum-key-manager
```

```
Configured-at: 11.09.23 (02:04:32)
```

```
Time-elapsed: 0 hrs 20 mins 23 secs
```

```
Url: https://kme.juniper.net
```

```
Local-sae-id: SAE_A
```

```
Local-certificate-id: SAE_A_CERT
```

```
Trusted-cas: [ Root-CA ]
```

```
Peer-sae-ids: N/A
```

```
Default-key-size: N/A
```

```
Request stats:
```

```
Received: 0
```

```
In-progress: 0
```

```
Success: 0
```

```
Failed: 0
```

```
??
```

```
?? show security pki ca-certificate ca-profile Root-CA PKI CA ???? ?, ???, ???, ?? ? ???? ? ????.
```

```
?? show security pki local-certificate certificate-id SAE_A_CERT ?? CA ???? ?, ???, ???, ?? ? ???? ? ?
??.
```

?? request security key-manager profiles get profile-keys name km\_profile\_1 peer-sae-id SAE\_B ?? ???? ? ??? ????  
? ? ?? ?????.

?? show security key-manager profiles name KM\_PROFILE\_1 detail ?? ? ??? ???? ??, URL, ?? ?? ?????.

**?: ??? ? IPsec VPN? ?? ?? ? ??? ? ???? ??**

**summary**

? ?? ???? ?? ? ??? ? ???? ???? IPsec ??? ? VPN ??  
?? ????.

**in this section**

- ?? ?? ?? ?? | 260
- ???? ?? | 260
- ?? ?? | 261
- ???? ?? | 264
- ???? ?? | 265
- SRX ??? ??? ???? ?? ?? ?? | 265
- ?? | 268
- ?? 1 : ?? ??? ?? ?? ?? | 273
- ?? 2 : DUT? ?? ?? ?? | 275

?? ? ??? ? ???? ???? IPsec ??? ? VPN ???? ???? ? ????.

? ?? ??? SRX1 ? SRX2 ???? ? ? ? ???? ???? IPsec VPN?? QKD ?? ?????. QKD ?? ???? ???? ? ? ?  
?? ???? ???? ? ????.



?:  
? 45: ?? ???

|       |         |
|-------|---------|
| ?? ?? | ? ?? ?? |
| ?? ?? | ? ?? ?? |



|        |                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------|
| ?? ??  | vLAB ?????                                                                                        |
| ??? ?? | RFC 8784 - ??? ?? ??? ?? Internet Key Exchange ???? ?? 2(IKEv2)?? ?? ?? ? ??<br>ETSI QKD Rest API |

?? ??

? 48: Quantum Key Manager ? ??? ?? ??

|                                 |                                                                                                                                           |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec VPN                       | ??? ?? ????? ????? VPN ??? ????? ??? ? ??? IPsec VPN ?????<br>? ??????. ??? VPN ??? ??? ?? ?? ?????? ?????? ?? ?? VPN ??? ??<br>?.        |
| IKE(Internet Key Exchange) ???? | ?? ??? ??????. IKE ?????? IKE ??? ?????? ?????? ?? ??? ?? ??<br>(CA) ??? ?????? ??? ??????.                                               |
| ??                              |                                                                                                                                           |
| IKE(Internet Key Exchange) ??   | ?? ?? ????????? ?? IKE ??? ????? ? ????? ?????? ? ?? ??????.<br><br>IKE(Internet Key Exchange)? ?? ?? ??(SA)? ????? IPsec? ?? ?????<br>?. |
| IPsec ??                        | ?? IPsec ??? ??? ?????, ????? ? ?? ????? ??????.                                                                                          |
| ??                              |                                                                                                                                           |
| IKE(Internet Key Exchange) ??   | IKE ?? ?? ??? ?? ?? ??(IKE ??)? ??? ??????.                                                                                               |
| IPsec ??                        | ???? ?? ?? ?? VPN ?????? ?????? ?? ? ?? ??? ??????.                                                                                       |

|              |                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>?? ??</p> | <p>IPsec SA? ?? ??? ??? ??? ??? ? ????.</p> <ul style="list-style-type: none"><li>• VPN-OUT—TRUST ??? VPN ????? ????. ?? ? ? ? ? ? ? ? ? ? ?.</li><li>• ?? ??: HOST-1-?</li><li>• ?? ??: HOST-2-?</li><li>• ??: ??</li><li>• VPN-IN—VPN ??? ? ? ???? ???? ?????. ?? ? ? ? ? ? ? ? ? ? ?.</li><li>• ?? ??: HOST-2-?</li><li>• ?? ??: HOST-1-?</li><li>• ??: ??</li></ul> |
| <p>???</p>   |                                                                                                                                                                                                                                                                                                                                                                         |





|          |                                     |
|----------|-------------------------------------|
| ??       | ??? ??? ????????                    |
| untrust  | ?? ?? ??? ????????                  |
| VPN      | ??? ????? ?? ????? ????? ??????     |
| ?? ?? ?? | ??? IKE ? IPsec SA? ?? ????? ?????? |

???? ??

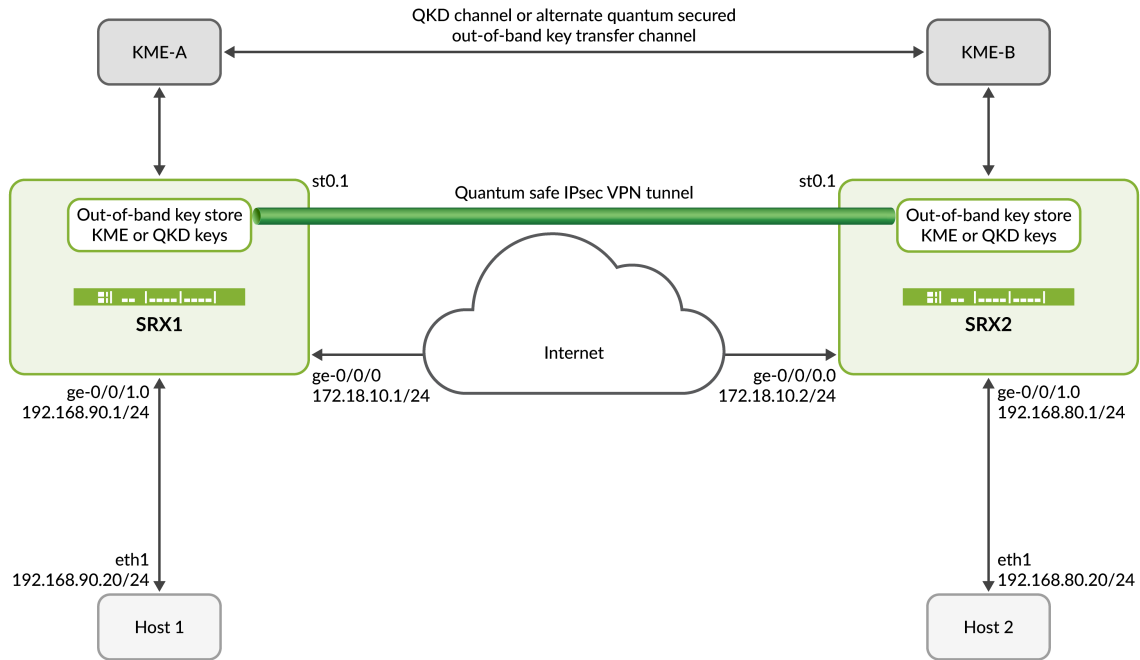
? ?????? ?? KME ?????? ?? ? ? ???? SRX1 ? SRX2 IPsec VPN ??? ??????. KME ?????(KME-A ? KME-B)? ?? ????? ?? ??? ??? ? ? ?????. SRX1 ? SRX2 ?????? ? ???? ????? ?? KME ??????? ?? ? ? ???? ?? ?? ????? VPN ??? ?? ????? ??????.

图 49: ? ??? ??? ??, ?? ? ??

| ??? ??       | ??/?                               | ??                                                                                         |
|--------------|------------------------------------|--------------------------------------------------------------------------------------------|
| SRX1         | IPsec ?? ??? ??? SRX ??? ??? ????? | IKE ?? IPsec SA ??? ????? KME-A QKD ?????? ??? QKD ?? ????? SRX2? ??? ?? IPsec ??? ??????. |
| SRX2         | IPsec ?? ??? ??? SRX ??? ??? ????? | IKE ?? IPsec SA ??? ????? KME-B QKD ?????? QKD ?? ????? ?? ?? IPsec ??? ??????.            |
| HOST1        | SRX1? ??? ? ?? ?? ?? LAN ? ???     | HOST 2? ?? ?????? ? ????? ??????.                                                          |
| HOST2        | SRX2? ??? ? ?? ?? ?? LAN ? ???     | HOST 1? ?????? ? ????? ??????.                                                             |
| ?????        | ?? ?? QKD ?????                    | SRX1? ? ??? ?? ????? QKD ?? ????? ?.                                                       |
| ?????(KME-B) | ?? ?? QKD ?????                    | SRX2? ? ??? ?? ????? QKD ?? ????? ?.                                                       |

?? ??

## ?? 20: ??? ? VPN



jin-000691

## SRX ??? ???? ???? ???? ??



?: DUT? ?? ?? ?? ???? ???? ???? ????.

- "SRX1?? ?? ??" ??? 273
- "SRX2 ?? ??" ??? 274

? ??? SRX1 ? SRX2 ???? ?????. ?? ???? ??, ???? ???? ???? ????.

### 1. ?????? ??????

```
[edit interfaces]
user@srx# set ge-0/0/0 unit 0 family inet address 172.18.10.1/24
user@srx# set st0 unit 1 family inet
user@srx# set ge-0/0/1 unit 0 family inet address 192.168.90.1/24
```

### 2. must, ?? ?? ?? ??? ???? quantum-key-manager ??? ? ???? ????.

CA `quantum-key-manager`, KME `quantum-key-manager` URL `https://www.kme_a-qkd-server.net`, `quantum-key-manager` SAE-ID `quantum-key-manager`, `quantum-key-manager` SAE-ID `quantum-key-manager`, `quantum-key-manager` CA `quantum-key-manager`.

```
[edit security pki]
user@srx# set ca-profile ROOT_CA_CERT ca-identity RootCA
```

```
[edit security key-manager profiles]
user@srx# set km_profile_1 quantum-key-manager url https://www.kme_a-qkd-server.net
```

```
[edit security key-manager profiles]
user@srx# set km_profile_1 quantum-key-manager local-sae-id SAE_A
user@srx# set km_profile_1 quantum-key-manager local-certificate-id SAE_A_CERT
user@srx# set km_profile_1 quantum-key-manager trusted-cas ROOT_CA_CERT
```

### 3. `quantum-key-manager` IPsec VPN `quantum-key-manager`. `quantum-key-manager` ID `quantum-key-manager` `quantum-key-manager` `quantum-key-manager`, `quantum-key-manager` `quantum-key-manager` `quantum-key-manager`.

```
[edit security zones]
user@srx# set security-zone untrust host-inbound-traffic system-services ike
user@srx# set security-zone untrust interfaces ge-0/0/0.0
user@srx# set security-zone vpn interfaces st0.1
user@srx# set security-zone trust host-inbound-traffic system-services ping
user@srx# set security-zone trust interfaces ge-0/0/1.0
```

```
[edit security policies]
user@srx# set from-zone trust to-zone vpn policy vpn_out match source-address any
user@srx# set from-zone trust to-zone vpn policy vpn_out match destination-address any
user@srx# set from-zone trust to-zone vpn policy vpn_out match application any
user@srx# set from-zone trust to-zone vpn policy vpn_out then permit
user@srx# set from-zone vpn to-zone trust policy vpn_in match source-address any
user@srx# set from-zone vpn to-zone trust policy vpn_in match destination-address any
user@srx# set from-zone vpn to-zone trust policy vpn_in match application any
user@srx# set from-zone vpn to-zone trust policy vpn_in then permit
```

```
[edit security ike proposal]
user@srx# set IKE_PROP authentication-method pre-shared-keys
user@srx# set IKE_PROP dh-group group14
```

```

user@srx# set IKE_PROP authentication-algorithm sha-256
user@srx# set IKE_PROP encryption-algorithm aes-256-cbc
user@srx# set IKE_PROP lifetime-seconds 3600

```

```

[edit security ike policy]
user@srx# set IKE_POL proposals IKE_PROP
user@srx# set IKE_POL pre-shared-key ascii-text ipsec-test

```

```

[edit security ike gateway]
user@srx# set IKE_GW ike-policy IKE_POL
user@srx# set IKE_GW address 172.18.10.2
user@srx# set IKE_GW external-interface ge-0/0/0.0
user@srx# set IKE_GW local-address 172.18.10.1
user@srx# set IKE_GW version v2-only
user@srx# set IKE_GW ppk-profile km_profile_1

```

```

[edit security ipsec proposal]
user@srx# set IPSEC_PROP protocol esp
user@srx# set IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@srx# set IPSEC_PROP encryption-algorithm aes-256-cbc
user@srx# set IPSEC_PROP lifetime-seconds 2400

```

```

[edit security ipsec policy]
user@srx# set IPSEC_POL proposals IPSEC_PROP

```

```

[edit security ipsec vpn]
user@srx# set IPSEC_VPN bind-interface st0.1
user@srx# set IPSEC_VPN ike gateway IKE_GW
user@srx# set IPSEC_VPN ike ipsec-policy IPSEC_POL
user@srx# set IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
user@srx# set IPSEC_VPN traffic-selector ts1 remote-ip 192.168.80.0/24
user@srx# set IPSEC_VPN establish-tunnels immediately

```

??

in this section

IKE(Internet Key Exchange) SA ?? | 268

IPsec SA ?? | 270

IPsec ?? ?? | 271

? ??? ????? ?? | 272

HOST 1?? HOST 2? ?? ? ??? ping | 272

? ????? ? ??? ??? ????? ? ??? ? ?? show ?? ??? ?????.

| ???                                            | ?? ??                                                  |
|------------------------------------------------|--------------------------------------------------------|
| ?? ike ?? ?? ?? ??<br>??                       | "IKE(Internet Key Exchange) SA? ?????? ??????" ??? 268 |
| ?? ipsec ?? ?? ??<br>?? ??                     | "IPsec SA? ?????? ??????" ??? 270                      |
| ?? ipsec ?? ??                                 | "IPsec ??? ? ??? ??? ??????" ??? 271                   |
| ?? ? ??? ??? ?? ?<br>? ??                      | "? ??? ??? ??????" ??? 272                             |
| ? 192.168.80.20 ?<br>? 192.168.90.20 ?<br>?? 5 | "HOST 1?? HOST 2? ?? ? ??? ping???" ??? 272            |

IKE(Internet Key Exchange) SA ??

??

IKE(Internet Key Exchange) SA? ?????.

??

?? ???? ???? show security ike security-associations detail IKE(Internet Key Exchange) SA? ?????.

```

user@srx> show security ike security-associations detail
IKE peer 172.18.10.2, Index 21, Gateway Name: IKE_GW
Role: Initiator, State: UP
Initiator cookie: 5a417d46cef3207d, Responder cookie: 57b9a17516bee31b Exchange type: IKEv2,
Authentication method: Pre-shared-keys
Local gateway interface: ge-0/0/2.0 Routing instance: default
Local: 172.18.10.1:500, Remote: 172.18.10.2:500
Lifetime: Expires in 3445 seconds Reauth Lifetime: Disabled
IKE Fragmentation: Enabled, Size: 576 SRG ID: 0
Remote Access Client Info: Unknown Client Peer ike-id: 172.18.10.2
AAA assigned IP: 0.0.0.0 PPK-profile: km_profile_1
Optional: No State      : Used
Algorithms:
Authentication      : hmac-sha256-128
Encryption          : aes256-cbc Pseudo random function: hmac-sha256 Diffie-Hellman group : DH-group-14
Traffic statistics:
Input bytes :      783
Output bytes :      831
Input packets:        2
Output packets:        2
Input fragmented packets:    0
Output fragmented packets:    0
IPsec security associations: 2 created, 0 deleted Phase 2 negotiations in progress: 1
IPsec Tunnel IDs: 500003
Negotiation type: Quick mode, Role: Initiator, Message ID: 0 Local: 172.18.10.1:500, Remote:
172.18.10.2:500
Local identity: 172.18.10.1
Remote identity: 172.18.10.2 Flags: IKE SA is created
IPsec SA Rekey CREATE_CHILD_SA exchange stats:
Initiator stats:      Responder stats:
Request Out   : 0     Request In    : 0
Response In   : 0     Response Out  : 0
No Proposal Chosen In   : 0     No Proposal Chosen Out   : 0
Invalid KE In   : 0     Invalid KE Out   : 0
TS Unacceptable In   : 0     TS Unacceptable Out   : 0
Res DH Compute Key Fail : 0     Res DH Compute Key Fail: 0 Res Verify SA Fail   : 0
Res Verify DH Group Fail: 0 Res Verify TS Fail   : 0

```

??

,, PPK-profile: km\_profile\_1IPSec security associations: 2 created, 0 deleted Phase 2 negotiations in progress:  
1Flags: IKE SA is created ? ???? Role: Initiator, State: UPIKE SA? ???? ???? ????.

## IPsec SA ??

??

IPsec SA? ????.

??

?? ???? ???? show security ipsec security-associations detail IPsec SA? ????.

```
user@srx> show security ipsec security-associations detail
```

```
ID: 500003 Virtual-system: root, VPN Name: IPSEC_VPN Local Gateway: 172.18.10.1, Remote Gateway:
172.18.10.2 Traffic Selector Name: ts1
```

```
Local Identity: ipv4(192.168.90.0-192.168.90.255)
```

```
Remote Identity: ipv4(192.168.80.0-192.168.80.255) TS Type: traffic-selector
```

```
Version: IKEv2 Quantum Secured: Yes PFS group: N/A
```

```
SRG ID: 0
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: IPSEC_POL Port:
500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
```

```
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0 Tunnel events:
```

```
Fri Mar 31 2023 01:41:52: IPsec SA negotiation succeeds (1 times)
```

```
Location: FPC 0, PIC 0, KMD-Instance 0
```

```
Anchorship: Thread 1
```

```
Distribution-Profile: default-profile Direction: inbound, SPI: 0xd1e1549c, AUX-SPI: 0
```

```
, VPN Monitoring: - Hard lifetime: Expires in 1916 seconds Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 1349 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits) Anti-replay
service: counter-based enabled, Replay window size: 64
```

```
Extended-Sequence-Number: Disabled
```

```
tunnel-establishment: establish-tunnels-immediately IKE SA Index: 21
```

```
Direction: outbound, SPI: 0xb5883167, AUX-SPI: 0
```

```
, VPN Monitoring: - Hard lifetime: Expires in 1916 seconds Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 1349 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```



```

Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits) Anti-replay
service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-immediately IKE SA Index: 21

```

??

, Policy-name: IPSEC\_POL, IPsec SA negotiation succeeds (1 times)tunnel-establishment: establish-tunnels-immediately IKE SA Index: 21 ? ???? Quantum Secured: YesIPsec SA? ???? ???? ????.

**IPsec** ?? ??

??

IPsec ??? ????.

??

?? ???? ???? show security ipsec statistics IPsec ??? ????.

```

user@srx> show security ipsec statistics
ESP Statistics:
Encrypted bytes:    780
Decrypted bytes:    780
Encrypted packets:  5
Decrypted packets:  5
AH Statistics:
Input bytes:        0
Output bytes:        0
Input packets:      0
Output packets:     0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0 Bad headers: 0, Bad trailers: 0
Invalid SPI: 0, TS check fail: 0 Exceeds tunnel MTU: 0
Discarded: 0

```

??

? AH Statistics ???? ESP Statistics IPsec ??? ????.

**?** **???** **????** **??**

??

??

```
?? ???? ???? show security key-manager profiles detail ? ??? ???? ????.
```

```
user@srx> show security key-manager profiles detail
Name: km_profile_1, Index: 3, Type: Quantum-key-manager
Configured-at: 31.03.23 (01:40:50)
Time-elapsed: 0 hrs 11 mins 30 secs Url: https://www.kme_a-qkd-server.net Local-sae-id: SAE_A
Local-certificate-id: SAE_A_CERT Trusted-cas: [ ROOT_CA_CERT ] Peer-sae-ids: N/A
Default-key-size: N/A Request stats:
Received: 1
In-progress: 0
Success: 1
Failed: 0
```

??

? Quantum-key-manager ???? ? ??? ???? Name: km\_profile\_1 ?????.

HOST 1?? HOST 2? ?? ? ??? ping

??

HOST 1?? HOST 2?? ??? ?????.

??

```
?? ???? ???? 5? ???? ping 192.168.80.20 source 192.168.90.20 HOST 1?? HOST 2?? ??? ?????.
```

```
user@HOST1# ping 192.168.80.20 source 192.168.90.20 count 5
PING 192.168.80.20 (192.168.80.20): 56 data bytes count 5
64 bytes from 192.168.80.1: icmp_seq=0 ttl=64 time=0.998 ms
64 bytes from 192.168.80.1: icmp_seq=1 ttl=64 time=1.594 ms
64 bytes from 192.168.80.1: icmp_seq=2 ttl=64 time=1.395 ms
```

```

64 bytes from 192.168.80.1: icmp_seq=3 ttl=64 time=1.536 ms
64 bytes from 192.168.80.1: icmp_seq=4 ttl=64 time=1.838 ms

--- 192.168.80.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max/stddev =
0.998/1.472/1.838/0.277 ms

Data traffic is successfully flowing between the HOSTs

```

??

HOST PING 192.168.80.20 (192.168.80.20): 56 data bytes count 5 1?? HOST 2?? ??? ?????.

?? 1 : ?? ??? ?? ?? ??

?? ????? ?? ??? ?????.

**SRX1?? ?? ??**

```

set security pki ca-profile ROOT_CA_CERT ca-identity RootCA
set security key-manager profiles km_profile_1 quantum-key-manager url https://www.kme_a-qkd-
server.net
set security key-manager profiles km_profile_1 quantum-key-manager local-sae-id SAE_A
set security key-manager profiles km_profile_1 quantum-key-manager local-certificate-id
SAE_A_CERT
set security key-manager profiles km_profile_1 quantum-key-manager trusted-cas ROOT_CA_CERT
set interfaces ge-0/0/0 unit 0 family inet address 172.18.10.1/24
set interfaces st0 unit 1 family inet
set interfaces ge-0/0/1 unit 0 family inet address 192.168.90.1/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any

```

```

set security policies from-zone vpn to-zone trust policy vpn_in then permit
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group14
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 3600
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text ipsec-test
set security ike gateway IKE_GW ike-policy IKE_POL
set security ike gateway IKE_GW address 172.18.10.2
set security ike gateway IKE_GW external-interface ge-0/0/0.0
set security ike gateway IKE_GW local-address 172.18.10.1
set security ike gateway IKE_GW version v2-only
set security ike gateway IKE_GW ppk-profile km_profile_1
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal IPSEC_PROP lifetime-seconds 2400
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN bind-interface st0.1
set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
set security ipsec vpn IPSEC_VPN traffic-selector ts1 remote-ip 192.168.80.0/24
set security ipsec vpn IPSEC_VPN establish-tunnels immediately

```

## SRX2

```

set security pki ca-profile ROOT_CA_CERT ca-identity RootCA
set security key-manager profiles km_profile_1 quantum-key-manager url https://www.kme_a-qkd-
server.net
set security key-manager profiles km_profile_1 quantum-key-manager local-sae-id SAE_B
set security key-manager profiles km_profile_1 quantum-key-manager local-certificate-id
SAE_B_CERT
set security key-manager profiles km_profile_1 quantum-key-manager trusted-cas ROOT_CA_CERT
set interfaces ge-0/0/0 unit 0 family inet address 172.18.10.2/24
set interfaces st0 unit 1 family inet
set interfaces ge-0/0/1 unit 0 family inet address 192.168.80.1/24
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone vpn interfaces st0.1

```

```

set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group14
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 3600
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text ipsec-test
set security ike gateway IKE_GW ike-policy IKE_POL
set security ike gateway IKE_GW address 172.18.10.1
set security ike gateway IKE_GW external-interface ge-0/0/0.0
set security ike gateway IKE_GW local-address 172.18.10.2
set security ike gateway IKE_GW version v2-only
set security ike gateway IKE_GW ppk-profile km_profile_1
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal IPSEC_PROP lifetime-seconds 2400
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN bind-interface st0.1
set security ipsec vpn IPSEC_VPN ike gateway IKE_GW
set security ipsec vpn IPSEC_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
set security ipsec vpn IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set security ipsec vpn IPSEC_VPN establish-tunnels immediately

```

## ?? 2 : DUT? ?? ?? ??

in this section

● SRX1 | 276

DUT ? ? ? ? ? ? ? ? ? ?.

## SRX1

```
user@srk1# show security pki
ca-profile ROOT_CA_CERT {
  ca-identity RootCA;
}
```

```
user@srk1# show security key-manager
profiles {
  km_profile_1 {
    quantum-key-manager {
      url https://www.kme_a-qkd-server.net;
      local-sae-id SAE_A;
      local-certificate-id SAE_A_CERT;
      trusted-cas ROOT_CA_CERT;
    }
  }
}
```

```
user@srk1# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 172.18.10.1/24;
      address 172.18.10.2/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {
      address 192.168.90.1/24;
```

```

        address 192.168.80.1/24;
        address 192.168.70.1/24;
    }
    family mpls;
}
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
            address 172.18.10.3/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
    unit 2 {
        family inet;
    }
}
}

```

```

user@srk1# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {

```

```

    interfaces {
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
}

```

```

user@srk1# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

```



```

    }
}

```

```

user@srk1# show security ike proposal IKE_PROP
authentication-method pre-shared-keys;
dh-group group14;
authentication-algorithm sha-256;
encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@srk1# show security ike policy IKE_POL
proposals IKE_PROP;
pre-shared-key ascii-text "$9$Nadwg4aUH.5Nds4aUiHu01RhrvWxVs4"; ## SECRET-DATA

```

```

user@srk1# show security ike gateway IKE_GW
ike-policy IKE_POL;
address 172.18.10.2;
external-interface ge-0/0/0.0;
local-address 172.18.10.1;
version v2-only;
ppk-profile km_profile_1;

```

```

user@srk1# show security ipsec proposal IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;
lifetime-seconds 2400;

```

```

user@srk1# show security ipsec policy IPSEC_POL
proposals IPSEC_PROP;

```

```

user@srk1# show security ipsec vpn IPSEC_VPN
bind-interface st0.1;
ike {
    gateway IKE_GW;
}

```

```

    ipsec-policy IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.90.0/24;
    remote-ip 192.168.80.0/24;
}
establish-tunnels immediately;

```

## SRX 2

```

user@srx2# show security key-manager
profiles {
    km_profile_1 {
        quantum-key-manager {
            url https://www.kme_a-qkd-server.net;
            local-sae-id SAE_B;
            local-certificate-id SAE_B_CERT;
            trusted-cas ROOT_CA_CERT;
        }
    }
}

```

```

user@srx2# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
            address 192.168.70.1/24;
        }
        family mpls;
    }
}

```

```

}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
            address 172.18.10.3/24;
        }
    }
}
ge-1/0/0 {
    unit 0 {
        family mpls;
    }
}
st0 {
    unit 1 {
        family inet;
    }
    unit 2 {
        family inet;
    }
}

```

```

user@srx2# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn {
    interfaces {
        st0.1;
    }
}
security-zone trust {

```

```

host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    ge-0/0/1.0;
}
}

```

```

user@srx2# show security policies
from-zone trust to-zone vpn {
    policy vpn_out {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_in {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
}

```

```

user@srx2# show security ike proposal IKE_PROP
authentication-method pre-shared-keys;
dh-group group14;
authentication-algorithm sha-256;

```

```

encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@srx2# show security ike gateway IKE_GW
ike-policy IKE_POL;
address 172.18.10.1;
external-interface ge-0/0/0.0;
local-address 172.18.10.2;
version v2-only;
ppk-profile km_profile_1;

```

```

user@srx2# show security ike policy IKE_POL
proposals IKE_PROP;
pre-shared-key ascii-text "$9$P5z6/Cu1EyP5F/CuB1-VwYgJD1.TF/"; ## SECRET-DATA

```

```

user@srx2# show security ipsec policy IPSEC_POL
proposals IPSEC_PROP;

```

```

user@srx2# show security ipsec vpn IPSEC_VPN
bind-interface st0.1;
ike {
    gateway IKE_GW;
    ipsec-policy IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.80.0/24;
    remote-ip 192.168.90.0/24;
}
establish-tunnels immediately;

```

?: Quantum Key Manager ? ???? ???? ? ? IPsec AutoVPN ???? ?

summary

? ? ???? ? ? ? ? ? ? ? ? IPsec AutoVPN ? ?  
? ????.

in this section

- ? ? ? ? ? | 284
- ???? ? | 285
- ? ? ? | 286
- ???? ? | 290
- ???? ? | 292
- ???? ? ? ? | 292
- ? ? ? ? ? ? ? ? | 296
- ? ? | 299
- ? ? 1 : ? ? ? ? ? ? ? ? | 308
- ? ? 2 : DUT ? ? ? ? ? | 313

?, ??? 1 ? ??? 2 ? ? ? ? ? ? ? ? KME ??, KME ??? 1 ? KME ??? 2 ? ???? QKD ? ? ? ? ? IPsec VPN ? ? ? ? ? ? ? ?.



?:

? 50: ? ? ? ? ?

|       |                    |
|-------|--------------------|
| ?? ?? | ? ??? ? ??? ?????. |
| ?? ?? | ? ??? ? ??? ?????. |

?? ?? ? ?

? 51: ???? ? ???? ? ?

|                   |                                                                                                                                                                                                            |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>?? ?? ?</p>    | <ul style="list-style-type: none"> <li>® ??? ???? SRX1500 ??? ? ? ? ? ? ? ? ® vSRX<br/>? ? ?(vSRX3.0)</li> <li>? ? ? ?(KME) ? ? ? ?(QKD) ??. KME ? ? ? ? <a href="#">ETSI GS QKD 014</a> ? ? ?.</li> </ul> |
| <p>???? ? ? ?</p> | <p>Junos OS ? ? 22.4R1 ?.</p>                                                                                                                                                                              |

□□□□ □□

52: 11, 12 13 14

|           |                                                                                                                                                                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??        | <ul style="list-style-type: none"> <li>?? ??<br/>?? ?? ?? ?? ??? ???? QKD ????? ?? ?? ?? ??? ?????.</li> <li>?? ??<br/>?? ?? ?? ?? ????? ?? VPN ????? ?? ??? ? ?????? IPsec VPN ????? ??? ??????</li> <li>RFC 8784 ??<br/>?? ????? RFC 8784 ??? ?????.</li> <li>?? ??? ??<br/><a href="#">ETSI QKD Rest API</a>? ????? ?? QKD ?????? ??? ? ?????.</li> </ul> |
| ??? ??    |                                                                                                                                                                                                                                                                                                                                                              |
| ??? ????? | <ul style="list-style-type: none"> <li>IPsec VPN</li> <li><a href="#">?? ? ??? ????? AutoVPN</a></li> </ul>                                                                                                                                                                                                                                                  |
| ?? ??     | vLab <a href="#">????</a> : IPsec VPN - <a href="#">?? ??</a>                                                                                                                                                                                                                                                                                                |
| ??? ??    | <ul style="list-style-type: none"> <li>RFC 8784 - <a href="#">???? ?? ??? ? Internet Key Exchange ????? ?? 2(IKEv2)?? ?? ?? ?</a><br/><a href="#">??</a></li> <li><a href="#">ETSI QKD Rest API</a></li> </ul>                                                                                                                                               |

?? ??

53 286 ??? ? ??? ??? ?? ?? ??? ?? ??? ??? ????

53: Quantum Key Manager ?? ??

|                                  |                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------|
| IPsec VPN                        | ??? ?? ????? ????? VPN ??? ????? ?? ? ??? IPsec VPN ??? ? ?????, ??? VPN ??? ?? ?? ????? ????? ?? ?? VPN ??? ? ?. |
| IKE(Internet Key Exchange) ????? | ?? ??? ????? IKE ????? IKE ??? ????? ????? ???? CA ?? (ca-profiles)?? ?????.                                      |
| ??                               |                                                                                                                   |
| IKE(Internet Key Exchange) ??    | ?? ?? ??????? ?? IKE(Internet Key Exchange) ??? ????? ? ????? ? ????? ? ?? ?????.                                 |
|                                  | IKE(Internet Key Exchange)? ?? SA? ????? IPsec? ?? ?????.                                                         |
| IPsec ??                         | ?? IPsec ??? ???, ????? ? ?? ????? ?????.                                                                         |
| ??                               |                                                                                                                   |
| IKE(Internet Key Exchange) ??    | IKE ?? ?? ??? ?? ?? ??(IKE ??)? ??? ?????.                                                                        |
| IPsec ??                         | ???? ?? ?? VPN ????? ?? ? ?? ??? ?????.                                                                           |



|              |                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>?? ??</p> | <p>IPsec SA? ?? ??? ??? ??? ??? ? ????.</p> <ul style="list-style-type: none"><li>• VPN-OUT – ?? ??? VPN ????? ??? ?????. ??? ?? ??? ? ? ???.</li><li>• ?? ??: HOST-1-?</li><li>• ?? ??: HOST-2-?</li><li>• ??: ??</li><li>• VPN-IN – VPN ??? ? ???? ???? ?????. ??? ?? ??? ? ? ???.</li><li>• ?? ??: HOST-2-?</li><li>• ?? ??: HOST-1-?</li><li>• ??: ??</li></ul> |
| <p>???</p>   |                                                                                                                                                                                                                                                                                                                                                                     |





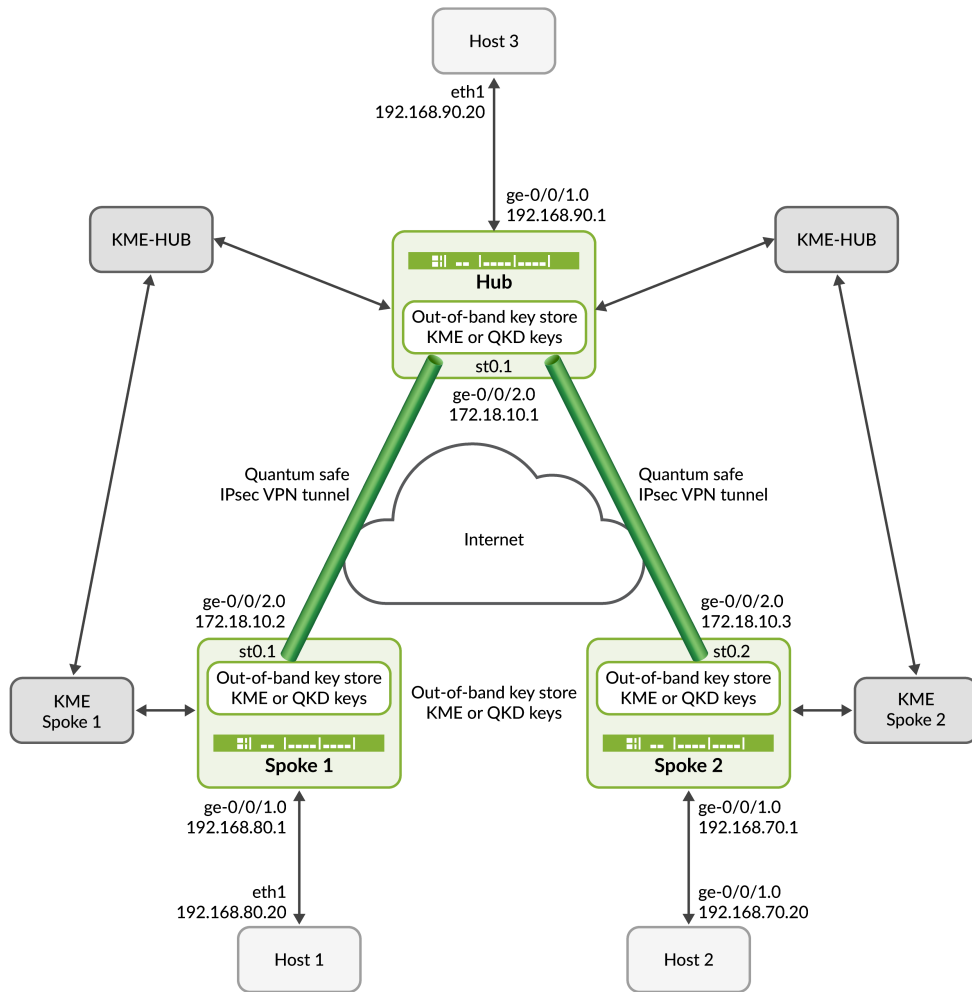


Figure 54: Quantum Key Manager (Continued)

| Entity      | IP Address                                                       | Port                                       |
|-------------|------------------------------------------------------------------|--------------------------------------------|
| HOST-1      | 192.168.1.10 LAN<br>192.168.1.10 SPOKE 1<br>192.168.1.10 SPOKE 1 | 192.168.1.10, HOST-3                       |
| HOST-2      | 192.168.1.11 LAN<br>192.168.1.11 SPOKE 2<br>192.168.1.11 SPOKE 2 | 192.168.1.11, HOST-3                       |
| HOST-3      | 192.168.1.12 LAN<br>192.168.1.12 Host 3<br>192.168.1.12 Hub      | 192.168.1.12 HOST-1<br>192.168.1.12 HOST-2 |
| KME-HUB     | 192.168.1.13 QKD                                                 | 192.168.1.13 QKD<br>HUB                    |
| KME-SPOKE-1 | 192.168.1.14 QKD                                                 | 192.168.1.14 QKD<br>SPOKE-1                |
| KME-SPOKE-2 | 192.168.1.15 QKD                                                 | 192.168.1.15 QKD<br>SPOKE-2                |

?? ??

## ?? 21: AutoVPN? Quantum Key Manager



jn-000641

???? ???? ??



?: ?? ? ??? ?????? ?? ?? ??? ??????.

- "?? 1 : ?? ??? ? ? ? ? ?" ??? 308
- "?? 2 : DUT ? ? ? ? ?" ??? 313

## 1. `?? ???? ??`.

```
[edit interfaces]
user@hub# set ge-0/0/2 unit 0 family inet address 172.18.10.1/24
user@hub# set ge-0/0/1 unit 0 family inet address 192.168.90.1/24
user@hub# set st0 unit 1 family inet
```

## 2. IPsec VPN `??-???? ?????. ???? ???? ID ? ? ? ? ? ? ? ? ? ?`, `?? ? ? ? ? ? ? ? ? ? ?`.

CA `????` CA `???? ???? ???? ? ? ? ? ? ? ? ? ? ?` CA `???? ???? ? ? ? ? ? ? ? ?`.



?: KME `???? ? ? ? ? ? ? ? ? ? ?`.

IPsec `?? ? ? ? ? ? ? ? ? ? ?`. IPsec VPN `??` IKE(Internet Key Exchange) `??`, `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones]
user@hub# set security-zone untrust host-inbound-traffic system-services ike
user@hub# set security-zone untrust interfaces ge-0/0/2.0
user@hub# set security-zone vpn interfaces st0.1
user@hub# set security-zone trust host-inbound-traffic system-services ping
user@hub# set security-zone trust interfaces ge-0/0/1.0
```

```
[edit security policies]
user@hub# set from-zone trust to-zone vpn policy vpn_out match source-address any
user@hub# set from-zone trust to-zone vpn policy vpn_out match destination-address any
user@hub# set from-zone trust to-zone vpn policy vpn_out match application any
user@hub# set from-zone trust to-zone vpn policy vpn_out then permit
user@hub# set from-zone vpn to-zone trust policy vpn_in match source-address any
user@hub# set from-zone vpn to-zone trust policy vpn_in match destination-address any
user@hub# set from-zone vpn to-zone trust policy vpn_in match application any
user@hub# set from-zone vpn to-zone trust policy vpn_in then permit
```

```
[edit security pki]
user@hub# set ca-profile Root-CA ca-identity Root-CA
```

```
user@hub# set ca-profile Root-CA enrollment url url-to-CA-server
user@hub# set ca-profile Root-CA revocation-check disable
```

```
user@hub> request security pki ca-certificate enroll ca-profile Root-CA
```

```
user@hub> request security pki generate-key-pair certificate-id HUB_CERT size 2048 type rsa
user@hub> request security pki local-certificate enroll certificate-id HUB_CERT challenge-
password password domain-name hub.juniper.net email hub@juniper.net subject
DC=juniper,CN=hub.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-profile
Root-CA
user@hub> request security pki local-certificate load certificate-id SAE_HUB filename
SAE_HUB.cert key SAE_HUB.key
```

```
[edit security ike proposal]
user@hub# set HUB_IKE_PROP authentication-method rsa-signatures
user@hub# set HUB_IKE_PROP dh-group group14
user@hub# set HUB_IKE_PROP authentication-algorithm sha-256
user@hub# set HUB_IKE_PROP encryption-algorithm aes-256-cbc
user@hub# set HUB_IKE_PROP lifetime-seconds 3600
```

```
[edit security ike policy]
user@hub# set HUB_IKE_POL proposals HUB_IKE_PROP
user@hub# set HUB_IKE_POL certificate local-certificate HUB_CERT
```

```
[edit security ike gateway]
user@hub# set HUB_IKE_GW local-address 172.18.10.1
user@hub# set HUB_IKE_GW ike-policy HUB_IKE_POL
user@hub# set HUB_IKE_GW external-interface ge-0/0/2.0
user@hub# set HUB_IKE_GW local-identity distinguished-name
user@hub# set HUB_IKE_GW dynamic ike-user-type group-ike-id
```



```
user@hub# set HUB_IKE_GW dynamic distinguished-name wildcard C=us,DC=juniper
user@hub# set HUB_IKE_GW version v2-only
```

```
[edit security ipsec proposal]
user@hub# set HUB_IPSEC_PROP protocol esp
user@hub# set HUB_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@hub# set HUB_IPSEC_PROP encryption-algorithm aes-256-cbc
```

```
[edit security ipsec vpn]
user@hub# set HUB_IPSEC_VPN bind-interface st0.1
user@hub# set HUB_IPSEC_VPN ike gateway HUB_IKE_GW
user@hub# set HUB_IPSEC_VPN ike ipsec-policy HUB_IPSEC_POL
user@hub# set HUB_IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
user@hub# set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0
```

```
[edit security ipsec policy]
user@hub# set HUB_IPSEC_POL proposals HUB_IPSEC_PROP
```

### 3. `set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0`.

```
[edit security key-manager profiles]
user@hub# set HUB_KM_PROFILE_1 quantum-key-manager url kme-server-url
set security key-manager profiles HUB_KM_PROFILE_1 quantum-key-manager local-sae-id SAE_HUB
user@hub# set HUB_KM_PROFILE_1 quantum-key-manager local-certificate-id SAE_HUB_CERT
user@hub# set HUB_KM_PROFILE_1 quantum-key-manager trusted-cas Root-CA
```

### 4. `set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0`.

```
[edit security ike gateway]
user@hub# set HUB_IKE_GW ppk-profile HUB_KM_PROFILE_1
```

`commit` (press `Enter`)



```
user@spoke# set from-zone vpn to-zone trust policy vpn_in match application any
user@spoke# set from-zone vpn to-zone trust policy vpn_in then permit
```

```
[edit security pki]
user@spoke# set ca-profile Root-CA ca-identity Root-CA
user@spoke# set ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
user@spoke# set ca-profile Root-CA revocation-check disable
```

```
user@spoke> request security pki ca-certificate enroll ca-profile Root-CA
```

```
user@spoke> request security pki generate-key-pair certificate-id SPOKE_1_CRT size 2048 type
rsa
user@spoke> request security pki local-certificate enroll certificate-id SPOKE_1_CRT
challenge-password <password> domain-name spoke_1.juniper.net email spoke_1@juniper.net
subject
DC=juniper,CN=spoke_1.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA
user@spoke> request security pki local-certificate load certificate-id SAE_SPOKE_1 filename
SAE_SPOKE_1.cert key SAE_SPOKE_1.key
```

```
[edit security ike proposal]
user@spoke# set SPOKE_1_IKE_PROP authentication-method rsa-signatures
user@spoke# set SPOKE_1_IKE_PROP dh-group group14
user@spoke# set SPOKE_1_IKE_PROP authentication-algorithm sha-256
user@spoke# set SPOKE_1_IKE_PROP encryption-algorithm aes-256-cbc
user@spoke# set SPOKE_1_IKE_PROP lifetime-seconds 3600
```

```
[edit security ike policy]
user@spoke# set SPOKE_1_IKE_POL proposals SPOKE_1_IKE_PROP
user@spoke# set SPOKE_1_IKE_POL certificate local-certificate SPOKE_1_CRT
```

```
[edit security ike gateway]
user@spoke# set SPOKE_1_IKE_GW address 172.18.10.1
user@spoke# set SPOKE_1_IKE_GW local-address 172.18.10.2
```

```

user@spoke# set SPOKE_1_IKE_GW ike-policy SPOKE_1_IKE_POL
user@spoke# set SPOKE_1_IKE_GW external-interface ge-0/0/2.0
user@spoke# set SPOKE_1_IKE_GW local-identity distinguished-name
user@spoke# set SPOKE_1_IKE_GW remote-identity distinguished-name
user@spoke# set SPOKE_1_IKE_GW version v2-only

```

```

[edit security ipsec proposal]
user@spoke# set SPOKE_1_IPSEC_PROP protocol esp
user@spoke# set SPOKE_1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@spoke# set SPOKE_1_IPSEC_PROP encryption-algorithm aes-256-cbc

```

```

[edit security ipsec vpn]
user@spoke# set SPOKE_1_IPSEC_VPN bind-interface st0.1
user@spoke# set SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW
user@spoke# set SPOKE_1_IPSEC_VPN ike ipsec-policy SPOKE_1_IPSEC_POL
user@spoke# set SPOKE_1_IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
user@spoke# set SPOKE_1_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24

```

```

[edit security ipsec policy]
user@spoke# set SPOKE_1_IPSEC_POL proposals SPOKE_1_IPSEC_PROP

```

### 3. `set security ipsec vpn SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW`.

```

[edit security key-manager profiles]
user@spoke# set SPOKE_1_KM_PROFILE_1 quantum-key-manager url https://www.kme_spoke_1-qkd-
server.net
user@spoke# set SPOKE_1_KM_PROFILE_1 quantum-key-manager local-sae-id SAE_SPOKE_1
user@spoke# set SPOKE_1_KM_PROFILE_1 quantum-key-manager local-certificate-id SAE_SPOKE_1_CERT
user@spoke# set profiles SPOKE_1_KM_PROFILE_1 quantum-key-manager trusted-cas Root-CA

```

### 4. `set security ipsec vpn SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW`.

```

[edit security ike gateway]
user@spoke# set SPOKE_1_IKE_GW ppk-profile SPOKE_1_KM_PROFILE_1

```

`commit`

??

in this section

- [IKE\(Internet Key Exchange\) SA ?? | 299](#)
- [IPsec SA ?? | 303](#)
- [IPsec ?? ?? | 305](#)
- [? ??? ??? ? | 306](#)
- [??? 1?? ??? 3?? Ping | 307](#)
- [??? 2?? ??? 3?? Ping | 307](#)

? ????? ? ??? ???? ? ???? ? ? show ?? ??? ????.

? 55: ?? ??

| ???                                       | ?? ??                                                           |
|-------------------------------------------|-----------------------------------------------------------------|
| ?? ike ?? ?? ?? ??                        | <a href="#">"IKE(Internet Key Exchange) SA? ?????." ??? 299</a> |
| ?? ipsec ?? ?? ?? ??                      | <a href="#">"IPsec SA? ?????." ??? 303</a>                      |
| ?? ipsec ?? ??                            | <a href="#">"IPsec ??? ? ??? ??? ?????." ??? 305</a>            |
| ?? ? ??? ??? ? ? ?                        | <a href="#">"? ??? ??? ?????." ??? 306</a>                      |
| ping 192.168.90.20 ?? 192.168.80.20 ??? 4 | <a href="#">"??? 1?? ??? 3?? ping???" ??? 307</a>               |
| ping 192.168.90.20 ?? 192.168.70.20 ??? 4 | <a href="#">"??? 2?? ??? 3?? ping???" ??? 307</a>               |

IKE(Internet Key Exchange) SA ??

??

IKE(Internet Key Exchange) SA? ?????.

??

?? ???? ???? show security ike security-associations detail IKE(Internet Key Exchange) SA? ?????.

```
user@hub> show security ike security-associations detail
```

```
IKE peer 172.18.10.3, Index 2161, Gateway Name: HUB_IKE_GW
```

```
Role: Responder, State: UP
```

```
Initiator cookie: bccc74c70f0b81b9, Responder cookie: 872d364f15b29c28
```

```
Exchange type: IKEv2, Authentication method: RSA-signatures
```

```
Local gateway interface: ge-0/0/2.0
```

```
Routing instance: default
```

```
Local: 172.18.10.1:500, Remote: 172.18.10.3:500
```

```
Lifetime: Expires in 3464 seconds
```

```
Reauth Lifetime: Disabled
```

```
IKE Fragmentation: Enabled, Size: 576
```

```
Remote Access Client Info: Unknown Client
```

```
Peer ike-id: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke_2.juniper.net
```

```
AAA assigned IP: 0.0.0.0
```

```
PPK-profile: HUB_KM_PROFILE_1
```

```
Optional: No
```

```
State : Used
```

```
Algorithms:
```

```
Authentication : hmac-sha256-128
```

```
Encryption : aes256-cbc
```

```
Pseudo random function: hmac-sha256
```

```
Diffie-Hellman group : DH-group-14
```

```
Traffic statistics:
```

```
Input bytes : 2661
```

```
Output bytes : 2586
```

```
Input packets: 5
```

```
Output packets: 5
```

```
Input fragmented packets: 4
```

```
Output fragmented packets: 4
```

```
IPSec security associations: 2 created, 0 deleted
```

```
Phase 2 negotiations in progress: 1
```

```
IPSec Tunnel IDs: 500446
```

```
Negotiation type: Quick mode, Role: Responder, Message ID: 0
```

```
Local: 172.18.10.1:500, Remote: 172.18.10.3:500
```

```
Local identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,
```

CN=hub.juniper.net

Remote identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke\_2.juniper.net

Flags: IKE SA is created

IPsec SA Rekey CREATE\_CHILD\_SA exchange stats:

| Initiator stats:          |     | Responder stats:         |   |
|---------------------------|-----|--------------------------|---|
| Request Out               | : 0 | Request In               | : |
| 0                         |     |                          |   |
| Response In               | : 0 | Response Out             | : |
| 0                         |     |                          |   |
| No Proposal Chosen In     | : 0 | No Proposal Chosen Out   | : |
| 0                         |     |                          |   |
| Invalid KE In             | : 0 | Invalid KE Out           | : |
| 0                         |     |                          |   |
| TS Unacceptable In        | : 0 | TS Unacceptable Out      | : |
| 0                         |     |                          |   |
| Res DH Compute Key Fail   | : 0 | Res DH Compute Key Fail: |   |
| 0                         |     |                          |   |
| Res Verify SA Fail        | : 0 |                          |   |
| Res Verify DH Group Fail: | 0   |                          |   |
| Res Verify TS Fail        | : 0 |                          |   |

IKE peer 172.18.10.2, Index 2162, Gateway Name: HUB\_IKE\_GW

Role: Responder, State: UP

Initiator cookie: 5e17d5924c619788, Responder cookie: 15f1e3c4252ba6f8

Exchange type: IKEv2, Authentication method: RSA-signatures

Local gateway interface: ge-0/0/2.0

Routing instance: default

Local: 172.18.10.1:500, Remote: 172.18.10.2:500

Lifetime: Expires in 3464 seconds

Reauth Lifetime: Disabled

IKE Fragmentation: Enabled, Size: 576

Remote Access Client Info: Unknown Client

Peer ike-id: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,  
CN=spoke.juniper.net

AAA assigned IP: 0.0.0.0

PPK-profile: HUB\_KM\_PROFILE\_1

Optional: No

State : Used

Algorithms:

Authentication : hmac-sha256-128

Encryption : aes256-cbc

```
Pseudo random function: hmac-sha256
Diffie-Hellman group   : DH-group-14
Traffic statistics:
Input  bytes   :           2645
Output bytes   :           2586
Input  packets :             5
Output packets :             5
Input  fragmented packets:    4
Output fragmented packets:    4
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1
IPSec Tunnel IDs: 500447

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 172.18.10.1:500, Remote: 172.18.10.2:500
Local identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,
CN=hub.juniper.net
Remote identity: C=us, DC=juniper, ST=california, L=sunnyvale, O=juniper, OU=security,
CN=spoke.juniper.net
Flags: IKE SA is created

IPsec SA Rekey CREATE_CHILD_SA exchange stats:
Initiator stats:
Request Out           : 0
0
Response In           : 0
0
No Proposal Chosen In : 0
0
Invalid KE In         : 0
0
TS Unacceptable In    : 0
0
Res DH Compute Key Fail : 0
0
Res Verify SA Fail    : 0
Res Verify DH Group Fail: 0
Res Verify TS Fail    : 0

Responder stats:
Request In            :
Response Out          :
No Proposal Chosen Out :
Invalid KE Out        :
TS Unacceptable Out   :
Res DH Compute Key Fail:
```

??

?? ???? IKE(Internet Key Exchange) SA? ??????.



IPsec SA [?]

[?]

IPsec SA [?] [?].

[?]

[?] [?] [?] [?] show security ipsec security-associations detail IPsec SA [?] [?].

```
user@hub> show security ipsec security-associations detail
```

```
ID: 500446 Virtual-system: root, VPN Name: HUB_IPSEC_VPN
Local Gateway: 172.18.10.1, Remote Gateway: 172.18.10.3
Traffic Selector Name: ts1
Local Identity: ipv4(192.168.90.0-192.168.90.255)
Remote Identity: ipv4(192.168.70.0-192.168.70.255)
TS Type: traffic-selector
Version: IKEv2
Quantum Secured: Yes
PFS group: N/A
Passive mode tunneling: Disabled
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: HUB_IPSEC_POL
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0
Multi-sa, Configured SAs# 0, Negotiated SAs#: 0
Tunnel events:
  Fri Jul 21 2023 00:31:08: IPsec SA negotiation succeeds (1 times)
Location: FPC 0, PIC 0
Anchorship: Thread 1
Distribution-Profile: default-profile
Direction: inbound, SPI: 0xcf48c0c9, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3464 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2778 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2161
```

Direction: outbound, SPI: 0x86c9ba76, AUX-SPI: 0  
 , VPN Monitoring: -  
 Hard lifetime: Expires in 3464 seconds  
 Lifesize Remaining: Unlimited  
 Soft lifetime: Expires in 2778 seconds  
 Mode: Tunnel(0 0), Type: dynamic, State: installed  
 Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)  
 Anti-replay service: counter-based enabled, Replay window size: 64  
 Extended-Sequence-Number: Disabled  
 tunnel-establishment: establish-tunnels-responder-only  
 IKE SA Index: 2161

ID: 500447 Virtual-system: root, VPN Name: HUB\_IPSEC\_VPN  
 Local Gateway: 172.18.10.1, Remote Gateway: 172.18.10.2  
 Traffic Selector Name: ts1  
 Local Identity: ipv4(192.168.90.0-192.168.90.255)  
 Remote Identity: ipv4(192.168.80.0-192.168.80.255)  
 TS Type: traffic-selector  
 Version: IKEv2  
 Quantum Secured: Yes  
 PFS group: N/A  
 Passive mode tunneling: Disabled  
 DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.1, Policy-name: HUB\_IPSEC\_POL  
 Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0  
 Multi-sa, Configured SAs# 0, Negotiated SAs#: 0  
 Tunnel events:  
 Fri Jul 21 2023 00:31:08: IPsec SA negotiation succeeds (1 times)  
 Location: FPC 0, PIC 0  
 Anchorship: Thread 1  
 Distribution-Profile: default-profile  
 Direction: inbound, SPI: 0x4275d756, AUX-SPI: 0  
 , VPN Monitoring: -  
 Hard lifetime: Expires in 3464 seconds  
 Lifesize Remaining: Unlimited  
 Soft lifetime: Expires in 2772 seconds  
 Mode: Tunnel(0 0), Type: dynamic, State: installed  
 Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)  
 Anti-replay service: counter-based enabled, Replay window size: 64  
 Extended-Sequence-Number: Disabled  
 tunnel-establishment: establish-tunnels-responder-only  
 IKE SA Index: 2162  
 Direction: outbound, SPI: 0xe37b5568, AUX-SPI: 0  
 , VPN Monitoring: -

```

Hard lifetime: Expires in 3464 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2772 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha256-128, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Extended-Sequence-Number: Disabled
tunnel-establishment: establish-tunnels-responder-only
IKE SA Index: 2162

```

??

?? ??? IPsec SA? ?????.

**IPsec** ?? ??

??

IPsec ??? ?????.

??

?? ????? ??? ????? show security ipsec statistics IPsec ??? ?????.

```

user@hub> show security ipsec statistics

```

ESP Statistics:

```

Encrypted bytes:      1560
Decrypted bytes:      1560
Encrypted packets:    10
Decrypted packets:    10

```

AH Statistics:

```

Input bytes:          0
Output bytes:          0
Input packets:         0
Output packets:        0

```

Errors:

```

AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
Invalid SPI: 0, TS check fail: 0

```

Exceeds tunnel MTU: 0  
Discarded: 0

??

?? ??? IPsec ??? ?????.

? ??? ????? ??

??

? ??? ????? ?????.

??

?? ????? ?? ???? show security key-manager profiles detail ??? Request stats ??? ??????Success.

```
user@hub> show security key-manager profiles detail

Name: HUB_KM_PROFILE_1, Index: 6, Type: Quantum-key-manager
Configured-at: 21.07.23 (00:14:00)
Time-elapsed: 0 hrs 19 mins 24 secs
Url: https://kme.juniper.net:8080
Local-sae-id: SAE_HUB
Local-certificate-id: SAE_HUB_CERT
Trusted-cas: [ ROOT_CA_CERT ]
Peer-sae-ids: N/A
Default-key-size: N/A
Request stats:
  Received: 2
  In-progress: 0
  Success: 2
  Failed: 0
```

??

?? ??? ? ? ???? ?????.

**?? 1?? ?? 3?? Ping****??****?? 1?? ?? 3??? ?? ?????.****??****?? ???? ?? ???? ping 192.168.90.20 source 192.168.80.20 count 5 Host 1?? Host 3??? ?? ?????.**

```

user@host1# ping 192.168.90.20 source 192.168.80.20 count 5
PING 192.168.90.20 (192.168.90.20): 56 data bytes
64 bytes from 192.168.90.20: icmp_seq=0 ttl=64 time=2.151 ms
64 bytes from 192.168.90.20: icmp_seq=1 ttl=64 time=1.710 ms
64 bytes from 192.168.90.20: icmp_seq=2 ttl=64 time=1.349 ms
64 bytes from 192.168.90.20: icmp_seq=3 ttl=64 time=1.597 ms
64 bytes from 192.168.90.20: icmp_seq=4 ttl=64 time=1.515 ms
--- 192.168.90.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.349/1.702/2.151/0.290 ms

```

Data traffic is successfully flowing between the HOSTs

**??****?? ???? ?? 1?? ?? 3??? ?? ?????.****?? 2?? ?? 3?? Ping****??****?? 2?? ?? 3??? ?? ?????.****??****?? ???? ?? ???? ping 192.168.90.20 source 192.168.80.20 count 5 Host 2?? Host 3??? ?? ?????.**

```

user@host2# ping 192.168.90.20 source 192.168.70.20 count 5
PING 192.168.90.20 (192.168.90.20): 56 data bytes
64 bytes from 192.168.90.20: icmp_seq=0 ttl=64 time=2.151 ms

```

```

64 bytes from 192.168.90.20: icmp_seq=1 ttl=64 time=1.710 ms
64 bytes from 192.168.90.20: icmp_seq=2 ttl=64 time=1.349 ms
64 bytes from 192.168.90.20: icmp_seq=3 ttl=64 time=1.597 ms
64 bytes from 192.168.90.20: icmp_seq=4 ttl=64 time=1.759 ms
--- 192.168.90.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.349/1.702/2.151/0.290 ms

```

Data traffic is successfully flowing between the HOSTs

??

?? ??? ??? 2?? ??? 3??? ??? ????

?? 1 : ?? ??? ?? ?? ??

?? ????? ?? ??? ??????

???? ? ? ?

```

set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
set security pki ca-profile Root-CA revocation-check disable
request security pki ca-certificate enroll ca-profile Root-CA
request security pki generate-key-pair certificate-id HUB_CRT size 2048 type rsa
request security pki local-certificate enroll certificate-id HUB_CRT challenge-password
<password> domain-name hub.juniper.net email hub@juniper.net subject
DC=juniper,CN=hub.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-profile
Root-CA
request security pki local-certificate load certificate-id SAE_HUB filename SAE_HUB.cert key
SAE_HUB.key
set security key-manager profiles HUB_KM_PROFILE_1 quantum-key-manager url https://www.kme_hub-
qkd-server.net
set security key-manager profiles HUB_KM_PROFILE_1 quantum-key-manager local-sae-id SAE_HUB
set security key-manager profiles HUB_KM_PROFILE_1 quantum-key-manager local-certificate-id
SAE_HUB_CERT
set security key-manager profiles HUB_KM_PROFILE_1 quantum-key-manager trusted-cas Root-CA
set security ike proposal HUB_IKE_PROP authentication-method rsa-signatures
set security ike proposal HUB_IKE_PROP dh-group group14

```

```

set security ike proposal HUB_IKE_PROP authentication-algorithm sha-256
set security ike proposal HUB_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal HUB_IKE_PROP lifetime-seconds 3600
set security ike policy HUB_IKE_POL proposals HUB_IKE_PROP
set security ike policy HUB_IKE_POL certificate local-certificate HUB_CERT
set security ike gateway HUB_IKE_GW local-address 172.18.10.1
set security ike gateway HUB_IKE_GW ike-policy HUB_IKE_POL
set security ike gateway HUB_IKE_GW external-interface ge-0/0/2.0
set security ike gateway HUB_IKE_GW local-identity distinguished-name
set security ike gateway HUB_IKE_GW dynamic ike-user-type group-ike-id
set security ike gateway HUB_IKE_GW dynamic distinguished-name wildcard C=us,DC=juniper
set security ike gateway HUB_IKE_GW ppk-profile HUB_KM_PROFILE_1
set security ike gateway HUB_IKE_GW version v2-only
set security ipsec proposal HUB_IPSEC_PROP protocol esp
set security ipsec proposal HUB_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal HUB_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy HUB_IPSEC_POL proposals HUB_IPSEC_PROP
set security ipsec vpn HUB_IPSEC_VPN bind-interface st0.1
set security ipsec vpn HUB_IPSEC_VPN ike gateway HUB_IKE_GW
set security ipsec vpn HUB_IPSEC_VPN ike ipsec-policy HUB_IPSEC_POL
set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 local-ip 192.168.90.0/24
set security ipsec vpn HUB_IPSEC_VPN traffic-selector ts1 remote-ip 0.0.0.0/0
set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.1/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.90.1/24
set interfaces st0 unit 1 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```

?? 1?? ?? ??

```

set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
set security pki ca-profile Root-CA revocation-check disable
request security pki ca-certificate enroll ca-profile Root-CA
request security pki generate-key-pair certificate-id SPOKE_1_CRT size 2048 type rsa
request security pki local-certificate enroll certificate-id SPOKE_1_CRT challenge-password
<password> domain-name spoke_1.juniper.net email spoke_1@juniper.net subject
DC=juniper,CN=spoke_1.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA
request security pki local-certificate load certificate-id SAE_SPOKE_1 filename SAE_SPOKE_1.cert
key SAE_SPOKE_1.key
set security key-manager profiles SPOKE_1_KM_PROFILE_1 quantum-key-manager url https://
www.kme_spoke_1-qkd-server.net
set security key-manager profiles SPOKE_1_KM_PROFILE_1 quantum-key-manager local-sae-id
SAE_SPOKE_1
set security key-manager profiles SPOKE_1_KM_PROFILE_1 quantum-key-manager local-certificate-id
SAE_SPOKE_1_CERT
set security key-manager profiles SPOKE_1_KM_PROFILE_1 quantum-key-manager trusted-cas Root-CA
set security ike proposal SPOKE_1_IKE_PROP authentication-method rsa-signatures
set security ike proposal SPOKE_1_IKE_PROP dh-group group14
set security ike proposal SPOKE_1_IKE_PROP authentication-algorithm sha-256
set security ike proposal SPOKE_1_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SPOKE_1_IKE_PROP lifetime-seconds 3600
set security ike policy SPOKE_1_IKE_POL proposals SPOKE_1_IKE_PROP
set security ike policy SPOKE_1_IKE_POL certificate local-certificate SPOKE_1_CRT
set security ike gateway SPOKE_1_IKE_GW address 172.18.10.1
set security ike gateway SPOKE_1_IKE_GW local-address 172.18.10.2
set security ike gateway SPOKE_1_IKE_GW ike-policy SPOKE_1_IKE_POL
set security ike gateway SPOKE_1_IKE_GW external-interface ge-0/0/2.0
set security ike gateway SPOKE_1_IKE_GW local-identity distinguished-name
set security ike gateway SPOKE_1_IKE_GW remote-identity distinguished-name
set security ike gateway SPOKE_1_IKE_GW ppk-profile SPOKE_1_KM_PROFILE_1
set security ike gateway SPOKE_1_IKE_GW version v2-only
set security ipsec proposal SPOKE_1_IPSEC_PROP protocol esp
set security ipsec proposal SPOKE_1_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SPOKE_1_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy SPOKE_1_IPSEC_POL proposals SPOKE_1_IPSEC_PROP
set security ipsec vpn SPOKE_1_IPSEC_VPN bind-interface st0.1

```



```

set security ipsec vpn SPOKE_1_IPSEC_VPN ike gateway SPOKE_1_IKE_GW
set security ipsec vpn SPOKE_1_IPSEC_VPN ike ipsec-policy SPOKE_1_IPSEC_POL
set security ipsec vpn SPOKE_1_IPSEC_VPN traffic-selector ts1 local-ip 192.168.80.0/24
set security ipsec vpn SPOKE_1_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.2/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.80.1/24
set interfaces st0 unit 1 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```

?? 2?? ?? ??

```

set security pki ca-profile Root-CA ca-identity Root-CA
set security pki ca-profile Root-CA enrollment url https://ca-server.juniper.net/certsrv/mscep/
mscep.dll
set security pki ca-profile Root-CA revocation-check disable
request security pki ca-certificate enroll ca-profile Root-CA
request security pki generate-key-pair certificate-id SPOKE_2_CRT size 2048 type rsa
request security pki local-certificate enroll certificate-id SPOKE_2_CRT challenge-password
<password> domain-name spoke_2.juniper.net email spoke_2@juniper.net subject
DC=juniper,CN=spoke_2.juniper.net,OU=security,O=juniper,L=sunnyvale,ST=california,C=us ca-
profile Root-CA
request security pki local-certificate load certificate-id SAE_SPOKE_2 filename SAE_SPOKE_2.cert
key SAE_SPOKE_2.key
set security key-manager profiles SPOKE_2_KM_PROFILE_1 quantum-key-manager url https://
www.kme_spoke_2-qkd-server.net
set security key-manager profiles SPOKE_2_KM_PROFILE_1 quantum-key-manager local-sae-id
SAE_SPOKE_2
set security key-manager profiles SPOKE_2_KM_PROFILE_1 quantum-key-manager local-certificate-id

```

```

SAE_SPOKE_2_CERT
set security key-manager profiles SPOKE_2_KM_PROFILE_1 quantum-key-manager trusted-cas Root-CA
set security ike proposal SPOKE_2_IKE_PROP authentication-method rsa-signatures
set security ike proposal SPOKE_2_IKE_PROP dh-group group14
set security ike proposal SPOKE_2_IKE_PROP authentication-algorithm sha-256
set security ike proposal SPOKE_2_IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal SPOKE_2_IKE_PROP lifetime-seconds 3600
set security ike policy SPOKE_2_IKE_POL proposals SPOKE_IKE_PROP
set security ike policy SPOKE_2_IKE_POL certificate local-certificate SPOKE_2_CERT
set security ike gateway SPOKE_2_IKE_GW address 172.18.10.1
set security ike gateway SPOKE_2_IKE_GW local-address 172.18.10.3
set security ike gateway SPOKE_2_IKE_GW ike-policy SPOKE_2_IKE_POL
set security ike gateway SPOKE_2_IKE_GW external-interface ge-0/0/2.0
set security ike gateway SPOKE_2_IKE_GW local-identity distinguished-name
set security ike gateway SPOKE_2_IKE_GW remote-identity distinguished-name
set security ike gateway SPOKE_2_IKE_GW ppk-profile SPOKE_2_KM_PROFILE_1
set security ike gateway SPOKE_2_IKE_GW version v2-only
set security ipsec proposal SPOKE_2_IPSEC_PROP protocol esp
set security ipsec proposal SPOKE_2_IPSEC_PROP authentication-algorithm hmac-sha-256-128
set security ipsec proposal SPOKE_2_IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy SPOKE_2_IPSEC_POL proposals SPOKE_2_IPSEC_PROP
set security ipsec vpn SPOKE_2_IPSEC_VPN bind-interface st0.2
set security ipsec vpn SPOKE_2_IPSEC_VPN ike gateway SPOKE_2_IKE_GW
set security ipsec vpn SPOKE_2_IPSEC_VPN ike ipsec-policy SPOKE_2_IPSEC_POL
set security ipsec vpn SPOKE_2_IPSEC_VPN traffic-selector ts1 local-ip 192.168.70.0/24
set security ipsec vpn SPOKE_2_IPSEC_VPN traffic-selector ts1 remote-ip 192.168.90.0/24
set interfaces ge-0/0/2 unit 0 family inet address 172.18.10.3/24
set interfaces ge-0/0/1 unit 0 family inet address 192.168.70.1/24
set interfaces st0 unit 2 family inet
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone vpn interfaces st0.2
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security policies from-zone trust to-zone vpn policy vpn_out match source-address any
set security policies from-zone trust to-zone vpn policy vpn_out match destination-address any
set security policies from-zone trust to-zone vpn policy vpn_out match application any
set security policies from-zone trust to-zone vpn policy vpn_out then permit
set security policies from-zone vpn to-zone trust policy vpn_in match source-address any
set security policies from-zone vpn to-zone trust policy vpn_in match destination-address any
set security policies from-zone vpn to-zone trust policy vpn_in match application any
set security policies from-zone vpn to-zone trust policy vpn_in then permit

```



```
    }
}
```

```
user@hub# show security ike proposal HUB_IKE_PROP
authentication-method rsa-signatures;
dh-group group14;
authentication-algorithm sha-256;
encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;
```

```
user@hub# show security ike policy HUB_IKE_POL
proposals HUB_IKE_PROP;
certificate {
    local-certificate HUB_CRT;
}
```

```
user@hub# show security ike gateway HUB_IKE_GW
ike-policy HUB_IKE_POL;
dynamic {
    distinguished-name {
        wildcard C=us,DC=juniper;
    }
    ike-user-type group-ike-id;
}
local-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.1;
version v2-only;
ppk-profile HUB_KM_PROFILE_1;
```

```
user@hub# show security ipsec proposal HUB_IPSEC_PROP
protocol esp;
```

```
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;
```

```
user@hub# show security ipsec policy HUB_IPSEC_POL
proposals HUB_IPSEC_PROP;
```

```
user@hub# show security ipsec vpn HUB_IPSEC_VPN
bind-interface st0.1;
ike {
    gateway HUB_IKE_GW;
    ipsec-policy HUB_IPSEC_POL;
}
traffic-selector ts1 {
    local-ip 192.168.90.0/24;
    remote-ip 0.0.0.0/0;
}
```

```
user@hub# show security zones security-zone untrust
host-inbound-traffic {
    system-services {
        ike;
    }
}
interfaces {
    ge-0/0/0.0;
    ge-0/0/2.0;
}
```

```
user@hub# show security zones security-zone trust
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
```

```

    ge-0/0/1.0;
}

```

```

user@hub# show security policies from-zone trust to-zone vpn
policy vpn_out {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

```

```

user@hub# show security policies from-zone vpn to-zone trust
policy vpn_in {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

```

```

user@hub# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
        }
    }
}

```

```

    }
}

ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
        }
    }
}

st0 {
    unit 1 {
        family inet;
    }
}

```

```
trusted-cas Root-CA;
}
```

```
user@spoke1# show security ike proposal SPOKE_1_IKE_PROP
authentication-method rsa-signatures;
dh-group group14;
authentication-algorithm sha-256;
encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;
```

```
user@spoke1# show security ike policy SPOKE_1_IKE_POL
proposals SPOKE_1_IKE_PROP;
certificate {
    local-certificate SPOKE_1_CRT;
}
```

```
user@spoke1# show security ike gateway SPOKE_1_IKE_GW
ike-policy SPOKE_1_IKE_POL;
address 172.18.10.1;
local-identity distinguished-name;
remote-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.2;
version v2-only;
ppk-profile SPOKE_1_KM_PROFILE_1;
```

```
user@spoke1# show security ipsec proposal SPOKE_1_IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;
```

```
user@spoke1# show security ipsec vpn SPOKE_1_IPSEC_VPN
bind-interface st0.1;
ike {
    gateway SPOKE_1_IKE_GW;
    ipsec-policy SPOKE_1_IPSEC_POL;
```



```

}
traffic-selector ts1 {
    local-ip 192.168.80.0/24;
    remote-ip 192.168.90.0/24;
}

```

```

user@spoke1# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}

```

```

user@spoke1# show security zones security-zone untrust
host-inbound-traffic {
    system-services {
        ike;
    }
}

```

```

    }
}
interfaces {
    ge-0/0/0.0;
    ge-0/0/2.0;
}

```

```

user@spoke1# show security zones security-zone trust
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    ge-0/0/1.0;
}

```

```

user@spoke1# show security policies from-zone trust to-zone vpn
policy vpn_out {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

```

```

user@spoke1# security policies from-zone vpn to-zone trust
policy vpn_in {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}

```

```
    }
}
```

## 2

user@spoke2# show security key-manager profiles SPOKE\_1\_KM\_PROFILE\_1, show security ike policy SPOKE\_1\_IKE\_POL show interfaces show security ipsec vpn SPOKE\_1\_IPSEC\_VPN show security zones security-zone untrust show security ipsec policy SPOKE\_1\_IPSEC\_POL show security policies from-zone vpn to-zone trust show security ike proposal SPOKE\_1\_IKE\_PROP show security policies from-zone trust to-zone vpn show security ike gateway SPOKE\_1\_IKE\_GW show security zones security-zone trust show security ipsec proposal SPOKE\_1\_IPSEC\_PROP user@spoke2# show security pki ca-profile Root-CA user@spoke2# show security pki ca-profile Root-CA

```
user@spoke2# show security pki ca-profile Root-CA
ca-identity Root-CA;
enrollment {
    url https://ca-server.juniper.net/certsrv/mscep/mscep.dll;
}
revocation-check {
    disable;
}
```

```
user@spoke2# show security key-manager profiles SPOKE_2_KM_PROFILE_1
quantum-key-manager {
    url https://www.kme_spoke_2-qkd-server.net;
    local-sae-id SAE_SPOKE_2;
    local-certificate-id SAE_SPOKE_2_CERT;
    trusted-cas Root-CA;
}
```

```
user@spoke2# show security ike proposal SPOKE_2_IKE_PROP
authentication-method rsa-signatures;
dh-group group14;
authentication-algorithm sha-256;
```

```

encryption-algorithm aes-256-cbc;
lifetime-seconds 3600;

```

```

user@spoke2# show security ike policy SPOKE_2_IKE_POL
##
## Warning: Referenced proposal is not defined
##
proposals SPOKE_IKE_PROP;
certificate {
    local-certificate SPOKE_2_CRT;
}

```

```

user@spoke2# show security ike gateway SPOKE_2_IKE_GW
ike-policy SPOKE_2_IKE_POL;
address 172.18.10.1;
local-identity distinguished-name;
remote-identity distinguished-name;
external-interface ge-0/0/2.0;
local-address 172.18.10.3;
version v2-only;
ppk-profile SPOKE_2_KM_PROFILE_1;

```

```

user@spoke2# show security ipsec proposal SPOKE_2_IPSEC_PROP
protocol esp;
authentication-algorithm hmac-sha-256-128;
encryption-algorithm aes-256-cbc;

```

```

user@spoke2# show security ipsec policy SPOKE_2_IPSEC_POL
proposals SPOKE_2_IPSEC_PROP;

[edit]
user@spoke2# show security ipsec vpn SPOKE_2_IPSEC_VPN
bind-interface st0.2;
ike {
    gateway SPOKE_2_IKE_GW;
    ipsec-policy SPOKE_2_IPSEC_POL;
}

```

```

traffic-selector ts1 {
    local-ip 192.168.70.0/24;
    remote-ip 192.168.90.0/24;
}

```

```

user@spoke2# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 192.168.90.1/24;
            address 192.168.80.1/24;
            address 192.168.70.1/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.18.10.1/24;
            address 172.18.10.2/24;
            address 172.18.10.3/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
    unit 2 {
        family inet;
    }
}

```

```
    }
}
```

```
user@spoke2# show security zones security-zone untrust
host-inbound-traffic {
    system-services {
        ike;
    }
}
interfaces {
    ge-0/0/0.0;
    ge-0/0/2.0;
}
```

```
user@spoke2# show security zones security-zone vpn
interfaces {
    st0.1;
    st0.2;
}
```

```
user@spoke2# show security zones security-zone trust
host-inbound-traffic {
    system-services {
        ping;
    }
}
interfaces {
    ge-0/0/1.0;
}
```

```
user@spoke2# show security policies from-zone trust to-zone vpn
policy vpn_out {
    match {
        source-address any;
        destination-address any;
        application any;
    }
}
```

```
    then {  
        permit;  
    }  
}
```

```
user@spoke2# show security policies from-zone vpn to-zone trust  
policy vpn_in {  
    match {  
        source-address any;  
        destination-address any;  
        application any;  
    }  
    then {  
        permit;  
    }  
}
```

# 4

CHAPTER LABEL COVER PAGE

## ?? ?? VPN

---

### in this chapter

- ?? ?? IPsec VPNs | 327
  - ????? ?? ?? IPsec VPN ?? | 355
  - ??? ?? ??? ?? OCSP? ????? IPsec VPN ?? | 387
  - IPv6 IPsec VPN | 409
-



- ?? ?? IPsec VPN ?? | 327
- ?: ?? ?? VPN ?? | 328
- ?? ?? VPN? ?? ?? VPN?? ?????? | 351

## ?? ?? IPsec VPN ??

[illegible]

- [?? ?? IPsec VPN? IKEv2?? ???? ????.](#)
- [IPsec VPN ???? ?? ???? ???? iked ???? ?? ???? ???? junos-ike ?? ?? ?? IPsec VPN? ?? ??? ??? ? ?? ??. ???? ???? junos-ike ?? ?? IPsec VPN ??? ??????? ?????. RE3 junos-ike ? ??? SRX5K-SPC3??? ?? ?? ?????? ??? ? ?????. SRX1500 ??? ??????? ??? ???????, ??? ??? ? ???? IPsec VPN ?? ??? ??????.](#)

## IPsec 00 | 11





### ? 57: IKE(Internet Key Exchange) 1?? ?? ?? ??

| ??    | ??      | ?? ?? ??                                                                                                                                                 |
|-------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??    | ??      | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> </ul>                                                                                 |
| ??    | IKE-POL | <ul style="list-style-type: none"> <li>?: main</li> <li>?? ??: ??</li> <li>IKE(Internet Key Exchange) 1?? ?? ?? ??: pre-shared-key ascii-text</li> </ul> |
| ????? | IKE-GW  | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: IKE-POL</li> <li>?? ??????: ge-0/0/1</li> <li>????? ??: 172.16.23.1</li> </ul>  |

### ? 58: IPsec 2?? ?? ?? ??

| ??  | ??           | ?? ?? ??                                                                                                                                                    |
|-----|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??  | ??           | <ul style="list-style-type: none"> <li>?? ?? ??</li> </ul>                                                                                                  |
| ??  | IPSEC-POL    | <ul style="list-style-type: none"> <li>?? ??, ??</li> </ul>                                                                                                 |
| VPN | VPN ?? ????? | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?????? ??: IKE-GW</li> <li>IPsec ?? ??: IPSEC-POL</li> <li>? establish-tunnels</li> </ul> |

59: ? ? ? ? ? ? ? ?

| ??                                                                                                                                                                                                                                                                            | ??      | ?? ?? ??                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>? ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????.</p>                                                                                                                                                                                                                | VPN-OUT | <ul style="list-style-type: none"> <li>• ?? ??:</li> <li>• source-address Host1-Net</li> <li>• destination-address Host2-Net</li> <li>• ?? ?????</li> <li>• Permit ??: ?? ipsec-vpn VPN-to-Host2</li> </ul> |
| <p>? ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????.</p>                                                                                                                                                                                                                | VPN-IN  | <ul style="list-style-type: none"> <li>• ?? ??:</li> <li>• source-address Host2-Net</li> <li>• destination-address Host1-Net</li> <li>• ?? ?????</li> <li>• Permit ??: ?? ipsec-vpn VPN-to-Host2</li> </ul> |
| <p>? ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????.</p> <p>VPN-OUT ??? default-permit ?? ?? ?? ???? ??. Junos OS? ??? ? ??? ?? ?? ???? ?????. default-permit ??? VPN-OUT ?? ?? ?? ??, ???? ?? ?? ???? default-permit ??? ?? ?????. ??? VPN-OUT ??? ???? ???? ????.</p> | ???? ?? | <ul style="list-style-type: none"> <li>• ?? ??:</li> <li>• ?? source-address</li> <li>• ?? source-destination</li> <li>• ?? ?????</li> <li>• ??: ??(Permit)</li> </ul>                                      |

```
set interfaces ge-0/0/0 unit 0 family inet address 10.100.11.1/24
set interfaces ge-0/0/1 unit 0 family inet address 172.16.13.1/24
set interfaces lo0 unit 0 family inet address 10.100.100.1/32
set routing-options static route 0.0.0.0/0 next-hop 172.16.13.2
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/0.0
```

```
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/1.0
```

??? ??

?? ?? ?? ????? ??? ??? ?????, ? ??? ????? ??? ?? ??? CLI ??? ????? ???????.

?????, ?? ?? ? ?? ?? ?? ??:

1. ?????? ??????.

```
[edit]
user@SRX1# set interfaces ge-0/0/0 unit 0 family inet address 10.100.11.1/24
user@SRX1# set interfaces ge-0/0/1 unit 0 family inet address 172.16.13.1/24
user@SRX1# set interfaces lo0 unit 0 family inet address 10.100.100.1/32
```

2. ?? ??? ??????.

```
[edit]
user@SRX1# set routing-options static route 0.0.0.0/0 next-hop 172.16.13.2
```

3. ??? ? ?? ?? ??? ??? ?? ?????? ??????.

```
[edit security zones security-zone untrust]
user@SRX1# set interfaces ge-0/0/1.0
```

4. ??? ? ?? ?? ??? ?? ??? ??? ????? ??????.

```
[edit security zones security-zone untrust]
user@SRX1# set host-inbound-traffic system-services ike
user@SRX1# set host-inbound-traffic system-services ping
```

5. ??? ? ?? ?? ??? Host1 ?? ?????? ??????.

```
[edit security zones security-zone trust]
user@SRX1# set interfaces ge-0/0/0.0
```

**6.**    ? ? ?   ?   ? ?   ? ?   ? ? ? ?   ? ?   ? ? ? ?   ? ? ? ?   ? ? ? ?   ? ? ? ? ? .

```
[edit security zones security-zone trust]
user@SRX1# set host-inbound-traffic system-services all
```

??

```
? ? show interfaces, show routing-options ? show security zones ??? ????? ???. ??? ??? ????? ?  
?, ? ? ? ? ? ? ? ?.
```

```
[edit]
user@SRX1# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.100.11.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.13.1/24;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.100.100.1/32;
        }
    }
}
```

```
[edit]
user@SRX1# show routing-options
static {
```



```
route 0.0.0.0/0 next-hop 172.16.13.2;
}
```

```
[edit]
user@SRX1# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
```

## IKE(Internet Key Exchange) ??

CLI

[illegible]

```
set security ike proposal standard authentication-method pre-shared-keys
set security ike policy IKE-POL mode main
set security ike policy IKE-POL proposals standard
set security ike policy IKE-POL pre-shared-key ascii-text $ABC123
set security ike gateway IKE-GW ike-policy IKE-POL
```

```
set security ike gateway IKE-GW address 172.16.23.1
set security ike gateway IKE-GW external-interface ge-0/0/1
```

???

?? ?? ? ???? ???? ???? ???? ?????. ??? ???? CLI ??? ???? ?????.

IKE(Internet Key Exchange) ??:

#### 1. IKE(Internet Key Exchange) ??? ????.

```
[edit security ike]
user@SRX1# set proposal standard
```

#### 2. IKE(Internet Key Exchange) ?? ?? ???? ????.

```
[edit security ike proposal standard]
user@SRX1# set authentication-method pre-shared-keys
```

#### 3. IKE(Internet Key Exchange) ??? ????.

```
[edit security ike]
user@SRX1# set policy IKE-POL
```

#### 4. IKE(Internet Key Exchange) ?? ??? ????.

```
[edit security ike policy IKE-POL]
user@SRX1# set mode main
```

#### 5. IKE(Internet Key Exchange) ??? ?? ???? ????.

```
[edit security ike policy IKE-POL]
user@SRX1# set proposals standard
```

## 6. IKE(Internet Key Exchange) `?? ?? ??? ?????`.

```
[edit security ike policy IKE-POL]
user@SRX1# set pre-shared-key ascii-text $ABC123
```

## 7. IKE(Internet Key Exchange) `?????? ????? ? ???? ???`.

```
[edit security ike gateway IKE-GW]
user@SRX1# set external-interface ge-0/0/1.0
```

## 8. IKE(Internet Key Exchange) `????? ??? ?????`.

```
[edit security ike gateway IKE-GW]
user@SRX1# address 172.16.23.1
```

## 9. IKE(Internet Key Exchange) `?? ??? ?????`.

```
[edit security ike gateway IKE-GW]
user@SRX1# set ike-policy IKE-POL
```

`??`

`?? ????? show security ike ??? ????? ???? ??????. ??? ??? ??? ????? ??, ? ?? ?? ??? ????? ?????.`

```
[edit]
user@host# show security ike
proposal standard {
    authentication-method pre-shared-keys;
}
policy IKE-POL {
    mode main;
    proposals standard;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway IKE-GW {
    ike-policy IKE-POL;
    address 172.16.23.1;
```



#### 4. IKE(Internet Key Exchange) `vpn VPN-to-Host2 ike gateway IKE-GW`.

```
[edit security ipsec]
user@SRX1# set vpn VPN-to-Host2 ike gateway IKE-GW
```

#### 5. IPsec `vpn VPN-to-Host2 ike ipsec-policy IPSEC-POL`.

```
[edit security ipsec]
user@SRX1# set vpn VPN-to-Host2 ike ipsec-policy IPSEC-POL
```

#### 6. `vpn VPN-to-Host2 establish-tunnels immediately`.

```
[edit security ipsec]
user@SRX1# set vpn VPN-to-Host2 establish-tunnels immediately
```

??

?? `show security ipsec` `vpn VPN-to-Host2 ike gateway IKE-GW`, `vpn VPN-to-Host2 ike ipsec-policy IPSEC-POL`, `vpn VPN-to-Host2 establish-tunnels immediately`.

```
[edit]
user@SRX1# show security ipsec
proposal standard;
policy IPSEC-POL {
    proposals standard;
}
vpn VPN-to-Host2 {
    ike {
        gateway IKE-GW;
        ipsec-policy IPSEC-POL;
    }
    establish-tunnels immediately;
}
```

?? ?? ??

CLI

```
SRX1? ?? ? ?? ??? ??????, ?? ??? ?????? ??? ??? ?? ??, ? ??? ?????, ????? ??? ????? ? ??? ?? ??? ?????, ??
????? ??? ????? CLI [edit] ? ????? ??, ?? ????? ? ??????? commit.
```

```
set security address-book Host1 address Host1-Net 10.100.11.0/24
set security address-book Host1 attach zone trust
set security address-book Host2 address Host2-Net 10.100.22.0/24
set security address-book Host2 attach zone untrust
set security policies from-zone trust to-zone untrust policy VPN-OUT match source-address Host1-Net
set security policies from-zone trust to-zone untrust policy VPN-OUT match destination-address Host2-Net
set security policies from-zone trust to-zone untrust policy VPN-OUT match application any
set security policies from-zone trust to-zone untrust policy VPN-OUT then permit tunnel ipsec-vpn VPN-to-Host2
set security policies from-zone trust to-zone untrust policy default-permit match source-address any
set security policies from-zone trust to-zone untrust policy default-permit match destination-address any
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone untrust to-zone trust policy VPN-IN match source-address Host2-Net
set security policies from-zone untrust to-zone trust policy VPN-IN match destination-address Host1-Net
set security policies from-zone untrust to-zone trust policy VPN-IN match application any
set security policies from-zone untrust to-zone trust policy VPN-IN then permit tunnel ipsec-vpn VPN-to-Host2
```

???

?? ?? ?? ??? ???? ???? ???? ?????. ??? ??? CLI ??? ??? ?????.

?? ?? ??:

1. `set security address-book Host1 address Host1-Net 10.100.11.0/24`

```
[edit]
user@SRX1# set security address-book Host1 address Host1-Net 10.100.11.0/24
user@SRX1# set security address-book Host1 attach zone trust
user@SRX1# set security address-book Host2 address Host2-Net 10.100.22.0/24
user@SRX1# set security address-book Host2 attach zone untrust
```

2. `set security policy VPN-OUT match source-address Host1-Net`

```
[edit security policies from-zone trust to-zone untrust]
user@SRX1# set policy VPN-OUT match source-address Host1-Net
user@SRX1# set policy VPN-OUT match destination-address Host2-Net
user@SRX1# set policy VPN-OUT match application any
user@SRX1# set policy VPN-OUT then permit tunnel ipsec-vpn VPN-to-Host2
```

3. `set security policy default-permit match source-address any`

```
[edit security policies from-zone trust to-zone untrust]
user@SRX1# set policy default-permit match source-address any
user@SRX1# set policy default-permit match destination-address any
user@SRX1# set policy default-permit match application any
user@SRX1# set policy default-permit then permit
```

4. `set security policy VPN-IN match source-address Host2-Net`

```
[edit security policies from-zone untrust to-zone trust]
user@SRX1# set policy VPN-IN match source-address Host2-Net
user@SRX1# set policy VPN-IN match destination-address Host1-Net
user@SRX1# set policy VPN-IN match application any
user@SRX1# set policy VPN-IN then permit tunnel ipsec-vpn VPN-to-Host2
```

`show`

`show security policies`

```
[edit]
user@SRX1# show security policies
```

```

from-zone trust to-zone untrust {
  policy VPN-OUT {
    match {
      source-address Host1-Net;
      destination-address Host2-Net;
      application any;
    }
    then {
      permit {
        tunnel {
          ipsec-vpn VPN-to-Host2;
        }
      }
    }
  }
  policy default-permit {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}

from-zone untrust to-zone trust {
  policy VPN-IN {
    match {
      source-address Host2-Net;
      destination-address Host1-Net;
      application any;
    }
    then {
      permit {
        tunnel {
          ipsec-vpn VPN-to-Host2;
        }
      }
    }
  }
}

```







in this section

- IKE(Internet Key Exchange) 222 222 | 345
- IPsec 222 222 222 | 348
- VPN 222 222 222 222 | 350
- IPsec 22 222 22 22 22 22 22 | 350

## IKE(Internet Key Exchange) ?? ??

IKE      .

??

?? show security ike security-associations ??. show security ike security-associations index *index\_number* detail ??.

```
user@SRX1> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|---------|-------|------------------|------------------|------|----------------|
| 1859361 | UP    | 9788fa59c3ee2e2a | 0b17e52f34b83aba | Main | 172.16.23.1    |

```
user@SRX1> show security ike security-associations index 1859361 detail
```

IKE peer 172.16.23.1, Index 1859361, Gateway Name: IKE-GW

Role: Responder, State: UP

Initiator cookie: 9788fa59c3ee2e2a, Responder cookie: 0b17e52f34b83aba

Exchange type: Main, Authentication method: Pre-shared-keys

Local: 172.16.13.1:500, Remote: 172.16.23.1:500

Lifetime: Expires in 17567 seconds

Reauth Lifetime: Disabled

IKE Fragmentation: Disabled, Size: 0

Remote Access Client Info: Unknown Client

Peer ike-id: 172.16.23.1

AAA assigned IP: 0.0.0.0

Algorithms:

Authentication : hmac-sha1-96

Encryption : 3des-cbc

Pseudo random function: hmac-sha1

Diffie-Hellman group : DH-group-2

Traffic statistics:

Input bytes : 1740

Output bytes : 1132

Input packets: 15

Output packets: 7

Input fragmentated packets: 0

Output fragmentated packets: 0

IPSec security associations: 4 created, 4 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0

Local: 172.16.13.1:500, Remote: 172.16.23.1:500

Local identity: 172.16.13.1

Remote identity: 172.16.23.1

Flags: IKE SA is created

??

?? show security ike security-associations ?? ?? IKE(Internet Key Exchange) 1?? ?? ??(SA)? ??????. SA? ??  
?? ?? ?? ??, 1?? ????? ?? ?? ?????. ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ?? ?? ?????.

SA? ????? ?? ?? ?? ????? ?????.

- ??? - ? ?? ? IKE(Internet Key Exchange)? ?? ??? ??? SA? ?? ??? ??? ?? ?? show security ike security-associations index detail???? ? ? ?????.
- ?? ?? - ?? IP ??? ????? ?????.
- ?
- UP—1?? SA? ????????
- DOWN—1?? SA? ????? ? ??? ?????.
- ?? - ??? ??? ????? ????? ?????.

???? ?? ??? ????? ?????.

- ?? ??????(?????? IKE ??? ????? ???)
- IKE(Internet Key Exchange) ?? ?? ??
- ?? ?? ? ??
- 1?? ?? ?? ??(? ?? ????? ????? ???)

show security ike security-associations index 1859361 detail ??? ??? ? 1859361?? ?? ??? ?? ?? ??? ?????.

- ??? ?? ? ??? ?????
- 1?? ??
- ??? ??(????? ?????? ?????? ??? ??? ????? ? ??? ? ????)
- ??? ? ??? ? ? ?

?? ??? ?????? ??? ?????? ?????? ?? ? ?????.

- ??? IPsec SA? ?
- ?? ?? 2?? ?? ?

## IPsec 2?? ? ? ?

??

IPsec 2?? ??? ?????.

??

?? ????? show security ipsec security-associations ??? ?????. ????? ???? ???? ? show security ipsec security-associations index *index\_number* detail ??? ?????.

```
user@SRX1 show security ipsec security-associations
```

```
Total active tunnels: 1      Total Ipsec sas: 1
```

| ID | Algorithm     | SPI      | Life:sec/kb | Mon | lsys | Port | Gateway     |
|----|---------------|----------|-------------|-----|------|------|-------------|
| <2 | ESP:3des/sha1 | ae5afc5a | 921/ unlim  | -   | root | 500  | 172.16.23.1 |
| >2 | ESP:3des/sha1 | 6388a743 | 921/ unlim  | -   | root | 500  | 172.16.23.1 |

```
user@SRX1> show security ipsec security-associations index 2 detail
```

```
ID: 2 Virtual-system: root, VPN Name: VPN-to-Host2
```

```
Local Gateway: 172.16.13.1, Remote Gateway: 172.16.23.1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=10.100.11.0/24)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=10.100.22.0/24)
```

```
Version: IKEv1
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Policy-name: VPN-OUT
```

```
Port: 500, Nego#: 30, Fail#: 0, Def-Del#: 0 Flag: 0x600829
```

```
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
```

```
Tunnel events:
```

```
Thu Jul 29 2021 14:29:22 -0700: IPSec SA negotiation successfully completed (29 times)
```

```
Thu Jul 29 2021 12:00:30 -0700: IKE SA negotiation successfully completed (4 times)
```

```
Wed Jul 28 2021 15:20:58
```

```
: IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
```

```
Wed Jul 28 2021 15:05:13 -0700: IPSec SA negotiation successfully completed (1 times)
```

```
Wed Jul 28 2021 15:05:13
```

```
: Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
```

```
Wed Jul 28 2021 15:05:13 -0700: External interface's address received. Information updated (1 times)
```

```
Wed Jul 28 2021 15:05:13 -0700: External interface's zone received. Information updated (1 times)
```

```
Wed Jul 28 2021 11:17:38
```

```
: Negotiation failed with error code NO_PROPOSAL_CHOSEN received from peer (1 times)
```



VPN **???** **???** **???** **???**

**??**

VPN **???** **???** **???** **???** **???**.

**??**

Host1 **?????** ping **???** **???** Host2**??** **???** **???** **???** **???**.

```
user@Host1> ping 10.100.22.1 rapid count 100
PING 10.100.22.1 (10.100.22.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
--- 10.100.22.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.300/3.936/8.562/0.720 ms
```

**??**

Host1**??** ping **???** **???** **??**, **???**, **??** **??**, **??** **???** **??** ESP **???** **???** **?** **???** **???** **??** **?** **???**.

IPsec **??** **???** **??** **??** **?** **??** **??**

**??**

IPsec **??** **???** **??** ESP **?** **??** **??** **???** **?** **???** **???** **???**.

**??**

**??** **???** **???** **??** **??** VPN**?** **??** **???** **???** show security ipsec statistics index *index\_number* **???** **???** **???**.

```
user@SRX1> show security ipsec statistics index 2
ESP Statistics:
  Encrypted bytes:      13600
  Decrypted bytes:      8400
  Encrypted packets:    100
  Decrypted packets:    100
AH Statistics:
  Input bytes:          0
```



```
Output bytes:          0
Input packets:         0
Output packets:        0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

?? ?? SA? ?? ? ??? ????? show security ipsec statistics ??? ??? ? ?????.

?? IPsec ??? ???? , clear security ipsec statistics ??? ?????.

??

VPN ??? ?? ?? ?? ??? ?? ??, ??? ?? ? ????? show security ipsec statistics ??? ? ????? ?? ????? ?????? ??? ? ?????. ?? ?? ?? ????? ?????? ????? ???.

SEE ALSO

- [?: ?? ?? VPN ?? | 453](#)
- [???? ????? ?? ?? IPsec ?? ?? VPN](#)

?? ?? VPN? ?? ?? VPN?? ???????

summary

?? point-to-point st0 ?????? ????? ?? ?? VPN?  
? ?? ?? VPN?? ?????????? ?? ? ??? ???????.

in this section

●

[?? | 352](#)

●

[?? ?? | 352](#)

SRX ??? ????? kmd ?????? ????? IPsec VPN? ????? ?????? ?? ?? VPN? ?????? ??? ?? ??? ?????, ??? ?????? ? ????? ? ?? ?? ????? VPN ??? ?????? ????? ? ??? IKEv1? SA(Security Association) ????? ????? ?? ?? ????? ????? ?????, ??? ????? ?? ?? VPN? ?????? ????? ?????? ??? ? ?????, ?? ?? VPN? ?? ?? VPN?? ?????????? ?? ? ???.

?? ?? VPN?? ?? ?? VPN?? ????????????? ?? ??? ?????.

- kmd ?????? ????? Junos OS ?????? ?? ?? IPsec VPN ??? ???????.

- junos-ike iked `???` `???` IPsec VPN `???` `???` `??` `???` `???`. `junos-ike` `???` `???` `???`.
- `??` point-to-point st0 `???` `???` `??` `??` `???` `???`. `??` Point-to-Point st0 `???` `???` `???`.
- `??` point-to-point st0 `???` `???` `???` `???` IPsec VPN `???` `???`.

**[?] [?] [??] [????] [?] [?????] [?] [??] [???] [??????] [????] [?] [????].**

??

- ?? point-to-point st0 ?????? ???? iked ?????? ????????? ???? kmd ?? IPsec VPN ????? ? ? ? ? ? ? ? ? ? ?
- ?? ?? VPN? ?? ??? ???? ?????? ??? ?? ??? ?????? ??? ??? ?????? ??????, ??? ?? ?? VPN? ??? ????? ?????? ?? VPN? ??? ??? ??? ????? ?????, ? ??? VPN ??? ??? ????? ????? ? ? ? ? ? ? ? ? ? ?

?? ??

????????? ? kmd ?????? ? ? IPsec VPN? ? ???? ???? ???? ?????. ? ? VPN? ? ????  
IKEv1???? ? ? ???? ? ???? ???? ???? ???? ???? ???? VPN ? ? ?????. ? ? IPsec VPN? ??????.

```
[edit security policies]
user@host# show
from-zone zone1 to-zone zone2 {
    policy policy1 {
        match {
            source-address 192.168.2.0/24;
            destination-address 10.0.2.0/24;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn vpn1;
                }
            }
        }
    }
}

from-zone zone3 to-zone zone4 {
    policy policy2 {
        match {
            source-address 192.168.3.0/24;
            destination-address 10.0.3.0/24;
        }
    }
}
```

```

        then {
            permit {
                tunnel {
                    ipsec-vpn vpn2;
                }
            }
        }
    }
}

```

```

[edit security ipsec]
user@host# show
proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 2400;
}
policy ipsec_pol {
    proposals ipsec_prop;
}
vpn vpn1 {
    ike {
        gateway gw1;
        ipsec-policy ipsec_pol;
    }
    establish-tunnels immediately;
}
vpn vpn2 {
    ike {
        gateway gw2;
        ipsec-policy ipsec_pol;
    }
    establish-tunnels immediately;
}

```





- Junos OS 9.4

- 

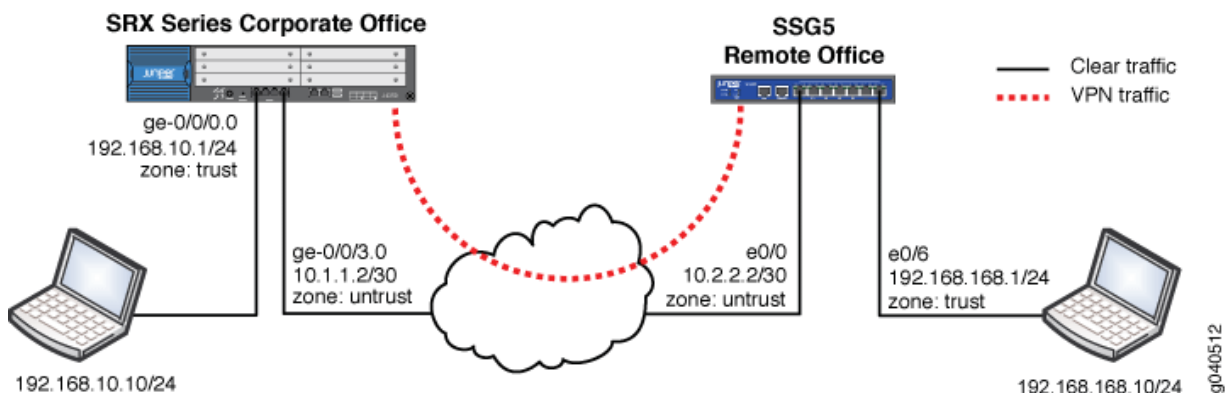
:

- SRX LAN ge-0/0/0 IP
- zone untrust ge-0/0/3 IP
- LAN
- SSG5, CA CRL
- SSG5 ssg5.example.net FQDN(IKE ID)
- 1024 PKI IKE
- CA VPN example.com CA

??

23 356 IPsec VPN

23: ? ? ? ? ?



PKI VPN VPN

VPN 10.1.1.1 ge-0/0/0.0 ge-0/0/3.0



- DC –

**?? ?? ?? ?? ???? ???? ???? ?????. ?? ? ??? ? ? ???? ? ? ????.**

- domain-name — FQDN[?], FQDN[?] IKE [?] [?] [?] [?] ID[?] [?] [?] [?] [?] [?] [?] [?].
- filename (path | terminal) — ([?] [?]) [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?].
- ip-address — ([?] [?]) [?] [?] IP [?] [?] [?].
- email — ([?] [?]) CA [?] [?] [?] [?] [?] [?] [?].

???, IP ?? ?? ??? ??? ???.

[illegible]

```
PKCS10 ??? ??? ??? ? ? ??? ????, ??? ???? ???? ???? CA ? ? ? ???, ?? ???? ???? ???? ? ? ? CLI??
??? ???? show security pki certificate-request certificate-id <id-name> PKCS10 ??? ? ? ???? ? ???? ?
? ??? ???? CA ??? ? ??? ??? ? ???? ? ? ? ? ???.
```

PKCS10 [redacted] CA [redacted](? [redacted] certadmin@example.com)[redacted]  
[redacted].

certificate-ID?? ? ID? ??? ? ?? ??? ????? ? ??????. ? ID? ??? ? ?? ????? ?? ??? ?? ? ?? ????? ??????. ???  
 ? ?? ??? ID? ??? ??? ??? ??? ????? ?????, ?? ??? 1024?? ?? 2048??? ? ????.

?? CA? ?????? ?? ????? ?? ?? ??(??) ????? ?? ? ??????. ?? ??? ?? ??? ??? CA ????? ?? ??? ??????.

CDP? ?? ?? ??? ?????.

- CA [ ] [ ] [ ] [ ]
- CA [ ] [ ] [ ] [ ] [ ] [ ] CDP
- [ ] [ ] CA [ ] [ ] [ ]

?? ??? ?? ?? CA ????? ???? ?? ?????.

???? CA? ??? ??? ?????, CA ????? ??? ??? ????? ?????? ?? ? ????? ??????, ??? ????? ?????? ????? CA ??? ?  
CRL? ?? ?????? ??????

CA?? CA ???, ????? ? ?? ??? ? CRL? ????? ?????? ?? ?? CA ?? ? ?????? ?????? ?? ?????.

Junos OS? ?? CA ??? ??????.

- 
- Verisign
- 



??

- PKI [?? ??] | 359
- CA [??? ??] | 360
- [???-???? ? ?? ??] | 361
- [? ???? ??] | 362
- CA ? [?? ???? ??] | 363
- [??? IPsec VPN ??] | 366

???

PKI[?] [?] [?] [?] [?] [?] [?] [?] [?] [?].

- ```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet address 192.168.10.1/24
user@host# set ge-0/0/3 unit 0 family inet address 10.1.1.2/30
```

- ```
[edit]
user@host# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
```

### 3. `set system time-zone PST8PDT`.

```
[edit]
user@host# set system time-zone PST8PDT
```

```
user@host# show system uptime
```

```
user@host> show system uptime
Current time: 2007-11-01 17:57:09 PDT
System booted: 2007-11-01 14:36:38 PDT (03:20:31 ago)
Protocols started: 2007-11-01 14:37:30 PDT (03:19:39 ago)
Last configured: 2007-11-01 17:52:32 PDT (00:04:37 ago) by root
5:57PM up 3:21, 4 users, load averages: 0.00, 0.00, 0.00
```

### 4. NTP `set date ntp 130.126.24.24`.

```
user@host> set date ntp 130.126.24.24
1 Nov 17:52:52 ntpdate[5204]: step time server 172.16.24.24 offset -0.220645 sec
```

### 5. DNS `set system name-server 172.31.2.1`.

```
[edit]
user@host# set system name-server 172.31.2.1
user@host# set system name-server 172.31.2.2
```

## CA `set security pki ca-profile ms-ca ca-identity example.com`

### 1. `set security pki ca-profile ms-ca ca-identity example.com`.

```
[edit]
user@host# set security pki ca-profile ms-ca ca-identity example.com
```

### 2. `set security pki ca-profile ms-ca ca-identity example.com`.

```

?? ?? ??(??)? ????? CRL? ?????? ??? ??????. ????? CRL? ?? ????? ?? ?? ?? ????? ??? ????? ?? ?? 1????
?.

```

```
[edit]
```

```
user@host# set security pki ca-profile ms-ca revocation-check crl refresh-interval 48
```

```

revocation-check ?? ??? ??? ????? disable ?? ??? ?????????? ??? ?????? crl CRL ??? ??? ? ?????. CA ??? ?
? CRL ?????? ??? ?? CA ????? ?????? ????? ?????? disable on-download-failure ? ?????. ??? ??? CA ??
?? ?? CRL? ?? ????? ??????.

```

### 3. CRL(HTTP ?? LDAP)? ??? ??(URL)? ??????. ?????? URL? ?? ??? CA ????? ??? CDP ??? ??????.

```
[edit]
```

```
user@host# set security pki ca-profile ms-ca revocation-check crl url http://srv1.example.com/
CertEnroll/EXAMPLE.crl
```

```

???? URL? ??? ??? ? ??????. ?? URL ??? ?? ??? ??? ? ??????.

```

### 4. CA ?????? ??? ??? ?? ?? ?? ?? ?? ??? ??????.

```
user@host# set security pki ca-profile ms-ca administrator email-address certadmin@example.com
```

### 5. ??? ??????.

```

user@host# commit and-quit
commit complete
Exiting configuration mode

```

```
???-???? ? ?? ??
```

```
??? ??
```

```
CA ????? ????? ?? ??? ??? ?????? ?????? ? ??? ????? ??????. ?? ? ?? ? ?? ?????? ??? ??????.
```

### 1. ??? ? ?? ??????.

```
user@host> request security pki generate-key-pair certificate-id ms-cert size 1024
```

??

???-???? ? ??? ??? ? ??? ????? ?????? ??? ?????.

Generated key pair ms-cert, key size 1024 bits

?? ??? ??

??? ??

1. PKCS-10 `request security pki generate-certificate-request` `certificate-id ms-cert subject "CN=john doe,CN=10.1.1.2,OU=sales,O=example, L=Sunnyvale,ST=CA,C=US" email user@example.net filename ms-cert-req`

```
user@host> request security pki generate-certificate-request certificate-id ms-cert subject
"CN=john doe,CN=10.1.1.2,OU=sales,O=example, L=Sunnyvale,ST=CA,C=US" email user@example.net
filename ms-cert-req
```

Generated certificate request

-----BEGIN CERTIFICATE REQUEST-----

```
MIIB3DCCAUAQAwbDERMA8GA1UEAxMIam9obiBkb2UxDjAMBgNVBAsTBXNhbGVz
MRkwFwYDVQQKEwBKdW5pcGVyIE5ldHdvcmZMRiWEAYDVQQHEw1TdW5ueXZhbGUx
CzAJBgNVBAGTAKNBMQswCQYDVQQGEwJVUzCBnzANBGMqhkiG9w0BAQEFAA0BjQAw
gYkCgYEA5EG6sgG/CTFzX6KC/hz6Czal0BxakUxfGxF7UWYWHaWFFYLqo6vXN08r
OS5Yak7rWANAsMob3E2X/1ad1QIRi4QFTjkBqGI+MTEDGnqFsJBqrB6oyqGtdcSU
u0qUivMvgKQVCx8hpx99J3EBTurfWL1pCNlBmZggNogb6MbwES0CAwEAaAwMC4G
CSqGSIB3DQEDJDjEhMB8wHQYDVVR0RBBYwFIESInVzZXJAanVuaXB1ci5uZXQiMA0G
CSqGSIB3DQEBBQUAA4GBAI6GhBaCsXk6/1lE2e5AakFFDhY7oqzHhgd1yMjiSUMV
djmf9JbDz2gM2UKpI+yKgtUjyCK/1V2ui57hpZMvnhAW4AmgwK0Jg6mpR5rsxdLr
4/HHSHuEGOF17RH06x0YwJ+KE1rYDRWj3DtZ447ynaLxcDF7buwd4IrMcRJJI9ws
```

-----END CERTIFICATE REQUEST-----

Fingerprint:

47:b0:e1:4c:be:52:f7:90:c1:56:13:4e:35:52:d8:8a:50:06:e6:c8 (sha1)

a9:a1:cd:f3:0d:06:21:f5:31:b0:6b:a8:65:1b:a9:87 (md5)

PKCS10 `request security pki generate-certificate-request` `certificate-id ms-cert subject "CN=john doe,CN=10.1.1.2,OU=sales,O=example, L=Sunnyvale,ST=CA,C=US" email user@example.net filename ms-cert-req`

2. CA `request security pki generate-certificate-request` `certificate-id ms-cert subject "CN=john doe,CN=10.1.1.2,OU=sales,O=example, L=Sunnyvale,ST=CA,C=US" email user@example.net filename ms-cert-req`



CRL? ?? ???? 5MB???? ???? ???? CA ????? ???? ????.

```
user@host> request security pki crl load ca-profile ms-ca filename certcrl.crl
CRL for CA profile ms-ca loaded successfully
```

??

?? ?? ????? ??????? ??????.

```
user@host> show security pki local-certificate certificate-id ms-cert detail Certificate
identifier: ms-cert
Certificate version: 3
Serial number: 3a01c5a0000000000011
Issuer:
Organization: Example, Organizational unit: example, Country: US, State:
CA, Locality: Sunnyvale,
Common name: LAB
Subject:
Organization: Example, Organizational unit: example, Country: US,
State: CA, Locality: Sunnyvale,
Common name: john doe
Alternate subject: "user@example.net", fqdn empty, ip empty
Validity:
Not before: 11- 2-2007 22:54
Not after: 11- 2-2008 23:04
Public key algorithm: rsaEncryption(1024 bits)
30:81:89:02:81:81:00:e4:41:ba:b2:01:bf:09:31:73:5f:a2:82:fe
1c:fa:0b:36:a5:d0:1c:5a:91:4c:5f:1b:11:7b:51:66:16:1d:a5:85
15:82:ea:a3:ab:d7:34:ef:2b:39:2e:58:6a:4e:eb:58:03:40:b0:ca
1b:dc:4d:97:ff:56:9d:95:02:11:8b:84:05:4e:39:01:a8:62:3e:31
31:03:1a:7a:85:b0:90:6a:ac:1e:a8:ca:a1:ad:75:c4:94:bb:4a:94
8a:f3:2f:80:a4:15:0b:1f:21:a7:1f:7d:27:71:01:4e:ea:df:58:bd
69:08:d9:41:99:98:20:36:88:1b:e8:c6:f0:11:2d:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
ldap:///CN=LAB,CN=LABSRV1,CN=CDP,CN=Public%20Key%20Services,CN=Services,
CN=Configuration,DC=domain,DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint
http://labsrv1.domain.com/CertEnroll/LAB.crl
Fingerprint:
```

```
c9:6d:3d:3e:c9:3f:57:3c:92:e0:c4:31:fc:1c:93:61:b4:b1:2d:58 (sha1)
50:5d:16:89:c9:d3:ab:5a:f2:04:8b:94:5d:5f:65:bd (md5)
```

```
certificate-ID 2222 22 222 22 222 222 2 2222.
```

```
CA 222 22 22 CA 2222(22) CA 2222 222222.
```

```
user@host> show security pki ca-certificate ca-profile ms-ca detail
Certificate identifier: ms-ca
Certificate version: 3
Serial number: 44b033d1e5e158b44597d143bbfa8a13
Issuer:
Organization: Example, Organizational unit: example, Country: US, State:
CA, Locality: Sunnyvale,
Common name: example
Subject:
Organization: Example, Organizational unit: example, Country: US, State:
CA, Locality: Sunnyvale,
Common name: example
Validity:
Not before: 09-25-2007 20:32
Not after: 09-25-2012 20:41
Public key algorithm: rsaEncryption(1024 bits)
30:81:89:02:81:81:00:d1:9e:6f:f4:49:c8:13:74:c3:0b:49:a0:56
11:90:df:3c:af:56:29:58:94:40:74:2b:f8:3c:61:09:4e:1a:33:d0
8d:53:34:a4:ec:5b:e6:81:f5:a5:1d:69:cd:ea:32:1e:b3:f7:41:8e
7b:ab:9c:ee:19:9f:d2:46:42:b4:87:27:49:85:45:d9:72:f4:ae:72
27:b7:b3:be:f2:a7:4c:af:7a:8d:3e:f7:5b:35:cf:72:a5:e7:96:8e
30:e1:ba:03:4e:a2:1a:f2:1f:8c:ec:e0:14:77:4e:6a:e1:3b:d9:03
ad:de:db:55:6f:b8:6a:0e:36:81:e3:e9:3b:e5:c9:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
ldap:///CN=LAB,CN=LABSRV1,CN=CDP,CN=Public%20Key%20Services,CN=Services,
CN=Configuration,DC=domain,DC=com?certificateRevocationList?base?
objectclass=cRLDistributionPoint
http://srv1.domain.com/CertEnroll/LAB.crl
Use for key: CRL signing, Certificate signing, Non repudiation
Fingerprint:
1b:02:cc:cb:0f:d3:14:39:51:aa:0f:ff:52:d3:38:94:b7:11:86:30 (sha1)
90:60:53:c0:74:99:f5:da:53:d0:a0:f3:b0:23:ca:a3 (md5)
```





### 3. `set security zone security-zone`

```
[edit security zones security-zone]
user@host# set trust address-book address local-net 192.168.10.0/24
user@host# set untrust address-book address remote-net 192.168.168.0/24
```

### 4. `set security ike proposal`

```
[edit security ike proposal rsa-prop1]
user@host# set authentication-method rsa-signatures
user@host# set encryption-algorithm 3des-cbc
user@host# set authentication-algorithm sha1
user@host# set dh-group group2
```

### 5. `set security ike policy`

`set security ike policy`

```
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals rsa-prop1
user@host# set certificate local-certificate ms-cert
user@host# set certificate peer-certificate-type x509- signature
user@host# set certificate trusted-ca use-all
```

### 6. `set security ike gateway`

`set security ike gateway`

```
[edit security ike gateway ike-gate]
user@host# set external-interface ge-0/0/3.0
user@host# set ike-policy ike-policy1
user@host# set dynamic hostname ssg5.example.net
```

### 7. `set security ipsec`

```
[edit security ipsec policy vpn-policy1]
user@host# set proposal-set standard
user@host# set perfect-forward-secrecy keys group2
```

8. IKE(Internet Key Exchange) ???? ? IPsec ??? ???? IPsec VPN? ?????.

? ???? ? ???? ???? ? ? ? ???? ike-vpn VPN ??? ????? ??. ?? ???? ? ? ? ? ? ID? ?? ? ? ? ? ?  
 ? ???? ? ????

```
[edit security ipsec vpn ike-vpn ike]
user@host# set gateway ike-gate
user@host# set ipsec-policy vpn-policy1
```

**9.** VPN [?] [?] [?] [?] [?] [?] [?] [?] [?] [?].

[illegible]

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy tunnel-policy-out match source-address local-net
user@host# set policy tunnel-policy-out match destination-address remote-net
user@host# set policy tunnel-policy-out match application any
user@host# set policy tunnel-policy-out then permit tunnel ipsec-vpn ike-vpn pair-policy
tunnel-policy-in
user@host# top edit security policies from-zone untrust to-zone trust
user@host# set policy tunnel-policy-in match source-address remote-net
user@host# set policy tunnel-policy-in match destination-address local-net
user@host# set policy tunnel-policy-in match application any
user@host# set policy tunnel-policy-in then permit tunnel ipsec-vpn ike-vpn pair-policy
tunnel-policy-out
```

10.       NAT      .

```

source-nat rule nat-out, match source-address 192.168.10.0/24
then ip 192.168.10.0/24

```

```

[edit security nat source rule-set nat-out]
user@host# set from zone trust
user@host# set to zone untrust
user@host# set rule interface-nat match source-address 192.168.10.0/24
user@host# set rule interface-nat match destination-address 0.0.0.0/0
user@host# set rule interface-nat then source-nat interface

```

```

[edit security policies from-zone trust to-zone untrust]
user@host# set policy any-permit match source-address any
user@host# set policy any-permit match destination-address any
user@host# set policy any-permit match application any
user@host# set policy any-permit then permit

```

#### 11. **any-permit** **any** **any**.

```

[edit security policies from-zone trust to-zone untrust]
user@host# insert policy tunnel-policy-out before policy any-permit

```

```

rule any-permit match source-address any
rule any-permit match destination-address any
rule any-permit match application any
rule any-permit then permit

```

#### 12. **tcp-mss** **ipsec-vpn** **mss** **1350**.

```

set security flow tcp-mss ipsec-vpn mss 1350

```

```

set security flow tcp-mss ipsec-vpn mss 1350
set security flow tcp-mss ipsec-vpn mss 1350

```

```

user@host# set security flow tcp-mss ipsec-vpn mss 1350
Example:
[edit]
user@host# set security flow tcp-mss ipsec-vpn mss 1350
user@host# commit and-quit

```

```
commit complete
Exiting configuration mode
```



in this section

- [IKE\(Internet Key Exchange\) 1?? ?? ?? | 370](#)
- [?? ?? ??? ?? ?? ?? ??? | 371](#)
- [IPsec 2?? ?? ?? | 372](#)
- [IPsec ?? ?? ?? ?? ?? | 373](#)
- [IPsec SA ?? ?? | 374](#)
- [VPN ??? ??? ??? ??? | 375](#)
- [?? ?? | 376](#)

??? ??? ???? ???? ????.

IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ?? ?? ??? ??? VPN ??? ???.

IPsec ??? ??? PKI? 1?? ?? ?? ????. 1??? ??? PKI? ??? ???.

??

?? ??? show security ike security-associations ??? ????.

```
user@host> show security ike security-associations
```



```

Algorithms:
Authentication : sha1
Encryption : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes : 10249
Output bytes : 4249
Input packets: 10
Output packets: 9
Flags: Caller notification sent
IPsec security associations: 2 created, 1 deleted
Phase 2 negotiations in progress: 0

```

??

???? ??(??? ?? ???), ??, ?? ??, ?? ??, ??? ?????, ??? ??, 2?? ?? ?? ?? ?? ?? IKE SA? ?? ??? ?????.

?? ????? ????? ??? ? ?????.

- IKE(Internet Key Exchange) SA? ??? ?????. ??? ??? ??? ?? ?? ? ?????.
- ??? ??? ??? ????? ??? ??? ?????.
- ?????? ?? ?? IPsec ?? ??? ?? ?????.
- ??? 2?? ??? ??? ?????.

## IPsec 2?? ?? ??

??

IPsec(2??) ?? ??? ???.

IKE(Internet Key Exchange) 1??? ????? IPsec(2??) ?? ??? ?????.

??

?? ????? show security ipsec security-associations ??? ?????.

```
user@host> show security ipsec security-associations
```

```
total configured sa: 2
```

```
ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys
```

```
<2 10.2.2.2 500 ESP:3des/sha1 bce1c6e0 1676/ unlim - 0
>2 10.2.2.2 500 ESP:3des/sha1 1a24eab9 1676/ unlim - 0
```

??

??? ??? ?????.

- ??? IPsec SA ?? ??? ? ?????. ?? ?? 500? ?? IKE ??? ????? ??????. ??? ??? NAT-T(Network Address Translation-Traversal), 4500 ?? ?? ?? ?????.
- SPI(?? ?? ?? ???) ? ?????? ??????. SA? ?? ?? ?? ??? ? ?? ?????? ??? ??????. ??? 1676/ unlim? ??? ?? ? 1676? ?? ?????? ??????? ???? ?? ??? ??? ?????.
- ID ??? ? IPsec SA? ?? ??? ? ? ?????.
- Mon ?? ???(-)? ? SA? ?? VPN ?????? ?????? ?????? ?????.
- ?? ???(vsys)? ????? 0???

2?? ??? VPN? ??? ? 1??? ????? ?? ??? 1?? ??? ? ? ????.

## IPsec ?? ?? ?? ?? ??

??

??? ??? ??? ?? IPsec SA ?? ??? ?????.

??

?? ????? show security ipsec security-associations index 2 detail ??? ?????.

```
user@host> show security ipsec security-associations index 2 detail
Virtual-system: Root
Local Gateway: 10.1.1.2, Remote Gateway: 10.2.2.2
Local Identity: ipv4_subnet(any:0,[0..7]=192.168.10.0/24)
Remote Identity: ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
DF-bit: clear
Policy-name: tunnel-policy-out
Direction: inbound, SPI: bce1c6e0, AUX-SPI: 0
Hard lifetime: Expires in 1667 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1093 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
```

```

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32
Direction: outbound, SPI: 1a24eab9, AUX-SPI: 0
Hard lifetime: Expires in 1667 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1093 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: enabled, Replay window size: 32

```

??

???? ID? ID? ?????.

??? ID ????? 2?? ??? ? ????. ??? ID? ?? ????(?? ?? VPN? ??). ?? ?? ? ?? ??? ??? ??? ?  
 ?? ????? ?? ?? ?? ?? ?????? ?????.

??? ID ????? 2???? ????? ??? ?? ??? ??? ????? ??? ?????? ??????. ?? ??? ?????? ??????. ?  
 ??? ?? ????? ?? ??? ?? ??? ?? ??? ?????? ?????.

?? ??, ??? ?? ?? ??????? ?? ?? ??? ?? ??? ?? ?? ?? ?? ?? ID? O?? ?????.

?? ?? ?? ??? ?? ??? ?? ?????? ?? ?????.

- ?? ?? 192.168.10.0/24 ? 10.10.20.0/24

- ?? ?? 192.168.168.0/24

- ??????? junos-http? ??

?? ??? ID? ?? 0.0.0.0/0, ?? 192.168.168.0/24, ??? 80???

?? ??? ID? ?? ??? ? ?? ????? ?? ????? ?? ?? ?? ????? ??? ? ???. ?? ?? ?????? ??????? ???? ? ?????  
 ??? ID? ????? ????? ? ?? ???.

IPsec? ????? ??? kmd ??? ?????? ??? ?????? set traceoptions. ??? ??? "IKE, PKI ? IPsec ?? ??" ??? 377? ?  
 ?????.

## IPsec SA ?? ??

??

IPsec SA? ?? ?? ? ??? ?????.

?? ??? ?? ESP/AH(Encapsulating Security Payload/Authentication Header) ????? ?? IPsec SA? ??? ???  
 ?.



??

?? **show security ipsec statistics index 2** ??? ?????.

```
user@host> show security ipsec statistics index 2
ESP Statistics:
Encrypted bytes: 674784
Decrypted bytes: 309276
Encrypted packets: 7029
Decrypted packets: 7029
AH Statistics:
Input bytes: 0
Output bytes: 0
Input packets: 0
Output packets: 0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, ESP decryption failures: 0
Bad headers: 0, Bad trailers: 0
```

??

??? ?? ? **0?** ?? ??? ?????.

? ??? ?? ? ??? **VPN** ??? ?? ?? ??? ????? ?? ?????, ? ??? ????? ??? ? ????? ?? ???, ?? ??? ?? ?? ??? ?????  
?

?? ??? ?? ??? ?????? ??? ????? **ESP** ??? ? ??? ????? ???. ??? ??? **"IKE, PKI ? IPsec ?? ??"** ??? **377?** ??????  
?

**VPN** ??? ??? ??? ???

??

1?? ? 2??? ?????? ??? ? **VPN?** ?? ??? ??? ???, ??? ????? ??? ??? ????? ? ????? ping . ?? ????? ?? ?????  
ping? ? ?????, ??? ????? ?????? ????? ping? ??? ?? ?????.

? ?? ??? ?????? ??????? ?? ????? ping ??? ?????? ??? ??????. ??? ????? ??????? ?? ??? ? ??? ?? ??? ?????? ??  
????? ??? ??? ?????? ?? ??????? ?????? ???.

? ??? **ge-0/0/0.0** ?????? ?? ????? ??? ?? ??? ?????, ?? ??? ? ??????? ? ??????? ????? ? ??? ? ??? ?????? ?  
??.

??

?? ping 192.168.168.10 interface ge-0/0/0 count 5 ???

```
user@host> ping 192.168.168.10 interface ge-0/0/0 count 5
PING 192.168.168.10 (192.168.168.10): 56 data bytes
64 bytes from 192.168.168.10: icmp_seq=0 ttl=127 time=8.287 ms
64 bytes from 192.168.168.10: icmp_seq=1 ttl=127 time=4.119 ms
64 bytes from 192.168.168.10: icmp_seq=2 ttl=127 time=5.399 ms
64 bytes from 192.168.168.10: icmp_seq=3 ttl=127 time=4.361 ms
64 bytes from 192.168.168.10: icmp_seq=4 ttl=127 time=5.137 ms
--- 192.168.168.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 4.119/5.461/8.287/1.490 ms
```

??

??

?? ping 192.168.10.10 from ethernet0/6 ???

??

?? ping 192.168.10.10 from ethernet0/6 ???

```
ssg5-> ping 192.168.10.10 from ethernet0/6

Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 192.168.10.10, timeout is 1 seconds from ethernet0/6
!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=4/4/5 ms
```

??

?? ping 192.168.10.10 from ethernet0/6 ??? SSG5

?? ping 192.168.10.10 from ethernet0/6 ESP

- ? ping 192.168.10.10 from ethernet0/6 IPsec "IPsec SA ? ?" 374

- [illegible]

## IKE, PKI, IPsec, VPN

in this section

- ?? ?? ?? ?? | 377
- ??? ?? ??? ??? ?? ?? | 378
- ?? ??? ??? ?? ??? ??? ?? ? FTP? ?? ?? ??? | 379
- IKE?? ??? ? ? ??? IKE ?? ?? ??? | 380
- PKI ?? ??? ??? IPsec?? ??? ?? | 381
- ???? IKE ?? ??? ??? ?? IKE ? PKI ?? ?? ?? | 382
- 1?? ?? ??? ?? | 382
- 1?? ?? ??? ??(?? ???) | 383
- 1?? ?? ??? ??(?? ??) | 384
- 1?? ?? ??? ??(?? ?? ??) | 384
- 2?? ?? ??? ?? | 385
- 2?? ?? ??? ?? | 386
- IKE ? PKI? ??? ??? ?? ?? | 386

IKE, PKI, IPsec, VPN.

?? ?? ?? ??

??

□□□□ □□ □□ □□□ □□□ □□□□.

1.    .
2.   .



```
/dev/md1 168M 7.6M 147M 5% /mfs
/cf/var/jail 213M 74M 137M 35% /jail/var
```

```
?( /dev/ad0s1a )  35%.
```

```
  FTP  
```

```
  
```

```
  IKE(Internet Key Exchange) ,  syslog  .
```

```
  
```

```
  , show log pkid, show log security-trace show log messages show log kmd.
```

```
user@host> show log kmd
user@host> show log pkid
user@host> show log security-trace
user@host> show log messages
```

```
  /var/log  show log .
```

```
  file copy FTP  .
```

```
(operational mode):
user@host> file copy path/filename dest-path/filename
Example:
```

```
user@host> file copy /var/log/kmd ftp://192.168.10.10/kmd.log
```

```
ftp://192.168.10.10/kmd.log 100% of 35 kB 12 MBps
```



**[?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?]. [?] [?] [?] [?] [?] [?].**

- [illegible]

??? ???? ???? ???? ????.

## PKI ??? ???? IPsec?? ??? ??

??

PKI [?] [?] [?] [?] [?] [?] IKE [?] [?] [?] [?] [?] [?] PKI [?] [?] [?] [?] [?] [?].

???

```
[edit security pki traceoptions]
```

```
user@host# set file ?
Possible completions:
<filename> Name of file in which to write trace information
files Maximum number of trace files (2..1000)
match Regular expression for lines to be logged
no-world-readable Don't allow any user to read the log file
size Maximum trace file size (10240..1073741824)
world-readable Allow any user to read the log file
```

```
[edit security pki traceoptions]
```

```
user@host# set flag ?
Possible completions:
all Trace with all flags enabled
```





???

```
Nov 7 11:52:14 Phase-1 [responder] done for local=ipv4(udp:500,[0..3]=
10.1.1.2) remote=fqdn(udp:500,[0..15]=ssg5.example.net)
Nov 7 11:52:14 Phase-2 [responder] done for
p1_local=ipv4(udp:500,[0..3]=10.1.1.2) p1_remote=fqdn(udp:500,[0..15]=ssg5.example.net)
p2_local=ipv4_subnet(any:0,[0..7]=192.168.10.0/24)
p2_remote=ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
```

?? ???? ???? ?????.

- 10.1.1.2- ?? ?????.
- ssg5.example.net - ?? ??(FQDN? ?? ???? ??).
- udp: 500- NAT-T? ???? ?????.
- Phase 1 [responder] done- ??(???? ?? ????)? ?? 1?? ??.
- Phase 2 [responder] done- ??? ID ??? ?? 1?? ??.

? ???? ?? ???? IPsec SA ??? ???? ???? "IKE(Internet Key Exchange) 1?? ?? ??" ??? 370.

**1?? ?? ???? ??(?? ???)**

??

IKE(Internet Key Exchange) 1?? ???? ???? show log kmd ??? ???? VPN? 1???? ???? ? ???? ???? ? ???? ?  
??.

???

```
Nov 7 11:52:14 Phase-1 [responder] failed with error(No proposal chosen) for
local=unknown(any:0,[0..0]=) remote=fqdn(udp:500,[0..15]=ssg5.example.net)
Nov 7 11:52:14 10.1.1.2:500 (Responder) <-> 10.2.2.2:500 { 011359c9 ddef501d - 2216ed2a bfc50f5f
[-
1] / 0x00000000 } IP; Error = No proposal chosen (14)
```

?? ???? ???? ?????.

- 10.1.1.2- ?? ?????.
- ssg5.example.net - ?? ??(FQDN? ?? ???? ??).

- udp: 500- NAT-T ???? ????.
- Phase-1 [responder] failed with error (No proposal chosen)—?? ???? ?? 1?? ??.

? ???? ???? ???? ???? ???? IKE(Internet Key Exchange) ???? 1?? ???? ?? ?? ???? ???? ???? ???? ???? VPN? ?? ?? ???? ???? ????.

**1?? ?? ???? ??(?? ??)**

??

IKE(Internet Key Exchange) 1?? ???? ???? ?? ???? show log kmd ??? ?????. ?? VPN? 1??? ???? ?? ???? ???? ? ???? ????.

???

```
Nov 7 12:06:36 Unable to find phase-1 policy as remote peer:10.2.2.2 is not recognized.
Nov 7 12:06:36 Phase-1 [responder] failed with error(Authentication failed) for
local=ipv4(udp:500,[0..3]=10.1.1.2) remote=ipv4(any:0,[0..3]=10.2.2.2)
Nov 7 12:06:36 10.1.1.2:500 (Responder) <-> 10.2.2.2:500 { f725ca38 dad47583 - dab1ba4c ae26674b
[-
1] / 0x00000000 } IP; Error = Authentication failed (24)
```

?? ???? ???? ????.

- 10.1.1.2- ?? ????.
- 10.2.2.2—?? ??
- Phase 1 [responder] failed with error (Authentication failed)—???? ???? ???? ???? ???? ???? ???? ???? ???? 1?? ??. PKI ???? ???? IKE? ?? ? ???? ???? ???? IKE ID ??? ???? ???? ????.

? ???? ???? ???? ???? ???? ???? ???? ???? IKE ID ??? ???? ????.

- ?? ?? ???? ?? ??
- ??? ???? ???? ???? ???? ???? DN ??

**1?? ?? ???? ??(?? ?? ??)**

??

IKE(Internet Key Exchange) 1?? ???? ???? ?? ???? show log kmd ??? ????.

???

```
Nov 7 13:52:39 Phase-1 [responder] failed with error(Timeout) for local=unknown(any:0,[0..0]=)
remote=ipv4(any:0,[0..3]=10.2.2.2)
```

?? ???? ???? ?????.

- 10.1.1.2- ?? ??.
- 10.2.2.2- ?? ??.
- Phase 1 [responder] failed with error(Timeout)- 1?? ??.

? ???? ?? ???? ?? ???? IKE ???? ???? ?? ???? ???? ???? ???? ????.

? ???? ?? ???? PKI ???? ???? ???? ???? PKI ?? ?? ???? ???? PKI? ???? ???? ???? ????.

**2?? ?? ???? ??**

??

IKE(Internet Key Exchange) 2?? ???? ???? ?? ???? show log kmd ???? ????.

???

```
Nov 7 11:52:14 Phase-1 [responder] done for local=ipv4(udp:500,[0..3]=
10.1.1.2) remote=fqdn(udp:500,[0..15]=ssg5.example.net)
Nov 7 11:52:14 Failed to match the peer proxy ids
p2_remote=ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
p2_local=ipv4_subnet(any:0,[0..7]=10.10.20.0/24) for the remote peer:ipv4(udp:500,
[0..3]=10.2.2.2)
Nov 7 11:52:14 KMD_PM_P2_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-2 [responder] failed for
p1_local=ipv4(udp:500,[0..3]=10.1.1.2) p1_remote=ipv4(udp:500,[0..3]=10.2.2.2)
p2_local=ipv4_subnet(any:0,[0..7]=10.10.20.0/24)
p2_remote=ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
Nov 7 11:52:14 10.1.1.2:500 (Responder) <-> 10.2.2.2:500 { 41f638eb cc22bbfe - 43fd0e85 b4f619d5
[0]
/ 0xc77fafcf } QM; Error = No proposal chosen (14)
```

?? ???? ???? ????.

- 10.1.1.2- ?? ????.

- ssg5.example.net - (FQDN IKE ID , ).
  - Phase 1 [responder] done—1.
  - Failed to match the peer proxy ids- ID. . ID 192.168.168.0/24( 10.10.20.0/24(?(service=any)(. . 192.168.10.0/24(?. . ID .
- ID .
- No proposal chosen. Failed to match the peer proxy ids.

## 2. .

.

IKE(Internet Key Exchange) . show log kmd .

.

```
Nov 7 11:52:14 Phase-1 [responder] done for local=ipv4(udp:500,[0..3]=
10.1.1.2) remote=fqdn(udp:500,[0..15]=ssg5.example.net)
Nov 7 11:52:14 10.1.1.2:500 (Responder) <-> 10.2.2.2:500 { cd9dff36 4888d398 - 6b0d3933 f0bc8e26
[0]
/ 0x1747248b } QM; Error = No proposal chosen (14)
```

.

- 10.1.1.2 - .
  - fqdn(udp:500,[0..15]=ssg5.example.net- .
  - Phase 1 [responder] done—1.
  - Error = No proposal chosen- 2. .
- 2.

## IKE ? PKI? ? ? ? ? ? ? ?

.

IKE ? PKI? ? ? ? ? ? ? ?.





? ?? IPsec VPN ??? ?? 1?? ????? ??? ????? ? ???? ???? OCSP(Online Certificate Status Protocol)? ????  
 ? ??? ?????? ???? ?????? ???? ??????.

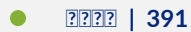
?? ??

.

- `?? ????? ? ?????. ? ?? ???? ???? SCRP(?? ?? ? ????)? ???? ? ? ????.`
- `??? ? ? ???? ? ? ?? ???? ????.`
- `?? ?????? ???? ???? ? ? ? ????.`

??

in this section



?? ???? ?? ??(CA) ??? OCSP-ROOT? ?? ???? ?????.

- CA `OCSP-ROOT`.
- `URL` `http://10.1.1.1:8080/scep/OCSP-ROOT/`. CA `SCEP` `URL`.
- OCSP `URL` `http://10.157.88.56:8210/OCSP-ROOT/`.
- `OCSP` `OCSP` `CRL` `URL` `http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45`.
- OCSP `CA` `OCSP` `CRL` `URL` `http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45`.

61 389 2(2) 2 222 222 122 222 22222.

61: OCSP 222 22 122 22 2

| 22                                   | 22 A                    | 22 B                    |
|--------------------------------------|-------------------------|-------------------------|
| IKE(Internet Key Exchange) 22        | ike_prop                | ike_prop                |
| 22 22                                | RSA 22                  | RSA 22                  |
| DH 22                                | group2                  | group2                  |
| 22 2222                              | SHA 1 (2222)            | SHA 1 (2222)            |
| 222 2222                             | 3DES CBC                | 3DES CBC                |
| IKE(Internet Key Exchange) 22        | ike_policy              | ike_policy              |
| 22                                   | 222                     | 222                     |
| 22                                   | ike_prop                | ike_prop                |
| 222                                  | 22 222 localcert1       | 22 222 localcert1       |
| IKE(Internet Key Exchange) 222<br>22 | jsr_gateway             | jsr_gateway             |
| 22                                   | ike_policy              | ike_policy              |
| 22222 22                             | 198.51.100.50           | 192.0.2.50              |
| 22 ID                                | localcert11.example.net | -                       |
| 22 ID                                | -                       | localcert11.example.net |

**61: OSCP 100 100 100 100 (Continued)**

| ??       | ?? A | ?? B       |
|----------|------|------------|
| ?? ????? | ??1  | ge-0/0/2.0 |
| ??       | v2   | v2         |

**62 390** (2) ? ??? ??? 2?? ??? ?????.

**62: OSCP 100 100 200 100**

| ??         | ?? A         | ?? B         |
|------------|--------------|--------------|
| IPsec ??   | ipsec_prop   | ipsec_prop   |
| ????       | ESP          | ESP          |
| ?? ?????   | HMAC SHA1-96 | HMAC SHA1-96 |
| ???? ????? | 3DES CBC     | 3DES CBC     |
| ????? ?(2) | 1200?        | 1200?        |
| ?? ?????   | 150,000      | 150,000      |
| IPsec ??   | ipsec_policy | ipsec_policy |
| PFC ?      | group2       | group2       |
| ??         | ipsec_prop   | ipsec_prop   |
| VPN        | test_vpn     | test_vpn     |
| ??? ?????  | st0.1        | st0.1        |







```

set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
set security ipsec proposal ipsec_prop lifetime-seconds 1200
set security ipsec proposal ipsec_prop lifetime-kilobytes 150000
set security ipsec policy ipsec_policy perfect-forward-secrecy keys group2
set security ipsec policy ipsec_policy proposals ipsec_prop
set security ipsec vpn test_vpn bind-interface st0.1
set security ipsec vpn test_vpn ike gateway jsr_gateway
set security ipsec vpn test_vpn ike ipsec-policy ipsec_policy

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? Junos OS CLI ??? ???? ?? ???? CLI ??? ??? ????  
??.

OCSP? ???? VPN ?? A? ???? ???? ????.

## 1. ???? ????.

```

[edit interfaces]
set ge-0/0/3 gigether-options redundant-parent reth1
set ge-9/0/3 gigether-options redundant-parent reth1
set lo0 unit 0 family inet address 172.16.1.100/24
set lo0 redundant-pseudo-interface-options redundancy-group 1
set reth1 redundant-ether-options redundancy-group 1
set reth1 unit 0 family inet address 192.0.2.0/24
set st0 unit 1 family inet address 172.18.1.100/24

```

## 2. CA ???? ????.

```

[edit security pki ca-profile OCSP-ROOT]
set ca-identity OCSP-ROOT
set enrollment url http://10.1.1.1:8080/scep/OCSP-ROOT/
set revocation-check ocs url http://10.157.88.56:8210/OCSP-ROOT/
set revocation-check use-ocsp
set revocation-check ocs disable-responder-revocation-check
set revocation-check ocs connection-failure fallback-crl
set revocation-check crl url http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45

```

### 3. 1?? 2?? 3????.

```
[edit security ike proposal ike_prop]
set authentication-method rsa-signatures
set dh-group group2
set authentication-algorithm sha1
set encryption-algorithm 3des-cbc

[edit security ike policy ike_policy]
set mode aggressive
set proposals ike_prop
set certificate local-certificate localcert1

[edit security ike gateway jsr_gateway]
set ike-policy ike_policy
set address 198.51.100.50
set remote-identity hostname localcert11.example.net
set external-interface reth1
set version v2-only
```

### 4. 2?? 3?? 4????.

```
[edit security ipsec proposal ipsec_prop]
set protocol esp
set authentication-algorithm hmac-sha1-96
set encryption-algorithm 3des-cbc
set lifetime-seconds 1200
set lifetime-kilobytes 150000

[edit security ipsec policy ipsec_policy]
set perfect-forward-secrecy keys group2
set proposals ipsec_prop

[edit security ipsec vpn test_vpn]
set bind-interface st0.1
set ike gateway jsr_gateway
set ike ipsec-policy ipsec_policy
```



```

    }
}
[edit]
user@host# show security pki ca-profile OCSP-ROOT
ca-identity OCSP-ROOT;
enrollment {
    url http://10.1.1.1:8080/scep/OCSP-ROOT/;
}
revocation-check {
    crl {
        url http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45;
    }
    ocsf {
        disable-responder-revocation-check;
        url http://10.157.88.56:8210/OCSP-ROOT/;
    }
    use-ocsp;
}
[edit]
user@host# show security ike
proposal ike_prop {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
policy ike_policy {
    mode aggressive;
    proposals ike_prop;
    certificate {
        local-certificate localcert1;
    }
}
gateway jsr_gateway {
    ike-policy ike_policy;
    address 10.10.2.50;
    remote-identity hostname localcert11.example.net;
    external-interface reth1;
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal ipsec_prop {

```

```

    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 1200;
    lifetime-kilobytes 150000;
}
policy ipsec_policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec_prop;
}
vpn test_vpn {
    bind-interface st0.1;
    ike {
        gateway jsr_gateway;
        ipsec-policy ipsec_policy;
    }
}

```

?? ?? ???? ? ???? commit?(?) ??????.

**?? B ??**

**CLI ?? ??**

OCSP? ?????? VPN ?? B? ????? ?????? ?? ??? ?????? ??? ??? ??????, ? ??? ?????, ?????? ??? ????? ? ??? ?? ??  
 ? ?????, ??? ????? [edit] ?? ??? CLI? ?????, ?? ????? ? ?????? **commit** .

```

set interfaces ge-0/0/2 unit 0 family inet address 198.51.100.0/24
set interfaces lo0 unit 0 family inet address 172.17.1.100/24
set interfaces st0 unit 1 family inet address 172.18.1.1/24
set security pki ca-profile OCSP-ROOT ca-identity OCSP-ROOT
set security pki ca-profile OCSP-ROOT enrollment url http://10.1.1.1:8080/scep/OCSP-ROOT/
set security pki ca-profile OCSP-ROOT revocation-check ocs url http://10.157.88.56:8210/OCSP-
ROOT/
set security pki ca-profile OCSP-ROOT revocation-check use-ocsp
set security pki ca-profile OCSP-ROOT revocation-check ocs disable-responder-revocation-check
set security pki ca-profile OCSP-ROOT revocation-check ocs connection-failure fallback-crl
set security pki ca-profile OCSP-ROOT revocation-check crl url http://10.1.1.1:8080/crl-as-der/
currentcrl-45.crlid=45

```

```

set security ike proposal ike_prop authentication-method rsa-signatures
set security ike proposal ike_prop dh-group group2
set security ike proposal ike_prop authentication-algorithm sha1
set security ike proposal ike_prop encryption-algorithm 3des-cbc
set security ike policy ike_policy mode aggressive
set security ike policy ike_policy proposals ike_prop
set security ike policy ike_policy certificate local-certificate localcert11
set security ike gateway jsr_gateway ike-policy ike_policy
set security ike gateway jsr_gateway address 192.0.2.50
set security ike gateway jsr_gateway local-identity hostname localcert11.example.net
set security ike gateway jsr_gateway external-interface ge-0/0/2.0
set security ike gateway jsr_gateway version v2-only
set security ipsec proposal ipsec_prop protocol esp
set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
set security ipsec proposal ipsec_prop lifetime-seconds 1200
set security ipsec proposal ipsec_prop lifetime-kilobytes 150000
set security ipsec policy ipsec_policy perfect-forward-secrecy keys group2
set security ipsec policy ipsec_policy proposals ipsec_prop
set security ipsec vpn test_vpn bind-interface st0.1
set security ipsec vpn test_vpn ike gateway jsr_gateway
set security ipsec vpn test_vpn ike ipsec-policy ipsec_policy
set security ipsec vpn test_vpn establish-tunnels immediately

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? Junos OS CLI ??? ???? ?? ???? CLI ??? ??? ????  
??.

OCSP? ???? VPN ?? B? ???? ???? ????.

1. ???? ????.

```

[edit interfaces]
set ge-0/0/2 unit 0 family inet address 198.51.100.0/24
set lo0 unit 0 family inet address 172.17.1.100/24
set st0 unit 1 family inet address 172.18.1.1/24

```



## 2. CA `ca` `ca`.

```
[edit security pki ca-profile OSCP-ROOT]
set ca-identity OSCP-ROOT
set enrollment url http://10.1.1.1:8080/scep/OCSP-ROOT/
set revocation-check ocs url http://10.157.88.56:8210/OCSP-ROOT/
set revocation-check use-ocs
set revocation-check ocs disable-responder-revocation-check
set revocation-check ocs connection-failure fallback-crl
set revocation-check crl url http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45
```

## 3. `1` `1` `1` `1`.

```
[edit security ike proposal ike_prop]
set authentication-method rsa-signatures
set dh-group group2
set authentication-algorithm sha1
set encryption-algorithm 3des-cbc

[edit security ike policy ike_policy]
set mode aggressive
set proposals ike_prop
set certificate local-certificate localcert1

[edit security ike gateway jsr_gateway]
set ike-policy ike_policy
set address 192.0.2.50
set local-identity hostname localcert11.example.net
set external-interface ge-0/0/2.0
set version v2-only
```

## 4. `2` `2` `2` `2`.

```
[edit security ipsec proposal ipsec_prop]
set protocol esp
set authentication-algorithm hmac-sha1-96
set encryption-algorithm 3des-cbc
set lifetime-seconds 1200
set lifetime-kilobytes 150000
```



```

enrollment {
    url http://10.1.1.1:8080/scep/OCSP-ROOT/;
}
revocation-check {
    crl {
        url http://10.1.1.1:8080/crl-as-der/currentcrl-45.crlid=45;
    }
    ocsd {
        disable-responder-revocation-check;
        url http://10.157.88.56:8210/OCSP-ROOT/;
    }
    use-ocsd;
}
[edit]
user@host# show security ike
proposal ike_prop {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
policy ike_policy {
    mode aggressive;
    proposals ike_prop;
    certificate {
        local-certificate localcert11;
    }
}
gateway jsr_gateway {
    ike-policy ike_policy;
    address 192.0.2.50;
    local-identity hostname localcert11.example.net;
    external-interface ge-0/0/2.0;
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 1200;
    lifetime-kilobytes 150000;
}

```



??

?? ???? ?? show security pki ca-certificate ca-profile OCSP-ROOT detail ?? show security pki ca-certificate ca-profile OCSP-ROOT ????.

```

user@host> show security pki ca-certificate ca-profile OCSP-ROOT
Certificate identifier: OCSP-ROOT
  Issued to: OCSP-ROOT, Issued by: C = US, O = example, CN = OCSP-ROOT
  Validity:
    Not before: 11-15-2013 22:26 UTC
    Not after: 11-14-2016 22:26 UTC
  Public key algorithm: rsaEncryption(2048 bits)

user@host> show security pki ca-certificate ca-profile OCSP-ROOT detail
Certificate identifier: OCSP-ROOT
  Certificate version: 3
  Serial number: 0000a17f
  Issuer:
    Organization: example, Country: US, Common name: OCSP-ROOT
  Subject:
    Organization: example, Country: US, Common name: OCSP-ROOT
  Subject string:
    C=US, O=example, CN=OCSP-ROOT
  Validity:
    Not before: 11-15-2013 22:26 UTC
    Not after: 11-14-2016 22:26 UTC
  Public key algorithm: rsaEncryption(2048 bits)
    30:82:01:0a:02:82:01:01:00:c6:38:e9:03:69:5e:45:d8:a3:ea:3d
    2e:e3:b8:3f:f0:5b:39:f0:b7:35:64:ed:60:a0:ba:89:28:63:29:e7
    27:82:47:c4:f6:41:53:c8:97:d7:1e:3c:ca:f0:a0:b9:09:0e:3d:f8
    76:5b:10:6f:b5:f8:ef:c5:e8:48:b9:fe:46:a3:c6:ba:b5:05:de:2d
    91:ce:20:12:8f:55:3c:a6:a4:99:bb:91:cf:05:5c:89:d3:a7:dc:a4
    d1:46:f2:dc:36:f3:f0:b5:fd:1d:18:f2:e6:33:d3:38:bb:44:8a:19
    ad:e0:b1:1a:15:c3:56:07:f9:2d:f6:19:f7:cd:80:cf:61:de:58:b8
    a3:f5:e0:d1:a3:3a:19:99:80:b0:63:03:1f:25:05:cc:b2:0c:cd:18
    ef:37:37:46:91:20:04:bc:a3:4a:44:a9:85:3b:50:33:76:45:d9:ba
    26:3a:3b:0d:ff:82:40:36:64:4e:ea:6a:d8:9b:06:ff:3f:e2:c4:a6
    76:ee:8b:58:56:a6:09:d3:4e:08:b0:64:60:75:f3:e2:06:91:64:73
    d2:78:e9:7a:cb:8c:57:0e:d1:9a:6d:3a:4a:9e:5b:d9:e4:a2:ef:31
    5d:2b:2b:53:ab:a1:ad:45:49:fd:a5:e0:8b:4e:0b:71:52:ca:6b:fa
    8b:0e:2c:7c:7b:02:03:01:00:01
  Signature algorithm: sha1WithRSAEncryption

```



Subject:  
 Organization: example, Organizational unit: example, State: california1, Locality: sunnyvale1, Common name: localcert1, Domain component: domain\_component1  
 Subject string:  
 DC=domain\_component1, CN=localcert1, OU=example, O=example, L=sunnyvale1, ST=california1, C=us1  
 Alternate subject: "localcert1@example.net", localcert1.example.net, 10.10.1.50  
 Validity:  
 Not before: 01-28-2014 22:23 UTC  
 Not after: 03-29-2014 22:53 UTC  
 Public key algorithm: rsaEncryption(1024 bits)  
 30:81:89:02:81:81:00:a6:df:c1:57:59:f8:4d:0f:c4:a8:96:25:97  
 03:c4:a0:fb:df:d5:f3:d5:56:b6:5a:26:65:b8:1a:ec:be:f6:c6:5f  
 b3:d7:d3:59:39:48:52:4a:e3:1b:e4:e0:6d:24:c3:c1:50:8c:55:3b  
 c0:c1:29:a0:45:29:8e:ec:3e:52:2f:84:b3:e8:89:9a:0f:8b:7d:e8  
 90:4b:c1:28:48:95:b3:aa:11:ab:b4:8c:a8:80:ce:90:07:2a:13:a2  
 2f:84:44:92:3b:be:7d:39:5b:2f:9a:4c:7a:2f:2d:31:8b:12:6d:52  
 34:7d:6b:e4:69:7e:f3:86:55:e2:89:31:98:c9:15:02:03:01:00:01  
 Signature algorithm: sha1WithRSAEncryption  
 Distribution CRL:  
 http://10.1.1.1:8080/crl-as-der/currentcrl-45.crl?id=45  
 Authority Information Access OCSP:  
 http://10.1.1.1/:8090/OCSP-ROOT/  
 Fingerprint:  
 00:c6:56:64:ad:e3:ce:8e:26:6b:df:17:1e:de:fc:14:a4:bb:8c:e4 (sha1)  
 7f:43:c6:ed:e4:b3:7a:4f:9a:8c:0b:61:95:01:c9:52 (md5)  
 Auto-re-enrollment:  
 Status: Disabled  
 Next trigger time: Timer not started

??

??? ??? ? ? ???? ? ? ???? ? ? ??? ???? ?????.

- DC- ??? ? ? ?.
- CN- ? ? ???? ?.
- OU- ? ? ? ? ?.
- O—??.
- L- ?/?/?

- ST- 00.
- C-00.
- Not before- 00 00 000000.
- Not after- 00 00 000000.

IKE(Internet Key Exchange) 100 00 00

00

0 00 0000000 IKE(Internet Key Exchange) 100 000 000000.

00

00 0000 show security ike security-associations 000 000000.

```
user@host> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
6534660 UP      3e62e05abd6a703f c552b238e8a26668 IKEv2 198.51.100.50
```

00 0000 show security ike security-associations detail 000 000000.

```
user@host> show security ike security-associations detail
IKE peer 198.51.100.50, Index 6534660, Gateway Name: jsr_gateway
Role: Responder, State: UP
Initiator cookie: 3e62e05abd6a703f, Responder cookie: c552b238e8a26668
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 192.0.2.50:500, Remote: 198.51.100.50:500
Lifetime: Expires in 26906 seconds
Peer ike-id: localcert11.example.net
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : 3des-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-2
Traffic statistics:
Input bytes  : 2152
Output bytes : 2097
Input packets: 4
```



```

Output packets:          4
Flags: IKE SA is created
IPSec security associations: 4 created, 0 deleted
Phase 2 negotiations in progress: 0

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 192.0.2.50:500, Remote: 198.51.100.50:500
Local identity: 192.0.2.50
Remote identity: localcert11.example.net
Flags: IKE SA is created

```

??

flags ??? ??? IKE(Internet Key Exchange) ?? ??? ???? ????.

## IPsec 2?? ?? ??

??

? ?? ???? IPsec 2?? ?? ????.

??

?? ???? show security ipsec security-associations ??? ????.

```

user@host> show security ipsec security-associations
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<131073 ESP:3des/sha1  9d1066e2 252/    150000 -   root 500    198.51.100.50
>131073 ESP:3des/sha1  82079c2c 252/    150000 -   root 500    198.51.100.50

```

?? ???? show security ipsec security-associations detail ??? ????.

```

user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: test_vpn
Local Gateway: 192.0.2.50, Remote Gateway: 198.51.100.50
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear

```

Bind-interface: st0.1

Port: 500, Nego#: 2, Fail#: 0, Def-Del#: 0 Flag: 0x600a29

Last Tunnel Down Reason: Delete payload received

Direction: inbound, SPI: 9d1066e2, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 249 seconds

Lifesize Remaining: 150000 kilobytes

Soft lifetime: Expires in 10 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc

Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: 82079c2c, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 249 seconds

Lifesize Remaining: 150000 kilobytes

Soft lifetime: Expires in 10 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc

Anti-replay service: counter-based enabled, Replay window size: 64

??

???? ipsec ?? ?? ?? ??? ?????.

?? ??

Junos OS?? PKI? ?? ??

# IPv6 IPsec VPN

summary

IPv6 IPsec VPN 配置步骤如下。

in this section

- IPv6 IPsec VPN 配置 | 409
- IPv6 IKE IPsec 配置 | 414
- IPv6 IPsec 配置 | 421
- 配置 IPv6 IPsec VPN | 421
- 配置 IPv6 IKE(Internet Key Exchange) IPsec VPN | 425
- 配置 IPv6 IPsec | 449

配置 IPv6 IPsec VPN 的步骤如下：  
1. 配置 IPv6 IPsec 配置。  
2. 配置 IPv6 IKE(Internet Key Exchange) IPsec VPN。  
3. 配置 IPv6 IPsec 配置。  
4. 配置 IPv6 IPsec VPN。

## IPv6 IPsec VPN 配置

配置 IPv6 IPsec VPN 的步骤如下：  
1. 配置 IPv6 IPsec 配置。  
2. 配置 IPv6 IKE(Internet Key Exchange) IPsec VPN。  
3. 配置 IPv6 IPsec 配置。  
4. 配置 IPv6 IPsec VPN。

63: VPN 配置 IPv6 IPsec

|               |    |                      |
|---------------|----|----------------------|
| 配置            | 配置 | 配置                   |
| IKEv1 和 IKEv2 | 配置 | 配置 IKEv1 和 IKEv2 配置。 |
| 配置 VPN        | 配置 | -                    |

### 63: VPN IPv6 (Continued)

| ??                                       | ??? | ?? ??                                                                                                                                                             |
|------------------------------------------|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?? ?? VPN                                | ?   | IPv6 ?? ?? VPN? ?? ???? ???? SRX ??? ???? ???? ????.                                                                                                              |
| ??? ? VPN                                | ?   | ???, ??? ? VPN? ?????. ??? NHTB(site-to-site VPN) ? ???? ?????. IPv4-in-IPv4 ?? ??? ? ???? ???? NHTB ??? ???? ? ????.                                             |
| ?? ????? VPN                             | ?   | –                                                                                                                                                                 |
| ?? ?? VPN                                | ?   | –                                                                                                                                                                 |
| AutoVPN                                  | ?   | ??? ? ??? ???? ? ? ? ???? ???? AutoVPN ???? ???? ???? ? IKE(Internet Key Exchange) ??? ? IPv6 ? ? ? ?????. Point-to-Multipoint ??? AutoVPN? IPv6 ? ??? ???? ????. |
| ?? VPN                                   | ??? | –                                                                                                                                                                 |
| ??? ? ??? ? ? ? ? ?                      | ?   | –                                                                                                                                                                 |
| Point-to-Multipoint ?? ? ? ? ?           | ??? | –                                                                                                                                                                 |
| ??? ? VPN? ?? ? ? ? ? ? ?                | ?   | –                                                                                                                                                                 |
| ??? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? | ?   | –                                                                                                                                                                 |
| ????? ? ? ? ?(RIP, OSPF, BGP) ???        | ?   | –                                                                                                                                                                 |
| ????? ? ? ? ?(PIM)                       | ??? | –                                                                                                                                                                 |
| ?? ???                                   | ?   | –                                                                                                                                                                 |

### 63: VPN **IPsec** IPv6 **IPsec** (Continued)

| ??                        | ??? | ?? ??                                                                                                                                                          |
|---------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ???                       | ??? | —                                                                                                                                                              |
| ?? ? ?? SA ? ? ??         | ?   | —                                                                                                                                                              |
| ?? SPU                    | ?   | —                                                                                                                                                              |
| ?? ?????                  | ?   | —                                                                                                                                                              |
| ??, ??, ??? ???           | ?   | —                                                                                                                                                              |
| SNMP ?? ?? ???(MIB)       | ?   | —                                                                                                                                                              |
| ?? ?? ??                  | ?   | <p>??? ?? ???? ?? ???? VPN ??? ?? ??? ?? ???? ???</p> <p>?? [edit security ike gateway <i>gateway-name</i>] ?? ???? ?</p> <p>? ???? local-address ?? ????.</p> |
| ??? ?? ??                 | ?   | —                                                                                                                                                              |
| IPv6? ?? Xauth ?? modecfg | ??? | —                                                                                                                                                              |
| SPC ???                   | ?   | —                                                                                                                                                              |
| ISSU                      | ?   | —                                                                                                                                                              |
| IKE ???? ???? DNS ??      | ?   | <p>IPv4 ??? ???? DNS ??? ?? ???? ?? ??? IPv6 ???? ???? ????.</p>                                                                                               |
| ?? ?? ? ?? ???? ??        | ?   | —                                                                                                                                                              |

### Table 63: VPN IPv6 (Continued)

| Feature                                              | Supported | Notes                                                                                                   |
|------------------------------------------------------|-----------|---------------------------------------------------------------------------------------------------------|
| IPv4 IKE(Internet Key Exchange) NAT-Traversal(NAT-T) | Yes       | NAT-T IKEv1 IPv6-in-IPv4 IPv4-in-IPv4 IPv6-in-IPv6 IPv4-in-IPv6. IKEv2 NAT-T IPv6 IPv4 IPv4 IPv6 NAT-T. |
| DPD(Dead Peer Detection) DPD                         | Yes       | DPD IPv6 IPv4.                                                                                          |
| SRX Junos OS 12.1X45-D10                             | Yes       | —                                                                                                       |
| IPv6 IPv4                                            | Yes       | —                                                                                                       |
| IKE(Internet Key Exchange) ID                        | Yes       | —                                                                                                       |
| ESP AH                                               | Yes       | IPv4.                                                                                                   |
| ESP AH                                               | Yes       | AH.                                                                                                     |
|                                                      | Yes       | —                                                                                                       |
| ID                                                   | Yes       | —                                                                                                       |
|                                                      | Yes       | IKEv1.                                                                                                  |
| IKE IPsec SA                                         | Yes       | —                                                                                                       |
| IKE SA                                               | Yes       | —                                                                                                       |
| VPN                                                  | Yes       | IPv6.                                                                                                   |

### 63: VPN IPv6 (Continued)

| ??                                                               | ??? | ?? ??                                                                                                                                                  |
|------------------------------------------------------------------|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| DF ??                                                            | ?   | IPv6-in-IPv6 ??? ?? DF ??? [edit security ipsec vpn <i>vpn-name</i> ] ?? ?????? ?????? ??????, df-bit clear ? ?? ?????.                                |
| ?? ???? ?????? ?? ?? ??(?? IPv4 ? IPv6 ??)                       | ?   | ?? ?? ??? ? VPN? ??, ?? IPv4 ??? IPv4-in-IPv4 ? IPv6-in-IPv4 ?? ?? ?????? ??? ? ???, ?? IPv6 ??? IPv4-in-IPv6 ? IPv6-in-IPv6 ?? ?? ?????? ??? ? ?????. |
| IPv6 ?? ??                                                       | ?   | IKE ? IPsec ??? ?? IPv6 ?? ??? IPv4 ??? ?????? ????? ? ?????, ?? ??? EH ? ??? ?? AH? ????? ?????.                                                      |
| ???? ? ???                                                       | ?   | –                                                                                                                                                      |
| VPN ?? ???                                                       | ?   | –                                                                                                                                                      |
| ????? ???                                                        | ??? | –                                                                                                                                                      |
| ?? IP ???(Screen, NAT, ALG, IPS, AppSecure)                      | ?   | –                                                                                                                                                      |
| ???? ?? IPv6 ??? ?? ?? ?? ??                                     | ??? | –                                                                                                                                                      |
| st0 ?????? OSPFv3 ??? ?? BFD(Bidirectional Forwarding Detection) | ??? | –                                                                                                                                                      |
| st0 ?????? ?? NDP(Neighbor Discovery Protocol)                   | ??? | –                                                                                                                                                      |
| PKI ??:                                                          |     |                                                                                                                                                        |
| ?? ????? PKI                                                     | ?   | –                                                                                                                                                      |
| RSA ?? ??(512??, 1024??, 2048?? ?? 4096?? ? ? ?)                 | ?   | –                                                                                                                                                      |

63: VPN IPsec (Continued)

| DSA (1024, 2048, 4096) |  | – |
|------------------------|--|---|
| ECDSA                  |  | – |
|                        |  | – |
| IPv4                   |  | – |
| IPv4                   |  | – |
| IPv6                   |  | – |
| IPv6                   |  | – |
| PKI IPsec              |  | – |

SEE ALSO

|                            |
|----------------------------|
| <a href="#">VPN   549</a>  |
| <a href="#">IPsec   11</a> |

IPv6 IKE IPsec

in this section

IPv6 IKE | 415

IPv6 IPsec | 416





## Table 64: ISAKMP ID Values (Continued)

| ID Value       | Description |
|----------------|-------------|
| ID_DER_ASN1_DN | 9           |
| ID_DER_ASN1_GN | 10          |
| ID_KEY_ID      | 11          |
| ID_LIST        | 12          |

ID\_IPV6\_ADDR\_RANGE: 16-255. IPv6 address range. 256-511. IPv6 address range. 512-767. IPv6 address range. 768-1023. IPv6 address range. 1024-1279. IPv6 address range. 1280-1535. IPv6 address range. 1536-2047. IPv6 address range. 2048-2559. IPv6 address range. 2560-3071. IPv6 address range. 3072-3583. IPv6 address range. 3584-4095. IPv6 address range. 4096-4607. IPv6 address range. 4608-5119. IPv6 address range. 5120-5631. IPv6 address range. 5632-6143. IPv6 address range. 6144-6655. IPv6 address range. 6656-7167. IPv6 address range. 7168-7679. IPv6 address range. 7680-8191. IPv6 address range. 8192-8703. IPv6 address range. 8704-9215. IPv6 address range. 9216-9727. IPv6 address range. 9728-10239. IPv6 address range. 10240-10751. IPv6 address range. 10752-11263. IPv6 address range. 11264-11775. IPv6 address range. 11776-12287. IPv6 address range. 12288-12799. IPv6 address range. 12800-13311. IPv6 address range. 13312-13823. IPv6 address range. 13824-14335. IPv6 address range. 14336-14847. IPv6 address range. 14848-15359. IPv6 address range. 15360-15871. IPv6 address range. 15872-16383. IPv6 address range. 16384-16895. IPv6 address range. 16896-17407. IPv6 address range. 17408-17919. IPv6 address range. 17920-18431. IPv6 address range. 18432-18943. IPv6 address range. 18944-19455. IPv6 address range. 19456-19967. IPv6 address range. 19968-20479. IPv6 address range. 20480-20991. IPv6 address range. 20992-21503. IPv6 address range. 21504-22015. IPv6 address range. 22016-22527. IPv6 address range. 22528-23039. IPv6 address range. 23040-23551. IPv6 address range. 23552-24063. IPv6 address range. 24064-24575. IPv6 address range. 24576-25087. IPv6 address range. 25088-25599. IPv6 address range. 25600-26111. IPv6 address range. 26112-26623. IPv6 address range. 26624-27135. IPv6 address range. 27136-27647. IPv6 address range. 27648-28159. IPv6 address range. 28160-28671. IPv6 address range. 28672-29183. IPv6 address range. 29184-29695. IPv6 address range. 29696-30207. IPv6 address range. 30208-30719. IPv6 address range. 30720-31231. IPv6 address range. 31232-31743. IPv6 address range. 31744-32255. IPv6 address range. 32256-32767. IPv6 address range. 32768-33279. IPv6 address range. 33280-33791. IPv6 address range. 33792-34303. IPv6 address range. 34304-34815. IPv6 address range. 34816-35327. IPv6 address range. 35328-35839. IPv6 address range. 35840-36351. IPv6 address range. 36352-36863. IPv6 address range. 36864-37375. IPv6 address range. 37376-37887. IPv6 address range. 37888-38399. IPv6 address range. 38400-38911. IPv6 address range. 38912-39423. IPv6 address range. 39424-39935. IPv6 address range. 39936-40447. IPv6 address range. 40448-40959. IPv6 address range. 40960-41471. IPv6 address range. 41472-41983. IPv6 address range. 41984-42495. IPv6 address range. 42496-43007. IPv6 address range. 43008-43519. IPv6 address range. 43520-44031. IPv6 address range. 44032-44543. IPv6 address range. 44544-45055. IPv6 address range. 45056-45567. IPv6 address range. 45568-46079. IPv6 address range. 46080-46591. IPv6 address range. 46592-47103. IPv6 address range. 47104-47615. IPv6 address range. 47616-48127. IPv6 address range. 48128-48639. IPv6 address range. 48640-49151. IPv6 address range. 49152-49663. IPv6 address range. 49664-50175. IPv6 address range. 50176-50687. IPv6 address range. 50688-51199. IPv6 address range. 51200-51711. IPv6 address range. 51712-52223. IPv6 address range. 52224-52735. IPv6 address range. 52736-53247. IPv6 address range. 53248-53759. IPv6 address range. 53760-54271. IPv6 address range. 54272-54783. IPv6 address range. 54784-55295. IPv6 address range. 55296-55807. IPv6 address range. 55808-56319. IPv6 address range. 56320-56831. IPv6 address range. 56832-57343. IPv6 address range. 57344-57855. IPv6 address range. 57856-58367. IPv6 address range. 58368-58879. IPv6 address range. 58880-59391. IPv6 address range. 59392-59903. IPv6 address range. 59904-60415. IPv6 address range. 60416-60927. IPv6 address range. 60928-61439. IPv6 address range. 61440-61951. IPv6 address range. 61952-62463. IPv6 address range. 62464-62975. IPv6 address range. 62976-63487. IPv6 address range. 63488-64000. IPv6 address range. 64000-64511. IPv6 address range. 64512-65023. IPv6 address range. 65024-65535. IPv6 address range. 65536-66047. IPv6 address range. 66048-66559. IPv6 address range. 66560-67071. IPv6 address range. 67072-67583. IPv6 address range. 67584-68095. IPv6 address range. 68096-68607. IPv6 address range. 68608-69119. IPv6 address range. 69120-69631. IPv6 address range. 69632-70143. IPv6 address range. 70144-70655. IPv6 address range. 70656-71167. IPv6 address range. 71168-71679. IPv6 address range. 71680-72191. IPv6 address range. 72192-72703. IPv6 address range. 72704-73215. IPv6 address range. 73216-73727. IPv6 address range. 73728-74239. IPv6 address range. 74240-74751. IPv6 address range. 74752-75263. IPv6 address range. 75264-75775. IPv6 address range. 75776-76287. IPv6 address range. 76288-76799. IPv6 address range. 76800-77311. IPv6 address range. 77312-77823. IPv6 address range. 77824-78335. IPv6 address range. 78336-78847. IPv6 address range. 78848-79359. IPv6 address range. 79360-79871. IPv6 address range. 79872-80383. IPv6 address range. 80384-80895. IPv6 address range. 80896-81407. IPv6 address range. 81408-81919. IPv6 address range. 81920-82431. IPv6 address range. 82432-82943. IPv6 address range. 82944-83455. IPv6 address range. 83456-83967. IPv6 address range. 83968-84479. IPv6 address range. 84480-84991. IPv6 address range. 84992-85503. IPv6 address range. 85504-86015. IPv6 address range. 86016-86527. IPv6 address range. 86528-87039. IPv6 address range. 87040-87551. IPv6 address range. 87552-88063. IPv6 address range. 88064-88575. IPv6 address range. 88576-89087. IPv6 address range. 89088-89599. IPv6 address range. 89600-90111. IPv6 address range. 90112-90623. IPv6 address range. 90624-91135. IPv6 address range. 91136-91647. IPv6 address range. 91648-92159. IPv6 address range. 92160-92671. IPv6 address range. 92672-93183. IPv6 address range. 93184-93695. IPv6 address range. 93696-94207. IPv6 address range. 94208-94719. IPv6 address range. 94720-95231. IPv6 address range. 95232-95743. IPv6 address range. 95744-96255. IPv6 address range. 96256-96767. IPv6 address range. 96768-97279. IPv6 address range. 97280-97791. IPv6 address range. 97792-98303. IPv6 address range. 98304-98815. IPv6 address range. 98816-99327. IPv6 address range. 99328-99839. IPv6 address range. 99840-100351. IPv6 address range. 100352-100863. IPv6 address range. 100864-101375. IPv6 address range. 101376-101887. IPv6 address range. 101888-102399. IPv6 address range. 102400-102911. IPv6 address range. 102912-103423. IPv6 address range. 103424-103935. IPv6 address range. 103936-104447. IPv6 address range. 104448-104959. IPv6 address range. 104960-105471. IPv6 address range. 105472-105983. IPv6 address range. 105984-106495. IPv6 address range. 106496-107007. IPv6 address range. 107008-107519. IPv6 address range. 107520-108031. IPv6 address range. 108032-108543. IPv6 address range. 108544-109055. IPv6 address range. 109056-109567. IPv6 address range. 109568-110079. IPv6 address range. 110080-110591. IPv6 address range. 110592-111103. IPv6 address range. 111104-111615. IPv6 address range. 111616-112127. IPv6 address range. 112128-112639. IPv6 address range. 112640-113151. IPv6 address range. 113152-113663. IPv6 address range. 113664-114175. IPv6 address range. 114176-114687. IPv6 address range. 114688-115199. IPv6 address range. 115200-115711. IPv6 address range. 115712-116223. IPv6 address range. 116224-116735. IPv6 address range. 116736-117247. IPv6 address range. 117248-117759. IPv6 address range. 117760-118271. IPv6 address range. 118272-118783. IPv6 address range. 118784-119295. IPv6 address range. 119296-119807. IPv6 address range. 119808-120319. IPv6 address range. 120320-120831. IPv6 address range. 120832-121343. IPv6 address range. 121344-121855. IPv6 address range. 121856-122367. IPv6 address range. 122368-122879. IPv6 address range. 122880-123391. IPv6 address range. 123392-123903. IPv6 address range. 123904-124415. IPv6 address range. 124416-124927. IPv6 address range. 124928-125439. IPv6 address range. 125440-125951. IPv6 address range. 125952-126463. IPv6 address range. 126464-126975. IPv6 address range. 126976-127487. IPv6 address range. 127488-127999. IPv6 address range. 128000-128511. IPv6 address range. 128512-129023. IPv6 address range. 129024-129535. IPv6 address range. 129536-130047. IPv6 address range. 130048-130559. IPv6 address range. 130560-131071. IPv6 address range. 131072-131583. IPv6 address range. 131584-132095. IPv6 address range. 132096-132607. IPv6 address range. 132608-133119. IPv6 address range. 133120-133631. IPv6 address range. 133632-134143. IPv6 address range. 134144-134655. IPv6 address range. 134656-135167. IPv6 address range. 135168-135679. IPv6 address range. 135680-136191. IPv6 address range. 136192-136703. IPv6 address range. 136704-137215. IPv6 address range. 137216-137727. IPv6 address range. 137728-138239. IPv6 address range. 138240-138751. IPv6 address range. 138752-139263. IPv6 address range. 139264-139775. IPv6 address range. 139776-140287. IPv6 address range. 140288-140799. IPv6 address range. 140800-141311. IPv6 address range. 141312-141823. IPv6 address range. 141824-142335. IPv6 address range. 142336-142847. IPv6 address range. 142848-143359. IPv6 address range. 143360-143871. IPv6 address range. 143872-144383. IPv6 address range. 144384-144895. IPv6 address range. 144896-145407. IPv6 address range. 145408-145919. IPv6 address range. 145920-146431. IPv6 address range. 146432-146943. IPv6 address range. 146944-147455. IPv6 address range. 147456-147967. IPv6 address range. 147968-148479. IPv6 address range. 148480-148991. IPv6 address range. 148992-149503. IPv6 address range. 149504-150015. IPv6 address range. 150016-150527. IPv6 address range. 150528-151039. IPv6 address range. 151040-151551. IPv6 address range. 151552-152063. IPv6 address range. 152064-152575. IPv6 address range. 152576-153087. IPv6 address range. 153088-153599. IPv6 address range. 153600-154111. IPv6 address range. 154112-154623. IPv6 address range. 154624-155135. IPv6 address range. 155136-155647. IPv6 address range. 155648-156159. IPv6 address range. 156160-156671. IPv6 address range. 156672-157183. IPv6 address range. 157184-157695. IPv6 address range. 157696-158207. IPv6 address range. 158208-158719. IPv6 address range. 158720-159231. IPv6 address range. 159232-159743. IPv6 address range. 159744-160255. IPv6 address range. 160256-160767. IPv6 address range. 160768-161279. IPv6 address range. 161280-161791. IPv6 address range. 161792-162303. IPv6 address range. 162304-162815. IPv6 address range. 162816-163327. IPv6 address range. 163328-163839. IPv6 address range. 163840-164351. IPv6 address range. 164352-164863. IPv6 address range. 164864-165375. IPv6 address range. 165376-165887. IPv6 address range. 165888-166399. IPv6 address range. 166400-166911. IPv6 address range. 166912-167423. IPv6 address range. 167424-167935. IPv6 address range. 167936-168447. IPv6 address range. 168448-168959. IPv6 address range. 168960-169471. IPv6 address range. 169472-169983. IPv6 address range. 169984-170495. IPv6 address range. 170496-171007. IPv6 address range. 171008-171519. IPv6 address range. 171520-172031. IPv6 address range. 172032-172543. IPv6 address range. 172544-173055. IPv6 address range. 173056-173567. IPv6 address range. 173568-174079. IPv6 address range. 174080-174591. IPv6 address range. 174592-175103. IPv6 address range. 175104-175615. IPv6 address range. 175616-176127. IPv6 address range. 176128-176639. IPv6 address range. 176640-177151. IPv6 address range. 177152-177663. IPv6 address range. 177664-178175. IPv6 address range. 178176-178687. IPv6 address range. 178688-179199. IPv6 address range. 179200-179711. IPv6 address range. 179712-180223. IPv6 address range. 180224-180735. IPv6 address range. 180736-181247. IPv6 address range. 181248-181759. IPv6 address range. 181760-182271. IPv6 address range. 182272-182783. IPv6 address range. 182784-183295. IPv6 address range. 183296-183807. IPv6 address range. 183808-184319. IPv6 address range. 184320-184831. IPv6 address range. 184832-185343. IPv6 address range. 185344-185855. IPv6 address range. 185856-186367. IPv6 address range. 186368-186879. IPv6 address range. 186880-187391. IPv6 address range. 187392-187903. IPv6 address range. 187904-188415. IPv6 address range. 188416-188927. IPv6 address range. 188928-189439. IPv6 address range. 189440-189951. IPv6 address range. 189952-190463. IPv6 address range. 190464-190975. IPv6 address range. 190976-191487. IPv6 address range. 191488-191999. IPv6 address range. 192000-192511. IPv6 address range. 192512-193023. IPv6 address range. 193024-193535. IPv6 address range. 193536-194047. IPv6 address range. 194048-194559. IPv6 address range. 194560-195071. IPv6 address range. 195072-195583. IPv6 address range. 195584-196095. IPv6 address range. 196096-196607. IPv6 address range. 196608-197119. IPv6 address range. 197120-197631. IPv6 address range. 197632-198143. IPv6 address range. 198144-198655. IPv6 address range. 198656-199167. IPv6 address range. 199168-199679. IPv6 address range. 199680-200191. IPv6 address range. 200192-200703. IPv6 address range. 200704-201215. IPv6 address range. 201216-201727. IPv6 address range. 201728-202239. IPv6 address range. 202240-202751. IPv6 address range. 202752-203263. IPv6 address range. 203264-203775. IPv6 address range. 203776-204287. IPv6 address range. 204288-204799. IPv6 address range. 204800-205311. IPv6 address range. 205312-205823. IPv6 address range. 205824-206335. IPv6 address range. 206336-206847. IPv6 address range. 206848-207359. IPv6 address range. 207360-207871. IPv6 address range. 207872-208383. IPv6 address range. 208384-208895. IPv6 address range. 208896-209407. IPv6 address range. 209408-209919. IPv6 address range. 209920-210431. IPv6 address range. 210432-210943. IPv6 address range. 210944-211455. IPv6 address range. 211456-211967. IPv6 address range. 211968-212479. IPv6 address range. 212480-212991. IPv6 address range. 212992-213503. IPv6 address range. 213504-214015. IPv6 address range. 214016-214527. IPv6 address range. 214528-215039. IPv6 address range. 215040-215551. IPv6 address range. 215552-216063. IPv6 address range. 216064-216575. IPv6 address range. 216576-217087. IPv6 address range. 217088-217599. IPv6 address range. 217600-218111. IPv6 address range. 218112-218623. IPv6 address range. 218624-219135. IPv6 address range. 219136-219647. IPv6 address range. 219648-220159. IPv6 address range. 220160-220671. IPv6 address range. 220672-221183. IPv6 address range. 221184-221695. IPv6 address range. 221696-222207. IPv6 address range. 222208-222719. IPv6 address range. 222720-223231. IPv6 address range. 223232-223743. IPv6 address range. 223744-224255. IPv6 address range. 224256-224767. IPv6 address range. 224768-225279. IPv6 address range. 225280-225791. IPv6 address range. 225792-226303. IPv6 address range. 226304-226815. IPv6 address range. 226816-227327. IPv6 address range. 227328-227839. IPv6 address range. 227840-228351. IPv6 address range. 228352-228863. IPv6 address range. 228864-229375. IPv6 address range. 229376-229887. IPv6 address range. 229888-230399. IPv6 address range. 230400-230911. IPv6 address range. 230912-231423. IPv6 address range. 231424-231935. IPv6 address range. 231936-232447. IPv6 address range. 232448-232959. IPv6 address range. 232960-233471. IPv6 address range. 233472-233983. IPv6 address range. 233984-234495. IPv6 address range. 234496-235007. IPv6 address range. 235008-235519. IPv6 address range. 235520-236031. IPv6 address range. 236032-236543. IPv6 address range. 236544-237055. IPv6 address range. 237056-237567. IPv6 address range. 237568-238079. IPv6 address range. 238080-238591. IPv6 address range. 238592-239103. IPv6 address range. 239104-239615. IPv6 address range. 239616-240127. IPv6 address range. 240128-240639. IPv6 address range. 240640-241151. IPv6 address range. 241152-241663. IPv6 address range. 241664-242175. IPv6 address range. 242176-242687. IPv6 address range. 242688-243199. IPv6 address range. 243200-243711. IPv6 address range. 243712-244223. IPv6 address range. 244224-244735. IPv6 address range. 244736-245247. IPv6 address range. 245248-245759. IPv6 address range. 245760-246271. IPv6 address range. 246272-246783. IPv6 address range. 246784-247295. IPv6 address range. 247296-247807. IPv6 address range. 247808-248319. IPv6 address range. 248320-248831. IPv6 address range. 248832-249343. IPv6 address range. 249344-249855. IPv6 address range. 249856-250367. IPv6 address range. 250368-250879. IPv6 address range. 250880-251391. IPv6 address range. 251392-251903. IPv6 address range. 251904-252415. IPv6 address range. 252416-252927. IPv6 address range. 252928-253439. IPv6 address range. 253440-253951. IPv6 address range. 253952-254463. IPv6 address range. 254464-254975. IPv6 address range. 254976-255487. IPv6 address range. 255488-255999. IPv6 address range. 256000-256511. IPv6 address range. 256512-257023. IPv6 address range. 257024-257535. IPv6 address range. 257536-258047. IPv6 address range. 258048-258559. IPv6 address range. 258560-259071. IPv6 address range. 259072-259583. IPv6 address range. 259584-260095. IPv6 address range. 260096-260607. IPv6 address range. 260608-261119. IPv6 address range. 261120-261631. IPv6 address range. 261632-262143. IPv6 address range. 262144-262655. IPv6 address range. 262656-263167. IPv6 address range. 263168-263679. IPv6 address range. 263680-264191. IPv6 address range. 264192-264703. IPv6 address range. 264704-265215. IPv6 address range. 265216-265727. IPv6 address range. 265728-266239. IPv6 address range. 266240-266751. IPv6 address range. 266752-267263. IPv6 address range. 267264-267775. IPv6 address range. 267776-268287. IPv6 address range. 268288-268799. IPv6 address range. 268800-269311. IPv6 address range. 269312-269823. IPv6 address range. 269824-270335. IPv6 address range. 270336-270847. IPv6 address range. 270848-271359. IPv6 address range. 271360-271871. IPv6 address range. 271872-272383. IPv6 address range. 272384-272895. IPv6 address range. 272896-273407. IPv6 address range. 273408-273919. IPv6 address range. 273920-274431. IPv6 address range. 274432-274943. IPv6 address range. 274944-275455. IPv6 address range. 275456-275967. IPv6 address range. 275968-276479. IPv6 address range. 276480-276991. IPv6 address range. 276992-277503. IPv6 address range. 277504-278015. IPv6 address range. 278016-278527. IPv6 address range. 278528-279039. IPv6 address range. 279040-279551. IPv6 address range. 279552-280063. IPv6 address range. 280064-280575. IPv6 address range. 280576-281087. IPv6 address range. 281088-281599. IPv6 address range. 281600-282111. IPv6 address range. 282112-282623. IPv6 address range. 282624-283135. IPv6 address range. 283136-283647. IPv6 address range. 283648-284159. IPv6 address range. 284160-284671. IPv6 address range. 284672-285183. IPv6 address range. 285184-285695. IPv6 address range. 285696-286207. IPv6 address range. 286208-286719. IPv6 address range. 286720-287231. IPv6 address range. 287232-287743. IPv6 address range. 287744-288255. IPv6 address range. 288256-288767. IPv6 address range. 288768-289279. IPv6 address range. 289280-289791. IPv6 address range. 289792-290303. IPv6 address range. 290304-290815. IPv6 address range. 290816-291327. IPv6 address range. 291328-291839. IPv6 address range. 291840-292351. IPv6 address range. 292352-292863. IPv6 address range. 292864-293375. IPv6 address range. 293376-293887. IPv6 address range. 293888-294399. IPv6 address range. 294400-294911. IPv6 address range. 294912-295423. IPv6 address range. 295424-295935. IPv6 address range. 295936-296447. IPv6 address range. 296448-296959. IPv6 address range. 296960-297471. IPv6 address range. 297472-297983. IPv6 address range. 297984-298495. IPv6 address range. 298496-299007. IPv6 address range. 299008-299519. IPv6 address range. 299520-300031. IPv6 address range. 300032-300543. IPv6 address range. 300544-301055. IPv6 address range. 301056-301567. IPv6 address range. 301568-302079. IPv6 address range. 302080-302591. IPv6 address range. 302592-303103. IPv6 address range. 303104-303615. IPv6 address range. 303616-304127. IPv6 address range. 304128-304639. IPv6 address range. 304640-305151. IPv6 address range. 305152-305663. IPv6 address range. 305664-306175. IPv6 address range. 306176-306687. IPv6 address range. 306688-307199. IPv6 address range. 307200-307711. IPv6 address range. 307712-308223. IPv6 address range. 308224-308735. IPv6 address range. 308736-309247. IPv6 address range. 309248-309759. IPv6 address range. 309760-310271. IPv6 address range. 310272-310783. IPv6 address range. 310784-311295. IPv6 address range. 311296-311807. IPv6 address range. 311808-312319. IPv6 address range. 312320-312831. IPv6 address range. 312832-313343. IPv6 address range. 313344-313855. IPv6 address range. 313856-314367. IPv6 address range. 314368-314879. IPv6 address range. 314880-315391. IPv6 address range. 315392-315903. IPv6 address range. 315904-316415. IPv6 address range. 316416-316927. IPv6 address range. 316928-317439. IPv6 address range. 317440-317951. IPv6 address range. 317952-318463. IPv6 address range. 318464-318975. IPv6 address range. 318976-319487. IPv6 address range. 319488-320000. IPv6 address range. 320000-32051



IPv4 ?? ?? ?? ? IPv6 ?? ??? AH ?????? ????? ?????.

?? ???? ?? ??

?? ???? ?? IPv4 ?? IPv6 ??? ?? ? ?? ???? ?? ??????? ?????. ?? IPv4 ?? IPv6 ??? ?? ? ?? ???? ?? ?? ? ?? ?? ? ? ?????. [? 66 ???? 419](#) ??? IPv6-in-IPv6 ?? IPv4-in-IPv6 ?? ???? ?? IPv6 ??? ?? IPv6 ?? IPv4 ??? ??? ? ? ???? ?????. ?? ?? ???? "Constructed"? ?? ?? ???? ?? ?? ?? ???? ?? ???? ???? ?????.

**? 66: IPv6-in-IPv6 ? IPv4-in-IPv6 ?? ???? ?? IPv6 ?? ??**

| ?? ??    | ??? ??? ?? ??    | ???????? ?? ?? |
|----------|------------------|----------------|
| ??       | 6.               | ?? ?? ??.      |
| DS ??    | ?? ???? ???????? | ?? ?? ??.      |
| ECN ??   | ?? ???? ???????? | ??.            |
| ??? ???? | 0.               | ?? ?? ??.      |
| ???? ??  | ??.              | ?? ?? ??.      |
| ?? ??    | AH, ESP ? ??? ?? | ?? ?? ??.      |
| ? ??     | 64.              | ??.            |
| src ??   | ??.              | ?? ?? ??.      |
| DEST ??  | ??.              | ?? ?? ??.      |
| ?? ??    | ???? ??????      | ?? ?? ??.      |

[? 67 ???? 420](#) ??? IPv6-in-IPv4 ?? IPv4-in-IPv4 ?? ???? ?? IPv4 ??? ?? IPv6 ?? IPv4 ??? ??? ???? ???? ? ? ???? ???? "Constructed"? ?? ?? ???? ?? ?? ?? ???? ?? ???? ???? ????.

## 67: IPv6-in-IPv4 ? IPv4-in-IPv4 ? ? ? ? ? IPv4 ? ? ?

| ?? ??       | ?? ??          | ?? ??     |
|-------------|----------------|-----------|
| ??          | 4.             | ?? ?? ??. |
| ?? ??       | ??.            | ?? ?? ??. |
| DS ??       | ?? ???? ?????. | ?? ?? ??. |
| ECN ??      | ?? ???? ?????. | ??.       |
| ? ??        | ??.            | ?? ?? ??. |
| ???         | ??.            | ?? ?? ??. |
| ???(DF, MF) | ??.            | ?? ?? ??. |
| ?? ???      | ??.            | ?? ?? ??. |
| TTL(TTL)    | 64.            | ??.       |
| ???         | ?, ESP         | ?? ?? ??. |
| ???         | ??.            | ??.       |
| src ??      | ??.            | ?? ?? ??. |
| DEST ??     | ??.            | ?? ?? ??. |
| ??          | ???? ????.     | ?? ?? ??. |

IPv6-in-IPv4 ?? ??? ? ? DF(Don't Fragment) ??? ???? ?????. df-bit set ?? df-bit copy ??? ? IPv4 VPN? ? [edit security ipsec vpn *vpn-name*] ? ???? ? ? , DF ??? ? IPv4 ??? ????.

IPv4-in-IPv4 [?? ???? ?? ??](#) IPv4 [????](#) DF [???? ??](#) IPv4 [???? ??](#) [???? ???? ?????](#) df-bit [????](#). [??](#) IPv4 [???? ?? ?\(?\)](#) [???? ?? ??](#) df-bit [??](#) IPv4 [????](#) DF [???? ?????](#).

SEE ALSO

- [IPsec \[??\]\(#\) | 11](#)
- [IPv6 IPsec \[?? ??\]\(#\) | 421](#)

IPv6 IPsec [?? ??](#)

[???? ?????](#) IPv6 IPsec VPN [?? ?? ?? ? ???? ???? ? ? ? ? ?](#) IKE(Internet Key Exchange) [? ?????](#).

- [?? ?](#) IKE(Internet Key Exchange) VPN - [?? ?](#) IKE(Internet Key Exchange) VPN [???? ? ? ?](#) IKE(Internet Key Exchange) [????? ???? ? ?](#) SA [???? ???? ???? ?](#). IPv6 [?? ?](#) IKE(Internet Key Exchange) VPN [? ???? 1???? 2???? ? ? ? ???? ???? ?](#).
- [1??](#) - [? ???? ???? IPsec SA ? ???? ? ? ? ? ? ? ?](#).
- [2??](#) - [? ???? ???? IPv6 ???? ???? ???? ???? ? ? IPsec SA ? ???? ?](#).

[1?? ? 2?? ???? ? ? ? ? ? ? ? "Internet Key Exchange" ???? 2? ???? ?](#)

SEE ALSO

- [?? ? IKE\(Internet Key Exchange\) ? ???? IPsec VPN \[?? ??\]\(#\) | 118](#)
- [?: IPv6 \[???? CA ???? ? ? ? ? ?\]\(#\)](#)

?: IPv6 IPsec [??](#) VPN [??](#)

in this section

[?? ?? | 422](#)

[?? | 422](#)

[?? | 422](#)





??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security ipsec vpn vpn-sunnyvale manual authentication algorithm hmac-md5-96 key ascii-text
"$ABC123"
set security ipsec vpn vpn-sunnyvale manual encryption algorithm 3des-cbc key ascii-text
"$ABC123"
set security ipsec vpn vpn-sunnyvale manual external-interface ge-0/0/14.0
set security ipsec vpn vpn-sunnyvale manual gateway 2001:db8:1212::1112
set security ipsec vpn vpn-sunnyvale manual protocol esp
set security ipsec vpn vpn-sunnyvale manual spi 12435
```

??? ??

?? ?? ?? ????? ??? ??? ??????. ?? ????? ??? ?? ??? CLI ??? ??? ? ? ???? CLI ??? ?? ??????.

?? ????? ?? ??:

1. ?? ?? ??? ??????.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set authentication algorithm hmac-md5-96 key ascii-text "$ABC123"
```

2. ??? ?? ??? ??????.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set encryption algorithm 3des-cbc key ascii-text "$ABC123"
```

3. SA? ?? ?? ??????? ??????.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set external-interface ge-0/0/14.0
```

#### 4. `set gateway 2001:db8:1212::1112`.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set gateway 2001:db8:1212::1112
```

#### 5. IPsec `set protocol esp`.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set protocol esp
```

#### 6. SPI `set spi 12435`.

```
[edit security ipsec vpn vpn-sunnyvale manual]
user@host# set spi 12435
```

??

?? `show security ipsec vpn vpn-sunnyvale` ??? ???? ???? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ???? ????  
 ????.

```
[edit]
[user@host]show security ipsec vpn vpn-sunnyvale
manual {
  gateway 2001:db8:1212::1112 ;
  external-interface ge-0/0/14.0 ;
  protocol esp ;
  spi 12435 ;
  authentication {
    algorithm hmac-md5-96 ;
    key ascii-text $ABC123" ;## SECRET DATA
  }
  encryption {
    algorithm 3des-cbc ;
    key ascii-text $ABC123"; ## SECRET DATA
  }
}
```

??

in this section

- [?? ???? ??](#) | 425

??? ??? ?????? ?????? ??? ??? ???????.

?? ???? ??

??

?? ?????? ?????? ??? ??????

??

?? ???? show security ipsec security-associations ??? ??????

SEE ALSO

- | [IPv6 IPsec ?? ??](#) | 421

**?: IPv6 ?? ? IKE(Internet Key Exchange) ?? ?? VPN ??**

in this section

- [?? ??](#) | 426
- [??](#) | 426
- [??](#) | 431
- [??](#) | 445



## Figure 27: IPv6 IKE(Internet Key Exchange) VPN

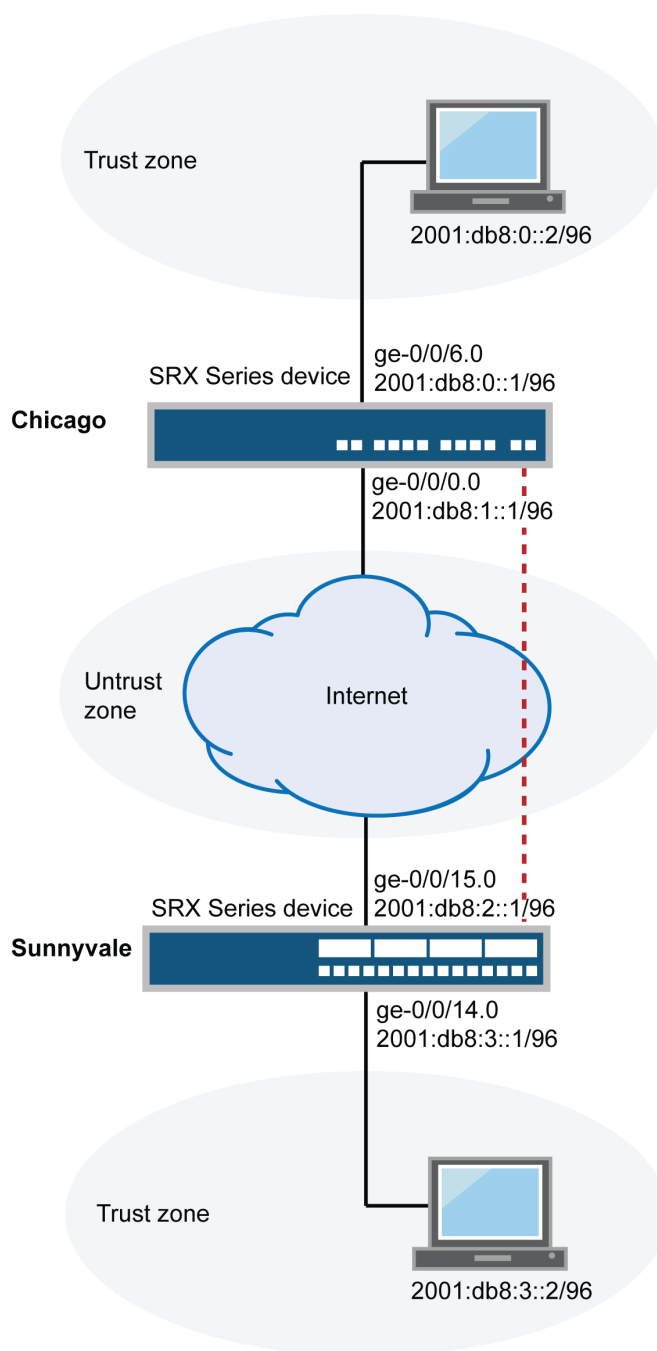


Figure 27 shows the IPv6 IKE VPN configuration. The configuration includes the following details:

- Chicago Site:**
  - Trust zone:** Contains a laptop with the IPv6 address `2001:db8:0::2/96`.
  - SRX Series device:**
    - Interface `ge-0/0/6.0` is connected to the Trust zone with address `2001:db8:0::1/96`.
    - Interface `ge-0/0/0.0` is connected to the Internet with address `2001:db8:1::1/96`.
- Internet:** Represented by a cloud, connecting the two sites.
- Sunnyvale Site:**
  - Untrust zone:** Contains the Internet cloud.
  - SRX Series device:**
    - Interface `ge-0/0/15.0` is connected to the Internet with address `2001:db8:2::1/96`.
    - Interface `ge-0/0/14.0` is connected to the Trust zone with address `2001:db8:3::1/96`.
  - Trust zone:** Contains a laptop with the IPv6 address `2001:db8:3::2/96`.

A red dashed line indicates the VPN tunnel between the `ge-0/0/0.0` interface in Chicago and the `ge-0/0/15.0` interface in Sunnyvale.

图 68: 配置策略, 策略 1 和策略 2

| 策略   | 策略          | 策略 1 和策略 2                                                                                                      |
|------|-------------|-----------------------------------------------------------------------------------------------------------------|
| 策略 1 | ge-0/0/14.0 | 2001::DB8:3::1/96                                                                                               |
|      | ge-0/0/15.0 | 2001::db8:0:2::1/96                                                                                             |
| 策略 2 | T1          | <ul style="list-style-type: none"><li>策略 1 和策略 2 配置。</li><li>ge-0/0/14.0 配置策略 1 和策略 2。</li></ul>                |
|      | 策略 2        | <ul style="list-style-type: none"><li>IKE(Internet Key Exchange)配置。</li><li>ge-0/0/15.0 配置策略 1 和策略 2。</li></ul> |
| 策略 3 | Sunnyvale   | <ul style="list-style-type: none"><li>策略 1 和策略 2 配置。</li><li>策略 1 和策略 2 配置 2001::db8:3::2/96。</li></ul>         |
|      | C1          | <ul style="list-style-type: none"><li>策略 1 和策略 2 配置。</li><li>策略 1 和策略 2 配置 2001::db8:0::2/96。</li></ul>         |

## ❓ 69: IPv6 IKE(Internet Key Exchange) 1?? ?? ?? ??

| ??    | ??                 | ?? ?? ??                                                                                                                                                                  |
|-------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??    | ipv6-ike-phase1-?? | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> <li>Diffie-Hellman ??: group2</li> <li>?? ?????: sha1</li> <li>??? ?????: aes-128-cbc</li> </ul>       |
| ??    | ipv6-ike-1??-??    | <ul style="list-style-type: none"> <li>?: ?????</li> <li>?? ??: ipv6-ike-phase1-??</li> <li>IKE(Internet Key Exchange) 1?? ?? ?? ??: pre-shared-key ascii-text</li> </ul> |
| ????? | gw-c ???           | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: ipv6-ike-1??-??</li> <li>?? ?????: ge-0/0/15.0</li> <li>????? ??: 2001:db8:1::96? 1?</li> </ul>  |

## ❓ 70: IPv6 IPsec 2?? ?? ?? ??

| ?? | ??                   | ?? ?? ??                                                                                                                     |
|----|----------------------|------------------------------------------------------------------------------------------------------------------------------|
| ?? | ipv6-ipsec-phase2-?? | <ul style="list-style-type: none"> <li>?????: esp</li> <li>?? ?????: hmac-sha1-96</li> <li>??? ?????: aes-128-cbc</li> </ul> |
| ?? | ipv6-ipsec-2??-??    | <ul style="list-style-type: none"> <li>?? ??: ipv6-ipsec-phase2-??</li> <li>PFS: Diffie-Hellman group2</li> </ul>            |





71: 71 71 71 71 71 (Continued)

| 71                                                                                                                                                                                                                                                                                                                                 | 71                | 71 71 71                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>7 71 7171 71717 71717 71717 71 71717 717177.</p> <p>permit-any 71 71 71 ipv6-vpn-tr-untr 7171 71717 7171.</p> <p>Junos OS 7171 7 7171 71 71 71717 717177. permit-any 71</p> <p>7 ipv6-vpn-tr-untr 71 71 71 71 71717 7171 71 71717</p> <p>permit-any 7171 71717 717177. 7171 ipv6-vpn-tr-untr 7171</p> <p>71717 71717 71717.</p> | <p>permit-any</p> | <ul style="list-style-type: none"><li>71 71:</li><li>71 source-address</li><li>71 source-destination</li><li>71 71717171</li><li>71: 71(Permit)</li></ul> |

72: TCP-MSS 71 71 71

| 71                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 71 71 71                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|
| <p>TCP-MSS TCP 371 7171717 7171 71717, TCP 717177 71 7171 71717 7171717 MTU 7171 7 7 7171 7171. IPsec</p> <p>7171 717177 IP 7 7171 717177 71 71 ESP 7171 7171 71717177 71 71 71(MTU)7 71717 71717 7171 7 71717 VPN 7</p> <p>7171 71 717177. 71717 71 71717 71717 7171 7171 717177.</p> <p>1500 7171 71 71 71(MTU)7 71 71717 7171 71 717177 71 71717 13507 71 717177. 7171 7171 71 71717 7171</p> <p>TCP-MSS 71 7171 7171 7 71717. 71 71, 7171 717177 71 71 71 71(MTU)7 71717 PPP 71 7171 71717 71 71 7171</p> <p>71 7171 71 71 71717 7 71 71717.</p> | <p>MSS 7:</p> <p>1350</p> |

71

in this section

- 71 717177, 71 7171 7 71717 7171 71 | 432
- IKE(Internet Key Exchange) 71 | 436
- IPsec 71 | 439
- 71 7171 71 | 441
- TCP-MSS 71 | 444

?? ???? , ?? ?? ? ??? ?? ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???? ???? , ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ?? , ?? ????? commit?(?) ?????.

```
set interfaces ge-0/0/14 unit 0 family inet6 address 2001:db8:3::1/96
set interfaces ge-0/0/15 unit 0 family inet6 address 2001:db8:2::1/96
set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
set security zones security-zone Untrust interfaces ge-0/0/15.0
set security zones security-zone Untrust host-inbound-traffic system-services ike
set security zones security-zone Trust interfaces ge-0/0/14.0
set security zones security-zone Trust host-inbound-traffic system-services all
set security address-book book1 address Sunnyvale 2001:db8:3::2/96
set security address-book book1 attach zone Trust
set security address-book book2 address Chicago 2001:db8:0::2/96
set security address-book book2 attach zone Untrust
```

??? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI ??? ?? ?????.

?? ???? , ?? ?? ? ??? ?? ????:

1. ??? ????? ???? ????.

```
[edit]
user@host# set interfaces ge-0/0/14 unit 0 family inet6 address 2001:db8:3::1/96
user@host# set interfaces ge-0/0/15 unit 0 family inet6 address 2001:db8:2::1/96
```

2. ?? ?? ??? ????.

```
[edit]
user@host# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
```

3. `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit]
user@host# edit security zones security-zone Untrust
```

4. `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone Untrust]
user@host# set interfaces ge-0/0/15.0
```

5. `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone Untrust]
user@host# set host-inbound-traffic system-services ike
```

6. TRust `? ? ? ? ? ? ? ?`.

```
[edit]
user@host# edit security zones security-zone Trust
```

7. `???? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone Trust]
user@host# set interfaces ge-0/0/14.0
```

8. `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone Trust]
user@host# set host-inbound-traffic system-services all
```

9. `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security address-book book1]
user@host# set address Sunnyvale 2001:db8:3::2/96
user@host# set attach zone Trust
```



```

        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/15.0;
    }
}
security-zone Trust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/14.0;
    }
}
[edit]
user@host# show security address-book
book1 {
    address Sunnyvale 2001:db8:3::2/96;
    attach {
        zone Trust;
    }
}
book2 {
    address Chicago 2001:db8:0::2/96;
    attach {
        zone Untrust;
    }
}

```

```

?? ?? ?? ?? ?? ?? commit?(?) ??.

```

```
[edit security ike proposal ipv6-ike-phase1-proposal]
user@host# set dh-group group2
```

4. IKE(Internet Key Exchange) `?? ?? ?????? ??????`.

```
[edit security ike proposal ipv6-ike-phase1-proposal]
user@host# set authentication-algorithm sha1
```

5. IKE(Internet Key Exchange) `?? ??? ?????? ??????`.

```
[edit security ike proposal ipv6-ike-phase1-proposal]
user@host# set encryption-algorithm aes-128-cbc
```

6. IKE(Internet Key Exchange) `1?? ??? ??????`.

```
[edit security ike]
user@host# set policy ipv6-ike-phase1-policy
```

7. IKE(Internet Key Exchange) `1?? ?? ??? ??????`.

```
[edit security ike policy ipv6-ike-phase1-policy]
user@host# set mode aggressive
```

8. IKE(Internet Key Exchange) `??? ?? ??? ??????`.

```
[edit security ike policy ipv6-ike-phase1-policy]
user@host# set proposals ipv6-ike-phase1-proposal
```

9. IKE(Internet Key Exchange) `1?? ?? ?? ??? ??????`.

```
[edit security ike policy ipv6-ike-phase1-policy]
user@host# set pre-shared-key ascii-text 1111111111111111
```

10. IKE(Internet Key Exchange) `1?? ?????? ?????? ?? ?????? ??????`.

```
[edit security ike]
user@host# set gateway gw-chicago external-interface ge-0/0/15.0
```

## 11. IKE(Internet Key Exchange) 1?? ? ???? ?????.

```
[edit security ike gateway gw-chicago]
user@host# set ike-policy ipv6-ike-phase1-policy
```

## 12. IKE(Internet Key Exchange) 1?? ?????? IP ??? ??????.

```
[edit security ike gateway gw-chicago]
user@host# set address 2001:db8:1::1
```

??

?? ????? show security ike ??? ????? ???? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ??? ?????? ?????.

```
[edit]
user@host# show security ike
proposal ipv6-ike-phase1-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ipv6-ike-phase1-policy {
    mode ;
    proposals ipv6-ike-phase1-proposal;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway gw-chicago {
    ike-policy ipv6-ike-phase1-policy;
    address 2001:db8:1::1;
    external-interface ge-0/0/15.0;
}
```

???? ???? ???? ? ? ???? commit?(?) ??????.







```

proposal ipv6-ipsec-phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy ipv6-ipsec-phase2-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipv6-ipsec-phase2-proposal;
}
vpn ipv6-ike-vpn-chicago {
    ike {
        gateway gw-chicago;
        ipsec-policy ipv6-ipsec-phase2-policy;
    }
}

```

?? ?? ???? ? ???? commit?(?) ??????.

?? ?? ??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?  
 ? ???? ???? CLI? ???? ???? ???? ???? ???? ???? ???? commit?(?) ??????.

```

set security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr match source-
address Sunnyvale
set security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr match destination-
address Chicago
set security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr match application
any
set security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr then permit tunnel
ipsec-vpn ipv6-ike-vpn-chicago
set security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr then permit tunnel
pair-policy ipv6-vpn-untr-tr
set security policies from-zone Untrust to-zone Trust policy ipv6-vpn-untr-tr match source-
address Chicago
set security policies from-zone Untrust to-zone Trust policy ipv6-vpn-untr-tr match destination-
address Sunnyvale
set security policies from-zone Untrust to-zone Trust policy ipv6-vpn-untr-tr match application

```

```
any
set security policies from-zone Untrust to-zone Trust policy ipv6-vpn-untr-tr then permit tunnel
ipsec-vpn ipv6-ike-vpn-chicago
set security policies from-zone Untrust to-zone Trust policy ipv6-vpn-untr-tr then permit tunnel
pair-policy ipv6-vpn-tr-untr
set security policies from-zone Trust to-zone Untrust policy permit-any match source-address any
set security policies from-zone Trust to-zone Untrust policy permit-any match destination-
address any
set security policies from-zone Trust to-zone Untrust policy permit-any match application any
set security policies from-zone Trust to-zone Untrust policy permit-any then permit
insert security policies from-zone Trust to-zone Untrust policy ipv6-vpn-tr-untr before policy
permit-any
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?? ?? ??:

1. ???? ???? ???? ???? ???? ???? ???? ????.

```
[edit security policies from-zone Trust to-zone Untrust]
user@host# set policy ipv6-vpn-tr-untr match source-address Sunnyvale
user@host# set policy ipv6-vpn-tr-untr match destination-address Chicago
user@host# set policy ipv6-vpn-tr-untr match application any
user@host# set policy ipv6-vpn-tr-untr then permit tunnel ipsec-vpn ipv6-ike-vpn-chicago
user@host# set policy ipv6-vpn-tr-untr then permit tunnel pair-policy ipv6-vpn-untr-tr
```

2. ?????(Untrust) ???? ???? ???? ???? ???? ???? ????.

```
[edit security policies from-zone Untrust to-zone Trust]
user@host# set policy ipv6-vpn-untr-tr match source-address Sunnyvale
user@host# set policy ipv6-vpn-untr-tr match destination-address Chicago
user@host# set policy ipv6-vpn-untr-tr match application any
user@host# set policy ipv6-vpn-untr-tr then permit tunnel ipsec-vpn ipv6-ike-vpn-chicago
user@host# set policy ipv6-vpn-untr-tr then permit tunnel pair-policy ipv6-vpn-tr-untr
```

3. `set policy permit-any match source-address any`

```
[edit security policies from-zone Trust to-zone Untrust]
user@host# set policy permit-any match source-address any
user@host# set policy permit-any match destination-address any
user@host# set policy permit-any match application any
user@host# set policy permit-any then permit
```

4. `vpn-tr-untr permit-any`

```
[edit security policies from-zone Trust to-zone Untrust]
user@host# insert policy ipv6-vpn-tr-untr before policy permit-any
```

??

?? show security policies

```
[edit]
user@host# show security policies
from-zone Trust to-zone Untrust {
  policy ipv6-vpn-tr-untr {
    match {
      source-address Sunnyvale;
      destination-address Chicago;
      application any;
    }
    then {
      permit {
        tunnel {
          ipsec-vpn ipv6-ike-vpn-chicago;
          pair-policy ipv6-vpn-untr-tr;
        }
      }
    }
  }
  policy permit-any {
    match {
      source-address any;
      destination-address any;
      application any;
```

```

    }
    then {
        permit
    }
}
}
from-zone Untrust to-zone Trust {
    policy ipv6-vpn-untr-tr {
        match {
            source-address Chicago;
            destination-address Sunnyvale;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn ipv6-ike-vpn-chicago;
                    pair-policy ipv6-vpn-tr-untr;
                }
            }
        }
    }
}
}
}

```

?? ?? ?? ?? commit?(?) ????.

## TCP-MSS ??

### CLI ?? ??

? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ???? ???? ? ???? ?? [edit] ?  
 ? ???? CLI? ??? ?? ??, ?? ???? commit?(?) ????.

```
set security flow tcp-mss ipsec-vpn mss 1350
```

?? ??

TCP-MSS ?? ??:

1. TCP-MSS `???` `??????`.

```
[edit]
user@host# set security flow tcp-mss ipsec-vpn mss 1350
```

??

?? `????` show security flow `??? ???? ???? ?????`. `??? ??? ???? ????? ???`, `? ?? ? ???? ???? ?????`.

```
[edit]
user@host# show security flow
tcp-mss {
  ipsec-vpn {
    mss 1350;
  }
}
```

???? `???` `????` `??` `????` commit`?(?)` `????`.

??

in this section

- [IKE\(Internet Key Exchange\) `1?? ?? ??` | 445](#)
- [IPsec `2?? ?? ??` | 448](#)

??? `???` `??????` `??????` `???` `???` `??????`:

**IKE(Internet Key Exchange) `1?? ?? ??`**

??

IKE(Internet Key Exchange) `1?? ??? ?????`.

??

?? ?????? ?????? ?? ?????? ?????? ?????? ?????? ?????? ?????? ?????? ?????? SRX  
 ?????? ?????? ?????? VPN ?????? ?????? ?????? ?????? VPN? ? ?? ?? ?????? VPN? ?? ?? ?? ? ?? ??????  
 ?? ?? ??????, ?? ?? 2001:db8:3::2/96 ?? 2001:db8:0::2/96?? ping? ??????.

?? ?????? show security ike security-associations ?????? ???????. ?????? ?????? ?? ? show security ike security-  
 associations index *index\_number* detail ?????? ??????.

```
user@host> show security ike security-associations
```

| Index | Remote Address | State | Initiator cookie | Responder cookie | Mode       |
|-------|----------------|-------|------------------|------------------|------------|
| 5     | 2001:db8:1::1  | UP    | e48efd6a444853cf | 0d09c59aafb720be | Aggressive |

```
user@host> show security ike security-associations index 5 detail
```

IKE peer 2001:db8:1::1, Index 5,

Role: Initiator, State: UP

Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aafb720be

Exchange type: Aggressive, Authentication method: Pre-shared-keys

Local: 2001:db8:2::1:500, Remote: 2001:db8:1::1:500

Lifetime: Expires in 19518 seconds

Peer ike-id: not valid

Xauth assigned IP: 0.0.0.0

Algorithms:

Authentication : sha1

Encryption : aes-128-cbc

Pseudo random function: hmac-sha1

Traffic statistics:

Input bytes : 1568

Output bytes : 2748

Input packets: 6

Output packets: 23

Flags: Caller notification sent

IPSec security associations: 5 created, 0 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 2900338624

Local: 2001:db8:2::1:500, Remote: 2001:db8:1::1:500

Local identity: ipv4\_subnet(any:0,[0..7]=0.0.0.0/0)

Remote identity: ipv4\_subnet(any:0,[0..7]=0.0.0.0/0)

Flags: Caller notification sent, Waiting for done





## IPsec 2?? ?? ??

??

IPsec 2?? ??? ?????.

??

?? ????? show security ipsec security-associations ??? ?????. ????? ??? ??? ? show security ipsec security-associations index *index\_number* detail ??? ?????.

```
user@host> show security ipsec security-associations
```

```
total configured sa: 2
```

| ID | Algorithm        | SPI      | Life:sec/kb | Mon | vsys | Port | Gateway       |
|----|------------------|----------|-------------|-----|------|------|---------------|
| 2  | ESP:aes-128/sha1 | 14caf1d9 | 3597/ unlim | -   | root | 500  | 2001:db8:1::1 |
| 2  | ESP:aes-128/sha1 | 9a4db486 | 3597/ unlim | -   | root | 500  | 2001:db8:1::1 |

```
user@host> show security ipsec security-associations index 2 detail
```

```
Virtual-system: Root
```

```
Local Gateway: 2001:db8:2::1, Remote Gateway: 2001:db8:1::1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
DF-bit: clear
```

```
Direction: inbound, SPI: 14caf1d9, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 3440 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2813 seconds
```

```
Mode: tunnel, Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 9a4db486, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 3440 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2813 seconds
```

```
Mode: tunnel, Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```



73: 73.1 73.2

| 73.1     | 73.2                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SRX 73.1 | <ul style="list-style-type: none"><li>IPv6 IPsec VPN 73.1.1 SRX300, SRX320, SRX340, SRX345 73.1.2 SRX550HM 73.1.3 73.1.4 73.1.5.</li><li>73.1.6 IPv6-in-IPv6 73.1.7 73.1.8 73.1.9 IPv6 IPsec VPN 73.1.10 73.1.11.</li><li>73.1.12 73.1.13 73.1.14/73.1.15 73.1.16 73.1.17 IPv6 IPsec VPN 73.1.18.</li><li>IPv6 IPsec VPN 73.1.19 SRX5400, SRX5600 73.1.20 SRX5800 73.1.21 73.1.22 73.1.23 73.1.24/73.1.25 73.1.26 73.1.27 IPv6 IPsec VPN 73.1.28 73.1.29 73.1.30.</li></ul> |

73.1 73.2

# 5

CHAPTER LABEL COVER PAGE

## ?? ?? VPN

---

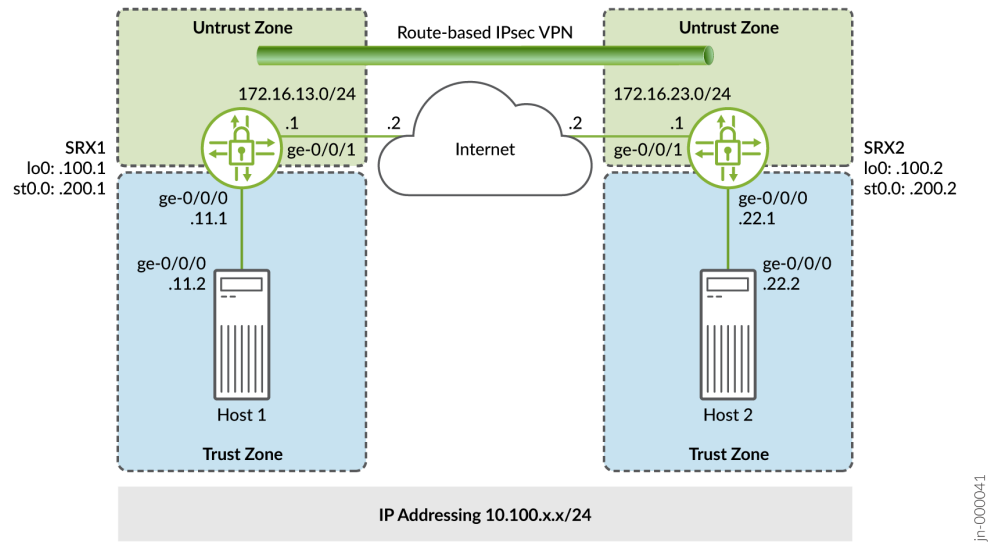
### in this chapter

- ?? ?? IPsec VPN | 452
  - IKEv2? ?? ?? VPN | 478
  - ?? ???? ?? ?? ???? | 537
  - ?? ??????? ?? ?? ?? ?? | 549
  - ?? ???? ?? IPsec VPN ?? | 567
  - ?? ?? VPN? ??? ??? | 578
-





?? 28: ?? ?? VPN ????



?? ?? ??, IPv4 ?? ?? ? ?? ??, ?? ?? IKE(Internet Key Exchange), ?? ?? ? TCP-MSS ?? ?? ??  
??, ? ?? ?? ?? ?? ?? ?? ?? ? 74 ??? 454~? 78 ??? 457(?) ??? ??.

? 74: SRX1? ????, ?? ??, ?? ?? ? ?? ?? ??

| ??     | ??               | ?? ?? ??                                                                       |
|--------|------------------|--------------------------------------------------------------------------------|
| ?????  | ge-0/0/0.0       | 10.100.11.1/24                                                                 |
|        | ge-0/0/1.0       | 172.16.13.1/24                                                                 |
|        | st0.0 (?? ?????) | 10.100.200.1/24                                                                |
| ?? ??? | 10.100.22.0/24   | ?? ?? st0.0???                                                                 |
|        | 0.0.0.0/0        | ?? ?? 172.16.13.2???                                                           |
| ?? ?   | ??               | <ul style="list-style-type: none"><li>ge-0/0/0.0 ?????? ? ??? ?????.</li></ul> |
|        | untrust          | <ul style="list-style-type: none"><li>ge-0/0/1.0 ?????? ? ??? ?????.</li></ul> |



#### 74: SRX1724F2, 7242, 7242 F242 F2 (Continued)

| ?? | ??  | ?? ?? ??                                                                       |
|----|-----|--------------------------------------------------------------------------------|
|    | VPN | <ul style="list-style-type: none"> <li>st0.0 222.222.2 222 222.222.</li> </ul> |

#### 75: IKE(Internet Key Exchange) 22 22 22

| ??     | ??      | ?? ?? ??                                                                                                                                                 |
|--------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??     | ??      | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> </ul>                                                                                 |
| ??     | IKE-POL | <ul style="list-style-type: none"> <li>?: main</li> <li>?? ??: ??</li> <li>IKE(Internet Key Exchange) 22 22 22: pre-shared-keys</li> </ul>               |
| 222222 | IKE-GW  | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) 22 22: IKE-POL</li> <li>?? 222222: ge-0/0/1</li> <li>222222 22: 172.16.23.1</li> </ul> |

#### 76: IPsec 22 22 22

| ?? | ??        | ?? ?? ??                                                    |
|----|-----------|-------------------------------------------------------------|
| ?? | ??        | <ul style="list-style-type: none"> <li>?? ?? ??</li> </ul>  |
| ?? | IPSEC-POL | <ul style="list-style-type: none"> <li>?? ??: ??</li> </ul> |

76: IPsec (Continued)

| VPN | VPN | <ul style="list-style-type: none"><li>• IKE(Internet Key Exchange) : IKE-GW</li><li>• IPsec : IPSEC-POL</li><li>• : st0.0</li><li>• establish-tunnels</li></ul> |
|-----|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|

77: VPN

| VPN | VPN-OUT | <ul style="list-style-type: none"><li>• :</li><li>• source-address Host1-Net</li><li>• destination-address Host2-Net</li><li>•</li><li>• : (Permit)</li></ul> |
|-----|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VPN | VPN-IN  | <ul style="list-style-type: none"><li>• :</li><li>• source-address Host2-Net</li><li>• destination-address Host1-Net</li><li>•</li><li>• : (Permit)</li></ul> |

```
set interfaces ge-0/0/0 unit 0 family inet address 10.100.11.1/24
set interfaces ge-0/0/1 unit 0 family inet address 172.16.13.1/24
set interfaces lo0 unit 0 family inet address 10.100.100.1/32
```





```

    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet {
      address 172.16.13.1/24;
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.100.100.1/32;
    }
  }
}
st0 {
  unit 0 {
    family inet {
      address 10.100.200.1/24;
    }
  }
}
}

```

```

[edit]
user@SRX1# show routing-options
static {
  route 10.100.22.0/24 next-hop st0.0;
  route 0.0.0.0/0 next-hop 172.16.13.2;
}

```

```

[edit]
user@SRX1# show security zones
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
  }
}

```

```

    interfaces {
        ge-0/0/0.0;
    }
}

security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
            ping;
        }
    }
}

interfaces {
    ge-0/0/1.0;
}

}

security-zone VPN {
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
}

interfaces {
    st0.0;
}

}

```

```
set security ike gateway IKE-GW address 172.16.23.1
set security ike gateway IKE-GW external-interface ge-0/0/1
```

???

?? ?? ? ???? ???? ???? ???? ?????. ??? ???? CLI ??? ???? ?????.

IKE(Internet Key Exchange) ??:

### 1. IKE(Internet Key Exchange) ??? ????.

```
[edit security ike]
user@SRX1# set proposal standard
```

### 2. IKE(Internet Key Exchange) ?? ?? ???? ????.

```
[edit security ike proposal standard]
user@SRX1# set authentication-method pre-shared-keys
```

### 3. IKE(Internet Key Exchange) ??? ????.

```
[edit security ike]
user@SRX1# set policy IKE-POL
```

### 4. IKE(Internet Key Exchange) ?? ??? ????.

```
[edit security ike policy IKE-POL]
user@SRX1# set mode main
```

### 5. IKE(Internet Key Exchange) ??? ?? ???? ????.

```
[edit security ike policy IKE-POL]
user@SRX1# set proposals standard
```



## 6. IKE(Internet Key Exchange) `?? ?? ??? ?????`.

```
[edit security ike policy IKE-POL]
user@SRX1# set pre-shared-key ascii-text $ABC123
```

## 7. IKE(Internet Key Exchange) `?????? ????? ? ???? ???? ?`.

```
[edit security ike]
user@SRX1# set gateway IKE-GW external-interface ge-0/0/1
```

## 8. IKE(Internet Key Exchange) `?? ??? ?????`.

```
[edit security ike gateway IKE-GW]
user@SRX1# set ike-policy IKE-POL
```

## 9. IKE(Internet Key Exchange) `????? ? ? ???? ?`.

```
[edit security ike gateway IKE-GW]
user@SRX1# set address 172.16.23.1
```

`??`

`?? ????? show security ike ??? ????? ???? ??????. ??? ??? ???? ???? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit]
user@SRX1# show security ike
proposal standard {
  authentication-method pre-shared-keys;
}
policy IKE-POL {
  mode main;
  proposals standard;
  pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway IKE-GW {
  ike-policy IKE-POL;
  address 172.16.23.1;
```

```
external-interface ge-0/0/1;
}
```

## IPsec [??](#)

### CLI [??](#) [??](#)

SRX1 [??](#) [?](#) [???](#) [???](#) [??????](#), [??](#) [???](#) [?????](#) [???](#) [???](#) [??](#) [??](#), [?????](#) [???](#) [?????](#) [??](#) [???](#) [??](#) [???](#) [?????](#), [??](#) [???](#) [edit] [?](#)  
[?](#) [???](#) CLI [??](#) [?](#) [???](#) [??](#) [??](#) [??](#) [???](#) **commit**[?](#)([?](#)) [??????](#).

```
set security ipsec proposal standard
set security ipsec policy IPSEC-POL proposals standard
set security ipsec vpn VPN-to-Host2 bind-interface st0.0
set security ipsec vpn VPN-to-Host2 ike gateway IKE-GW
set security ipsec vpn VPN-to-Host2 ike ipsec-policy IPSEC-POL
set security ipsec vpn VPN-to-Host2 establish-tunnels immediately
```

[????](#) [??](#)

[??](#) [??](#) [??](#) [?????](#) [???](#) [???](#) [???](#) [??????](#). [???](#) [???](#) CLI [???](#) [?????](#) [????????](#).

IPsec [??](#):

#### 1. IPsec [???](#) [??????](#).

```
[edit]
user@SRX1# set security ipsec proposal standard
```

#### 2. IPsec [???](#) [??????](#).

```
[edit security ipsec]
user@SRX1# set policy IPSEC-POL
```

#### 3. IPsec [??](#) [???](#) [??????](#).

```
[edit security ipsec policy IPSEC-POL]
user@SRX1# set proposals standard
```

#### 4. IKE(Internet Key Exchange) `???` `???`.

```
[edit security ipsec]
user@SRX1# set vpn VPN-to-Host2 ike gateway IKE-GW
```

#### 5. IPsec `???` `???`.

```
[edit security ipsec]
user@host# set vpn VPN-to-Host2 ike ipsec-policy IPSEC-POL
```

#### 6. `???` `???` `???`.

```
[edit security ipsec]
user@host# set vpn VPN-to-Host2 bind-interface st0.0
```

#### 7. `??` `???` `??` `???` `???`.

```
[edit security ipsec]
user@host# set vpn VPN-to-Host2 establish-tunnels immediately
```

`??`

`??` `???` show security ipsec `???` `???` `???` `???`. `???` `???` `???` `???` `???`, `?` `??` `??` `???` `???` `???`.

```
[edit]
user@host# show security ipsec
proposal standard;
policy IPSEC-POL {
    proposals standard;
}
vpn VPN-to-Host2 {
    bind-interface st0.0;
    ike {
        gateway IKE-GW;
        ipsec-policy IPSEC-POL;
    }
}
```

```
    establish-tunnels immediately;
}
```

?? ?? ??

## CLI ?? ??

SRX1? ?? ?? ??? ??? ?????, ? ?? ??? ?????, ?? ??? ??? ??? ??? ?? ?? ?? ??? ?????, ??? ?  
 ??? ? ??? ?? ??? ??? [edit] ?? ??? ??? CLI? ??? ?? ?? ?? ?? ??? **commit**?(?) ?????.

```
set security address-book Host1 address Host1-Net 10.100.11.0/24
set security address-book Host1 attach zone trust
set security address-book Host2 address Host2-Net 10.100.22.0/24
set security address-book Host2 attach zone VPN
set security policies from-zone trust to-zone untrust policy default-permit match source-address
any
set security policies from-zone trust to-zone untrust policy default-permit match destination-
address any
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone trust to-zone VPN policy VPN-OUT match source-address Host1-Net
set security policies from-zone trust to-zone VPN policy VPN-OUT match destination-address Host2-
Net
set security policies from-zone trust to-zone VPN policy VPN-OUT match application any
set security policies from-zone trust to-zone VPN policy VPN-OUT then permit
set security policies from-zone VPN to-zone trust policy VPN-IN match source-address Host2-Net
set security policies from-zone VPN to-zone trust policy VPN-IN match destination-address Host1-
Net
set security policies from-zone VPN to-zone trust policy VPN-IN match application any
set security policies from-zone VPN to-zone trust policy VPN-IN then permit
```

??? ??

?? ?? ?? ??? ???? ???? ???? ??????. ??? ??? CLI ??? ???? ??????.

?? ?? ??:

1. `?? ???? ???? ???? ? ? ? ? ? ? ? ?`.

```
[edit]
user@SRX1# set security address-book Host1 address Host1-Net 10.100.11.0/24
user@SRX1# set security address-book Host1 attach zone trust
user@SRX1# set security address-book Host2 address Host2-Net 10.100.22.0/24
user@SRX1# set security address-book Host2 attach zone VPN
```

2. `??????? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security policies from-zone trust to-zone untrust]
user@SRX1# set policy default-permit match source-address any
user@SRX1# set policy default-permit match destination-address any
user@SRX1# set policy default-permit match application any
user@SRX1# set policy default-permit then permit
```

3. `??? ? ? ? ? Host1?? VPN ??? Host2? ??? ???? ???? ? ? ? ?`.

```
[edit security policies from-zone trust to-zone VPN]
user@SRX1# set policy VPN-OUT match source-address Host1-Net
user@SRX1# set policy VPN-OUT match destination-address Host2-Net
user@SRX1# set policy VPN-OUT match application any
user@SRX1# set policy VPN-OUT then permit
```

4. `VPN ??? Host2?? ??? ? ? ? ? Host1? ???? ???? ? ? ? ?`.

```
[edit security policies from-zone VPN to-zone trust]
user@host# set policy VPN-IN match source-address Host2-Net
user@host# set policy VPN-IN match destination-address Host1-Net
user@host# set policy VPN-IN match application any
user@host# set policy VPN-IN then permit
```

??

?? ???? show security address-book ? show security policies ??? ???? ???? ?????. ??? ??? ???? ???? ???? ? ??  
 ?? ??? ???? ?????.

```
[edit]
user@host# show security address-book
Host1 {
    address Host1-Net 10.100.11.0/24;
    attach {
        zone trust;
    }
}
Host2 {
    address Host2-Net 10.100.22.0/24;
    attach {
        zone VPN;
    }
}
user@host# show security policies
from-zone trust to-zone untrust {
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone trust to-zone VPN {
    policy VPN-OUT {
        match {
            source-address Host1-Net;
            destination-address Host2-Net;
            application any;
        }
        then {
            permit;
        }
    }
}
```



??

?? ???? show security flow ??? ???? ???? ?????. ??? ??? ??? ???? ???? , ? ?? ?? ??? ???? ?????.

```
[edit]
user@SRX1# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```

???? ??? ???? ? ? ???? commit?(?) ?????.

## SRX2 ??

### CLI ?? ??

??? SRX2? ??? ?????.

? ?? ??? ??? ?????, ?? ??? ???? ???? ???? ? ? ? ? ? ? ???? ???? , ???? ???? ???? ? ???? ? ? ???? ????  
 ?? ???? [edit] ??? ???? CLI? ?? ?? ?? , ?? ???? commit?(?) ?????.

```
set security ike proposal standard authentication-method pre-shared-keys
set security ike policy IKE-POL mode main
set security ike policy IKE-POL proposals standard
set security ike policy IKE-POL pre-shared-key ascii-text $ABC123
set security ike gateway IKE-GW ike-policy IKE-POL
set security ike gateway IKE-GW address 172.16.13.1
set security ike gateway IKE-GW external-interface ge-0/0/1
set security ipsec proposal standard
set security ipsec policy IPSEC-POL proposals standard
set security ipsec vpn VPN-to-Host1 bind-interface st0.0
set security ipsec vpn VPN-to-Host1 ike gateway IKE-GW
set security ipsec vpn VPN-to-Host1 ike ipsec-policy IPSEC-POL
set security ipsec vpn VPN-to-Host1 establish-tunnels immediately
set security address-book Host1 address Host1-Net 10.100.11.0/24
set security address-book Host1 attach zone VPN
set security address-book Host2 address Host2-Net 10.100.22.0/24
set security address-book Host2 attach zone trust
```



```

set security flow tcp-mss ipsec-vpn mss 1350
set security policies from-zone trust to-zone untrust policy default-permit match source-address
any
set security policies from-zone trust to-zone untrust policy default-permit match destination-
address any
set security policies from-zone trust to-zone untrust policy default-permit match application any
set security policies from-zone trust to-zone untrust policy default-permit then permit
set security policies from-zone trust to-zone VPN policy VPN-OUT match source-address Host2-Net
set security policies from-zone trust to-zone VPN policy VPN-OUT match destination-address Host1-
Net
set security policies from-zone trust to-zone VPN policy VPN-OUT match application any
set security policies from-zone trust to-zone VPN policy VPN-OUT then permit
set security policies from-zone VPN to-zone trust policy VPN-IN match source-address Host1-Net
set security policies from-zone VPN to-zone trust policy VPN-IN match destination-address Host2-
Net
set security policies from-zone VPN to-zone trust policy VPN-IN match application any
set security policies from-zone VPN to-zone trust policy VPN-IN then permit
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone VPN host-inbound-traffic system-services ping
set security zones security-zone VPN interfaces st0.0
set interfaces ge-0/0/0 unit 0 family inet address 10.100.22.1/24
set interfaces ge-0/0/1 unit 0 family inet address 172.16.23.1/24
set interfaces lo0 unit 0 family inet address 10.100.100.2/32
set interfaces st0 unit 0 family inet address 10.100.200.2/24
set routing-options static route 10.100.11.0/24 next-hop st0.0
set routing-options static route 0.0.0.0/0 next-hop 172.16.23.2

```

??

#### in this section

- [IKE\(Internet Key Exchange\) ?? ?? | 472](#)
- [IPsec ??? ???? | 474](#)
- [VPN ??? ??? ???? | 476](#)
- [IPsec ?? ???? ?? ?? ? ?? | 476](#)



```
show security ike security-associations [?] [?] [?] IKE(Internet Key Exchange) SA? [?] [?] SA? [?] [?] [?] [?]
[?] , IKE [?] [?] [?] [?] [?] [?] [?] IKE(Internet Key Exchange) [?] [?] [?] [?] [?] [?] [?] [?] [?] [?].
```

- `?? - ? ? ? IKE(Internet Key Exchange) ? ? ? ? ? SA ? ? ? ? ? ? ? ? show security ike security-associations index detail ? ? ? ? ? ? ? ?`.

● ?

- **IPsec** - IKE(Internet Key Exchange) SA, SPI, ID, etc.

□□□□ □□ □□□ □□□□ □□□□□.

- IKE(Internet Key Exchange) ?? ?? ??

- $\boxed{??} \boxed{??} \boxed{??} (\boxed{?} \boxed{???} \boxed{??} \boxed{????} \boxed{???})$

● ☐ ☐

- ??? ??(???? ???? ???? ?? ???? ? ???? ? ????)

- `?? ??`

`?? ??? ???? ???? ???? ???? ? ? ?????.`

- `??? ? ??? ??`
- `??? IPsec SA? ?`
- `?? ?? ?? ?`

## IPsec `??? ?????.`

`??`

IPsec `??? ?????.`

`??`

`?? ???? show security ipsec security-associations ??? ?????.` `??? ???? ???? ? ? show security ipsec security-associations index index_number detail ??? ?????.`

```
user@SRX1> show security ipsec security-associations
```

```
Total active tunnels: 1      Total Ipsec sas: 1
```

| ID      | Algorithm     | SPI      | Life:sec/kb | Mon | lsys | Port | Gateway     |
|---------|---------------|----------|-------------|-----|------|------|-------------|
| <131074 | ESP:3des/sha1 | 912f9063 | 3403/ unlim | -   | root | 500  | 172.16.23.1 |
| >131074 | ESP:3des/sha1 | 71dbaa56 | 3403/ unlim | -   | root | 500  | 172.16.23.1 |

```
user@SRX1> show security ipsec security-associations index 131074 detail
```

```
ID: 131074 Virtual-system: root, VPN Name: VPN-to-Host2
```

```
Local Gateway: 172.16.13.1, Remote Gateway: 172.16.23.1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Version: IKEv1
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.0
```

```
Port: 500, Nego#: 26, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
```

```
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
```

```
Tunnel events:
```

```
Fri Jul 23 2021 10:46:34 -0700: IPsec SA negotiation successfully completed (23 times)
```

```
Fri Jul 23 2021 09:07:24 -0700: IKE SA negotiation successfully completed (3 times)
```

```
Thu Jul 22 2021 16:34:17 -0700: Negotiation failed with INVALID_SYNTAX error (3 times)
```

```
Thu Jul 22 2021 16:33:50 -0700: Tunnel configuration changed. Corresponding IKE/IPsec SAs are deleted (1 times)
```

```

Thu Jul 22 2021 16:23:49 -0700: IPSec SA negotiation successfully completed (2 times)
Thu Jul 22 2021 15:34:12
: IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
Thu Jul 22 2021 15:33:25 -0700: IPSec SA negotiation successfully completed (1 times)
Thu Jul 22 2021 15:33:25
: Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
Thu Jul 22 2021 15:33:25 -0700: External interface's address received. Information updated
(1 times)
Thu Jul 22 2021 15:33:25 -0700: Bind-interface's zone received. Information updated (1 times)
Thu Jul 22 2021 10:34:55 -0700: IKE SA negotiation successfully completed (1 times)
Thu Jul 22 2021 10:34:46 -0700: No response from peer. Negotiation failed (16 times)
Direction: inbound, SPI: 912f9063, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3302 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2729 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 71dbaa56, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3302 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2729 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64

```

??

```
show security ipsec security-associations [?? [??] [?] [??] [????].
```

- ID 131074. SA 131074 show security ipsec security-associations index 131074.
- 500 IPsec SA 131074, NAT-Traversal 131074. (NAT-traversal 131074 4500 131074 131074.)
- SPI, 131074 131074(131074 KB 131074) 131074 131074. 3403/ 131074 131074 3403 131074, 131074 131074 131074 131074. VPN 131074 131074 131074 IPsec IKE(Internet Key Exchange) 131074 131074, 131074 131074 131074.
- VPN 131074 Mon 131074 131074, SA 131074 131074. VPN 131074 131074 131074, U 131074 up 131074 D 131074 131074 down 131074 131074.

- `?? ?(vsys)? ?? ????? ?? 0? ?????.`

```
show security ipsec security-associations index 131074 detail [redacted] [redacted] [redacted] [redacted] [redacted].
```

- $?? \text{ ID } ? \text{ } ?? \text{ ID } ? \text{ SA } ? \text{ } ??? \text{ ID } ? \text{ } ??????$ .

```

[??] ID [??] IPsec [??] [?] [??] [?] [?] [??]. IPsec SA? [??] [?] [?] [??] ID [??] [??] IPsec [??] [?] [??] [??]
[?] [??]. [?] [?] VPN? [?] [?] [??] ID? local=0.0.0.0/0, remote=0.0.0.0/0, [??] service=any[??]. [??] [?]
IP? [?] [?] [?] VPN?? [??] [??] [?] [??]. [?] [?] IPsec SA? [?] [?] [??] ID? [??] [??]. [?] [?] [??] [?] [??] ID?
[??] [??] [??] [??].

```

- IPsec `???` `??` `?` `??` `????` `????` ST `?????` `????` `????` `????` `??????`. IPsec `????` `??` `??` kmd `??` `??` `??` `???` `????` `??`.

## VPN [ ] [ ] [ ] [ ]

??

VPN [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ].

??

Host1 [?] ping [?] Host2[?] [?] [?] [?] [?].

```
user@Host1> ping 10.100.22.1 rapid count 100
PING 10.100.22.1 (10.100.22.1): 56 data bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
--- 10.100.22.1 ping statistics ---
100 packets transmitted, 100 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.146/3.824/6.193/0.402 ms
```

??

Host1?? ping ??? ???? ??, ???, ?? ??, ?? ??? ?? ESP ??? ??? ? ???? ???? ?? ? ?????.

**IPsec**

??

IPsec [??] [???] [??] ESP [?] [??] [??] [???] [?] [???] [?????].



# IKEv2? ???? ?? ?? VPN

in this section

- [?: IKEv2? ?? ?? ?? VPN ?? | 479](#)
- [?: IKEv2 ?? ?????? ??? Pico ? ??????? ?? SRX ??? ?? | 503](#)
- [??? ? ?? CA? IKE\(Internet Key Exchange\) ?? | 535](#)

IKEv2(Internet Key Exchange version 2)? ?? VPN ????? ?? ?? VPN ?? ??? ???? IPsec SA(?? ??)? ?? ?? ?  
???? ???? ???? ???? IPsec ?? ??? ????????

[? 79](#) [??? 478](#) ?(?) IPsec Radius xAuth ?? CP ?? ??????

**? 79: IPsec RADIUS xAuth ?? CP ?**

| Radius ?? | ?? ID | ?? ??            | ???? ID(??)      | ???? ?? ID | ?? ?  | ??      |
|-----------|-------|------------------|------------------|------------|-------|---------|
| ??        | 8     | ???? IP ??       | NA               | NA         | IP ?? | IPv4 ?? |
| ??        | 9     | ??? IP ?????     | NA               | NA         | IP ?? | IPv4 ?? |
| ??        | 88    | ?? ???           | NA               | NA         | ??    | ?? ???  |
| ??        | 100   | ??? IPv6 ?       | NA               | NA         | ??    | ?? ???  |
| ??        | 26    | ?? DNS           | 4874(???<br>ERX) | 4          | IP ?? | IPv4 ?? |
| ??        | 26    | ?? DNS           | 4874(???<br>ERX) | 5          | IP ?? | IPv4 ?? |
| ??        | 26    | ??<br>WINS(NBNS) | 4874(???<br>ERX) | 6          | IP ?? | IPv4 ?? |
| ??        | 26    | ??<br>WINS(NBNS) | 4874(???<br>ERX) | 7          | IP ?? | IPv4 ?? |



Figure 79: IPsec RADIUS xAuth Configuration CP (Continued)

| Radius Attribute | Attribute ID | Attribute Name   | Attribute Value ID(Oct) | Attribute Value ID | Attribute Type | Attribute Value      |
|------------------|--------------|------------------|-------------------------|--------------------|----------------|----------------------|
| 47               | 26           | IPv6 Address DNS | 4874(Oct ERX)           | 47                 | IP Address     | hex-string 16 octets |
| 48               | 26           | IPv6 Address DNS | 4874(Oct ERX)           | 48                 | IP Address     | hex-string 16 octets |

1. IKEv2 Configuration VPN

in this section

- [IPsec VPN](#) | 479
- [VPN](#) | 479
- [VPN](#) | 483
- [VPN](#) | 497

1. IPsec VPN Configuration

1.1

1.1.1

- SRX240
- SSG140

1.1.2 "IPsec" 11(2)

1.1.3

1.1.3.1 VPN Configuration

1.1.3.1.1 IPv4, IPv6, IKE(Internet Key Exchange) 1, IPsec 2, TCP-MSS 3, 80 480~84 483(2)

图 80: 配置策略, 策略 1, 策略 2 和策略 3

| 策略   | 策略               | 策略 1 策略 2                                                                                                             |
|------|------------------|-----------------------------------------------------------------------------------------------------------------------|
| 策略 1 | ge-0/0/0.0       | 192.168.10.1/24                                                                                                       |
|      | ge-0/0/3.0       | 10.1.1.2/30                                                                                                           |
|      | st0.0 (策略 1策略 2) | 10.11.11.10/24                                                                                                        |
| 策略 2 | 0.0.0.0/0(策略 2)  | 策略 2 10.1.1.1策略 2.                                                                                                    |
|      | 192.168.168.0/24 | 策略 2 st0.0策略 2.                                                                                                       |
| 策略 3 | 策略               | <ul style="list-style-type: none"> <li>策略 策略 策略 策略.</li> <li>ge-0/0/0.0 策略策略 策略策略.</li> </ul>                         |
|      | untrust          | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange)策略策略策略策略策略.</li> <li>ge-0/0/3.0 策略策略策略策略.</li> </ul> |
|      | VPN-策略           | st0.0 策略策略策略策略策略.                                                                                                     |
| 策略 4 | 策略 策略            | <ul style="list-style-type: none"> <li>策略策略策略策略策略策略策略.</li> <li>策略策略策略策略 192.168.10.0/24策略.</li> </ul>                |
|      | 策略               | <ul style="list-style-type: none"> <li>策略策略策略策略策略策略策略.</li> <li>策略策略策略策略 192.168.168.0/24策略.</li> </ul>               |

## ? 81: IKE(Internet Key Exchange) 1?? ?? ?? ??

| ??    | ??                  | ?? ?? ??                                                                                                                                                                  |
|-------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??    | ike-phase1-proposal | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> <li>Diffie-Hellman ??: group2</li> <li>?? ?????: sha1</li> <li>??? ?????: aes-128-cbc</li> </ul>       |
| ??    | ike-phase1-policy   | <ul style="list-style-type: none"> <li>?: main</li> <li>?? ??: ike-phase1-proposal</li> <li>IKE(Internet Key Exchange) 1?? ?? ?? ??: pre-shared-key ascii-text</li> </ul> |
| ????? | GW-???              | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: ike-phase1-policy</li> <li>?? ?????: ge-0/0/3.0</li> <li>????? ??: 10.2.2.2</li> </ul>           |

## ? 82: IPsec 2?? ?? ?? ??

| ?? | ??                    | ?? ?? ??                                                                                                                     |
|----|-----------------------|------------------------------------------------------------------------------------------------------------------------------|
| ?? | ipsec-phase2-proposal | <ul style="list-style-type: none"> <li>?????: esp</li> <li>?? ?????: hmac-sha1-96</li> <li>??? ?????: aes-128-cbc</li> </ul> |
| ?? | ipsec-phase2-policy   | <ul style="list-style-type: none"> <li>?? ??: ipsec-phase2-proposal</li> <li>PFS: Diffie-Hellman group2</li> </ul>           |



84: TCP-MSS

| <p>TCP-MSS TCP 3, TCP , TCP<br/> MTU , VPN , IPSec<br/> IP , ESP<br/> (MTU) ,<br/> .</p> <p>1500 (MTU) ,<br/> 1350 , TCP-MSS<br/> , (MTU) PPP<br/> .</p> | <p>MSS : 1350</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|

in this section

- , , | 483
- IKE(Internet Key Exchange) | 488
- IPsec | 491
- | 493
- TCP-MSS | 495
- SSG | 496

, ,

CLI

, , , , , [edit]  
 CLI, , commit(?).

```
set interfaces ge-0/0/0 unit 0 family inet address 192.168.10.1/24
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/30
set interfaces st0 unit 0 family inet address 10.11.11.10/24
set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
```

```

set routing-options static route 192.168.168.0/24 next-hop st0.0
set security zones security-zone untrust interfaces ge-0/0/3.0
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust address-book address sunnyvale 192.168.10.0/24
set security zones security-zone vpn-chicago interfaces st0.0
set security zones security-zone vpn-chicago address-book address chicago 192.168.168.0/24

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?????, ?? ??, ?? ?? ? ???? ?? ?? ??:

1. ??? ????? ???? ????.

```

[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.168.10.1/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/30
user@host# set interfaces st0 unit 0 family inet address 10.11.11.10/24

```

2. ?? ?? ???? ????.

```

[edit]
user@host# set routing-options static route 0.0.0.0/0 next-hop 10.1.1.1
user@host# set routing-options static route 192.168.168.0/24 next-hop st0.0

```

3. ?????(untrust) ?? ??? ????.

```

[edit ]
user@host# edit security zones security-zone untrust

```

4. ?????? ?? ??? ????.

```

[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/3.0

```

5. `?? ??? ???? ???? ???? ?????.`

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services ike
```

6. `???? ? ? ? ????.`

```
[edit]
user@host# edit security zones security-zone trust
```

7. `?????? ???? ? ? ? ????.`

```
[edit security zones security-zone trust]
user@host# set interfaces ge-0/0/0.0
```

8. `???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?.`

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
```

9. `???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?.`

```
[edit security zones security-zone trust]
user@host# set address-book address sunnyvale 192.168.10.0/24
```

10. vpn-chicago `?? ??? ????.`

```
[edit]
user@host# edit security zones security-zone vpn-chicago
```

11. `?????? ? ? ? ? ? ? ? ?.`

```
[edit security zones security-zone vpn-chicago]
user@host# set interfaces st0.0
```

## 12. vpn-chicago `???` `??` `???` `???` `???` `???`.

```
[edit security zones security-zone vpn-chicago]
user@host# set address-book address chicago 192.168.168.0/24
```

`??`

`??` `???` `???` `???` show interfaces, show routing-options `?` show security zones `???` `???` `???` `???` `???`. `???` `???` `???` `???` `??`  
`?`, `?` `??` `??` `???` `???` `???` `???`.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 192.168.10.1/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.1.1.2/30
    }
  }
}
st0{
  unit 0 {
    family inet {
      address 10.11.11.10/24
    }
  }
}
```

```
[edit]
user@host# show routing-options
static {
  route 0.0.0.0/0 next-hop 10.1.1.1;
```



```

    route 192.168.168.0/24 next-hop st0.0;
}

```

```

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone trust {
    address-book {
        address sunnyvale 192.168.10.0/24;
    }
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn-chicago {
    address-book {
        address chicago 192.168.168.0/24;
    }
    interfaces {
        st0.0;
    }
}

```

```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

```

## IKE(Internet Key Exchange) ??

CLI  [illegible]

```
set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
set security ike proposal ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-phase1-policy proposals ike-phase1-proposal
set security ike policy ike-phase1-policy pre-shared-key ascii-text "$ABC123"
set security ike gateway gw-chicago external-interface ge-0/0/3.0
set security ike gateway gw-chicago ike-policy ike-phase1-policy
set security ike gateway gw-chicago address 10.2.2.2
set security ike gateway gw-chicago version v2-only
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ??/ ???? CLI ??? ???? ?????.

## IKE(Internet Key Exchange) ??:

- 1. IKE(Internet Key Exchange) 1?? ???? ????.**

```
[edit security ike]
user@host# set proposal ike-phase1-proposal
```

- ## 2. IKE(Internet Key Exchange) ?? ?? ??? ????

```
[edit security ike proposal ike-phase1-proposal]
user@host# set authentication-method pre-shared-keys
```

- ### 3. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ?????.

```
[edit security ike proposal ike-phase1-proposal]
user@host# set dh-group group2
```

4. IKE(Internet Key Exchange) 100 100 100000 100000.

```
[edit security ike proposal ike-phase1-proposal]
user@host# set authentication-algorithm sha1
```

5. IKE(Internet Key Exchange) 100 1000 100000 100000.

```
[edit security ike proposal ike-phase1-proposal]
user@host# set encryption-algorithm aes-128-cbc
```

6. IKE(Internet Key Exchange) 100 1000 100000.

```
[edit security ike]
user@host# set policy ike-phase1-policy
```

7. IKE(Internet Key Exchange) 1000 100 1000 100000.

```
[edit security ike policy ike-phase1-policy]
user@host# set proposals ike-phase1-proposal
```

8. IKE(Internet Key Exchange) 1000 100 100 1000 100000.

```
[edit security ike policy ike-phase1-policy]
user@host# set pre-shared-key ascii-text "$ABC123"
```

9. IKE(Internet Key Exchange) 100 1000000 10000 100 1000000 100000.

```
[edit security ike]
user@host# set gateway gw-chicago external-interface ge-0/0/3.0
```

10. IKE(Internet Key Exchange) 1000 100 1000 100000.

```
[edit security ike gateway gw-chicago]
user@host# set ike-policy ike-phase1-policy
```

## 11. IKE(Internet Key Exchange) 1?? 2222? 22? 2222?.

```
[edit security ike gateway gw-chicago]
user@host# set address 10.2.2.2
```

## 12. IKE(Internet Key Exchange) 1?? 2222? 22? 2222?.

```
[edit security ike gateway gw-chicago]
user@host# set version v2-only
```

??

?? 2222? show security ike 22? 2222? 22? 22222?. 22? 22? 22? 2222? 22?, ? 22 ?2 22? 2222? 22222?.

```
[edit]
user@host# show security ike
proposal ike-phase1-proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-phase1-policy {
    proposals ike-phase1-proposal;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway gw-chicago {
    ike-policy ike-phase1-policy;
    address 10.2.2.2;
    external-interface ge-0/0/3.0;
    version v2-only;
}
```

2222? 22? 2222? ?? 2222? commit?(?) 22222?.

## IPsec **??**

### CLI **?? ??**

**?** **??** **???** **??????**, **??** **???** **?????** **???** **???** **??** **??** **??** **??** **??????????** **?????**, **?????** **???** **?????** **?** **???** **??** **????** **????** [edit] **?**  
**?** **?????** **????** CLI **?** **????** **??** **??** **??**, **??** **?????** commit**?(?)** **????????**.

```
set security ipsec proposal ipsec-phase2-proposal protocol esp
set security ipsec proposal ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy ipsec-phase2-policy proposals ipsec-phase2-proposal
set security ipsec policy ipsec-phase2-policy perfect-forward-secrecy keys group2
set security ipsec vpn ipsec-vpn-chicago ike gateway gw-chicago
set security ipsec vpn ipsec-vpn-chicago ike ipsec-policy ipsec-phase2-policy
set security ipsec vpn ipsec-vpn-chicago bind-interface st0.0
```

**???? ??**

**??** **??** **??** **?????** **????** **????** **????????**. **??** **?????** **????** **??** **????** CLI **????** **?????** **??** **?????** CLI **????** **????** **????????**.

IPsec **??**:

1. IPsec **2??** **???** **?????**.

```
[edit]
user@host# set security ipsec proposal ipsec-phase2-proposal
```

2. IPsec **2??** **??** **??????** **??????**.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@host# set protocol esp
```

3. IPsec **2??** **??** **??** **??????** **??????**.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@host# set authentication-algorithm hmac-sha1-96
```

4. IPsec 2?? ?? ??? ????? ?????.

```
[edit security ipsec proposal ipsec-phase2-proposal]
user@host# set encryption-algorithm aes-128-cbc
```

5. IPsec 2?? ??? ????.

```
[edit security ipsec]
user@host# set policy ipsec-phase2-policy
```

6. IPsec 2?? ?? ??? ?????.

```
[edit security ipsec policy ipsec-phase2-policy]
user@host# set proposals ipsec-phase2-proposal
```

7. Diffie-Hellman ☐ 2<sup>?</sup> ☐ ☐ ☐ ☐ ☐ IPsec 2<sup>??</sup> PFS? ☐ ☐ ☐ ☐ ☐.

```
[edit security ipsec policy ipsec-phase2-policy]
user@host# set perfect-forward-secrecy keys group2
```

8. IKE(Internet Key Exchange) ?????? ??????.

```
[edit security ipsec]
user@host# set vpn ipsec-vpn-chicago ike gateway gw-chicago
```

9. IPsec 2?? ???? ?????.

```
[edit security ipsec]
user@host# set vpn ipsec-vpn-chicago ike ipsec-policy ipsec-phase2-policy
```

- 10.**    □□□□ □□□□□□ □□□□?

```
[edit security ipsec]
user@host# set vpn ipsec-vpn-chicago bind-interface st0.0
```

??

?? ???? show security ipsec ??? ???? ???? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show security ipsec
proposal ipsec-phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy ipsec-phase2-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
vpn ipsec-vpn-chicago {
    bind-interface st0.0;
    ike {
        gateway gw-chicago;
        ipsec-policy ipsec-phase2-policy;
    }
}
```

???? ???? ???? ???? commit?(?) ?????.

?? ?? ??

## CLI ?? ??

? ?? ???? ?????. ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? , ???? ???? ???? ? ???? ???? ???? [edit] ?  
? ???? ???? CLI? ???? ???? ???? , ?? ???? commit?(?) ?????.

```
set security policies from-zone trust to-zone vpn-chicago policy vpn-tr-chi match source-address
sunnyvale
set security policies from-zone trust to-zone vpn-chicago policy vpn-tr-chi match destination-
address chicago
set security policies from-zone trust to-zone vpn-chicago policy vpn-tr-chi match application
any
set security policies from-zone trust to-zone vpn-chicago policy vpn-tr-chi then permit
```

```

set security policies from-zone vpn-chicago to-zone trust policy vpn-chi-tr match source-address
chicago
set security policies from-zone vpn-chicago to-zone trust policy vpn-chi-tr match destination-
address sunnyvale
set security policies from-zone vpn-chicago to-zone trust policy vpn-chi-tr match application
any
set security policies from-zone vpn-chicago to-zone trust policy vpn-chi-tr then permit

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ?? ????.

?? ?? ??:

1. ???? ???? vpn-chicago ???? ???? ???? ?? ???? ????.

```

[edit security policies from-zone trust to-zone vpn-chicago]
user@host# set policy vpn-tr-chi match source-address sunnyvale
user@host# set policy vpn-tr-chi match destination-address chicago
user@host# set policy vpn-tr-chi match application any
user@host# set policy vpn-tr-chi then permit

```

2. vpn-chicago ???? ???? ???? ???? ???? ?? ???? ????.

```

[edit security policies from-zone vpn-chicago to-zone trust]
user@host# set policy vpn-chi-tr match source-address sunnyvale
user@host# set policy vpn-chi-tr match destination-address chicago
user@host# set policy vpn-chi-tr match application any
user@host# set policy vpn-chi-tr then permit

```

??

?? ???? show security policies ??? ???? ???? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```

[edit]
user@host# show security policies
from-zone trust to-zone vpn-chicago {
  policy vpn-tr-vpn {
    match {

```





## 1. TCP-MSS `???` `??????`.

```
[edit]
user@host# set security flow tcp-mss ipsec-vpn mss 1350
```

`??`

`??` `?????` show security flow `????` `?????` `????` `??????`. `????` `????` `????` `?????` `????`, `?` `??` `??` `????` `?????` `??????`.

```
[edit]
user@host# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```

`????` `????` `?????` `??` `?????` commit`?(?)` `??????`.

## SSG `????` `?????` `??`

### CLI `??` `??`

`????` SSG `????` `?????` `????` `??????`. SSG `????` `??????` `??` `????` [https://www.juniper.net/documentation](https://www.juniper.net/documentation/Concepts & Examples ScreenOS Reference Guide?)`??`  
*Concepts & Examples ScreenOS Reference Guide*`?(?)` `??????`.

`?` `??` `????` `????` `??????`, `??` `????` `?????` `????` `????` `??` `??` `??` `?????????` `?????`, `?????` `????` `???????` `?` `????` `??` `????` `?????`  
`??` `?????` [edit] `????` `?????` CLI`?` `??` `??` `??`, `??` `?????` commit`?(?)` `??????`.

```
set zone name vpn-chicago
set interface ethernet0/6 zone Trust
set interface ethernet0/0 zone Untrust
set interface tunnel.1 zone vpn-chicago
set interface ethernet0/6 ip 192.168.168.1/24
set interface ethernet0/6 route
set interface ethernet0/0 ip 10.2.2.2/30
set interface ethernet0/0 route
set interface tunnel.1 ip 10.11.11.11/24
set flow tcp-mss 1350
set address Trust "192.168.168-net" 192.168.168.0 255.255.255.0
```

```

set address vpn-chicago "192.168.10-net" 192.168.10.0 255.255.255.0
set ike gateway corp-ike address 10.1.1.2 IKEv2 outgoing-interface ethernet0/0 preshare
395psksecr3t sec-level standard
set vpn corp-vpn gateway corp-ike replay tunnel idletime 0 sec-level standard
set vpn corp-vpn monitor optimized rekey
set vpn corp-vpn bind interface tunnel.1
set policy from Trust to Untrust "ANY" "ANY" "ANY" nat src permit
set policy from Trust to vpn-chicago "192.168.168-net" "192.168.10-net" "ANY" permit
set policy from vpn-chicago to Trust "192.168.10-net" "192.168.168-net" "ANY" permit
set route 192.168.10.0/24 interface tunnel.1
set route 0.0.0.0/0 interface ethernet0/0 gateway 10.2.2.1

```

??

#### in this section

- IKE(Internet Key Exchange) 1?? ?? ?? | 497
- IPsec 2?? ?? ?? | 499
- IPsec ?? ??? ?? ?? ? ?? ?? | 501
- VPN ??? ??? ??? ??? | 502

??? ????? ???? ???? ?????.

**IKE(Internet Key Exchange) 1?? ?? ??**

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

?? ?????? ????? ?? 192.168.10/24 ?????? ?????? 192.168.168/24 ?????? ?????? ?????? ????. ?? ?? VPN? ??, SRX ??? ?????? ?? ?? ?????? ?? ? ??????. IPsec ??? ?????? ?, VPN ??? ?? ??? ??????? VPN? ?????? ?? ? ?? ?????? ?????? ?????? ?? ??????. ?? ??, 192.168.10.10?? 192.168.168.10?? ping? ??????.

?? ???? show security ike security-associations ??? ?????. ??? ???? ? ? show security ike security-associations index *index\_number* detail ??? ?????.

```
user@host> show security ike security-associations
```

| Index | Remote Address | State | Initiator cookie | Responder cookie | Mode  |
|-------|----------------|-------|------------------|------------------|-------|
| 1     | 10.2.2.2       | UP    | 744a594d957dd513 | 1e1307db82f58387 | IKEv2 |

```
user@host> show security ike security-associations index 1 detail
```

```
IKE peer 10.2.2.2, Index 1,
  Role: Responder, State: UP
  Initiator cookie: 744a594d957dd513, Responder cookie: 1e1307db82f58387
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local: 10.1.1.2:500, Remote: 10.2.2.2:500
  Lifetime: Expires in 28570 seconds
  Algorithms:
    Authentication      : sha1
    Encryption          : aes-cbc (128 bits)
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes      :          852
    Output bytes     :          940
    Input packets    :           5
    Output packets   :           5
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
```

??

show security ike security-associations ??? ? ? IKE(Internet Key Exchange) 1?? SA? ?????. SA? ???? ? ? ? ? ? , 1?? ???? ???? ? ?????. ???? IKE(Internet Key Exchange) ?? ?? ? ? ? ???? ???? ?????.

SA? ???? ? ? ? ? ? ????.

- ??? - ? ? ? ? IKE(Internet Key Exchange)? ? ???? ???? SA? ? ???? ???? ? ? ? ? show security ike security-associations index detail??? ???? ? ????.
- ?? ?? - ?? IP ??? ???? ????.
- ?
  - UP—1?? SA? ????.

- DOWN—1?? SA? ???? ? ??? ?????.
  - ?? - ??? ??? ????? ??? ?????.
- ???? ? ? ? ? ? ? ? ? ? ?
- ?? ??????(?????? IKE ??? ????? ??????? ?).
  - IKE(Internet Key Exchange) ?? ?? ??
  - ?? ? ? ? ?
  - 1?? ?? ? ?( ? ? ? ? ? ? ? ? ? ? )

```
?? show security ike security-associations index 1 detail ??? ??? 1? SA? ?? ?? ??? ?????.
```

- $\frac{1}{n} \sum_{i=1}^n x_i$
- $\frac{1}{n} \sum_{i=1}^n y_i$
- $\frac{1}{n} \sum_{i=1}^n (x_i + y_i)$
- $\frac{1}{n} \sum_{i=1}^n x_i y_i$

[illegible]

- ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐
- ☐ ☐ ☐ IPsec SA ☐ ☐

## IPsec 2?? ?? ??

??

IPsec 2?? ???? ?????.

??

`?? ???? show security ipsec security-associations ??? ?????, ???? ???? ???? ? show security ipsec security-associations index index_number detail ??? ????????`.

```
user@host> show security ipsec security-associations
total configured sa: 2
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
```









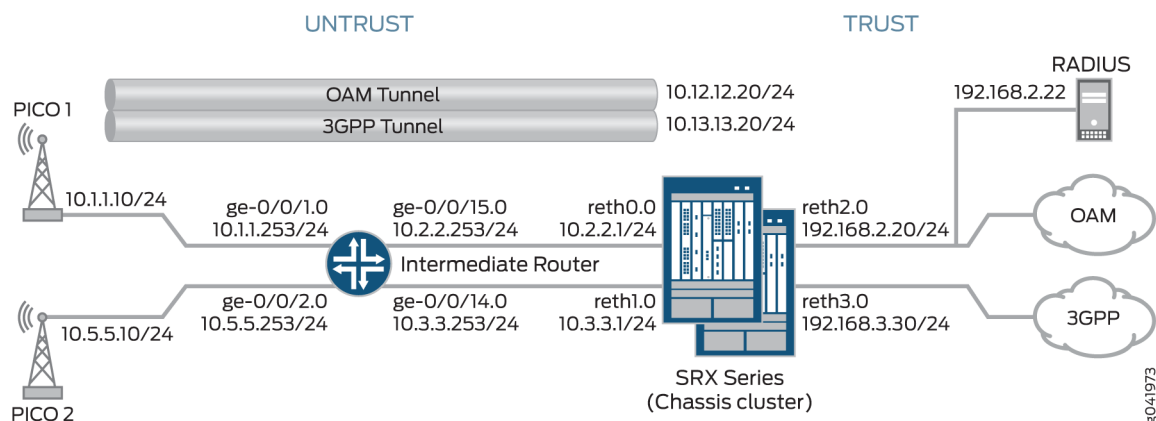


[illegible]

Junos OS 20.3R1 ike SRX5000 IPv6 IKEv2 IPv6  
Junos OS 21.1R1 ike vSRX IPv6

29 504 SRX IKEv2

?? 29: IKEv2 ?? ????? ?? Pico ? ?????? ?? SRX ??? ??



2 222222 2 22 22 2 22 IPsec VPN? 222222. 222 222222 22 222 22222222. 2 222 22 2222 OAM 222 2222 222 2  
 22 2222 22, 222 2222 3GPP 222 2222 222 222 22 2222. 2 222 222 22 222 222222 OAM 2 3GPP 22222 22  
 22 222 222222 222 222 2222 2 VPN? 222222. 2 2222 OAM 2 3GPP VPN? 2222 22 IKE(Internet Key  
 Exchange) 122 2 222 222 222222.

? SRX IKeV2 ? ?, RADIUS ? ? ? ? ? ? ? ?. SRX  
? ? ? ? ? ? ? ? IKeV2 ? ? ? ? ? ? ? ? ? ? ? ? ? ? . SRX ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

```
?? SRX [?] IKEv2 ?? [?] [?] [?] [?] [?] [?] [?] TSi(Traffic Selector Initiator) ? TSr(Traffic  
Selector Responder) ?? [?] [?] [edit security ipsec vpn vpn-name ike) ?? [?] proxy-  
identity SRX [?] TSi ? TSr ?? [?]. TSi ? TSr ?? ? VPN? ?? [?] [?] [?].
```

?? ???? ?? ? ???? SRX ???? ???? ????? ?????.

☐? ? ☐? ? ? ? ? ? ? ? ☐? ? ☐? ? ? ? ☐? ? ☐? ? ? ? ? ? .

1. `?? ?? ?? ??? ????? SRX ????? IPsec ??? ?????.`
2. `SRX ????? SRX ????? ??? CA? ?? ????? ?????? ??? ??? ????? ??????? ??????. ?? ? SRX ????? ?? ?????? ???  
?? ????? IKE ID ??? RADIUS ??? ?????.`

## IKE(Internet Key Exchange) ??:

85: SRX 122 222 (Continued)

|                                       |                                   |
|---------------------------------------|-----------------------------------|
|                                       |                                   |
|                                       | IKE_PROP                          |
|                                       | RSA 2048                          |
| DH(Diffie-Hellman) 2048               | group5                            |
|                                       | SHA-1                             |
|                                       | AES 256 CBC                       |
| IKE(Internet Key Exchange) 2048:      |                                   |
| IKE(Internet Key Exchange) 2048 2048  | IKE_POL                           |
|                                       | Example_SRX                       |
| IKE(Internet Key Exchange) 2048(OAM): |                                   |
| IKE(Internet Key Exchange) 2048       | IKE_POL                           |
| 2048 IP 2048                          | 2048                              |
| IKE 2048 2048                         | ike-id                            |
| 2048 IKE(Internet Key Exchange) ID    | 2048 2048: srx_series.example.net |
| 2048 IKE(Internet Key Exchange) ID    | 2048 2048.pico_cell.net           |
| 2048 20482048                         | reth0.0                           |
| 2048 2048                             | radius_pico                       |

85: SRX 1000 100 200 200 (Continued)

|         |        |
|---------|--------|
| 100     | 100    |
| IKE 100 | v2 100 |

IKE(Internet Key Exchange) 100000(3GPP):

|                                   |                              |
|-----------------------------------|------------------------------|
| IKE(Internet Key Exchange) 100    | IKE_POL                      |
| 100 IP 100                        | 100                          |
| IKE 1000 100                      | 100 ike-id                   |
| 100 IKE(Internet Key Exchange) ID | 100 100 100000 OU=srx_series |
| 100 IKE(Internet Key Exchange) ID | 100 100 100000 OU=pico_cell  |
| 100 100000                        | 1001                         |
| 1000 1000                         | radius_pico                  |
| IKE 100                           | v2 100                       |

IPsec 100:

|             |               |
|-------------|---------------|
| 100 100     | IPSEC_PROP    |
| 100000      | ESP           |
| 100 100000  | HMAC SHA-1 96 |
| 1000 100000 | AES 256 CBC   |

IPsec 100:

85: SRX 1000 100 200 (Continued)

|                                   |                |
|-----------------------------------|----------------|
| 100                               | 100            |
| 100 100                           | IPSEC_POL      |
| PFS(Perfect Forward Secrecy) 100  | group5         |
| IPsec 100                         | IPSEC_PROP     |
| IPsec VPN(OAM):                   |                |
| 1000 100000                       | st0.0          |
| IKE(Internet Key Exchange) 100000 | OAM_GW         |
| 100 1000 ID                       | 192.168.2.0/24 |
| 100 1000 ID                       | 0.0.0.0/0      |
| IPsec 100                         | IPSEC_POL      |
| IPsec VPN(3GPP):                  |                |
| 1000 100000                       | st0.1          |
| IKE(Internet Key Exchange) 100000 | 3GPP_GW        |
| 100 1000 ID                       | 192.168.3.0/24 |
| 100 1000 ID                       | 0.0.0.0/0      |
| IPsec 100                         | IPSEC_POL      |

1000 100 100 SRX 1000 100000.

100000 100 100000 100000 100 100 1000 100 100000 100000. 100 1000 100 100 100000 100 1000 100000 1000. 100 100 1000 1000000.

- SRX `???` `??` | 509
- `??` `????` `??` | 522
- Pico `?` `??`(`??` `??`) | 525
- RADIUS `??` `??`(FreeRADIUS`?` `???` `??` `??`) | 527

CLI

我 想 知 道 你 們 有 沒 有 在 想 這 個 問 題 嗎 ？ 我 們 有 一 個 人 在 想 這 個 問 題 嗎 ？ 我 們 有 一 個 人 在 想 這 個 問 題 嗎 ？ [edit]

我 們 有 一 個 人 在 想 這 個 問 題 嗎 ？ 我 們 有 一 個 人 在 想 這 個 問 題 嗎 ？ 我 們 有 一 個 人 在 想 這 個 問 題 嗎 ？

```
set chassis cluster reth-count 5
set chassis cluster node 0
set chassis cluster node 1
set chassis cluster redundancy-group 0 node 0 priority 250
set chassis cluster redundancy-group 0 node 1 priority 150
set chassis cluster redundancy-group 1 node 0 priority 220
set chassis cluster redundancy-group 1 node 1 priority 149
set chassis cluster redundancy-group 1 interface-monitor ge-3/0/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/0/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-3/0/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/0/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-3/2/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/2/0 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-3/2/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/2/1 weight 255
set interfaces ge-3/0/0 gigether-options redundant-parent reth0
set interfaces ge-3/0/1 gigether-options redundant-parent reth1
set interfaces ge-3/2/0 gigether-options redundant-parent reth2
set interfaces ge-3/2/1 gigether-options redundant-parent reth3
set interfaces ge-8/0/0 gigether-options redundant-parent reth0
set interfaces ge-8/0/1 gigether-options redundant-parent reth1
set interfaces ge-8/2/0 gigether-options redundant-parent reth2
```

```

set interfaces ge-8/2/1 gigether-options redundant-parent reth3
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 10.2.2.1/24
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.3.3.1/24
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth2 unit 0 family inet address 192.168.2.20/24
set interfaces reth3 redundant-ether-options redundancy-group 1
set interfaces reth3 unit 0 family inet address 192.168.3.20/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.12.1.20/24
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet address 10.13.1.20/24
set routing-options static route 10.1.0.0/16 next-hop 10.2.2.253
set routing-options static route 10.5.0.0/16 next-hop 10.2.2.253
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces reth0.0
set security zones security-zone untrust interfaces reth1.0
set security zones security-zone oam-trust host-inbound-traffic system-services all
set security zones security-zone oam-trust host-inbound-traffic protocols all
set security zones security-zone oam-trust interfaces reth2.0
set security zones security-zone oam-trust interfaces st0.0
set security zones security-zone 3gpp-trust host-inbound-traffic system-services all
set security zones security-zone 3gpp-trust host-inbound-traffic protocols all
set security zones security-zone 3gpp-trust interfaces reth3.0
set security zones security-zone 3gpp-trust interfaces st0.1
set access profile radius_pico authentication-order radius
set access profile radius_pico radius-server 192.168.2.22 secret "$ABC123"
set access profile radius_pico radius-server 192.168.2.22 routing-instance VR-OAM
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate example_SRX
set security ike gateway OAM_GW ike-policy IKE_POL
set security ike gateway OAM_GW dynamic hostname .pico_cell.net
set security ike gateway OAM_GW dynamic ike-user-type group-ike-id
set security ike gateway OAM_GW local-identity hostname srx_series.example.net
set security ike gateway OAM_GW external-interface reth0.0
set security ike gateway OAM_GW aaa access-profile radius_pico
set security ike gateway OAM_GW version v2-only

```



```
set security ike gateway 3GPP_GW ike-policy IKE_POL
set security ike gateway 3GPP_GW dynamic distinguished-name wildcard OU=pico_cell
set security ike gateway 3GPP_GW dynamic ike-user-type group-ike-id
set security ike gateway 3GPP_GW local-identity distinguished-name wildcard OU=srx_series
set security ike gateway 3GPP_GW external-interface reth1.0
set security ike gateway 3GPP_GW aaa access-profile radius_pico
set security ike gateway 3GPP_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec proposal IPSEC_PROP lifetime-seconds 300
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn OAM_VPN bind-interface st0.0
set security ipsec vpn OAM_VPN ike gateway OAM_GW
set security ipsec vpn OAM_VPN ike proxy-identity local 192.168.2.0/24
set security ipsec vpn OAM_VPN ike proxy-identity remote 0.0.0.0/0
set security ipsec vpn OAM_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn 3GPP_VPN bind-interface st0.1
set security ipsec vpn 3GPP_VPN ike gateway 3GPP_GW
set security ipsec vpn 3GPP_VPN ike proxy-identity local 192.168.3.0/24
set security ipsec vpn 3GPP_VPN ike proxy-identity remote 0.0.0.0/0
set security ipsec vpn 3GPP_VPN ike ipsec-policy IPSEC_POL
set routing-instances VR-OAM instance-type virtual-router
set routing-instances VR-OAM interface reth2.0
set routing-instances VR-OAM interface st0.0
set routing-instances VR-3GPP instance-type virtual-router
set routing-instances VR-3GPP interface reth3.0
set routing-instances VR-3GPP interface st0.1
set security policies default-policy permit-all
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ????/??? ?? ?????.

SRX   :

**1.**    ??    ??????    ??????.

```
[edit chassis cluster]
user@host# set reth-count 5
user@host# set node 0
```

```

user@host# set node 1
user@host# set redundancy-group 0 node 0 priority 250
user@host# set redundancy-group 0 node 1 priority 150
user@host# set redundancy-group 1 node 0 priority 220
user@host# set redundancy-group 1 node 1 priority 149
user@host# set redundancy-group 1 interface-monitor ge-3/0/0 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/0/0 weight 255
user@host# set redundancy-group 1 interface-monitor ge-3/0/1 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/0/1 weight 255
user@host# set redundancy-group 1 interface-monitor ge-3/2/0 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/2/0 weight 255
user@host# set redundancy-group 1 interface-monitor ge-3/2/1 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/2/1 weight 255

```

## 2. `set redundancy-group 1 interface-monitor ge-3/0/0 weight 255`

```

[edit interfaces]
user@host# set ge-3/0/0 gigether-options redundant-parent reth0
user@host# set ge-3/0/1 gigether-options redundant-parent reth1
user@host# set ge-3/2/0 gigether-options redundant-parent reth2
user@host# set ge-3/2/1 gigether-options redundant-parent reth3
user@host# set ge-8/0/0 gigether-options redundant-parent reth0
user@host# set ge-8/0/1 gigether-options redundant-parent reth1
user@host# set ge-8/2/0 gigether-options redundant-parent reth2
user@host# set ge-8/2/1 gigether-options redundant-parent reth3
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 10.2.2.1/24
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 10.3.3.1/24
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth2 unit 0 family inet address 192.168.2.20/24
user@host# set reth3 redundant-ether-options redundancy-group 1
user@host# set reth3 unit 0 family inet address 192.169.3.20/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.12.1.20/24
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 10.13.1.20/24

```

3. `???` `???` `??????`.

```
[edit routing-options]
user@host# set static route 10.1.0.0/16 next-hop 10.2.2.253
user@host# set static route 10.5.0.0/16 next-hop 10.2.2.253
```

4. `??` `???` `??????`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic protocols all
user@host# set host-inbound-traffic system-services all
user@host# set interfaces reth0.0
user@host# set interfaces reth1.0
[edit security zones security-zone oam-trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces reth2.0
user@host# set interfaces st0.0
[edit security zones security-zone 3gpp-trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces reth3.0
user@host# set interfaces st0.1
```

5. RADIUS `??????` `??????`.

```
[edit access profile radius_pico]
user@host# set authentication-order radius
user@host# set radius-server 192.168.2.22 secret "$ABC123"
user@host# set radius-server 192.168.2.22 routing-instance VR-OAM
```

6. `1??` `???` `??????`.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy IKE_POL]
```

```

user@host# set proposals IKE_PROP
user@host# set certificate local-certificate example_SRX
[edit security ike gateway OAM_GW]
user@host# set ike-policy IKE_POL
user@host# set dynamic hostname .pico_cell.net
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity hostname srx.example.net
user@host# set external-interface reth0.0
user@host# set aaa access-profile radius_pico
user@host# set version v2-only
[edit security ike gateway 3GPP_GW]
user@host# set ike-policy IKE_POL
user@host# set dynamic distinguished-name wildcard OU=pico_cell
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name wildcard OU=srx_series
user@host# set external-interface reth1.0
user@host# set aaa access-profile radius_pico
user@host# set version v2-only

```

## 7. 2?? ???? ?????.

```

[edit set security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 300
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn OAM_VPN]
user@host# set bind-interface st0.0
user@host# set ike gateway OAM_GW
user@host# set ike proxy-identity local 192.168.2.0/24
user@host# set ike proxy-identity remote 0.0.0.0/0
user@host# set ike ipsec-policy IPSEC_POL
[edit security ipsec vpn 3GPP_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway 3GPP_GW
user@host# set ike proxy-identity local 192.168.3.0/24
user@host# set ike proxy-identity remote 0.0.0.0/0
user@host# set ike ipsec-policy IPSEC_POL

```

8. `?? ???? ????.`

```
[edit routing-instances VR-OAM]
user@host# set instance-type virtual router
user@host# set interface reth2.0
user@host# set interface st0.0
[edit routing-instances VR-3GPP]
user@host# set instance-type virtual router
user@host# set interface reth3.0
user@host# set interface st0.1
```

9. `?? ? ???? ???? ? ???? ????.`

```
[edit security policies]
user@host# set default-policy permit-all
```

`??`

`?? ???? , show interfaces, , show access profile radius_picoshow security zones, show security ike, show security ipsec, show routing-instances? show security policies ??? ???? show chassis cluster??? ???? . ??? ??? ???? ???? ? ???? , ? ?? ?? ???? ???? ????.`

```
[edit]
user@host# show chassis cluster
reth-count 5
node 0
node 1
redundancy-group 0{
  node 0 priority 250;
  node 1 priority 150;
  redundancy-group 1 {
    node 0 priority 220;
    node 1 priority 149;
    interface-monitor {
      ge-3/0/0 weight 255;
      ge-8/0/0 weight 255;
      ge-3/0/1 weight 255;
      ge-8/0/1 weight 255;
      ge-3/2/0 weight 255;
```

```

        ge-8/2/0 weight 255;
        ge-3/2/1 weight 255;
        ge-8/2/1 weight 255;
    }
}
[edit]
user@host# show interfaces
ge-3/0/0 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-3/0/1 {
    gigether-options {
        redundant-parent reth1;
    }
}
ge-3/2/0 {
    gigether-options {
        redundant-parent reth2;
    }
}
ge-3/2/1 {
    gigether-options {
        redundant-parent reth3;
    }
}
ge-8/0/0 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-8/0/1 {
    gigether-options {
        redundant-parent reth1;
    }
}
ge-8/2/0 {
    gigether-options {
        redundant-parent reth2;
    }
}
ge-8/2/1 {

```

```
    ggether-options {
        redundant-parent reth3;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 10.2.2.1/24;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 10.3.3.1/24;
        }
    }
}
reth2 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 192.168.2.20/24;
        }
    }
}
reth3 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 192.168.3.20/24;
        }
    }
}
```

```

}
st0 {
    unit 0{
        multipoint;
        family inet {
            address 12.12.1.20/24;
        }
    }
    unit 1{
        multipoint;
        family inet {
            address 13.13.1.20/24;
        }
    }
}
[edit]
user@host# show routing-options
static {
    route 10.1.0.0/16 next-hop 10.2.2.253;
    route 10.5.0.0/16 next-hop 10.2.2.253;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth1.0;
        reth0.0;
    }
}
security-zone oam-trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {

```



```

        all;
    }
}
interfaces {
    reth2.0;
    st0.0;
}
}
security-zone 3gpp-trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth3.0;
        st0.1;
    }
}
[edit]
user@host# show access profile radius_pico
authentication-order radius;
radius-server {
    192.168.2.22 {
        secret "$ABC123";
        routing-instance VR-OAM;
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate example_SRX;
    }
}

```

```

    }
}
gateway OAM_GW {
    ike-policy IKE_POL;
    dynamic {
        hostname .pico_cell.net;
        ike-user-type group-ike-id;
    }
    local-identity hostname srx_series.example.net;
    external-interface reth0.0;
    aaa access-profile radius_pico;
    version v2-only;
}
gateway 3GPP_GW {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=pico_cell;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface reth1.0;
    aaa access-profile radius_pico;
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 300;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}
vpn OAM_VPN {
    bind-interface st0.0;
    ike {

```

```

        gateway OAM_GW;
        proxy-identity {
            local 192.168.2.0/24;
            remote 0.0.0.0/0;
        }
        ipsec-policy IPSEC_POL;
    }
}
vpn 3GPP_VPN {
    bind-interface st0.1;
    ike {
        gateway 3GPP_GW;
        proxy-identity {
            local 192.168.3.0/24;
            remote 0.0.0.0/0;
        }
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show routing-instances
VR-OAM {
    instance-type virtual-router;
    interface reth2.0;
    interface st0.0;
}
VR-3GPP {
    instance-type virtual-router;
    interface reth3.0;
    interface st0.1;
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

?? ?? ?? ?? ?? commit?(?) ??.

```

?? ???? ??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ????? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?  
? ????? ???? CLI? ???? ???? ???? ???? ???? ???? **commit**(?) ??????.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.253/24
set interfaces ge-0/0/2 unit 0 family inet address 10.5.5.253/24
set interfaces ge-0/0/14 unit 0 family inet address 10.3.3.253/24
set interfaces ge-0/0/15 unit 0 family inet address 10.2.2.253/24
set routing-options static route 192.168.3.0/24 next-hop 10.2.2.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/14.0
set security zones security-zone trust interfaces ge-0/0/15.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces ge-0/0/2.0
set security policies default-policy permit-all
```

??? ??

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? *?? ???? CLI ???? ???? ?????.*

?? ????? ???? ???? ?????.

### 1. ?????? ????.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.1.1.253/24
user@host# set ge-0/0/2 unit 0 family inet address 10.5.5.253/24
user@host# set ge-0/0/14 unit 0 family inet address 10.3.3.253/24
user@host# set ge-0/0/15 unit 0 family inet address 10.2.2.253/24
```

2. `?? ? ? ? ? ? ? ? ?`.

```
[edit routing-options]
user@host# set static route 192.168.3.0/24 next-hop 10.2.2.1
```

3. `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic protocols all
user@host# set host-inbound-traffic system-services all
user@host# set interfaces ge-0/0/14.0
user@host# set interfaces ge-0/0/15.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces ge-0/0/2.0
```

4. `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security policies]
user@host# set default-policy permit-all
```

`??`

`?? ? ? ? ? ?` show interfaces, show routing-options, show security zones `?` show security policies `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.  
`?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`, `?` `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.1.1.253/24;
    }
  }
}
ge-0/0/2 {
  unit 0 {
```

```

        family inet {
            address 10.5.5.253/24;
        }
    }
}
ge-0/0/14 {
    unit 0 {
        family inet {
            address 10.3.3.253/24;
        }
    }
}
ge-0/0/15 {
    unit 0 {
        family inet {
            address 10.2.2.253/24;
        }
    }
}
[edit]
user@host# show routing-options
static {
    route 192.168.3.0/24 next-hop 10.2.2.1;
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/14.0;
        ge-0/0/15.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {

```

```

        all;
    }
    protocols {
        all;
    }
}

interfaces {
    ge-0/0/1.0;
    ge-0/0/2.0;
}
}
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

    keylife=1h
    rekeymargin=1m
    keyingtries=1
    keyexchange=ikev2
    authby=pubkey
    mobike=no

conn oam
    left=%any
    leftsourceip=%config
    leftcert=/usr/local/etc/ipsec.d/certs/<cert_name>
    leftid=pico1.pico_cell.net
    leftfirewall=yes
    reauth=yes
    right=10.2.2.1/24
    rightid=srx_series.example.net
    rightsubnet=0.0.0.0/0 #peer net for proxy id
    ike=aes256-sha-modp1536!
    esp=aes256-sha-modp1536!
    auto=add

conn 3gpp
    left=%any
    leftsourceip=%config
    leftcert=/usr/local/etc/ipsec.d/certs/<cert_name>
    leftid="C=US, ST=CA, L=Sunnyvale, O=org, OU=pico_cell, CN=pico1"
    leftfirewall=yes
    reauth=yes
    right=10.3.3.1/24
    rightid="OU=srx_series"
    rightsubnet=0.0.0.0/0 #peer net for proxy id
    ike=aes256-sha-modp1536!
    esp=aes256-sha-modp1536!
    auto=add

```

## 2. Pico 2 `???` `??????`.

### Pico 2 `??` `??`

```

conn %default
    ikelifetime=8h
    keylife=1h

```



```

    rekeymargin=1m
    keyingtries=1
    keyexchange=ikev2
    authby=pubkey
    mobike=no

conn oam
    left=%any
    leftsourceip=%config
    leftcert=/usr/local/etc/ipsec.d/certs/<cert_name>
    leftid=pico2.pico_cell.net
    leftfirewall=yes
    #reauth=no
    right=10.2.2.1/24
    rightid=srx_series.example.net
    rightsubnet=0.0.0.0/0 #peer net for proxy id
    ike=aes256-sha-modp1536!
    esp=aes256-sha-modp1536!
    auto=add

conn 3gpp
    left=%any
    leftsourceip=%config
    leftcert=/usr/local/etc/ipsec.d/certs/<cert_name>
    leftid="C=US, ST=CA, L=Sunnyvale, O=org, OU=pico_cell, CN=pico2"
    leftfirewall=yes
    #reauth=no
    right=10.3.3.1/24
    rightid="OU=srx_series"
    rightsubnet=0.0.0.0/0 #peer net for proxy id
    ike=aes256-sha-modp1536!
    esp=aes256-sha-modp1536!
    auto=add

```

## RADIUS (FreeRADIUS)

RADIUS . RADIUS . RADIUS SRX .

- IP

- Framed-IP-Netmask(??)
- Primary-DNS ? Secondary-DNS(?? ??)

```
? ? ? ? RADIUS ? ? ? ? OAM ? 3GPP ? ? ? ? ? ? ? ? ? ? ? ? ? ? . User-Name? SRX ? ? ? ? ? ? ? ? ? ? ? ?  
? ? ? ? ? ? ? ? ? ?.
```

RADIUS [redacted] DHCP [redacted] [redacted] [redacted] [redacted] [redacted] [redacted], RADIUS [redacted] DHCP [redacted] [redacted] [redacted] ID [redacted] SRX [redacted]  
[redacted] [redacted] [redacted] RADIUS [redacted] [redacted] [redacted] IKE ID [redacted] [redacted] [redacted], [redacted] [redacted] [redacted] [redacted] [redacted] ID [redacted] [redacted] [redacted].

SRX [?] [?] [?] RADIUS [?] [?] [?] [?] [?] RADIUS [?] [?] [?] [?] [?].

1. Pico 1 OAM VPN? ?? RADIUS ??? ??????. RADIUS ????? ?? ??? ?????.

15.1X49-D160, 17.3R3, 17.4R2, 18.1R3, 18.2R2, 18.3R1 ? 18.1R3-S2 ??? Junos OS ??? 12.3X48 ?  
Junos OS ???? ?? RADIUS ??:

FreeRADIUS 3.0.18-1

```

DEFAULT User-Name =~ "device@example.net", Cleartext-Password := "juniper"
    Service-Type = Framed-User,
    Framed-IP-Address = 10.12.1.201,
    Framed-IP-Netmask = 255.255.255.255,
    Primary-Dns = 192.168.2.104,
    Secondary-Dns = 192.168.2.106,

```

Junos OS  15.X49-D161, 15.1X49-D170, 17.3R3, 17.4R2, 18.1R3, 18.2R2, 18.3R1 ☐ 18.1R3-S2?  
☐      RADIUS :

FreeRADIUS [?] [?] [?] [?] [?] [?] [?]:

```
DEFAULT User-Name =~ "device@example.net", Auth-Type := "Accept"
    Service-Type = Framed-User,
    Framed-IP-Address = 10.12.1.201,
    Framed-IP-Netmask = 255.255.255.255,
    Primary-Dns = 192.168.2.104,
    Secondary-Dns = 192.168.2.106,
```

?? RADIUS ??? ? ???? ???? ?? ????(255.255.255.255)? ?????.

2. Pico 1 3GPP VPN? ?? RADIUS ?????? ??????. RADIUS ????? ?? ??? ?????.

15.1X49-D160, 17.3R3, 17.4R2, 18.1R3, 18.2R2, 18.3R1 ? 18.1R3-S2 ??? Junos OS ??? 12.3X48 ?  
Junos OS ???? ?? RADIUS ??:



SRX **IKE(Internet Key Exchange)**

IKE(Internet Key Exchange)

**show security ike security-associations** **show security ike security-associations detail**

```
user@host# show security ike security-associations
```

```
node0:
```

```
-----
Index      State Initiator cookie Responder cookie Mode Remote Address
553329718 UP      99919a471d1a5278 3be7c5a49172e6c2 IKEv2 10.1.1.1
1643848758 UP      9e31d4323195a195 4d142438106d4273 IKEv2 10.1.1.1
```

```
user@host# show security ike security-associations index 553329718 detail
```

```
node0:
```

```
-----
IKE peer 10.1.1.1, Index 553329718, Gateway Name: OAM_GW
Location: FPC 2, PIC 0, KMD-Instance 1
Role: Responder, State: UP
Initiator cookie: 99919a471d1a5278, Responder cookie: 3be7c5a49172e6c2
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 10.2.2.1:500, Remote: 10.1.1.1:500
Lifetime: Expires in 28738 seconds
Peer ike-id: C=US, ST=CA, L=Sunnyvale, O=org, OU=pico_cell, CN=pico1
aaa assigned IP: 10.12.1.201
Algorithms:
Authentication      : hmac-sha1-96
Encryption           : aes256-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes  : 2104
Output bytes : 425
Input packets: 2
Output packets: 1
```

```

Z show security ike security-associations [redacted] [redacted] [redacted] [redacted] IKE(Internet Key Exchange) 1[redacted] SA[redacted]
[redacted]. SA[redacted] [redacted] [redacted] [redacted], 1[redacted] [redacted] [redacted] [redacted] [redacted]. [redacted] IKE(Internet Key Exchange) [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]
[redacted]. [redacted] [redacted] OAM VPN[redacted] [redacted] IKE(Internet Key Exchange) 1[redacted] SA[redacted] [redacted]. [redacted] 3GPP VPN[redacted] [redacted] IKE 1[redacted] [redacted]
[redacted] [redacted] [redacted] IKE 1[redacted] SA[redacted] [redacted].

```

- `? ? ? - ? ? ? IKE(Internet Key Exchange) SA ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? show security ike security-associations index detail SA ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? ? ? - ? ? IP ? ? ? ? ? ? ? ? ? ? 500 ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? ? ? ? ? ? ?`:
  - `? - 1 ? ? SA ? ? ? ? ? ? ? ? ? ?`.
  - `? ? - 1 ? ? SA ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? (? ? ) IKE ID - ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? ID ? ? ? ID - ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? - ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

- **?? ?????(?????? IKE ??? ???? ??????? ??)**
- **IKE(Internet Key Exchange) ?? ?? ??**
- **1?? ?? ?? ??(?? ?? ????? ?)**

- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$
- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$
- $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$

?? ???? ???? ???? ???? ???? ?? ? ?????.

- `?? ? ?? ?`
- `??? IPsec SA? ?`
- `?? ?? 2?? ?? ?`

**SRX `???? ??` IPsec `?? ?? ??`**

`??`

IPsec `??? ?????`.

`??`

`?? 0? ?? ????? show security ipsec security-associations ??? ??????, ????? ???? ? ? show security ipsec security-associations detail ??? ??????`

```
user@host# show security ipsec security-associations
```

```
node0:
```

```
-----
Total active tunnels: 2
ID           Algorithm          SPI      Life:sec/kb Mon lsys Port Gateway
<214171651 ESP:aes-cbc-256/sha1 cc2869e2 3529/      - root 500 10.1.1.1
>214171651 ESP:aes-cbc-256/sha1 c0a54936 3529/      - root 500 10.1.1.1
<205520899 ESP:aes-cbc-256/sha1 84e49026 3521/      - root 500 10.1.1.1
>205520899 ESP:aes-cbc-256/sha1 c4ed1849 3521/      - root 500 10.1.1.1
```

```
user@host# show security ipsec security-associations detail
```

```
node0:
```

```
-----
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x604a29
Last Tunnel Down Reason: SA not initiated
ID: 214171651 Virtual-system: root, VPN Name: 3GPP_VPN
Local Gateway: 10.3.3.1, Remote Gateway: 10.1.1.1
Local Identity: list(any:0,ipv4_subnet(any:0-65535,[0..7]=192.168.3.0/24),
ipv4_subnet(any:0-65535,[0..7]=10.13.0.0/16))
Remote Identity: ipv4(any:0,[0..3]=10.13.1.201)
DF-bit: clear
Bind-interface: st0.1

Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
```

Last Tunnel Down Reason: SA not initiated

Location: FPC 6, PIC 0, KMD-Instance 2

Direction: inbound, SPI: cc2869e2, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 3523 seconds

Lifesize Remaining:

Soft lifetime: Expires in 2965 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

Location: FPC 6, PIC 0, KMD-Instance 2

Direction: outbound, SPI: c0a54936, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 3523 seconds

Lifesize Remaining:

Soft lifetime: Expires in 2965 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

ID: 205520899 Virtual-system: root, VPN Name: OAM\_VPN

Local Gateway: 10.2.2.1, Remote Gateway: 10.1.1.1

Local Identity: ipv4\_subnet(any:0-65535,[0..7]=192.168.2.0/24)

Remote Identity: ipv4(any:0,[0..3]=10.12.1.201)

Version: IKEv2

DF-bit: clear

Bind-interface: st0.0

Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x608a29

Last Tunnel Down Reason: SA not initiated

Location: FPC 2, PIC 0, KMD-Instance 1

Direction: inbound, SPI: 84e49026, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 3515 seconds

Lifesize Remaining:

Soft lifetime: Expires in 2933 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

Location: FPC 2, PIC 0, KMD-Instance 1

Direction: outbound, SPI: c4ed1849, AUX-SPI: 0





```
user@host# set security ike policy ike_policy proposals ike_prop
```

## 5. IKE(Internet Key Exchange) `set security ike policy ike_policy certificate local-certificate SPOKE`.

```
[edit]
user@host# set security ike policy ike_policy certificate local-certificate SPOKE
```

## 6. IKE(Internet Key Exchange) `set security ike policy ike_policy certificate trusted-ca ca-profile root-ca`.

```
[edit]
user@host# set security ike policy ike_policy certificate trusted-ca ca-profile root-ca
```

`show security pki` .

```
user@host# show security ike
  proposal ike_prop {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
  }
  policy ike_policy {
    proposals ike_prop;
    certificate {
      local-certificate SPOKE;
      trusted-ca ca-profile root-ca;
    }
  }
```

`show security ike` `IKE ike_policy (Internet Key Exchange)` `CA` `trusted-ca` `ca-profile root-ca` `IKE(Internet Key Exchange)` .

## SEE ALSO

[Junos OS PKI](#)

?? ???? ?? ?? ?????

summary

?? ???? ?? ??(stO) ???? ?? ???? ? ???? ????.

in this section

- [?? ?? VPN? ?? ?? ???? ?? ?? | 537](#)
- [?: ?? ???? stO ???? ?? | 538](#)

?? ?? ?????(stO)? ?? ??? ???? IPsec VPN ??? ???? ?? ?? ?? VPN?? ???? ?? ????.

?? ?? VPN? ?? ?? ???? ?? ??

in this section

- [?? ???? ?? ?? ?? | 538](#)

? ???? ?? ?? VPN? ?? ??? ???? ???? ?????. ?? ???? stO ???? ?? ?? ?? ???? ???? ? ???? VPN  
??? ??? ???? ?????. stO ???? ?? ?? ???? ???? ? ???? ?? ?? ???? ???? ? ???? ???? ? ?????. ??? VPN  
???? ?? ??? ?? VR?? ???? ?????. ?? ?? ?? ???? ???? stO ???? ?? ?? ?? ???? ? ?????. ??? ?? ???  
????? ?? ???? ???? ????.

- ?? ? ??
- ?? ???
- ?? ???
- VPN ????
- ?? ? ???? (hub-and-spoke) VPN
- ESP(Encapsulating Security Payload) ????
- ?? ??(AH) ????
- ???? ?? ?? ?? ??

- `???(lo0) ?????? ??? st0`
- `SRX ??? ?????? ???? ?? ?? ???(VR) ?`
- `ALG(Application Layer Gateway), ?? ?? ? ??(IDP), ??? ??? ?? ???????`
- `DPD(Dead Peer Detection)`
- `?? ???????/??`
- `st0? ?? OSPF(Open Shortest Path First)`
- `st0? ?? RIP(Routing Information Protocol)`
- `VR ??? ?? ?? VPN`

?? ?? ?? ?? ??

SRX [redacted] VPN[redacted] IP [redacted] [redacted].

- IKE `?? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `st0 ???? ? ? NHTB? ? ? point-to-multipoint ? ? ? ? ? ? VPN? ? ? ? ? ? ? ?`.
- `st0 ???? ? ? ? ? ? ? ? ? ? ? VPN? ? ? ? ? ? ? ?`.

## SEE ALSO

IPsec ?? | 11

?: ?? ????? st0 ????? ??

in this section

- ?? ?? | 539  
 ●    ?? | 539  
 ●    ?? | 542  
 ●    ?? | 548

?
??
??
?????
st0
??????
?????
???
?????
???

?? ??

???? ?? ??????? ?????? ??????? ?? ??? ??????. "?? ?? ??" ? ??????.

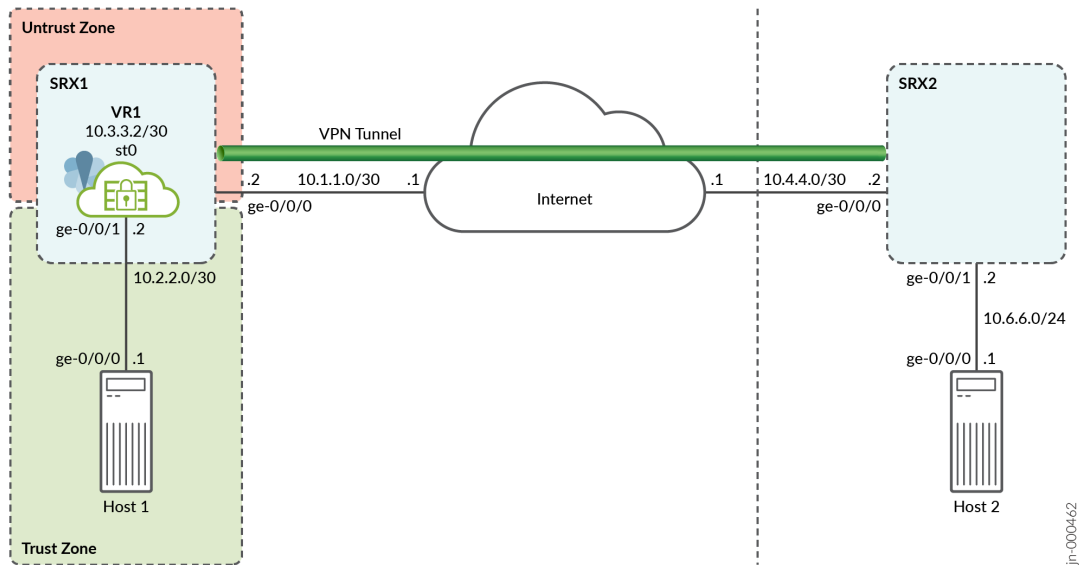
??

☐   ☒☒☒☒☒   ☒☒   ☒☒☒   ☒☒☒☒☒.

- [?][?][?][?][?] [?][?][?][?].
- IKE(Internet Key Exchange) 1[?][?] [?][?] [?][?][?][?].
- IKE(Internet Key Exchange) [?][?] [?][?][?] [?][?] [?][?][?][?].
- IKE(Internet Key Exchange) [?][?][?][?][?] [?][?][?] [?][?] [?][?][?][?].
- 2[?][?] [?][?] [?][?] [?][?][?][?].
- [?][?] [?][?][?] [?][?] [?][?][?][?].
- [?][?] [?] IKE(Internet Key Exchange)[?] [?][?][?] [?][?] [?] [?][?][?][?][?] [?][?][?][?].
- [?][?] [?][?] [?][?][?][?].
- [?][?] [?][?][?][?] [?][?][?][?][?].
- [?][?] [?][?][?][?][?] VPN [?][?][?] [?][?][?][?].
- [?][?] [?][?] [?][?] [?][?][?][?].

?? 30 ??? 540 ? ???? ???? ???? ????.

?? 30: ?? ???? ? ? ???? ?



?? ???? ? ? ???? ? ? ????.

? 86: SRX1? ?? ???? ??, ??? ???? , ?? ? ? ? ? ? ? ?

| ??                  | ??                | ?? ? ? ?                           |
|---------------------|-------------------|------------------------------------|
| ?????               | ge-0/0/0.0        | 10.1.1.2/30                        |
|                     | ge-0/0/1.0        | 10.2.2.2/30                        |
|                     | st0.0 (?? ???? ?) | 10.3.3.2/30                        |
| ??? ???? (?? ? ? ?) | VR1               | ge-0/0/1.0<br>st0.0                |
| ?? ? ? ?            | 10.6.6.0/24       | ?? ? ? st0.0????.                  |
| ?? ?                | ??                | • ge-0/0/1 ?????? ? ? ? ? ? ? ? ?. |

### 86: SRX1700, SRX1702, SRX1705, SRX1708 (Continued)

| ?? | ??      | ?? ?? ??                                                                                                                |
|----|---------|-------------------------------------------------------------------------------------------------------------------------|
|    | untrust | <ul style="list-style-type: none"> <li>ge-0/0/0 172.16.1.1 172.16.1.2.</li> <li>st0.0 172.16.1.1 172.16.1.2.</li> </ul> |

### 87: IKE(Internet Key Exchange) 1700 1702 1705

| ??         | ??            | ?? ?? ??                                                                                                                                                           |
|------------|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??         | first_ikeprop | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> </ul>                                                                                           |
| ??         | first_ikepol  | <ul style="list-style-type: none"> <li>??: main</li> <li>?? ??: first_ikeprop</li> <li>IKE(Internet Key Exchange) 1700 1702: pre-shared-keys</li> </ul>            |
| 172.16.1.1 | 1             | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) 1700 1702: first_ikepol</li> <li>172.16.1.1: ge-0/0/0.0</li> <li>172.16.1.1: 10.4.4.2</li> </ul> |

### 88: IPsec 1700 1702 1705

| ?? | ??              | ?? ?? ??                                                                                                                         |
|----|-----------------|----------------------------------------------------------------------------------------------------------------------------------|
| ?? | first_ipsecprop | <ul style="list-style-type: none"> <li>172.16.1.1: esp</li> <li>172.16.1.1: hmac-md5-96</li> <li>172.16.1.1: 3des-cbc</li> </ul> |
| ?? | first_ipsecpol  | <ul style="list-style-type: none"> <li>IPsec 1700 1702: first_ipsecprop</li> </ul>                                               |

88: IPsec (Continued)

| VPN | first_vpn | <ul style="list-style-type: none"><li>• IKE(Internet Key Exchange) : </li><li>• IPsec : first_ipsecpol</li><li>• : st0.0</li><li>• establish-tunnels</li></ul> |
|-----|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|

in this section

| 542

CLI

,
,
,
[edit]
CLI,
commit()
.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.2/30
set interfaces ge-0/0/1 unit 0 family inet address 10.2.2.2/30
set interfaces st0 unit 0 family inet address 10.3.3.2/30
set security zones security-zone trust interfaces ge-0/0/1
set security zones security-zone untrust interfaces ge-0/0/0
set security zones security-zone untrust interfaces st0.0
set security ike proposal first_ikeprop authentication-method pre-shared-keys
set security ike proposal first_ikeprop dh-group group2
set security ike proposal first_ikeprop authentication-algorithm md5
set security ike proposal first_ikeprop encryption-algorithm 3des-cbc
set security ike policy first_ikepol mode main
set security ike policy first_ikepol proposals first_ikeprop
set security ike policy first_ikepol pre-shared-key ascii-text "$ABC123"
```



```

set security ike gateway first ike-policy first_ikepol
set security ike gateway first address 10.4.4.2
set security ike gateway first external-interface ge-0/0/0.0
set security ipsec proposal first_ipsecprop protocol esp
set security ipsec proposal first_ipsecprop authentication-algorithm hmac-md5-96
set security ipsec proposal first_ipsecprop encryption-algorithm 3des-cbc
set security ipsec policy first_ipsecpol perfect-forward-secrecy keys group1
set security ipsec policy first_ipsecpol proposals first_ipsecprop
set security ipsec vpn first_vpn bind-interface st0.0
set security ipsec vpn first_vpn ike gateway first
set security ipsec vpn first_vpn ike ipsec-policy first_ipsecpol
set security ipsec vpn first_vpn establish-tunnels immediately
set security policies from-zone trust to-zone untrust policy p1 match source-address any
set security policies from-zone trust to-zone untrust policy p1 match destination-address any
set security policies from-zone trust to-zone untrust policy p1 match application any
set security policies from-zone trust to-zone untrust policy p1 then permit
set security policies from-zone untrust to-zone trust policy p2 match source-address any
set security policies from-zone untrust to-zone trust policy p2 match destination-address any
set security policies from-zone untrust to-zone trust policy p2 match application any
set security policies from-zone untrust to-zone trust policy p2 then permit
set routing-instances VR1 instance-type virtual-router
set routing-instances VR1 interface ge-0/0/1.0
set routing-instances VR1 interface st0.0
set routing-instances VR1 routing-options static route 10.6.6.0/24 next-hop st0.0

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? Junos OS CLI ??? ???? ?? ???? CLI ??? ???? ????  
??.

VR?? st0? ???? ??:

1. ???? ????.

[edit]

```

user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.2/30
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.2.2.2/30
user@host# set interfaces st0 unit 0 family inet address 10.3.3.2/30

```

2. `?? ??? ????`.

```
[edit]
user@host# set security zones security-zone trust interfaces ge-0/0/1
user@host# set security zones security-zone untrust interfaces ge-0/0/0
user@host# set security zones security-zone untrust interfaces st0.0
```

3. IPsec `??? 1??? ?????`.

```
[edit security ike]
user@host# set proposal first_ikeprop authentication-method pre-shared-keys
user@host# set proposal first_ikeprop dh-group group2
user@host# set proposal first_ikeprop authentication-algorithm md5
user@host# set proposal first_ikeprop encryption-algorithm 3des-cbc
```

4. IKE(Internet Key Exchange) `??? ????? ??? ?????`.

```
[edit security ike]
user@host# set policy first_ikepol mode main
user@host# set policy first_ikepol proposals first_ikeprop
user@host# set policy first_ikepol pre-shared-key ascii-text "$ABC123"
```

5. IKE(Internet Key Exchange) `??????? ????? ??? ?????`.

```
[edit security ike]
user@host# set gateway first ike-policy first_ikepol
user@host# set gateway first address 10.4.4.2
user@host# set gateway first external-interface ge-0/0/0.0
```

6. IPsec `??? 2??? ?????`.

```
[edit security ipsec]
user@host# set proposal first_ipsecprop protocol esp
user@host# set proposal first_ipsecprop authentication-algorithm hmac-md5-96
user@host# set proposal first_ipsecprop encryption-algorithm 3des-cbc
```

7. `set policy first_ipsecpol perfect-forward-secrecy keys group1`

```
[edit security ipsec]
user@host# set policy first_ipsecpol perfect-forward-secrecy keys group1
user@host# set policy first_ipsecpol proposals first_ipsecprop
```

8. `set vpn first_vpn ike gateway first`

```
[edit security ipsec]
user@host# set vpn first_vpn ike gateway first
user@host# set vpn first_vpn ike ipsec-policy first_ipsecpol
user@host# set vpn first_vpn establish-tunnels immediately
```

9. `set vpn first_vpn bind-interface st0.0`

```
[edit security ipsec]
user@host# set vpn first_vpn bind-interface st0.0
```

10. `set from-zone trust to-zone untrust policy p1 match source-address any`

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy p1 match source-address any
user@host# set from-zone trust to-zone untrust policy p1 match destination-address any
user@host# set from-zone trust to-zone untrust policy p1 match application any
user@host# set from-zone trust to-zone untrust policy p1 then permit
user@host# set from-zone untrust to-zone trust policy p2 match source-address any
user@host# set from-zone untrust to-zone trust policy p2 match destination-address any
user@host# set from-zone untrust to-zone trust policy p2 match application any
user@host# set from-zone untrust to-zone trust policy p2 then permit
```

11. `set VR1 instance-type virtual-router`

```
[edit routing-instances]
user@host# set VR1 instance-type virtual-router
user@host# set VR1 interface ge-0/0/1.0
user@host# set VR1 interface st0.0
```

[illegible]

```
[edit routing-instances VR1 routing-options]
user@host# set static route 10.6.6.0/24 next-hop st0.0
```

??

```

?? ? show security ? show routing-instances ??? ??. ??? ???? ???? ???? ???? ? ? ? ? ? ? ? ?
?????.

```

```

user@host# show security
ike {
proposal first_ikeprop {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
}
policy first_ikepol {
    mode main;
    proposals first_ikeprop;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway first {
    ike-policy first_ikepol;
    address 10.4.4.2;
    external-interface ge-0/0/0.0;
}
}

ipsec {
    proposal first_ipsecprop {
        protocol esp;
        authentication-algorithm hmac-md5-96;
        encryption-algorithm 3des-cbc;
    }
    policy first_ipsecpol {
        perfect-forward-secret {
            keys group1;
        }
        proposals first_ipsecprop;
    }
}

```

```

    vpn first_vpn {
        bind-interface st0.0;
        ike {
            gateway first;
            ipsec-policy first_ipsecpol;
        }
        establish-tunnels immediately;
    }
}
policies {
    from-zone trust to-zone untrust {
        policy p1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone untrust to-zone trust {
        policy p2 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit;
            }
        }
    }
}
zones {
    security-zone trust {
        interfaces {
            ge-0/0/1.0;
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/0.0;
        }
    }
}

```

```
        st0.0;
    }
}

user@host# show routing-instances
    VR1 {
        instance-type virtual-router;
        interface ge-0/0/1.0;
        interface st0.0;
        routing-options {
            static {
                route 10.6.6.0/24 next-hop st0.0;
            }
        }
    }
}
```

user@host# commit

user@host#

**in this section**

[Configure st0](#) | 548

user@host# show interfaces st0.0 detail

user@host# show st0

user@host#

user@host# show st0

user@host#

user@host# show interfaces st0.0 detail, user@host# show st0, user@host# show route all

SEE ALSO

[VPN](#) | 537

[Feature Explorer](#).

| release heading in release-history | desc heading in release-history |
|------------------------------------|---------------------------------|
| 10.4                               | Junos OS 10.4 st0               |

[IPsec VPN](#) | 452

summary

IPsec VPN

in this section

- [VPN](#) | 549
- [:](#)  | 553

VPN IPv4 IPv6 VPN IPv4 IPv6

VPN

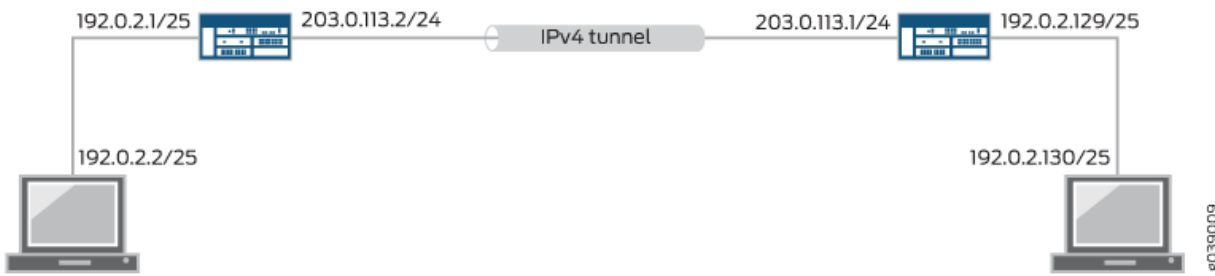
in this section

- | 551

VPN `??` `????` IPsec `??` IP `???` `???` `??` IP `???????` `?` `??` IP `?????` `??` `???????`, `??` IP `?????` `???????` IP `???` `???`  
`?`, `??` `?????` `??` `??` `?` `??` IP `???` `???????`, `??` `?` `??` IP `???` IPv4 `??` IPv6 `???` `?????` `??` `?` `?????`, SRX `????` `?????` `??` `?`  
`?` `?????` `?` VPN `??` `4??` `??` `????` `???????`.

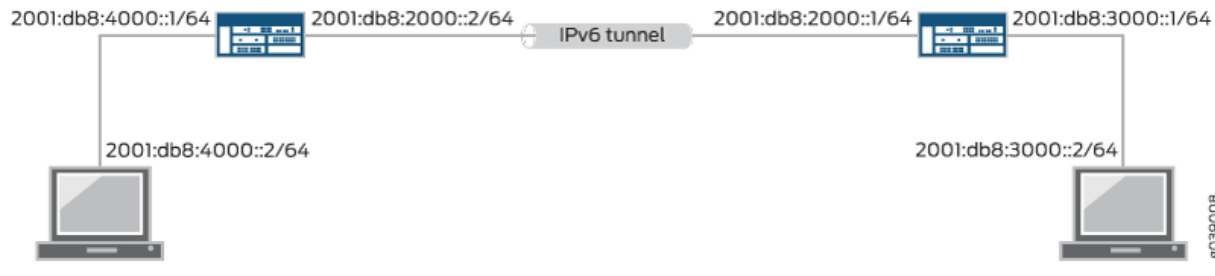
IPv4-in-IPv4 `???` `?` `???` `??` `31` `???` `550` `??` IPv4 `???` IPv4 `??` `????` `???????`, `??` `?` `??` `??` `???` `??` `?????` `???`  
IPv4 `???`.

`??` **31: IPv4-in-IPv4** `??`



IPv6-in-IPv6 `???` `?` `???` `??` `32` `???` `550` `??` IPv6 `???` IPv6 `??` `????` `???????`, `??` `?` `??` `??` `???` `??` `?????` `???`  
IPv6 `???`.

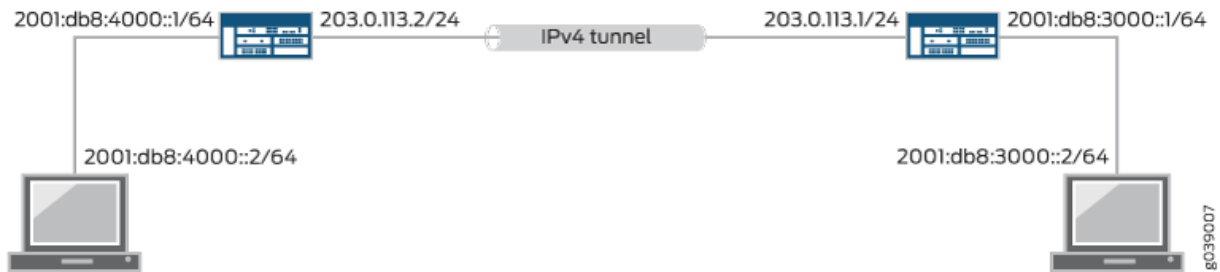
`??` **32: IPv6-in-IPv6** `??`



IPv6-in-IPv4 `???` `?` `???` `??` `33` `???` `551` `??` IPv6 `???` IPv4 `??` `????` `???????`, `??` `???` `?????` `???` IPv4 `???` `??` `???`  
`?????` `???` IPv6 `???`.

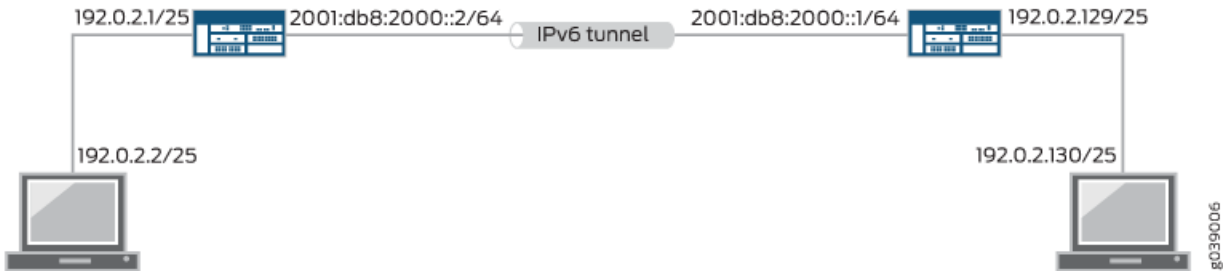


### ?? 33: IPv6-in-IPv4 ??



IPv4-in-IPv6 ??? ? ??? [?? 34](#) ??? [551](#)?? IPv4 ??? IPv6 ?? ??? ??????, ?? ??? ? ???? ??? IPv6?? ? ?  
?? ?? ????? ??? IPv4???

### ?? 34: IPv4-in-IPv6 ??



?? IPsec VPN ??? IPv4 ? IPv6 ????? ? ???? ? ?????. ?? ??, IPv4 ??? IPv4-in-IPv4 ? IPv6-in-IPv4 ?? ?????  
??? ??? ? ?????. ?? IPsec VPN ??? ?? IPv4 ? IPv6 ????? ? ???? ? ???? st0 ?????? ? family inet ?  
family inet6???? ????.

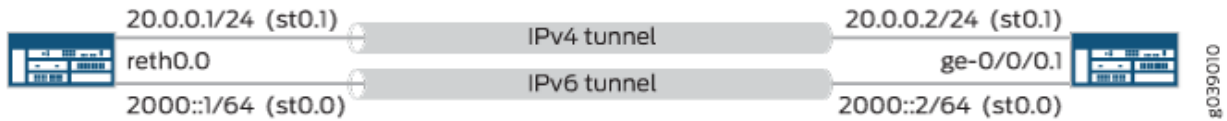
IPv4 ? IPv6 ??? ??? ????? ? ? ???? ? VPN? ??? ?? ?? IPv4 ? IPv6 ??? ? ???? ? ? ? ?????. ? ?  
?? ?? ?? ?? ? ? ? ? ? ? st0 ?????? ??????.

?? ?? VPN? ?? IPv6-in-IPv6? ????? ? ? ?????. [IPv6 IPsec VPN? ???????](#).

?? ?????? ? ? ? ? ? ?

?? ?? ??(?? ???? ?????? ? ? ? ? ? ? IPv4 ? IPv6 ??) ? ? ? ? ? ? VPN? ??????. IPv4 ? IPv6 ??? ? ? ?  
????? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?  
?? [?? 35](#) [?? 552](#)?? ? ? ?  
?? reth0.0 ? ge-0/0/0.1 ? ? ? ? ? ? ? ? IPv4 ? IPv6 ??? ??????.

?? 35: ?? ?? ??



??? ?? 35 ??? 552? IPsec VPN ??? ?? ??? ?? ??(st0) ?????? ????? ???. ??? st0 ?????? ????? ?? IPv4 ? IPv6 ??? ????? ?????.

?? IPsec VPN ??? IPv4 ? IPv6 ????? ?? ??? ? ?????. ?? ??, IPv4 ??? IPv4-in-IPv4 ? IPv6-in-IPv4 ?? ????? ????? ? ?????. ?? IPsec VPN ??? ?? IPv4 ? IPv6 ????? ?? ?????? ?? ??? ????? st0 ?????? ? family inet ? family inet6????? ???.

??? ?? ????? ?? ??? VPN ??? ?? ??? ?? ??????? ??? ?? [edit security ike gateway *gateway-name*] ?? ????? ??? ? local-address ?? ?????.

?(?) ??? ?? local-address , ??? IPv4 ?? IPv6 ??? ?? ?????? ??? ??????. ??? ?? ??????? local-address IPv4 ??? IPv6 ??? ??? ????? ????? ????? ?????.

local-address ?? SRX ??? ????? ??????? ??? IP ????? ???. IKE(Internet Key Exchange) ??????? ?? ??????? ?? ? ?? local-address ?????. ?(?) IKE(Internet Key Exchange) ??????? ?? ??????? ??? ?? ?? local-address ??????? IKE(Internet Key Exchange) ??????? ?? ??????? ??? ??? ??? ?? ????? ?????? ?? ? ?? ??? ????? ???.

local-address ?? ?? IKE(Internet Key Exchange) ?????? ??? ??? ?? ???(IPv4 ?? IPv6)? ??? ???.

?(?) ????? ?? ?? local-address , ?? ?????? ??? ?? ?????? ??? ????? ????. ?? ?????? ??? IPv4 ??? ??, ?? ?????? ??? ?? ?????? ??? IPv4 ??????. ?? ?????? ??? IPv6 ??? ??, ?? ?????? ??? ?? ??? ??????? ?? IPv6 ????? ?.

SEE ALSO

|                                 |
|---------------------------------|
| IPv6 ??? ?? VPN ?? ??   409     |
| IPv6 IKE ? IPsec ?? ?? ??   414 |
| IPv6 ??? ?? VPN ?? ??   409     |



?? ?? | 553

?? | 553

?? | 557

?? | 563

?? ??

? ?? ???? ???? ?? ?? ??? ? VPN???? ?????.

??

● ??? | 556

- IPv4  IPv6  . IPv6-in-IPv4   . IPv4      st0.0  inet6    .

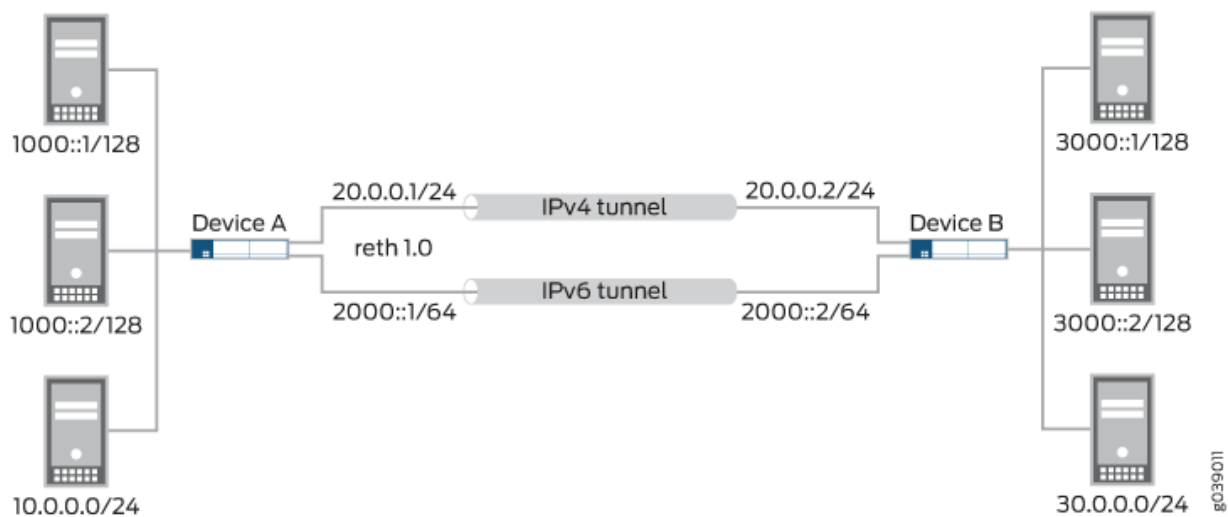
- IPv6 [?] IPv4 [?] IPv6 [?] [?] [?] [?], IPv4-in-IPv6 [?] IPv6-in-IPv6 [?] [?] [?] [?]. IPv6 [?] [?] [?] [?] [?] [?] [?] st0.1[?] family inet [?] family inet6 [?] [?] [?] [?].

[89](#) [554](#) [\(?\)](#) [???](#) [???](#) [1??](#) [???](#) [????](#). [1??](#) [??](#) [????](#) IPv6 [???](#) IPv4 [???](#) [??](#) [?](#) [??](#) IKE [????](#) [???](#) [???](#) [??](#).









??

● ?? | 557

??

CLI    

? ?? ??? ??????, ?? ??? ????? ??? ??? ? ? ? ? ? ???? ???, ????? ??? ??? ? ??? ? ? ??? [edit] ?  
? ??????? CLI? ??? ? ? ? ?, ? ???? commit?(?) ??????.

```
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-8/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 20.0.0.1/24
set interfaces reth1 unit 0 family inet6 address 2000::1/64
set interfaces st0 unit 0 family inet6
set interfaces st0 unit 1 family inet
set interfaces st0 unit 1 family inet6
```

```

set security ike proposal ike_proposal authentication-method pre-shared-keys
set security ike proposal ike_proposal authentication-algorithm md5
set security ike proposal ike_proposal encryption-algorithm 3des-cbc
set security ike proposal ike_proposal lifetime-seconds 3600
set security ike policy ike_policy mode aggressive
set security ike policy ike_policy proposals ike_proposal
set security ike policy ike_policy pre-shared-key ascii-text "$ABC123"
set security ike gateway ike_gw_v6 ike-policy ike_policy
set security ike gateway ike_gw_v6 address 2000::2
set security ike gateway ike_gw_v6 external-interface reth1.0
set security ike gateway ike_gw_v6 version v2-only
set security ike gateway ike_gw_v4 ike-policy ike_policy
set security ike gateway ike_gw_v4 address 20.0.0.2
set security ike gateway ike_gw_v4 external-interface reth1.0
set security ipsec proposal ipsec_proposal protocol esp
set security ipsec proposal ipsec_proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_proposal encryption-algorithm 3des-cbc
set security ipsec policy ipsec_policy proposals ipsec_proposal
set security ipsec vpn test_s2s_v6 bind-interface st0.1
set security ipsec vpn test_s2s_v6 ike gateway ike_gw_v6
set security ipsec vpn test_s2s_v6 ike ipsec-policy ipsec_policy
set security ipsec vpn test_s2s_v6 establish-tunnels immediately
set security ipsec vpn test_s2s_v4 bind-interface st0.0
set security ipsec vpn test_s2s_v4 ike gateway ike_gw_v4
set security ipsec vpn test_s2s_v4 ike ipsec-policy ipsec_policy
set routing-options rib inet6.0 static route 3000::1/128 next-hop st0.0
set routing-options rib inet6.0 static route 3000::2/128 next-hop st0.1
set routing-options static route 30.0.0.0/24 next-hop st0.1
set security forwarding-options family inet6 mode flow-based

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? Junos OS CLI ??? ???? ?? ???? CLI ??? ??? ????  
??.

?? ?? ?? ?? ??:

1. ?? ?????? ??????.

```

[edit interfaces]
user@host# set ge-0/0/1 gigether-options redundant-parent reth1
user@host# set ge-8/0/1 gigether-options redundant-parent reth1

```



```

user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 20.0.0.1/24
user@host# set reth1 unit 0 family inet6 address 2000::1/64

```

2. `set st0 unit 0 family inet6`.

```

[edit interfaces]
user@host# set st0 unit 0 family inet6
user@host# set st0 unit 1 family inet
user@host# set st0 unit 1 family inet6

```

3. `set security ike proposal ike_proposal`.

```

[edit security ike proposal ike_proposal]
user@host# set authentication-method pre-shared-keys
user@host# set authentication-algorithm md5
user@host# set encryption-algorithm 3des-cbc
user@host# set lifetime-seconds 3600
[edit security ike policy ike_policy]
user@host# set mode aggressive
user@host# set proposals ike_proposal
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security ike gateway ike_gw_v6]
user@host# set ike-policy ike_policy
user@host# set address 2000::2
user@host# set external-interface reth1.0
user@host# set version v2-only
[edit security ike gateway ike_gw_v4]
user@host# set ike-policy ike_policy
user@host# set address 20.0.0.2
user@host# set external-interface reth1.0

```

4. `set security ipsec proposal ipsec_proposal`.

```

[edit security ipsec proposal ipsec_proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm 3des-cbc
[edit security ipsec policy ipsec_policy]
user@host# set proposals ipsec_proposal

```

```
[edit security ipsec vpn test_s2s_v6 ]
user@host# set bind-interface st0.1
user@host# set ike gateway ike_gw_v6
user@host# set ike ipsec-policy ipsec_policy
user@host# set establish-tunnels immediately
[edit security ipsec vpn test_s2s_v4]
user@host# set bind-interface st0.0
user@host# set ike gateway ike_gw_v4
user@host# set ike ipsec-policy ipsec_policy
```

##### 5. `set static route`.

```
[edit routing-options rib inet6.0]
user@host# set static route 3000::1/128 next-hop st0.0
user@host# set static route 3000::2/128 next-hop st0.1
[edit routing-options]
user@host# set static route 30.0.0.0/24 next-hop st0.1
```

##### 6. IPv6 `set family inet6 mode flow-based`.

```
[edit security forwarding-options]
user@host# set family inet6 mode flow-based
```

`show`

`show interfaces`, `show security ike`, `show security ipsec`, `show routing-options` `show security forwarding-options` `show security ipsec`, `show security ike`, `show security ipsec`, `show security forwarding-options`.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  gigether-options {
    redundant-parent reth1;
  }
}
ge-8/0/1 {
  gigether-options {
    redundant-parent reth1;
  }
}
```

```

}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 20.0.0.1/24;
        }
        family inet6 {
            address 2000::1/64;
        }
    }
}
st0 {
    unit 0 {
        family inet;
        family inet6;
    }
    unit 1 {
        family inet6;
    }
}
[edit]
user@host# show security ike
proposal ike_proposal {
    authentication-method pre-shared-keys;
    authentication-algorithm md5;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
}
policy ike_policy {
    mode aggressive;
    proposals ike_proposal;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway ike_gw_v6 {
    ike-policy ike_policy;
    address 2000::2;
    external-interface reth1.0;
    version v2-only;
}
gateway ike_gw_4 {

```

```

    ike-policy ike_policy;
    address 20.0.0.2;
    external-interface reth1.0;
}
[edit]
user@host# show security ipsec
proposal ipsec_proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
}
policy ipsec_policy {
    proposals ipsec_proposal;
}
vpn test_s2s_v6 {
    bind-interface st0.1;
    ike {
        gateway ike_gw_v6;
        ipsec-policy ipsec_policy;
    }
    establish-tunnels immediately;
}
vpn test_s2s_v4 {
    bind-interface st0.0;
    ike {
        gateway ike_gw_4;
        ipsec-policy ipsec_policy;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 3000::1/128 next-hop st0.0;
        route 3000::2/128 next-hop st0.1;
    }
}
static {
    route 30.0.0.0/24 next-hop st0.1;
}
[edit]
user@host# show security forwarding-options
family {

```

```
        inet6 {
            mode flow-based;
        }
    }
```

?? ?? ?? ?? ?? commit?(?) ????.

??

**in this section**

- [IKE\(Internet Key Exchange\) 1?? ?? ?? | 563](#)
- [IPsec 2?? ?? ?? | 564](#)
- [?? ?? | 564](#)

??? ????? ????? ???? ?????.

### IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

?? ????? show security ike security-associations ??? ?????.

```
user@host> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode      Remote Address
1081812113 UP    51d9e6df8a929624 7bc15bb40781a902 IKEv2     2000::2
1887118424 UP    d80b55b949b54f0a b75ecc815529ae8f Aggressive 20.0.0.2
```

??

show security ike security-associations **???** **??** **??** IKE(Internet Key Exchange) **1??** SA? **??????**. SA? **?????** **??** **??**, **1??** **????** **????** **??** **?????**. **?????** IKE(Internet Key Exchange) **??** **??** **??** **?** **??** **??????** **????** **??????**. **1??** **??** **??** **????** **??** **???????** **?????** **????**.

**IPsec 2?? ??**

??

IPsec **2??** **????** **??????**.

??

**??** **?????** show security ipsec security-associations **????** **??????**.

```
user@host> show security ipsec security-associations
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<131074 ESP:3des/sha1 8828bd36 3571/  unlim      -   root 500   20.0.0.2
>131074 ESP:3des/sha1 c968afd8 3571/  unlim      -   root 500   20.0.0.2
<131073 ESP:3des/sha1 8e9e695a 3551/  unlim      -   root 500   2000::2
>131073 ESP:3des/sha1 b3a254d1 3551/  unlim      -   root 500   2000::2
```

??

show security ipsec security-associations **????** **??** **??** IKE **2??** SA? **??????**. SA? **?????** **??** **??** **??**, **2??** **????** **????** **??** **?????**. **?????** IKE(Internet Key Exchange) **??** **??** **??** **?** **??** **??????** **????** **??????**. **2??** **??** **??** **????** **??** **???????** **?????** **??** **??**.

**??** **??**

??

**??** **????** **???????**.

??

?? ???? show route ??? ?????.

```

user@host> show route
inet.0: 20 destinations, 20 routes (20 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.5.0.0/16      *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.10.0.0/16     *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.150.0.0/16    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.150.48.0/21   *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.155.0.0/16    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.157.64.0/19   *[Direct/0] 3d 01:43:23
                  > via fxp0.0
10.157.72.36/32  *[Local/0] 3d 01:43:23
                  Local via fxp0.0
10.204.0.0/16    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.206.0.0/16    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
10.209.0.0/16    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
20.0.0.0/24      *[Direct/0] 03:45:41
                  > via reth1.0
20.0.0.1/32      *[Local/0] 03:45:41
                  Local via reth1.0
30.0.0.0/24      *[Static/5] 00:07:49
                  > via st0.1
50.0.0.0/24      *[Direct/0] 03:45:42
                  > via reth0.0
50.0.0.1/32      *[Local/0] 03:45:42
                  Local via reth0.0
172.16.0.0/12    *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0
192.168.0.0/16   *[Static/5] 3d 01:43:23
                  > to 10.157.64.1 via fxp0.0

```

```

192.168.102.0/23    *[Static/5] 3d 01:43:23
                   > to 10.157.64.1 via fxp0.0
207.17.136.0/24    *[Static/5] 3d 01:43:23
                   > to 10.157.64.1 via fxp0.0
207.17.136.192/32  *[Static/5] 3d 01:43:23
                   > to 10.157.64.1 via fxp0.0

inet6.0: 10 destinations, 14 routes (10 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2000::/64          *[Direct/0] 03:45:41
                   > via reth1.0
2000::1/128         *[Local/0] 03:45:41
                   Local via reth1.0
3000::1/128         *[Static/5] 00:03:45
                   > via st0.0
3000::2/128         *[Static/5] 00:03:45
                   > via st0.1
5000::/64          *[Direct/0] 03:45:42
                   > via reth0.0
5000::1/128         *[Local/0] 03:45:42
                   Local via reth0.0
fe80::/64          *[Direct/0] 03:45:42
                   > via reth0.0
                   [Direct/0] 03:45:41
                   > via reth1.0
                   [Direct/0] 03:45:41
                   > via st0.0
                   [Direct/0] 03:45:13
                   > via st0.1
fe80::210:dbff:feff:1000/128
                   *[Local/0] 03:45:42
                   Local via reth0.0
fe80::210:dbff:feff:1001/128
                   *[Local/0] 03:45:41
                   Local via reth1.0

```

??

show route ??? ???? ???? ? ? ? ? ? ? ? ?.



?? ??

IPv6 IPsec VPN | 409

IPsec VPN ?? | 88

## ?? ???? ? IPsec VPN ??

in this section

?? ???-?? IPsec VPN ?? ???? ?? | 567

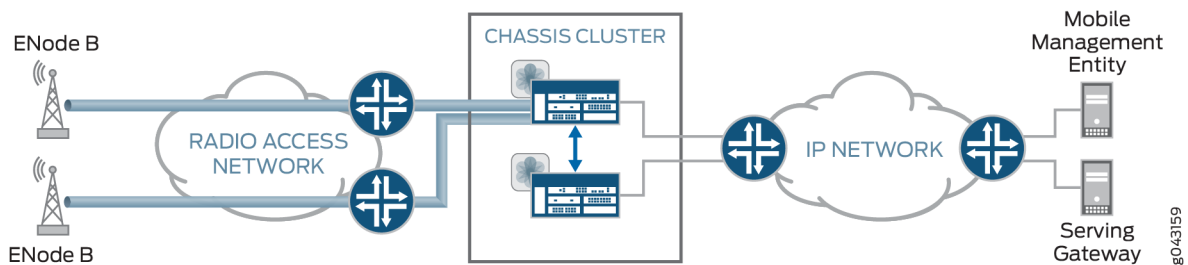
?: ??? ?????? ?? ??? ?? ?? | 569

SRX ??? ???? ?? ???? ???? IPsec VPN ??? ?????, ???/??? ?? ??????? ?? VPN ??? ??? ???? ?????. ??  
?/??? ?? ?????? VPN ??? ? ?? ? ???? ??? ? ????.

### ?? ???-?? IPsec VPN ?? ???? ??

???/??? ?? ?????? ?? VPN ??? ? ?? 37 ??? 567??? ?? ??? ????.

?? 37: IPsec VPN ??? ?? ???/??? ?? ?????



???/??? ?? ?????? VPN ??? ? ?? ? ???? ??? ? ?????. ? ??? ?? 38 ??? 568??? ?? ?????? ? ??? ???? ? ??  
? VPN ??? ?? ???? ???? ? ?????. ? ??? ?? ???-?? IPsec VPN ?? ?????? ???.



SEE ALSO

| [SRX 569 572 576 579 582 585 588 591 594 597 600 603 606 609 612 615 618 621 624 627 630 633 636 639 642 645 648 651 654 657 660 663 666 669 672 675 678 681 684 687 690 693 696 699 702 705 708 711 714 717 720 723 726 729 732 735 738 741 744 747 750 753 756 759 762 765 768 771 774 777 780 783 786 789 792 795 798 801 804 807 810 813 816 819 822 825 828 831 834 837 840 843 846 849 852 855 858 861 864 867 870 873 876 879 882 885 888 891 894 897 900 903 906 909 912 915 918 921 924 927 930 933 936 939 942 945 948 951 954 957 960 963 966 969 972 975 978 981 984 987 990 993 996 999](#)

?: 569 572 576 579 582 585 588 591 594 597 600 603 606 609 612 615 618 621 624 627 630 633 636 639 642 645 648 651 654 657 660 663 666 669 672 675 678 681 684 687 690 693 696 699 702 705 708 711 714 717 720 723 726 729 732 735 738 741 744 747 750 753 756 759 762 765 768 771 774 777 780 783 786 789 792 795 798 801 804 807 810 813 816 819 822 825 828 831 834 837 840 843 846 849 852 855 858 861 864 867 870 873 876 879 882 885 888 891 894 897 900 903 906 909 912 915 918 921 924 927 930 933 936 939 942 945 948 951 954 957 960 963 966 969 972 975 978 981 984 987 990 993 996 999

| in this section |                           |
|-----------------|---------------------------|
| •               | <a href="#">569</a>   569 |
| •               | <a href="#">572</a>   569 |
| •               | <a href="#">576</a>   572 |
| •               | <a href="#">579</a>   576 |

VPN (Virtual Private Network) is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.

VPN

VPN is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.

- VPN is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.
- SSG140 is a firewall device that can be used to protect a network. It is part of a Redundancy Group (RG) and can be configured to protect the VPN.
- SSG140 is a firewall device that can be used to protect a network. It is part of a Redundancy Group (RG) and can be configured to protect the VPN.
- SSG140 is a firewall device that can be used to protect a network. It is part of a Redundancy Group (RG) and can be configured to protect the VPN.
- SSG140 is a firewall device that can be used to protect a network. It is part of a Redundancy Group (RG) and can be configured to protect the VPN.

VPN is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.

VPN is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.

VPN

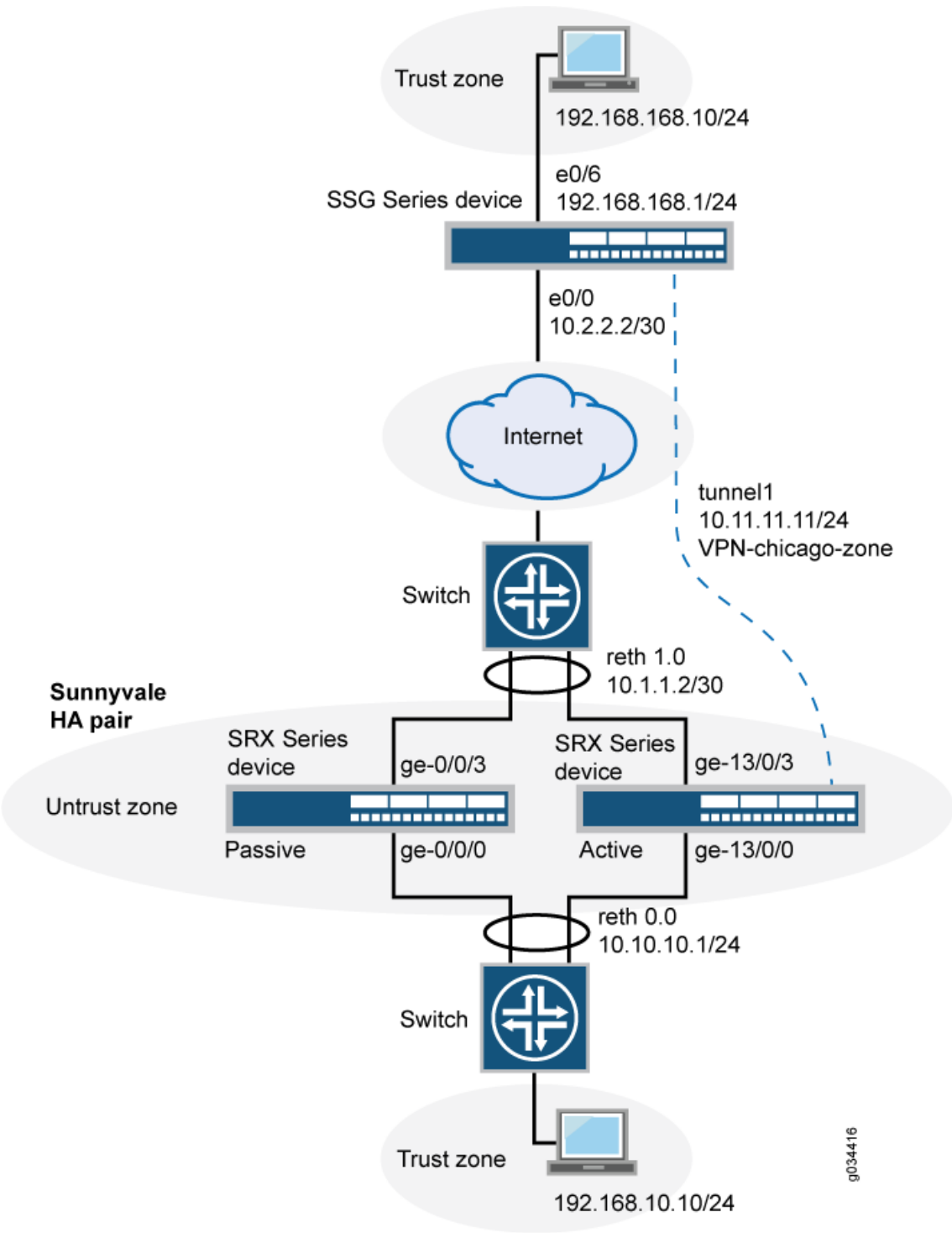
IKE (Internet Key Exchange) is a protocol that is used to establish a secure connection between two devices. It is often used to protect the VPN. The IKE is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the IKE is always available, even if one of the servers fails. The IKE is also protected by a firewall, which prevents unauthorized access to the network.

VPN is a technology that allows secure communication over a public network. It is often used to connect remote users to a private network. The VPN is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the VPN is always available, even if one of the servers fails. The VPN is also protected by a firewall, which prevents unauthorized access to the network.

SPU (Services Processing Unit) is a device that is used to process services. It is often used to protect the VPN. The SPU is managed by a central server, which is part of a Redundancy Group (RG). The RG ensures that the SPU is always available, even if one of the servers fails. The SPU is also protected by a firewall, which prevents unauthorized access to the network.



?? 39: ?? ???? VPN? ?? ??? ?????



|                                             |                                                                                                                         |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| lo0.1<br>10.3.3.3/30<br>Untrust zone        | A logical interface on loopback that may be active on either node in the cluster depending on the activeness of its RG. |
| st0.0<br>10.11.11.10/24<br>vpn-chicago-zone | A logical interface on the secure tunnel interface for IPSec VPN tunnel.                                                |

??

## in this section

● ?? | 572

??

## CLI ?? ??

?? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ?? ?? ?? ?? ??, ?? ?? ?? ?? ??  
 ?? ?? [edit] ??? ??? CLI? ?? ?? ??, ?? ??? **commit?**(?) ????

```

set interfaces lo0 redundant-pseudo-interface-options redundancy-group 1
set interfaces lo0 unit 1 family inet address 10.3.3.3/30
set routing-instances vr1 instance-type virtual-router
set routing-instances vr1 interface lo0.1
set routing-instances vr1 interface reth0.0
set routing-instances vr1 interface reth1.0
set routing-instances vr1 interface st0.0
set routing-instances vr1 routing-options static route 192.168.168.1/24 next-hop st0.0
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposal-set standard
set security ike policy ike-policy1 pre-shared-key ascii-text "$ABC123"
set security ike gateway t-ike-gate ike-policy ike-policy1
set security ike gateway t-ike-gate address 10.2.2.2
set security ike gateway t-ike-gate external-interface lo0.1
set security ipsec proposal p2-std-p1 authentication-algorithm hmac-sha1-96
set security ipsec proposal p2-std-p1 encryption-algorithm 3des-cbc
set security ipsec proposal p2-std-p1 lifetime-seconds 180
set security ipsec proposal p2-std-p2 authentication-algorithm hmac-sha1-96
set security ipsec proposal p2-std-p2 encryption-algorithm aes-128-cbc
set security ipsec proposal p2-std-p2 lifetime-seconds 180
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group2
set security ipsec policy vpn-policy1 proposals p2-std-p1
set security ipsec policy vpn-policy1 proposals p2-std-p2
set security ipsec vpn t-ike-vpn bind-interface st0.0
set security ipsec vpn t-ike-vpn ike gateway t-ike-gate
set security ipsec vpn t-ike-vpn ike proxy-identity local 10.10.10.1/24

```



## 5. IPsec `???` `??????`.

```
[edit security ipsec]
user@host# set proposal p2-std-p1 authentication-algorithm hmac-sha1-96
user@host# set proposal p2-std-p1 encryption-algorithm 3des-cbc
user@host# set proposal p2-std-p1 lifetime-seconds 180
user@host# set proposal p2-std-p2 authentication-algorithm hmac-sha1-96
user@host# set proposal p2-std-p2 encryption-algorithm aes-128-cbc
user@host# set proposal p2-std-p2 lifetime-seconds 180
user@host# set policy vpn-policy1 perfect-forward-secrecy keys group2
user@host# set policy vpn-policy1 proposals p2-std-p1
user@host# set policy vpn-policy1 proposals p2-std-p2
user@host# set vpn t-ike-vpn bind-interface st0.0
user@host# set vpn t-ike-vpn ike gateway t-ike-gate
user@host# set vpn t-ike-vpn ike proxy-identity local 10.10.10.1/24
user@host# set vpn t-ike-vpn ike proxy-identity remote 192.168.168.1/24
user@host# set vpn t-ike-vpn ike ipsec-policy vpn-policy1
```

`??`

`??` `????` show interfaces lo0, show routing-instances, show security ike `?` show security ipsec `???` `?????` `???` `?????`  
`?.` `??` `????` `????` `?????` `?????` `???` `?` `??` `????` `?????` `????` `????????`.

```
[edit]
user@host# show interfaces lo0
    unit 1 {
        family inet {
            address 10.3.3.3/30;
        }
    }
    redundant-pseudo-interface-options {
        redundancy-group 1;
    }
```

```
[edit]
user@host# show routing-instances
    vr1 {
        instance-type virtual-router;
        interface lo0.1;
```



```

interface reth0.0;
interface reth1.0;
interface st0.0;
routing-options {
    static {
        route 192.168.168.1/24 next-hop st0.0;
    }
}
}

```

```

[edit]
user@host# show security ike
    policy ike-policy1 {
        mode main;
        proposal-set standard;
        pre-shared-key ascii-text "$ABC123";
    }
    gateway t-ike-gate {
        ike-policy ike-policy1;
        address 10.2.2.2;
        external-interface lo0.1;
    }

```

```

[edit]
user@host# show security ipsec
    proposal p2-std-p1 {
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 180;
    }
    proposal p2-std-p2 {
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-128-cbc;
        lifetime-seconds 180;
    }
    policy vpn-policy1 {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals [ p2-std-p1 p2-std-p2 ];
    }

```

```
    }
    policy vpn-policy2 {
        perfect-forward-secrecy {
            keys group2;
        }
        proposals [ p2-std-p1 p2-std-p2 ];
    }
    vpn t-ike-vpn {
        bind-interface st0.0;
        ike {
            gateway t-ike-gate;
            proxy-identity {
                local 10.10.10.1/24;
                remote 192.168.168.1/24;
            }
            ipsec-policy vpn-policy1;
        }
    }
}
```

```
root@host# commit
root@host#
```

??

in this section

?? ?? | 576

?? ??

??

```
root@host# show chassis cluster interfaces
```

??

```
?? show chassis cluster interfaces
```

```
user@host> show chassis cluster interfaces
Control link status: Up
```

```
Control interfaces:
  Index  Interface  Status
    0      em0           Up
    1      em1          Down
Fabric link status: Up
Fabric interfaces:
  Name    Child-interface  Status
  fab0    ge-0/0/7         Up   / Up
  fab0
  fab1    ge-13/0/7        Up   / Up
  fab1
Redundant-ethernet Information:
  Name      Status    Redundancy-group
  reth0      Up         1
  reth1      Up         1
  reth2      Up         1
  reth3      Down       Not configured
  reth4      Down       Not configured
Redundant-pseudo-interface Information:
  Name      Status    Redundancy-group
  lo0       Up         1
```

??

?? show chassis cluster interfaces ?? ???? ???? ???? ?????. Redundant-pseudo-interface Information  
?? ???? Up?? lo0 ?????? ???? Redundant-ethernet Information ??? ???? reth0, reth1 ? reth2 ??? Up??  
???? ???? ???? ????.

SEE ALSO

| [???? VPN? ?? ??? ?????? ???? | 1366](#)

?? ??

| [SRX ??? ?????? ?? ????? ???? ???](#)

?? ?? ???? ??, ?? ? ?? ??? ?? ?? ??? ????? ??????. ??? ????? IPv4 ?? IPv6 ??? ??? ? ?????. ?? ?? ? ????  
???? ? ????? ??? ? ?????.



**???** **????** IP **??** **????** **????**

? ? ? ? ? ? ? ? ? ? IP ? ? ? ? ? ? ? ? ? ? .

st0 VPN IP

2 22222 222 222222 2222 2222. 222 2222 22 222 22 222 P2MP(Point-to-multipoint) 222222 2222 22 VPN  
22 222 2 2222.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
}
vpn vpn-2 {
    bind-interface st0.1;
}
```

st0 VPN IP

**VPN? ?? ??? ???? ?? ????? IP ??? ??? ?, ??? ???? ? ??? ??? ???? ???? ???? ???? ???? ????.**

?? ????? point-to-point st0.1 ?????? VPN(vpn-1)? ?? 4?? ??? ???(ts-1, ts-2, ts-3, ts-4)? ??????.

```
[edit]
user@host# show security ipsec vpn vpn-1
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 192.168.5.0/24;
        remote-ip 10.1.5.0/24;
    }
    traffic-selector ts-2 {
        local-ip 192.168.0.0/16;
        remote-ip 10.1.0.0/16;
    }
    traffic-selector ts-3 {
        local-ip 172.16.0.0/16;
        remote-ip 10.2.0.0/16;
    }
    traffic-selector ts-4 {
```

[illegible]

?? ?? point-to-point st0 ?????? ???? ?? ?? VPN? ?? ??? ????? ?? ????? IP ??? ??? ??, st0 ?????? ?? ??  
 ??? ?? ??? ??? ? ???? ?????, ??? st0 ?????? ????? VPN ??? ??? ????? ??? ?? ????? ??? ?? ?? ???? ?  
 ????.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 192.168.1.0/24;
        remote-ip 10.1.1.0/24;
    }
}
vpn vpn-2 {
    bind-interface st0.2;
    traffic-selector ts-2 {
        local-ip 192.168.1.0/24;
        remote-ip 10.2.2.0/24;
    }
}
```

? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? VPN ? ? ? ? stO ? ? ? ? ? ?  
? ? ? .





? ??, ??? ????? ?????? ?????. ??? ?????? ??? ?? ?????????? ??? ??? ??? ????? ? ?? ?? ??? ??????. ?? ??? ???  
VPN? ????? st0 ?????? ??????.

?? ????? ??? ????? ? ?? VPN ????? ??????. ??? ????? ??? ?? ?????????? ??????. ? ??? ????? ?? ??? ?? ??????????  
?????? ?? ?? ????? ?? ??????.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 192.168.1.0/24;
        remote-ip 10.1.1.0/24;
    }
}
vpn vpn-2 {
    bind-interface st0.2;
    traffic-selector ts-2 {
        local-ip 192.168.1.0/24;
        remote-ip 10.1.0.0/16;
    }
}
```

ts-1???? remote-ip?(?) 10.1.1.0/24??, ts-2???? remote-ip?(?) 10.1.0.0/16???. 10.1.1.1? ??? ??? ??,  
?? ??? ??? ??? ? ? st0.1 ?????? ??????. ??? st0.1 ?????? ??? ?????? ??????.

?? ??, ??? ?????? ??? ?????? ?? ??? ??? ??? ? ?????. ?? ????? ??? ????? ? ?? VPN ????? ??????. ??? ????? ?? ?  
? ?? ?????????? ??????. ? ??? ????? ?? ??? ?? ?????????? ?????? ?? ?? ????? ?? ??????.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 192.168.1.0/24;
        remote-ip 10.1.1.0/24;
    }
}
vpn vpn-2 {
    bind-interface st0.2;
    traffic-selector ts-2 {
        local-ip 172.16.1.0/16;
```

```
remote-ip 10.1.0.0/16;
}
}
```

10.1.1.0? ?? 2?? ??(????? st0.1? ??? 10.1.1.0/24, ????? st0.2? ??? 10.1.0.0/16)? ??? ????? ??????. ??  
172.16.1.1?? ?? 10.1.1.1? ??? ??? ?????? st0.1? ??? 10.1.1.0/24? ??? ??? ????? ??????. ??? ??? ??? ???  
ts-1? ?? ??? ?????? ????? ?? ??????.

??? ?? ?????? ? ?????? ?? ?? ??? ?????? ??? ??, ??? ?? ??? ??? ?????? ??????. ??? ??? ??? ? ?????? ? ??? ??  
? ?????? ?????? ??????

SEE ALSO

| [VPN ?? ?? ??](#) | [549](#)

**?: ?? ?? VPN?? ??? ???? ??**

in this section

- [?? ??](#) | [584](#)
- [??](#) | [585](#)
- [??](#) | [586](#)
- [??](#) | [600](#)

?? ????? ?? ?? VPN? ?? ??? ????? ?????? ??? ?? ???.

?? ??

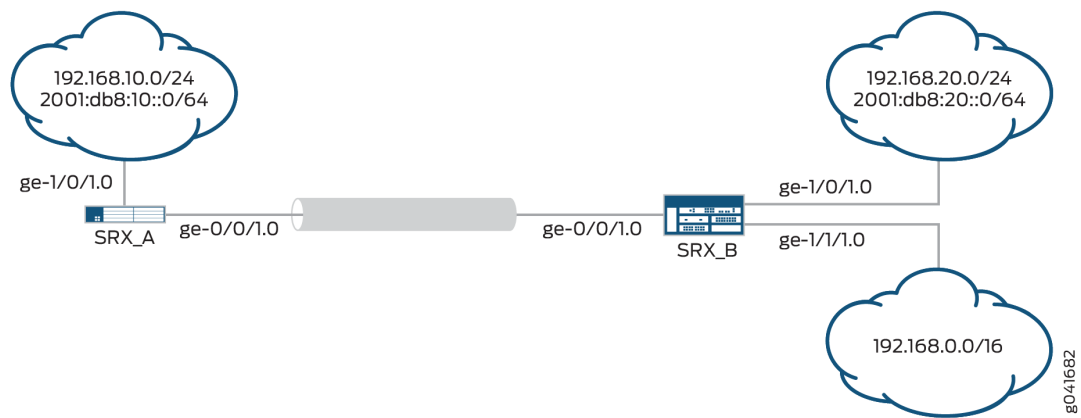
????? ?? ??? ??????.

- "[?? ?? VPN? ??? ??? ?????](#)" [???](#) [578](#)? ??????
- IKE(Internet Key Exchange) [????? ??????](#).

```
request system software add optional://junos-ike.tgz
```



?? 40: ??? ??? ?? ??



??

#### in this section

- SRX\_A ??? | 586
- SRX\_B ??? | 593

### SRX\_A ???

#### CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ??????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ????? ?? ?? ??, ?? ????? commit?(?) ?????.

```
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:2000::1/64
set interfaces st0 unit 1 family inet
set interfaces st0 unit 1 family inet6
set interfaces ge-1/0/1 unit 0 family inet address 192.168.10.1/24
set interfaces ge-1/0/1 unit 0 family inet6 address 2001:db8:10::0/64
set security ike proposal PSK-DH14-AES256-SHA256 authentication- method pre-shared-keys
set security ike proposal PSK-DH14-AES256-SHA256 dh-group group14
set security ike proposal PSK-DH14-AES256-SHA256 authentication- algorithm sha-256
set security ike proposal PSK-DH14-AES256-SHA256 encryption-algorithm aes-256-cbc
```

```
set security ike policy site-2-site mode main
set security ike policy site-2-site proposals PSK-DH14-AES256-SHA256
set security ike policy site-2-site pre-shared-key ascii-text "$ABC123"
set security ike gateway SRX_A-to-SRX_B ike-policy site-2-site
set security ike gateway SRX_A-to-SRX_B address 192.168.20.2
set security ike gateway SRX_A-to-SRX_B external-interface ge-0/0/1.0
set security ike gateway SRX_A-to-SRX_B local-address 192.168.10.1
set security ipsec proposal ESP-AES256-SHA256 protocol esp
set security ipsec proposal ESP-AES256-SHA256 authentication- algorithm hmac-sha-256-128
set security ipsec proposal ESP-AES256-SHA256 encryption-algorithm aes-256-cbc
set security ipsec policy site-2-site perfect-forward-secrecy keys group14
set security ipsec policy site-2-site proposals ESP-AES256-SHA256
set security ipsec vpn SRX_A-to-SRX_B bind-interface st0.1
set security ipsec vpn SRX_A-to-SRX_B ike ipsec-policy site-2-site
set security ipsec vpn SRX_A-to-SRX_B ike gateway SRX_A-to-SRX_B
set security ipsec vpn SRX_A-to-SRX_B traffic-selector TS1-ipv6 term term1 local-ip
2001:db8:10::0/64 remote-ip 2001:db8:20::0/64
set security ipsec vpn SRX_A-to-SRX_B traffic-selector TS2-ipv4 term term2 local-ip
192.168.10.0/24 remote-ip 192.168.0.0/16
set security forwarding-options family inet6 mode flow-based
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-1/0/1.0
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone VPN interfaces st0.1
set security policies from-zone VPN to-zone trust policy 1 match source-address any
set security policies from-zone VPN to-zone trust policy 1 match destination-address any
set security policies from-zone VPN to-zone trust policy 1 match application any
set security policies from-zone VPN to-zone trust policy 1 then permit
set security policies from-zone trust to-zone VPN policy 1 match source-address any
set security policies from-zone trust to-zone VPN policy 1 match destination-address any
set security policies from-zone trust to-zone VPN policy 1 match application any
set security policies from-zone trust to-zone VPN policy 1 then permit
set security policies default-policy deny -all
```

???

?? ?? ?? ???? ??? ??? ???? ?????. ?? ????? ??? ?? ??? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

1. `?? ?????? ??????`.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:2000::1/64
```

2. `??? ?? ?????? ??????`.

```
[edit interfaces]
user@host# set st0 unit 1 family inet
user@host# set st0 unit 1 family inet6
```

3. `?? ?????? ??????`.

```
[edit interfaces]
user@host# set ge-1/0/1 unit 0 family inet address 192.168.10.1/24
user@host# set ge-1/0/1 unit 0 family inet6 address 2001:db8:10::0/64
```

4. `1?? ??? ??????`.

```
[edit security ike proposal PSK-DH14-AES256-SHA256]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy site-2-site]
user@host# set mode main
user@host# set proposals PSK-DH14-AES256-SHA256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security ike gateway SRX_A-to-SRX_B]
user@host# set ike-policy site-2-site
user@host# set address 192.168.20.2
user@host# set external-interface ge-0/0/1.0
user@host# set local-address 192.168.10.1
```

5. `2?? ??? ??????`.

```
[edit security ipsec proposal ESP-AES256-SHA256]
user@host# set protocol esp
```

```

user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy site-2-site]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ESP-AES256-SHA256
[edit security ipsec vpn SRX_A-to-SRX_B]
user@host# set bind-interface st0.1
user@host# set ike gateway SRX_A-to-SRX_B
user@host# set ike ipsec-policy site-2-site
user@host# set traffic-selector TS1-ipv6 term term1 local-ip 2001:db8:10::0/64 remote-ip
2001:db8:20::0/64
user@host# set traffic-selector TS2-ipv4 term term2 local-ip 192.168.10.0/24 remote-ip
192.168.0.0/16

```

## 6. IPv6 `???` `??` `????` `??????`.

```

[edit security forwarding-options]
user@host# set family inet6 mode flow-based

```

## 7. `??` `????` `??` `????` `??????`.

```

[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-1/0/1.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services ike
user@host# set interfaces ge-0/0/1.0
[edit security zones security-zone VPN]
user@host# set interfaces st0.1
[edit security policies from-zone VPN to-zone trust ]
user@host# set policy 1 match source-address any
user@host# set policy 1 match destination-address any
user@host# set policy 1 match application any
user@host# set policy 1 then permit
[edit security policies from-zone trust to-zone VPN ]
user@host# set policy 1 match source-address any
user@host# set policy 1 match destination-address any
user@host# set policy 1 match application any
user@host# set policy 1 then permit

```

```
[edit security policies]
user@host# set default-policy deny-all
```

??

?? ???? show interfaces, show security ike, show security ipsec, show security forwarding-options, show security zones ? show security policies ??? ???? ???? ?????, ??? ??? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:2000::1/64;
    }
  }
}
ge-1/0/1 {
  unit 0 {
    family inet {
      address 192.168.10.1/24;
    }
    family inet6 {
      address 10::1/64;
    }
  }
}
st0 {
  unit 1 {
    family inet;
    family inet6;
  }
}
[edit]
user@host# show security ike
proposal PSK-DH14-AES256-SHA256 {
  authentication-method pre-shared-keys;
  dh-group group14;
  authentication-algorithm sha-256;
  encryption-algorithm aes-256-cbc;
}
```



```

policy site-2-site {
    mode main;
    proposals PSK-DH14-AES256-SHA256;
        pre-shared-key ascii-text
        "$ABC123"; ## SECRET-DATA
    }
gateway SRX_A-to-SRX_B {
    ike-policy site-2-site;
    address 192.168.20.2;
    external-interface ge-0/0/1.0;
    local-address 192.168.10.1;
}
[edit]
user@host# show security ipsec
proposal ESP-AES256-SHA256 {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
}
policy site-2-site {
    perfect-forward-secrecy keys group14;
    proposals ESP-AES256-SHA256;
}
vpn SRX_A-to-SRX_B {
    bind-interface st0.1;
    ike {
        ipsec-policy site-2-site;
        gateway SRX_A-to-SRX_B;
    }
    traffic-selector TS1-ipv6 {
        local-ip 2001:db8:10::0/64;
        remote-ip 2001:db8:20::0/64;
    }
    traffic-selector TS2-ipv4 {
        local-ip 192.168.10.0/24;
        remote-ip 192.168.0.0/16;
    }
}
[edit]
user@host# show security forwarding-options
family {
    inet6 {
        mode flow-based;

```

```

    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-1/0/1.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone VPN {
    interfaces {
        st0.1;
    }
}
[edit]
user@host# show security policies
from-zone VPN to-zone trust {
    policy 1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;

```

```

    }
  }
}
from-zone trust to-zone VPN {
  policy 1 {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
}
}

```

```

?? ?? ?? ?? commit?(?) ??.

```

**SRX\_B** ????

**CLI** ?? ??

```

? ?? ??? ????, ?? ??? ??? ???? ???? ???? ???? ???? ???? ???? [edit] ?
? ???? ???? CLI? ??? ???? ???? ???? ???? commit?(?) ??.

```

```

set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:2000::2/64
set interfaces st0 unit 1 family inet
set interfaces st0 unit 1 family inet6
set interfaces ge-1/0/1 unit 0 family inet address 192.168.20.1/24
set interfaces ge-1/0/1 unit 0 family inet6 address 2001:db8:20::0/64
set interfaces ge-1/1/1 unit 0 family inet address 192.168.0.1/24
set security ike proposal PSK-DH14-AES256-SHA256 authentication-method pre-shared-keys
set security ike proposal PSK-DH14-AES256-SHA256 dh-group group14
set security ike proposal PSK-DH14-AES256-SHA256 authentication-algorithm sha-256
set security ike proposal PSK-DH14-AES256-SHA256 encryption-algorithm aes-256-cbc
set security ike policy site-2-site mode main
set security ike policy site-2-site proposals PSK-DH14-AES256-SHA256
set security ike policy site-2-site pre-shared-key ascii-text "$ABC123"
set security ike gateway SRX_B-to-SRX_A ike-policy site-2-site
set security ike gateway SRX_B-to-SRX_A address 192.168.10.1
set security ike gateway SRX_B-to-SRX_A external-interface ge-0/0/1.0
set security ike gateway SRX_B-to-SRX_A local-address 192.168.20.2

```

```

set security ipsec proposal ESP-AES256-SHA256 protocol esp
set security ipsec proposal ESP-AES256-SHA256 authentication-algorithm hmac-sha-256-128
set security ipsec proposal ESP-AES256-SHA256 encryption-algorithm aes-256-cbc
set security ipsec policy site-2-site perfect-forward-secrecy keys group14
set security ipsec policy site-2-site proposals ESP-AES256-SHA256
set security ipsec vpn SRX_B-to-SRX-A bind-interface st0.1
set security ipsec vpn SRX_B-to-SRX-A ike ipsec-policy site-2-site
set security ipsec vpn SRX_B-to-SRX-A ike gateway SRX_B-to-SRX_A
set security ipsec vpn SRX_B-to-SRX-A traffic-selector TS1-ipv6 local-ip 2001:db8:20::0/64
remote-ip 2001:db8:10::0/64
set security ipsec vpn SRX_B-to-SRX-A traffic-selector TS2-ipv4 local-ip 192.168.0.0/16 remote-
ip 192.168.10.0/24
set security forwarding-options family inet6 mode flow-based
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-1/0/1.0
set security zones security-zone trust interfaces ge-1/1/1.0
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone VPN interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/1.0
set security policies from-zone VPN to-zone trust policy 1 match source-address any
set security policies from-zone VPN to-zone trust policy 1 match destination-address any
set security policies from-zone VPN to-zone trust policy 1 match application any
set security policies from-zone VPN to-zone trust policy 1 then permit
set security policies from-zone trust to-zone VPN policy 1 match source-address any
set security policies from-zone trust to-zone VPN policy 1 match destination-address any
set security policies from-zone trust to-zone VPN policy 1 match application any
set security policies from-zone trust to-zone VPN policy 1 then permit
set security policies default-policy deny -all

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

??? ???? ?????.

1. ?? ???? ????.

[edit interfaces]

```
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:2000::2/64
```

2. `set st0 unit 1 family inet`.

```
[edit interfaces]
user@host# set st0 unit 1 family inet
user@host# set st0 unit 1 family inet6
```

3. `set ge-1/0/1 unit 0 family inet address 192.168.20.1/24`.

```
[edit interfaces]
user@host# set ge-1/0/1 unit 0 family inet address 192.168.20.1/24
user@host# set ge-1/0/1 unit 0 family inet6 address 2001:db8:20::0/64
user@host# set ge-1/1/1 unit 0 family inet address 192.168.0.1/24
```

4. `set authentication-method pre-shared-keys`.

```
[edit security ike proposal PSK-DH14-AES256-SHA256]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy site-2-site]
user@host# set mode main
user@host# set proposals PSK-DH14-AES256-SHA256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security ike gateway SRX_B-to-SRX_A]
user@host# set ike-policy site-2-site
user@host# set address 192.168.10.1
user@host# set external-interface ge-0/0/1.0
user@host# set local-address 192.168.20.2
```

5. `set protocol esp`.

```
[edit security ipsec proposal ESP-AES256-SHA256]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy site-2-site]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ESP-AES256-SHA256
```

```
[edit security ipsec vpn SRX_B-to-SRX-A]
user@host# set bind-interface st0.1
user@host# set ike gateway SRX_B-to-SRX_A
user@host# set ike ipsec-policy site-2-site
user@host# set traffic-selector TS1-ipv6 local-ip 2001:db8:20::0/64 remote-ip
2001:db8:10::0/64
user@host# set traffic-selector TS2-ipv4 local-ip 192.168.0.0/16 remote-ip 192.168.10.0/24
```

## 6. IPv6 `???` `??` `????` `??????`.

```
[edit security forwarding-options]
user@host# set family inet6 mode flow-based
```

## 7. `??` `????` `??` `???` `??????`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-1/0/1.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services ike
user@host# set interfaces ge-0/0/1.0
[edit security zones security-zone VPN]
user@host# set interfaces st0.1
[edit security policies from-zone VPN to-zone trust ]
user@host# set policy 1 match source-address any
user@host# set policy 1 match destination-address any
user@host# set policy 1 match application any
user@host# set policy 1 then permit
[edit security policies from-zone trust to-zone VPN ]
user@host# set policy 1 match source-address any
user@host# set policy 1 match destination-address any
user@host# set policy 1 match application any
user@host# set policy 1 then permit
[edit security policies]
user@host# set default-policy deny-all
```

??

[illegible]

```
[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet6 {
            address 2001:db8:2000::2/64;
        }
    }
}
ge-1/0/1 {
    unit 0 {
        family inet {
            address 192.168.20.1/24;
        }
        family inet6 {
            address 2001:db8:20::0/64;
        }
    }
}
ge-1/1/1 {
    unit 0 {
        family inet {
            address 192.168.0.1/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
        family inet6;
    }
}
[edit]
user@host# show security ike
proposal PSK-DH14-AES256-SHA256 {
    authentication-method pre-shared-keys;
    dh-group group14;
```

```

    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
}
policy site-2-site {
    mode main;
    proposals PSK-DH14-AES256-SHA256;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
}
gateway SRX_B-to-SRX_A {
    ike-policy site-2-site;
    address 192.168.10.1;
    external-interface ge-0/0/1.0;
    local-address 192.168.20.2;
}
[edit]
user@host# show security ipsec
proposal ESP-AES256-SHA256 {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
    encryption-algorithm aes-256-cbc;
}
policy site-2-site {
    perfect-forward-secrecy keys group14;
    proposals ESP-AES256-SHA256;
}
vpn SRX_B-to-SRX_A {
    bind-interface st0.1;
    ike {
        ipsec-policy site-2-site;
        gateway SRX_B-to-SRX_A;
    }
    traffic-selector TS1-ipv6 {
        local-ip 2001:db8:20::0/64;
        remote-ip 2001:db8:10::0/64;
    }
    traffic-selector TS2-ipv4 {
        local-ip 192.168.0.0/16;
        remote-ip 192.168.10.0/24;
    }
}
[edit]
user@host# show security forwarding-options
family {

```



```

        inet6 {
            mode flow-based;
        }
    }
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-1/0/1.0;
        ge-1/1/1.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone VPN {
    interfaces {
        st0.1;
    }
}
[edit]
user@host# show security policies
from-zone VPN to-zone trust {
    policy 1 {
        match {
            source-address any;
            destination-address any;
            application any;

```

```
    }
    then {
        permit;
    }
}
}
from-zone trust to-zone VPN {
    policy 1 {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

set security ipsec policy 1 then { match { source-address any; destination-address any; application any; } then { permit; } }

set

in this section

- [IPsec 200 20 20 | 600](#)
- [200 200 20 | 603](#)
- [20 20 | 603](#)

set security ipsec policy 1 then { match { source-address any; destination-address any; application any; } then { permit; } }

set security ipsec policy 1 then { match { source-address any; destination-address any; application any; } then { permit; } }

IPsec 200 20 20

set

IPsec 200 200 20000.

??

?? ???? show security ipsec security-associations ??? ????.

```
user@host> show security ipsec security-associations
```

Total active tunnels: 3

| ID         | Algorithm | SPI              | Life:sec/kb | Mon   | lsys | Port     | Gateway          |
|------------|-----------|------------------|-------------|-------|------|----------|------------------|
| <268173313 | ESP:3des/ | sha-256 3d75aeff | 2984/       | unlim | -    | root 500 | 2001:db8:2000::2 |
| >268173313 | ESP:3des/ | sha-256 a468fece | 2984/       | unlim | -    | root 500 | 2001:db8:2000::2 |
| <268173316 | ESP:3des/ | sha-256 417f3cea | 3594/       | unlim | -    | root 500 | 2001:db8:2000::2 |
| >268173316 | ESP:3des/ | sha-256 a4344027 | 3594/       | unlim | -    | root 500 | 2001:db8:2000::2 |

?? ???? show security ipsec security-associations detail ??? ????.

```
user@host> show security ipsec security-associations detail
```

ID: 268173313 Virtual-system: root, VPN Name: SRX\_A-to-SRX\_B

Local Gateway: 192.168.10.1, Remote Gateway: 2192.168.20.2

Traffic Selector Name: TS1-ipv6

Local Identity: ipv6(2001:db8:10::-2001:db8:10::ffff:ffff:ffff:ffff)

Remote Identity: ipv6(2001:db8:20::-2001:db8:20::ffff:ffff:ffff:ffff)

Version: IKEv1

DF-bit: clear

Bind-interface: st0.1

Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: c608b29

Tunnel Down Reason: SA not initiated

Direction: inbound, SPI: 3d75aeff, AUX-SPI: 0  
 , VPN Monitoring: -

Hard lifetime: Expires in 2976 seconds

Lifsize Remaining: Unlimited

Soft lifetime: Expires in 2354 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: a468fece, AUX-SPI: 0  
 , VPN Monitoring: -

Hard lifetime: Expires in 2976 seconds

Lifsize Remaining: Unlimited

Soft lifetime: Expires in 2354 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc  
 Anti-replay service: counter-based enabled, Replay window size: 64

ID: 268173316 Virtual-system: root, VPN Name: SRX\_A-to-SRX\_B

Local Gateway: 192.168.10.1, Remote Gateway: 192.168.20.2

Traffic Selector Name: TS2-ipv4

Local Identity: ipv4(192.168.10.0-192.168.10.255)

Remote Identity: ipv4(192.168.20.0-192.168.20.255)

Version: IKEv1

DF-bit: clear

Bind-interface: st0.1

Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: c608b29

Tunnel Down Reason: SA not initiated

Direction: inbound, SPI: 417f3cea, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 3586 seconds

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 2948 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: a4344027, AUX-SPI: 0

, VPN Monitoring: -

Hard lifetime: Expires in 3586 seconds

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 2948 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha-256-128, Encryption: aes-256-cbc

Anti-replay service: counter-based enabled, Replay window size: 64

??

show security ipsec security-associations ??? ?? IKE 2?? SA? ??????. SA? ????? ?? ?? ??, 2?? ??? ??? ??  
 ?????. ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ??????. 2?? ?? ?? ??? ?? ??????? ????? ?  
 ??.

???

??

[illegible]

??

```
[[ ]] show security ipsec traffic-selector st0.1 [[ ]]
```

```
user@host> show security ipsec traffic-selector st0.1
```

| Source IP                                      | Destination |           |                  |
|------------------------------------------------|-------------|-----------|------------------|
| IP                                             | Interface   | Tunnel-id | IKE-ID           |
| 2001:db8:10::-2001:db8:10::ffff:ffff:ffff:ffff |             |           |                  |
| 2001:db8:20::-2001:db8:20::ffff:ffff:ffff:ffff | st0.1       | 268173313 | 2001:db8:2000::1 |
| 192.168.10.0-192.168.10.255                    |             |           |                  |
| 192.168.0.0-192.168.255.255                    | st0.1       | 268173316 |                  |
| 2001:db8:2000::1                               |             |           |                  |
| 192.168.10.0-192.168.10.255                    |             |           |                  |
| 192.168.20.0-192.168.20.255                    | st0.1       | 268173317 |                  |
| 2001:db8:2000::1                               |             |           |                  |

?? ??

??

?? ?? ??

??

```
?? ???? show route ??? ?????.
```

```
user@host> show route
```

```
inet.0: 24 destinations, 24 routes (24 active, 0 holddown, 0 hidden)
```

+ = Active Route, - = Last Active, \* = Both

```
192.168.0.0/16      *[ARI-TS/5] 00:00:32
> via st0.1
```

```
2001:db8:20::0/64      *[ARI-TS/5] 00:00:34
> via st0.1
```

??

show route `???` `???` `??????` `??` `???` `??????`, `?` `???` `?????` `???` `??` IP `?????` `???` `???` stO `???????` `??` `???????` `???`.

SEE ALSO

| [VPN ?? ?? ??](#) | 549

?? ?? ?

?? `????` `??` `??` `?????` `?????` `??` `??????`. [Feature Explorer](#) `?` `?????` `???????` `???` `???????` `???????`.

| release heading in release-history | desc heading in release-history                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21.1R1                             | Junos OS <code>???</code> 21.1R1 <code>??</code> <code>??</code> <code>??</code> IP <code>???</code> , <code>??</code> IP <code>???</code> , <code>??</code> <code>??</code> <code>??</code> , <code>??</code> <code>??</code> <code>??</code> <code>?</code> <code>????</code> <code>????</code> <code>??</code> <code>?????</code> <code>????</code> <code>??</code> <code>??</code> .                                                                                                                                                  |
| 15.1X49-D140                       | Junos OS <code>???</code> 15.1X49-D140 <code>??</code> <code>??</code> SRX <code>???</code> <code>???</code> <code>?</code> vSRX <code>??</code> <code>???</code> <code>???????????</code> 0::0(IPv6) <code>??</code> <code>???</code> traffic-selector <code>?</code> <code>????</code> <code>??</code> <code>??</code> <code>??</code> <code>?</code> <code>??</code> <code>???????</code> <code>?????</code> <code>???</code> <code>??</code> <b>"error: configuration check-out failed"</b> <code>?????</code> <code>???????</code> . |
| 15.1X49-D100                       | Junos OS <code>???</code> 15.1X49-D100 <code>??</code> IKEv2 site-to-site VPN <code>??</code> <code>???</code> <code>?????</code> <code>????</code> <code>?</code> <code>?????</code> .                                                                                                                                                                                                                                                                                                                                                   |
| 12.1X46-D10                        | Junos OS <code>???</code> 12.1X46-D10 <code>?</code> Junos OS <code>???</code> 17.3R1 <code>??</code> IKEv1 site-to-site VPN <code>??</code> <code>???</code> <code>?????</code> <code>????</code> <code>?</code> <code>???</code> .                                                                                                                                                                                                                                                                                                      |

?? ??

| [?? ?? IPsec VPN](#) | 452



CHAPTER LABEL COVER PAGE

## ?? ? ? VPN

---

**in this chapter**

- CoS ?? IPsec VPN | 606
-

## CoS IPsec VPN

## summary

CoS [?] IPsec VPN? Junos OS [?] [?] [?] [?] [?]  
[?] [?] [?] [?] [?] [?] [?] [?].

in this section

- ?? IPsec SA? ???? CoS ?? IPsec VPN ?  
? | 606
- ??? ??? ? CoS ?? IPsec VPN ?? | 609
- ?: CoS ?? IPsec VPN ?? | 611
- st0 ?????? ?? CoS ?? ?? | 640
- ???? CoS ?? IPsec VPN ?? | 642

VPN? ?? ???? ???? ? ?? Junos CoS(Class of Service) ??? ??????. ?????? ?? ??? ?? ?? ??? ????? ?????, ? ?? ?? ????? ???? ?????. ? ?? ?? ?? ??? ??? ?????, ??? ??? ? ?????. IKE?? FC(???) ???)?? IPsec ??? ??? ? ? FC? DSCP(Differentiated Services Code Point) ? ??? ?????.

[illegible]

???? ??? ??? "???? CoS ?? IPsec VPN ??" ??? 642 ???? ?????.

**?? IPsec SA? ???? CoS ?? IPsec VPN ??**

in this section

- **?? | 607**
- **?? | 607**
- **FC? IPsec SA? ?? | 607**
- **IPsec SA ?? | 607**
- **? ???? | 608**
- **VPN?? FC ?? ?? ?? | 608**
- **DPD(Dead Peer Detection) | 608**
- **??? | 608**



??

??

- IPsec SA? ?? FC? ??? ?? VPN ??????? ??????. ?? ? ?? ?????? ?? ?? ??? ??? FC? ?? ? ????? . ? ?? ???????
- IPsec SA ??? ??? ??? FC? ??????. ??? ?? ? ?? ??????? ?? ?? FC? IPsec SA ?? ??? ?? ? ??????. ??? FC ??
- ????? ??????? ? IPsec SA ??? ??????, ?? ?????? ? ?? ??????? ??? FC ??? ? ?? IPsec SA? ??? ? ?????, ? ?? ??





```

    }
}

```

? ?? ???? VPN vpn1? 2?? ???? ts1 ? ts2? 3?? FC? ?????. ? ???? 4?? IPsec SA? ??? ts1? ??  
 ???? 4?? IPsec SA? ??? ts2? ?? ?????. ? ???? ?? ?? IPsec SA? ?? ?? IPsec SA? FC? ??? IPsec  
 SA? ?? ?? IPsec SA? ? ? ????.

```

ipsec {
    vpn vpn1 {
        ts1 {
            local-ip 192.168.3.0/24;
            remote-ip 192.168.4.0/24;
        }
        ts2 {
            local-ip 192.168.6.0/24;
            remote-ip 192.168.7.0/24;
        }
    }

    multi-sa {
        forwarding-class web-data;
        forwarding-class voip-data;
        forwarding-class control-data;
    }
}

```

? ?? ???? ???? ts1 ? ts2? ?? ?? FC ?????. ??? ???? ?? ?? VPN? ?? ???? ???? ? ???? VPN  
 vpn1? ??? ts1? ?? 4?? IPsec SA? ?????. ??? ?? IPsec SA?? 3?? FC? ???? IPsec SA???

```

ipsec {
    vpn vpn1 {
        bind-interface st0.0;
        ts1 {
            local-ip 192.168.3.0/24;
            remote-ip 192.168.4.0/24;
        }
        multi-sa {
            forwarding-class web-data;
            forwarding-class voip-data;
            forwarding-class control-data;
        }
    }
}

```

```
vpn vpn2 {
  bind-interface st0.0;
  ts2 {
    local-ip 192.168.6.0/24;
    remote-ip 192.168.7.0/24;
  }
  multi-sa {
    forwarding-class web-data;
    forwarding-class voip-data;
  }
}
```

SEE ALSO

[?? IPsec SA? ???? CoS ?? IPsec VPN ?? | 606](#)

---

[?: CoS ?? IPsec VPN ?? | 611](#)

**?: CoS ?? IPsec VPN ??**

in this section

- [?? ?? | 611](#)
- [?? | 612](#)
- [?? | 616](#)
- [?? | 636](#)

? ???? ? ???? ???? ? ???? ? IPsec SA? ???? ? ???? ? IPsec SA? ?? CoS ?? IPsec VPN? ???? ? ???? ? ???? ? CoS? ???? ???? ????.

? ??? ??? ???? ???? , ???? Junos OS ???? ? Junos OS ???? ???? , VPN ?? ???? ? ???? ???? Junos OS ???? ? ????.

**?? ??**

? ?? ?? ???? ????.

- SRX 220 2200 22 Junos OS 2200

2200 22:

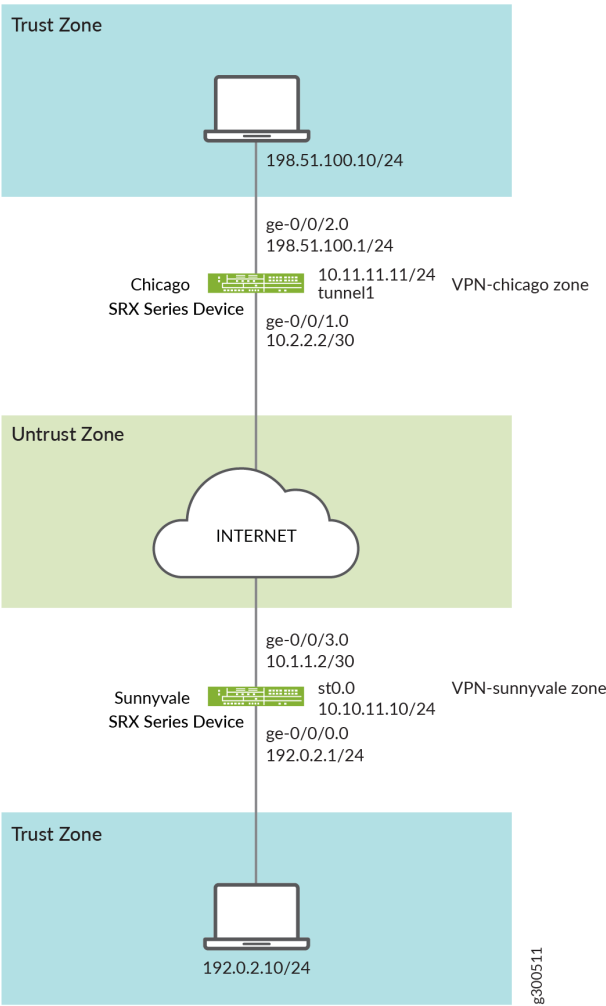
- SRX 220 2200 2200 CoS(Class of Service) 220 220(FC) IPsec SA(Security Association) 2 2200 220 2200  
2. 22 IPsec SA 2 2200 CoS 22 IPsec VPN 220 2200000.
- 220 220 2 CoS 22 IPsec VPN 2 22 2200000. 220 220 2 CoS 22 IPsec VPN 220000 2200000.

22

2 2200 22 2200 220000 220 2200 2200 220000 22 22 22 2200 220 220 22 2200 2200 220 22 IPsec 22 22 VPN 2  
220000. 220 2200 2200 VPN 2 2200 220000 22 2200 220000.

22 41 220 613 2(2) IPsec 22 22 VPN 220000 22 220000. 2 220000 SRX 220 220 122 220000, SRX 220 220 1  
22 2200 220000.

?? 41: IPsec ?? ?? VPN ?????



?????, IPv4 ?? ?? ? ?? ???? ?????. ?? ?? IKE(Internet Key Exchange), IPsec, ?? ?? ? CoS ?? ???? ? ?????. ??? ? 95 ??? 615??? 92 ??? 613.

? 92: ?????, ?? ?? ? ?? ?? ??

| ??    | ??         | ?? ?? ??     |
|-------|------------|--------------|
| ????? | ge-0/0/0.0 | 192.0.2.1/24 |
|       | ge-0/0/3.0 | 10.1.1.2/30  |

**92: 10.10.11.10/24 (Continued)**

| ??             | ??                        | ?? ?? ??                                                                                                                   |
|----------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------|
|                | st0.0 (?? 10.10.11.10/24) | 10.10.11.10/24                                                                                                             |
| ?? 10.10.11.10 | 0.0.0.0/0(?? 10.10.11.10) | ?? 10.10.11.10 st0.0???                                                                                                    |
| ?? ?           | ??                        | <ul style="list-style-type: none"> <li>?? 10.10.11.10 10.10.11.10.</li> <li>ge-0/0/0.0 10.10.11.10 10.10.11.10.</li> </ul> |
|                | untrust                   | <ul style="list-style-type: none"> <li>?? 10.10.11.10 10.10.11.10.</li> <li>ge-0/0/3.0 10.10.11.10 10.10.11.10.</li> </ul> |
|                | VPN                       | st0.0 10.10.11.10 10.10.11.10.                                                                                             |

**93: IKE(Internet Key Exchange) ?? ?? ??**

| ?? | ??     | ?? ?? ??                                                                                                                                                                  |
|----|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?? | IKE-?? | <ul style="list-style-type: none"> <li>?? ??: RSA ??</li> <li>Diffie-Hellman ??: group14</li> <li>?? 10.10.11.10: sha-256</li> <li>?? 10.10.11.10: AES-256-CBC</li> </ul> |
| ?? | IKE-?? | <ul style="list-style-type: none"> <li>??: main</li> <li>?? 10.10.11.10: IKE-??</li> <li>IKE(Internet Key Exchange) ?? 10.10.11.10: RSA ??</li> </ul>                     |



### 93: IKE(Internet Key Exchange) (Continued)

| ??    | ??           | ?? ?? ??                                                                                                                                      |
|-------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ????? | gw-sunnyvale | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ?? : IKE-??</li> <li>?? ??: ge-0/0/3.0</li> <li>???: 10.2.2.2</li> </ul> |

### 94: IPsec

| ??  | ??         | ?? ?? ??                                                                                                                 |
|-----|------------|--------------------------------------------------------------------------------------------------------------------------|
| ??  | ipsec_prop | <ul style="list-style-type: none"> <li>?: esp</li> <li>?: hmac-sha-256</li> <li>?: AES-256-CBC</li> </ul>                |
| ??  | ipsec_pol  | <ul style="list-style-type: none"> <li>?: ipsec_prop</li> </ul>                                                          |
| VPN | ipsec_vpn1 | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ?? : GW-??</li> <li>IPsec ?? : ipsec_pol</li> </ul> |

### 95: ? ? ? ? ?

| ??                          | ??  | ?? ?? ??                                                                                                                                     |
|-----------------------------|-----|----------------------------------------------------------------------------------------------------------------------------------------------|
| ?? ? ? ? ? ? VPN ? ? ? ? ?. | VPN | <ul style="list-style-type: none"> <li>?:</li> <li>?? ? ? ? ? ?</li> <li>?? ? ? ? ? ?</li> <li>?? ? ? ? ? ?</li> <li>?: ?(Permit)</li> </ul> |

95: 22 22 22 22 22 (Continued)

| ??                                  | ??  | ?? ?? ??                                                                                                                                                                     |
|-------------------------------------|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?? ??? VPN ??? ???? ???? ???? ????. | VPN | <ul style="list-style-type: none"><li>?? ??:<ul style="list-style-type: none"><li>?? ?? ???</li><li>??? ?? ?????</li><li>?? ??????</li></ul></li><li>?: ??(Permit)</li></ul> |

??

in this section

- ?? ????? ? ?? ?? ?? ?? | 616
- CoS ?? | 621
- IKE(Internet Key Exchange) ?? | 627
- IPsec ?? | 630
- ?? ?? ?? | 634

?? ????? ? ?? ?? ?? ??

CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CL|? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```
set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.1/24
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/30
set interfaces st0 unit 0 family inet address 10.10.11.10/24
set routing-options static route 0.0.0.0/0 next-hop st0.0
set security zones security-zone untrust interfaces ge-0/0/3.0
set security zones security-zone untrust host-inbound-traffic system-services ike
```

```

set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone vpn-chicago interfaces st0.0
set security zones security-zone vpn-chicago host-inbound-traffic protocols all
set security zones security-zone vpn-chicago host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone untrust host-inbound-traffic protocols all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

?????, ?? ?? ? ?? ?? ?? ??:

1. ??? ????? ???? ????.

```

[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 192.0.2.1/24
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/30
user@host# set interfaces st0 unit 0 family inet address 10.10.11.10/24

```

2. ?? ?? ???? ????.

```

[edit]
user@host# set routing-options static route 0.0.0.0/0 next-hop st0.0

```

3. ?????(untrust) ?? ??? ????.

```

[edit ]
user@host# edit security zones security-zone untrust

```

4. ?????(untrust) ?? ??? ???? ???? ???? ????.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic protocols all

```

5. `set interfaces ge-0/0/3.0`.

```
[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/3.0
```

6. `set host-inbound-traffic system-services ike`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services ike
```

7. `edit security zones security-zone trust`.

```
[edit]
user@host# edit security zones security-zone trust
```

8. `set interfaces ge-0/0/0.0`.

```
[edit security zones security-zone trust]
user@host# set interfaces ge-0/0/0.0
```

9. `set host-inbound-traffic system-services all`  
`set host-inbound-traffic protocols all`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
```

10. `edit security zones security-zone vpn`.

```
[edit]
user@host# edit security zones security-zone vpn
```

11. `set interfaces st0.0`.

```
[edit security zones security-zone vpn-chicago]
user@host# set interfaces st0.0
```

```
user@host# set host-inbound-traffic protocols all
user@host# set host-inbound-traffic system-services all
```

??

?? ???? show interfaces, show routing-options ? show security zones ??? ???? ???? ??????. ??? ???? ???? ???? ??  
?, ? ?? ?? ???? ???? ?????.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 192.0.2.1/24;
        }
    }
}
ge-0/0/3 {
    unit 0 {
        family inet {
            address 10.1.1.2/30;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.10.11.10/24;
        }
    }
}
```

```
[edit]
user@host# show routing-options
static {
```

```

    route 0.0.0.0/0 next-hop st0.0;
}

```

```

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            ike;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn-chicago {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {

```

```
        st0.0;
    }
}
```

```
???? ???? ???? ?? ???? commit?(?) ??????.
```

CoS

CLI    

? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? CLI ? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? ? .

```

set class-of-service classifiers dscp ba-classifier import default
set class-of-service classifiers dscp ba-classifier forwarding-class best-effort loss-priority
high code-points 000000
set class-of-service classifiers dscp ba-classifier forwarding-class ef-class loss-priority high
code-points 000001
set class-of-service classifiers dscp ba-classifier forwarding-class af-class loss-priority high
code-points 001010
set class-of-service classifiers dscp ba-classifier forwarding-class network-control loss-
priority high code-points 000011
set class-of-service classifiers dscp ba-classifier forwarding-class res-class loss-priority
high code-points 000100
set class-of-service classifiers dscp ba-classifier forwarding-class web-data loss-priority high
code-points 000101
set class-of-service classifiers dscp ba-classifier forwarding-class control-data loss-priority
high code-points 000111
set class-of-service classifiers dscp ba-classifier forwarding-class voip-data loss-priority
high code-points 000110
set class-of-service forwarding-classes queue 7 voip-data
set class-of-service forwarding-classes queue 6 control-data
set class-of-service forwarding-classes queue 5 web-data
set class-of-service forwarding-classes queue 4 res-class
set class-of-service forwarding-classes queue 2 af-class
set class-of-service forwarding-classes queue 1 ef-class
set class-of-service forwarding-classes queue 0 best-effort
set class-of-service forwarding-classes queue 3 network-control
set class-of-service interfaces ge-0/0/3 unit 0 classifiers dscp ba-classifier
set class-of-service interfaces ge-0/0/3 unit 0 scheduler-map sched_1
set class-of-service scheduler-maps sched_1 forwarding-class voip-data scheduler Q7
set class-of-service scheduler-maps sched_1 forwarding-class control-data scheduler Q6

```

```

set class-of-service scheduler-maps sched_1 forwarding-class web-data scheduler Q5
set class-of-service scheduler-maps sched_1 forwarding-class res-class scheduler Q4
set class-of-service scheduler-maps sched_1 forwarding-class af-class scheduler Q2
set class-of-service scheduler-maps sched_1 forwarding-class ef-class scheduler Q1
set class-of-service scheduler-maps sched_1 forwarding-class best-effort scheduler Q0
set class-of-service scheduler-maps sched_1 forwarding-class network-control scheduler Q3
set class-of-service schedulers Q7 transmit-rate percent 5
set class-of-service schedulers Q7 priority strict-high
set class-of-service schedulers Q6 transmit-rate percent 25
set class-of-service schedulers Q6 priority high
set class-of-service schedulers Q5 transmit-rate remainder
set class-of-service schedulers Q5 priority high
set class-of-service schedulers Q4 transmit-rate percent 25
set class-of-service schedulers Q4 priority medium-high
set class-of-service schedulers Q3 transmit-rate remainder
set class-of-service schedulers Q3 priority medium-high
set class-of-service schedulers Q2 transmit-rate percent 10
set class-of-service schedulers Q2 priority medium-low
set class-of-service schedulers Q1 transmit-rate percent 10
set class-of-service schedulers Q1 priority medium-low
set class-of-service schedulers Q0 transmit-rate remainder
set class-of-service schedulers Q0 priority low

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ???? ???? ?? ???? CLI ???? ???? ?????.

CoS ?? ??:

#### 1. DiffServ CoS? ?? ?? ?? ???? ????.

```

[edit class-of-service]
user@host# edit classifiers dscp ba-classifier
user@host# set import default

```

#### 2. best-effort ??? ???? ????.

```

[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class best-effort loss-priority high code-points 000000

```



3. `?? ???? ? DSCP ?? ?????.`

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class ef-class loss-priority high code-points 000001
user@host# set forwarding-class af-class loss-priority high code-points 001010
user@host# set forwarding-class network-control loss-priority high code-points 000011
user@host# set forwarding-class res-class loss-priority high code-points 000100
user@host# set forwarding-class web-data loss-priority high code-points 000101
user@host# set forwarding-class control-data loss-priority high code-points 000111
user@host# set forwarding-class voip-data loss-priority high code-points 000110
```

4. `8?? ???? ?? 8?? ??? ???(?? ?)? ?????.`

```
[edit class-of-service forwarding-classes]
user@host# set queue 7 voip-data
user@host# set queue 6 control-data
user@host# set queue 5 web-data
user@host# set queue 4 res-class
user@host# set queue 2 af-class
user@host# set queue 1 ef-class
user@host# set queue 0 best-effort
user@host# set queue 3 network-control
```

5. `?(ge) ???????? ????? ?????.`

```
[edit class-of-service]
user@host# set interfaces ge-0/0/3 unit 0 classifiers dscp ba-classifier
```

6. `???? ? ge ?????? ?????.`

```
[edit class-of-service]
user@host# set interfaces ge-0/0/3 unit 0 scheduler-map sched_1
```

7. `????? ??? ???? ?????? ?????? ???? ? ????.`

```
[edit class-of-service]
user@host# set scheduler-maps sched_1 forwarding-class voip-data scheduler Q7
user@host# set scheduler-maps sched_1 forwarding-class control-data scheduler Q6
```

```

user@host# set scheduler-maps sched_1 forwarding-class web-data scheduler Q5
user@host# set scheduler-maps sched_1 forwarding-class res-class scheduler Q4
user@host# set scheduler-maps sched_1 forwarding-class af-class scheduler Q2
user@host# set scheduler-maps sched_1 forwarding-class ef-class scheduler Q1
user@host# set scheduler-maps sched_1 forwarding-class best-effort scheduler Q0
user@host# set scheduler-maps sched_1 forwarding-class network-control scheduler Q3

```

## 8. `show class-of-service`

```

[edit set class-of-service]
user@host# set schedulers Q7 transmit-rate percent 5
user@host# set schedulers Q7 priority strict-high
user@host# set schedulers Q6 transmit-rate percent 25
user@host# set schedulers Q6 priority high
user@host# set schedulers Q5 transmit-rate remainder
user@host# set schedulers Q5 priority high
user@host# set schedulers Q4 transmit-rate percent 25
user@host# set schedulers Q4 priority medium-high
user@host# set schedulers Q3 transmit-rate remainder
user@host# set schedulers Q3 priority medium-high
user@host# set schedulers Q2 transmit-rate percent 10
user@host# set schedulers Q2 priority medium-low
user@host# set schedulers Q1 transmit-rate percent 10
user@host# set schedulers Q1 priority medium-low
user@host# set schedulers Q0 transmit-rate remainder
user@host# set schedulers Q0 priority low

```

`??`

`?? show class-of-service` `???` `????` `???` `??????`. `???` `???` `???` `????` `???`, `?` `??` `??` `???` `????` `??????`.

```

[edit]
user@host# show class-of-service
classifiers {
    dscp ba-classifier {
        import default;
        forwarding-class best-effort {
            loss-priority high code-points 000000;
        }
        forwarding-class ef-class {

```

```

        loss-priority high code-points 000001;
    }
    forwarding-class af-class {
        loss-priority high code-points 001010;
    }
    forwarding-class network-control {
        loss-priority high code-points 000011;
    }
    forwarding-class res-class {
        loss-priority high code-points 000100;
    }
    forwarding-class web-data {
        loss-priority high code-points 000101;
    }
    forwarding-class control-data {
        loss-priority high code-points 000111;
    }
    forwarding-class voip-data {
        loss-priority high code-points 000110;
    }
}

forwarding-classes {
    queue 7 voip-data;
    queue 6 control-data;
    queue 5 web-data;
    queue 4 res-class;
    queue 2 af-class;
    queue 1 ef-class;
    queue 0 best-effort;
    queue 3 network-control;
}

interfaces {
    ge-0/0/3 {
        unit 0 {
            classifiers {
                dscp ba-classifier;
            }
        }
    }
}

ge-0/0/3 {
    unit 0 {
        scheduler-map sched_1;
    }
}

```

```

    }
  }
}
scheduler-maps {
  sched_1 {
    forwarding-class voip-data scheduler Q7;
    forwarding-class control-data scheduler Q6;
    forwarding-class web-data scheduler Q5;
    forwarding-class res-class scheduler Q4;
    forwarding-class af-class scheduler Q2;
    forwarding-class ef-class scheduler Q1;
    forwarding-class best-effort scheduler Q0;
    forwarding-class network-control scheduler Q3;
  }
}
schedulers {
  Q7 {
    transmit-rate percent 5;
    priority strict-high;
  }
  Q6 {
    transmit-rate percent 25;
    priority high;
  }
  Q5 {
    transmit-rate {
      remainder;
    }
    priority high;
  }
  Q4 {
    transmit-rate percent 25;
    priority medium-high;
  }
  Q3 {
    transmit-rate {
      remainder;
    }
    priority medium-high;
  }
  Q2 {
    transmit-rate percent 10;
    priority medium-low;
  }
}

```

```

    }
    Q1 {
        transmit-rate percent 10;
        priority medium-low;
    }
    Q0 {
        transmit-rate {
            remainder;
        }
        priority low;
    }
}

```

?? ?? ?? ?? commit?(?) ????.

## IKE(Internet Key Exchange) ??

### CLI ?? ??

? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ??? ?? ?? ?? ? ?? ?? ?? ?? [edit] ?  
 ? ?? ?? ?? CLI? ?? ?? ?? ??, ?? ?? ?? commit?(?) ????.

```

set security ike proposal ike-proposal authentication-method pre-shared-keys
set security ike proposal ike-proposal dh-group group14
set security ike proposal ike-proposal authentication-algorithm sha-256
set security ike proposal ike-proposal encryption-algorithm aes-256-cbc
set security ike policy ike-policy mode main
set security ike policy ike-policy proposals ike-proposal
set security ike policy ike-policy pre-shared-key ascii-text $ABC123
set security ike gateway gw-sunnyvale external-interface ge-0/0/3.0
set security ike gateway gw-sunnyvale ike policy ike-policy
set security ike gateway gw-sunnyvale address 10.2.2.2
set security ike gateway gw-sunnyvale version v2-only

```

??? ??

?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? CLI ??? ??? ?/? ??? CLI ??? ?? ???.

IKE(Internet Key Exchange) ??:

1. IKE(Internet Key Exchange) ??? ?????.

```
[edit security ike]
user@host# set proposal ike-proposal
```

2. IKE(Internet Key Exchange) ?? ?? ??? ?????.

```
[edit security ike proposal ike-proposal]
user@host# set authentication-method pre-shared-keys
```

3. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ?????.

```
[edit security ike proposal ike-proposal]
user@host# set dh-group group14
```

4. IKE(Internet Key Exchange) ?? ?? ?????? ?????.

```
[edit security ike proposal ike-proposal]
user@host# set authentication-algorithm sha-256
```

5. IKE(Internet Key Exchange) ?? ??? ?????? ?????.

```
[edit security ike proposal ike-proposal]
user@host# set encryption-algorithm aes-256-cbc
```

6. IKE(Internet Key Exchange) ??? ?????.

```
[edit security ike]
user@host# set policy ike-policy
```

7. IKE(Internet Key Exchange) ?? ??? ?????.

```
[edit security ike policy ike-policy]
user@host# set mode main
```



```

proposal ike-proposal {
    authentication-method pre-shared-keys;
    dh-group group14;
    authentication-algorithm sha-256;
    encryption-algorithm aes-256-cbc;
}
policy ike-policy {
    mode main;
    proposals ike-proposal;
    pre-shared-key ascii-text "$ABC123";
}
gateway gw-sunnyvale {
    ike policy ike-policy;
    address 10.2.2.2;
    external-interface ge-0/0/3.0;
    version v2-only;
}

```

```

?? ?? ?? ?? commit?(?) ?????.

```

## IPsec ??

### CLI ?? ??

```

? ?? ??? ?????, ?? ??? ??? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?
? ????? ??? CLI? ??? ???? ???? ???? ???? commit?(?) ?????.

```

```

set security ipsec traceoptions flag all
set security ipsec proposal ipsec_prop protocol esp
set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha-256
set security ipsec proposal ipsec_prop encryption-algorithm aes256-cbc
set security ipsec proposal ipsec_prop lifetime-seconds 3600
set security ipsec policy ipsec_pol proposals ipsec_prop
set security ipsec vpn ipsec_vpn1 bind-interface st0.0
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class ef-class
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class af-class
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class res-class
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class web-data
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class control-data
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class voip-data
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class network-control
set security ipsec vpn ipsec_vpn1 multi-sa forwarding-class best-effort

```



```

set security ipsec vpn ipsec_vpn1 ike gateway gw_sunnyvale
set security ipsec vpn ipsec_vpn1 ike ipsec-policy ipsec_pol
set security ipsec vpn ipsec_vpn1 establish-tunnels immediately
set security ipsec vpn ipsec_vpn1 traffic-selector ipsec_vpn1_TS1 local-ip 203.0.113.2/25
set security ipsec vpn ipsec_vpn1 traffic-selector ipsec_vpn1_TS1 remote-ip 192.0.2.30/24

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

IPsec ??:

1. IPsec ?? ???? ?????.

```

[edit]
user@host# set security ipsec traceoptions flag all

```

2. IPsec ??? ????.

```

[edit]
user@host# set security ipsec proposal ipsec_prop

```

3. IPsec ?? ???? ????.

```

[edit security ipsec proposal ipsec_prop]
user@host# set protocol esp

```

4. IPsec ?? ?? ???? ????.

```

[edit security ipsec proposal ipsec_prop]
user@host# set authentication-algorithm hmac-sha-256

```

5. IPsec ?? ??? ???? ????.

```

[edit security ipsec proposal ipsec_prop]
user@host# set encryption-algorithm aes256-cbc

```

6. IPsec SA(Security Association) `? ?(?)? ?????.`

```
[set security ipsec proposal ipsec_prop]
user@host# set lifetime-seconds 3600
```

7. IPsec `??? ?????.`

```
[edit security ipsec]
user@host# set policy ipsec_pol
```

8. IPsec `? ???? ?????.`

```
[edit security ipsec policy ipsec_pol]
user@host# set proposals ipsec_prop
```

9. `???? ?????.`

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 bind-interface st0.0
```

10. `? ? IPsec SA? ? ???? ???? ????.`

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class ef-class
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class af-class
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class res-class
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class web-data
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class control-data
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class voip-data
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class network-control
user@host# set vpn ipsec_vpn1 multi-sa forwarding-class best-effort
```

11. IKE(Internet Key Exchange) `????? ????.`

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 ike gateway gw_sunnyvale
```

## 12. IPsec `???` `??????`.

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 ike ipsec-policy ipsec_pol
```

## 13. `?` `??` `????` `????` `????` `?` IPsec SA `?????` `??` `????` `??` `??????` `??????`.

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 establish-tunnels immediately
```

## 14. `????` `?????` `??` `??` IP `????` `??????`.

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 traffic-selector ipsec_vpn1_TS1 local-ip 203.0.113.2/25
```

## 15. `????` `?????` `??` `??` IP `????` `??????`.

```
[edit security ipsec]
user@host# set vpn ipsec_vpn1 traffic-selector ipsec_vpn1_TS1 remote-ip 192.0.2.30/24
```

`??`

`??` `?????` show security ipsec `????` `?????` `????` `??????`. `????` `????` `????` `?????` `????`, `?` `??` `??` `????` `?????` `??????`.

```
[edit]
user@host# show security ipsec
traceoptions {
    flag all;
}
proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-sha-256;
    encryption-algorithm aes256-cbc;
}
proposal ipsec_prop {
    lifetime-seconds 3600;
}
policy ipsec_pol {
```

```

    proposals ipsec_prop;
}
vpn ipsec_vpn1 {
    bind-interface st0.0;
    multi-sa {
        forwarding-class ef-class;
        forwarding-class af-class;
        forwarding-class res-class;
        forwarding-class web-data;
        forwarding-class control-data;
        forwarding-class voip-data;
        forwarding-class network-control;
        forwarding-class best-effort;
    }
    ike {
        gateway gw_sunnyvale;
        ipsec-policy ipsec_pol;
    }
    traffic-selector ipsec_vpn1_TS1 {
        local-ip 203.0.113.2/25;
        remote-ip 192.0.2.30/24;
    }
    establish-tunnels immediately;
}

```

?? ?? ?? ?? commit?(?) ?????.

?? ?? ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???? ????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set security policies from-zone trust to-zone vpn policy vpn match source-address sunnyvale
set security policies from-zone trust to-zone vpn policy vpn match destination-address chicago
set security policies from-zone trust to-zone vpn policy vpn match application any
set security policies from-zone trust to-zone vpn policy vpn then permit
set security policies from-zone vpn to-zone trust policy vpn match source-address chicago
set security policies from-zone vpn to-zone trust policy vpn match destination-address sunnyvale

```

```
set security policies from-zone vpn to-zone trust policy vpn match application any
set security policies from-zone vpn to-zone trust policy vpn then permit
```

?? ?? ??? ????? ?? ?? ?? ?? ??? ?????.

??? ??

?? ?? ?? ????? ??? ??? ??? ?????, ?? ????? ??? ?? ??? CLI ??? ??? ?? ????? CLI ??? ?? ?????.

?? ?? ??:

1. ????? ????? VPN ????? ????? ?? ?? ?????.

```
[edit security policies from-zone trust to-zone vpn]
user@host# set policy vpn match source-address sunnyvale
user@host# set policy vpn match destination-address chicago
user@host# set policy vpn match application any
user@host# set policy vpn then permit
```

2. VPN ????? ????? ????? ????? ????? ?? ?? ?????.

```
[edit security policies from-zone vpn to-zone trust]
user@host# set policy vpn match source-address chicago
user@host# set policy vpn match destination-address sunnyvale
user@host# set policy vpn match application any
user@host# set policy vpn then permit
```

??

?? ????? show security policies ??? ????? ??? ?????, ??? ??? ??? ?????, ? ?? ?? ??? ?????.

```
[edit]
user@host# show security policies
from-zone trust to-zone vpn {
  policy vpn {
    match {
      source-address sunnyvale;
      destination-address chicago;
      application any;
    }
  }
}
```

```
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn {
        match {
            source-address chicago;
            destination-address sunnyvale;
            application any;
        }
        then {
            permit;
        }
    }
}
```

```
set security ipsec vpn tunnel commit
```

??

in this section

● IPsec ?? ?? ?? | 636

```
set security ipsec vpn tunnel
```

IPsec ?? ?? ??

??

IPsec ??? ?????.

??

```
show security ipsec security-associations detail. show security ipsec
statistics index 131073 detail.
```



```

Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1563 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: default
Direction: outbound, SPI: 5f3a3239, AUX-SPI: 0
                , VPN Monitoring: -
Hard lifetime: Expires in 1930 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1563 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: default
Direction: inbound, SPI: 5d227e19, AUX-SPI: 0
                , VPN Monitoring: -
Hard lifetime: Expires in 1930 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1551 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Multi-sa FC Name: best-effort
Direction: outbound, SPI: 5490da, AUX-SPI: 0
                , VPN Monitoring: -
Hard lifetime: Expires in 1930 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 1551 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha-256, Encryption: aes-256-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
...

```

```
user@host> show security ipsec statistics index 131073
```

#### ESP Statistics:

|                    |     |
|--------------------|-----|
| Encrypted bytes:   | 952 |
| Decrypted bytes:   | 588 |
| Encrypted packets: | 7   |
| Decrypted packets: | 7   |





- ? ?? ? ? ? ??? VPN ??? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? .

## SEE ALSO

?? IPsec SA? ??? CoS ?? IPsec VPN ?? | 606

??? ??? ? CoS ?? IPsec VPN ?? | 609

IPsec ?? | 11

?: CoS ?? IPsec VPN ?? | 611

Junos OS IKE(Internet Key Exchange) | 27

st0         CoS

in this section

- VPN st0 [?] [?] [?] [?] [?] [?] CoS [?] [?] [?] | 641

point-to-point VPN (st0), , , , , CoS(Class of Service) .

```
st0 ?? ?????? ?? ??? ????? IPsec VPN ??? ?????? ?? ?? ?? VPN?? ??? ? ?? ?? ??????????. ?? CoS ??? ??
???? ?? SRX ??? ??? ? vSRX2.0? st0 ???????? ??????.
```

- $???$
- $???$
- $??, ???? ? ???$
- $?? ?? ??$
- Virtual channels

- SRX300, SRX320, SRX340, SRX345 ? SRX550HM ?????? ?? st0 ??? ?????? ?? VPN ??? ??? ? ??  
??. st0 ??? ?????? 8? ????? ???? ???? ???? ? ???? ? ???? ???? ?????.
- ?? ?? ??? SRX300, SRX320, SRX340, SRX345 ? SRX550HM ?????? ?? ????? ??? ? ????
- st0 ?? ??????? CoS ??? ??? ? ???? ?? ?? ??? ??????
  - ?? ?????? ??? ??? ?? ?????? ??? ????? ???
  - ??? ??? ESP/AH ??? ?? IP ?? ????? ?? ?? ??? 3 ?? ??? ??? ????? ?? ??? ??????. ??? ?????? ?? ???  
?? ??? 2 ????? ?? ??? ????? ????
  - ??? ?????? ??? GRE ?? IP-IP ?? ????? ??? ? CoS ??? ????? ??????. ??? ?????? ?? ????? ????? ?? ?  
????? ????? ?? ??? ????? ??? CoS ??? ????? ?????
- SRX550M, SRX5400, SRX5600 ? SRX5800 ?????? ??? ??? ?? ? ??? ?? ?? ?? ????? ??? ??? SPU  
?????, ?? ??? ?????????? ??? ??? ?????.



?? ??

|     ??? ??? ????(?? ?????)

# 7

CHAPTER LABEL COVER PAGE

## NAT-T

---

in this chapter

- NAT-T [???](#) [??](#) [??](#) [?](#) [??](#) [??](#) VPN | 645
-



- IKEv1 ?? IKEv2 ?????? ?????? ?? ??(NAT) ?????? ?? ??????. ?? ?????? ??? ?????? ?? ??(NAT) ?????? ?? ?? ? ??  
??. ?????? ?? ?? ?????? ?? ??(NAT) ?????? ?? ?????? ??? ? ??????.
- IKEv1 ?? IKEv2 ?????? ?????? ?? ??(NAT) ?????? ?? ??????.
- IKEv1 ?? IKEv2 ?????? ?????? ?? ?????? ?? ??(NAT) ?????? ?? ??????.

?? ?????? VPN? ?????? IKE ?? ??? ?????? ?????? ? ? ?? ?????? ??????. ??? ?????? ??? ISP? ?? ?????? ?????? ??????  
???? ?? ?? ?????? ?????? ?? ?????? ?? ??(NAT) ?????? ??? ? ??? ? ??????.

NAT-T? ?? ?? ?????? ?????? ?? ??(NAT) ?????? ?? ?? ?????? ?????? ??? ?? NAT ?????? ?? ?? ?????? ??????.

NAT-T? ?? ?????? ? IKE(Internet Key Exchange) ?????? ??? ??? ? ??? ?????? ???????. ?? IKE(Internet Key  
Exchange) ID? IKE(Internet Key Exchange) ?? ??? 1?? ?? ?????? ?? IKE ID? ?????? ? ???????. ??? ? ??? ??????  
local-identity ? remote-identity ??? ??????.

SEE ALSO

| [IPsec ??](#) | 11

**?: ?????? ?? ??(NAT) ?????? ?? ?? ?????? ?????? ?? ?? VPN ??**

in this section

- [?? ??](#) | 646
- [??](#) | 646
- [??](#) | 652
- [??](#) | 671

? ?????? ??? ?? ?? ?? ?????? ?? ??(NAT) ?????? ?? ?? ?????? ?????? ?? ?? VPN? ?????? ??? ?????? ??????.

?? ??

????? ?? "IPsec ??" [???](#) 11?(?) ??????.

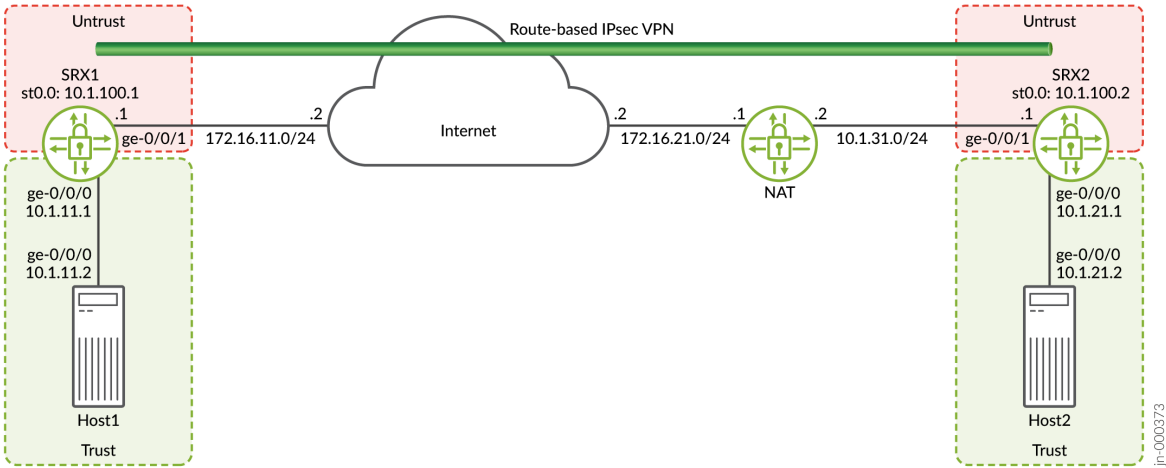
??

? ?????? ?? ?? VPN? ??????. Host1? VPN? ?????? SRX2? ?? ??? ??????.



?? 42 ??? 647?? ???? ?? ??(NAT) ???? ?? ???? ?? ?? ?? VPN? ???? ?? ?? ???? ????.

?? 42: ???? ?? ??(NAT) ???? ?? ???? ?? ?? ?? VPN ?????



? ???? , SRX1? ???? SRX2? ???? ?? ???? , IPsec ? ?? ???? ?????. ?? ?? IKE(Internet Key Exchange) 1 ?? ? IPsec 2?? ?? ???? ????.

SRX1? ?? ???? 172.16.21.1? ???? ???? VPN? ?????.???? ?? ??(NAT) ???? ?? ???? 10.1.31.1? ????.

???? ???? ???? ?? ?? ?? ???? ? 98 ??? 647~? 100 ??? 649?(?) ????.

? 98: SRX1? ?? ???? , ??? ?? ? ?? ?? ??

| ??     | ??              | ?? ?? ??             |
|--------|-----------------|----------------------|
| ?????  | ge-0/0/1        | 172.16.11.1/24       |
|        | ge-0/0/0        | 10.1.11.1/24         |
|        | st0.0(?? ?????) | 10.1.100.1/24        |
| ?? ??? | 10.1.21.0/24    | ?? ?? st0.0???       |
|        | 172.16.21.1/32  | ?? ?? 172.16.11.2??? |

**98: SRX17 17 171717, 1717 17 17 17 17 (Continued)**

| ??    | ??      | ?? ?? ??                                                                                                                                      |
|-------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| ?? ?  | untrust | <ul style="list-style-type: none"> <li>IKE ? ping? ??? ??? .</li> <li>ge-0/0/1.0 ? st0.0 17171717 ? 1717 171717.</li> </ul>                   |
|       | ??      | <ul style="list-style-type: none"> <li>?? 1717 1717 171717.</li> <li>?? 171717 171717.</li> <li>ge-0/0/0.0 17171717 ? 1717 171717.</li> </ul> |
| ?? ?? | SRX2?   | 1717 1717 10.1.11.0/24?? 171717 1717 10.1.21.0/24?? 1717 171717.                                                                              |
|       | -SRX2?? | 17171717 10.1.21.0/24?? 1717 1717 10.1.11.0/24?? 1717 171717.                                                                                 |

**99: SRX17 17 IKE(Internet Key Exchange) 1717 17 17 17**

| ?? | ??       | ?? ?? ??                                                                                                                                                            |
|----|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?? | ike_prop | <ul style="list-style-type: none"> <li>?? 17: pre-shared-keys</li> <li>Diffie-Hellman 17: group2</li> <li>?? 171717: sha1</li> <li>1717 171717: 3des-cbc</li> </ul> |
| ?? | ike_pol  | <ul style="list-style-type: none"> <li>17: main</li> <li>?? 17: ike_prop</li> <li>IKE(Internet Key Exchange) 1717 17 17 17: pre-shared-key ascii-text</li> </ul>    |

## 99: SRX17 IKE(Internet Key Exchange) 177 77 77 77 (Continued)

| ??     | ??  | ?? ?? ??                                                                                                                                                                                                                                                              |
|--------|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 777777 | gw1 | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) 77 77: ike_pol</li> <li>• 77 777777: ge-0/0/1.0</li> <li>• 777777 77: 172.16.21.1</li> <li>• 77 77(7777): branch_natt1@example.net</li> <li>• 77 77(7777): responder_natt1@example.net</li> </ul> |

## 100: SRX17 IPsec 277 77 77 77

| ??  | ??         | ?? ?? ??                                                                                                                                                                             |
|-----|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 77  | ipsec_prop | <ul style="list-style-type: none"> <li>• 777777: esp</li> <li>• 77 777777: hmac-sha1-96</li> <li>• 777 777777: 3des-cbc</li> </ul>                                                   |
| 77  | ipsec_pol  | <ul style="list-style-type: none"> <li>• 77 77: ipsec_prop</li> <li>• PFS(Perfect Forward Secrecy) 7: group2</li> </ul>                                                              |
| VPN | vpn1       | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) 777777 77: gw1</li> <li>• IPsec 77 77: ipsec_pol</li> <li>• 77777777 7777: st0.0</li> <li>• 777 77 77</li> </ul> |

77777 77777 77777 77 77 77 7777 101 7777 650~7 103 7777 6517(7) 77777777.

# 101: SRX22 SRX222, SRX22 SRX22

| ??     | ??              | ?? ?? ??                                                                                                                                             |
|--------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| ?????  | ge-0/0/1        | 10.1.31.1/24                                                                                                                                         |
|        | ge-0/0/0        | 10.1.21.1/24                                                                                                                                         |
|        | st0.0(?? ?????) | 10.1.100.2/24                                                                                                                                        |
| ?? ??? | 172.16.11.1/32  | ?? ?? 10.1.31.2???                                                                                                                                   |
|        | 10.1.11.0/24    | ?? ?? st0.0???                                                                                                                                       |
| ?? ?   | untrust         | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?<br/>ping ??? ??????</li> <li>ge-0/0/1.0 ? st0.0 ????? ? ???<br/>?????</li> </ul> |
|        | ??              | <ul style="list-style-type: none"> <li>?? ??? ??????</li> <li>?? ????? ??????</li> <li>ge-0/0/0.0 ????? ? ??? ??????</li> </ul>                      |
| ?? ??  | SRX1?           | ???? ??? 10.1.21.0/24?? ????? ???<br>10.1.11.0/24?? ????? ??????                                                                                     |
|        | -SRX1??         | ???? ??? 10.1.11.0/24?? ????? ???<br>10.1.21.0/24?? ????? ??????                                                                                     |

## ? 102: SRX2? ?? IKE(Internet Key Exchange) 1?? ?? ?? ??

| ??    | ??       | ?? ?? ??                                                                                                                                                                                                                                                |
|-------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??    | ike_prop | <ul style="list-style-type: none"> <li>?? ??: pre-shared-keys</li> <li>Diffie-Hellman ??: group2</li> <li>?? ?????: sha1</li> <li>??? ?????: 3des-cbc</li> </ul>                                                                                        |
| ??    | ike_pol  | <ul style="list-style-type: none"> <li>?: main</li> <li>?? ??: ike_prop</li> <li>IKE(Internet Key Exchange) 1?? ?? ?? ??: pre-shared-key ascii-text</li> </ul>                                                                                          |
| ????? | gw1      | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) ?? ??: ike_pol</li> <li>?? ?????: ge-0/0/1.0</li> <li>????? ??: 172.16.11.1</li> <li>?? ??(???): responder_natt1@example.net</li> <li>?? ??(???): branch_natt1@example.net</li> </ul> |

## ? 103: SRX2? ?? IPSec 2?? ?? ?? ??

| ?? | ??         | ?? ?? ??                                                                                                                  |
|----|------------|---------------------------------------------------------------------------------------------------------------------------|
| ?? | ipsec_prop | <ul style="list-style-type: none"> <li>?????: esp</li> <li>?? ?????: hmac-sha1-96</li> <li>??? ?????: 3des-cbc</li> </ul> |
| ?? | ipsec_pol  | <ul style="list-style-type: none"> <li>?? ??: ipsec_prop</li> <li>PFS ?: group2</li> </ul>                                |

103: SRX2 IPsec (Continued)

| VPN | vpn1 | <ul style="list-style-type: none"><li>• IKE(Internet Key Exchange) : gw1</li><li>• IPsec : ipsec_pol</li><li>• : st0.0</li><li>•</li></ul> |
|-----|------|--------------------------------------------------------------------------------------------------------------------------------------------|

in this section

- SRX1, , | 652
- SRX1 IKE(Internet Key Exchange) | 658
- SRX1 IPsec | 660
- SRX2, , | 662
- SRX2 IKE(Internet Key Exchange) | 667
- SRX2 IPsec | 669
- (NAT) | 671

SRX1, ,

CLI

, , , , , [edit]   
 CLI, , commit() .

```
set security address-book book1 address Host1 10.1.11.0/24
set security address-book book1 attach zone trust
set security address-book book2 address Host2 10.1.21.0/24
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy to-SRX2 match source-address Host1
```

```

set security policies from-zone trust to-zone untrust policy to-SRX2 match destination-address
Host2
set security policies from-zone trust to-zone untrust policy to-SRX2 match application any
set security policies from-zone trust to-zone untrust policy to-SRX2 then permit
set security policies from-zone untrust to-zone trust policy from-SRX2 match source-address Host2
set security policies from-zone untrust to-zone trust policy from-SRX2 match destination-address
Host1
set security policies from-zone untrust to-zone trust policy from-SRX2 match application any
set security policies from-zone untrust to-zone trust policy from-SRX2 then permit
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet address 10.1.11.1/24
set interfaces ge-0/0/1 unit 0 family inet address 172.16.11.1/24
set interfaces st0 unit 0 family inet address 10.1.100.1/24
set routing-options static route 10.1.21.0/24 next-hop st0.0
set routing-options static route 172.16.21.1/32 next-hop 172.16.11.2

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?????, ?? ??? ? ?? ?? ?? ?? ??:

## 1. VPN? ???? ???? , Host1 ? ?????? ???? ?????? ??????.

[edit]

```

user@SRX1# set interfaces ge-0/0/0 unit 0 family inet address 10.1.11.1/24
user@SRX1# set interfaces ge-0/0/1 unit 0 family inet address 172.16.11.1/24
user@SRX1# set interfaces st0 unit 0 family inet address 10.1.100.1/24

```

## 2. VPN? ??? ???? SRX1? ???? ? ?(NAT) ????? ???? ? ???? ?????.

[edit]

```

user@SRX1# set routing-options static route 10.1.21.0/24 next-hop st0.0
user@SRX1# set routing-options static route 172.16.21.1/32 next-hop 172.16.11.2

```

### 3. `set security zones security-zone untrust`.

```
[edit]
user@SRX1# set security zones security-zone untrust host-inbound-traffic system-services ike
user@SRX1# set security zones security-zone untrust host-inbound-traffic system-services ping
user@SRX1# set security zones security-zone untrust interfaces st0.0
user@SRX1# set security zones security-zone untrust interfaces ge-0/0/1.0
```

### 4. `set security zones security-zone trust`.

```
[edit]
user@SRX1# set security zones security-zone trust host-inbound-traffic system-services all
user@SRX1# set security zones security-zone trust host-inbound-traffic protocols all
user@SRX1# set security zones security-zone trust interfaces ge-0/0/0.0
```

### 5. `set security address-book`.

```
[edit]
user@SRX1# set security address-book book1 address Host1 10.1.11.0/24
user@SRX1# set security address-book book1 attach zone trust
user@SRX1# set security address-book book2 address Host2 10.1.21.0/24
user@SRX1# set security address-book book2 attach zone untrust
```

### 6. `set security policies`.

```
[edit]
user@SRX1# set security policies from-zone trust to-zone untrust policy to-SRX2 match source-
address Host1
user@SRX1# set security policies from-zone trust to-zone untrust policy to-SRX2 match
destination-address Host2
user@SRX1# set security policies from-zone trust to-zone untrust policy to-SRX2 match
application any
user@SRX1# set security policies from-zone trust to-zone untrust policy to-SRX2 then permit
user@SRX1# set security policies from-zone untrust to-zone trust policy from-SRX2 match
source-address Host2
user@SRX1# set security policies from-zone untrust to-zone trust policy from-SRX2 match
destination-address Host1
user@SRX1# set security policies from-zone untrust to-zone trust policy from-SRX2 match
```



```

application any
user@SRX1# set security policies from-zone untrust to-zone trust policy from-SRX2 then permit

```

??

?? show interfaces, show routing-options? show security??? ??. ?? ??. ??. ??. ??.  
 ? ?? ??. ??. ??. ??. ??. ??.

```

[edit]
user@SRX1# show interfaces
ge-0/0/0 {
    unit 0 {
        family inet {
            address 10.1.11.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet {
            address 172.16.11.1/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.1.100.1/24;
        }
    }
}

```

```

[edit]
user@SRX1# show routing-options
static {
    route 10.1.21.0/24 next-hop st0.0;
}

```

```

    route 172.16.21.1/32 next-hop 172.16.11.2;
}

```

```

[edit]
user@SRX1# show security
address-book {
    book1 {
        address Host1 10.1.11.0/24;
        attach {
            zone trust;
        }
    }
    book2 {
        address Host2 10.1.21.0/24;
        attach {
            zone untrust;
        }
    }
}
policies {
    from-zone trust to-zone untrust {
        policy to-SRX2 {
            match {
                source-address Host1;
                destination-address Host2;
                application any;
            }
            then {
                permit;
            }
        }
    }
    from-zone untrust to-zone trust {
        policy from-SRX2 {
            match {
                source-address Host2;
                destination-address Host1;
                application any;
            }
            then {
                permit;
            }
        }
    }
}

```

```

    }
  }
}
zones {
  security-zone untrust {
    host-inbound-traffic {
      system-services {
        ike;
        ping;
      }
    }
    interfaces {
      st0.0;
      ge-0/0/1.0;
    }
  }
  security-zone trust {
    host-inbound-traffic {
      system-services {
        all;
      }
      protocols {
        all;
      }
    }
    interfaces {
      ge-0/0/0.0;
    }
  }
}
}

```

?? ?? ?? ?? ?? commit?(?) ??.

## SRX1? ?? IKE(Internet Key Exchange) ??

### CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ??? ????? ????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security ike proposal ike_prop authentication-method pre-shared-keys
set security ike proposal ike_prop dh-group group2
set security ike proposal ike_prop authentication-algorithm sha1
set security ike proposal ike_prop encryption-algorithm 3des-cbc
set security ike policy ike_pol mode main
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"
set security ike gateway gw1 ike-policy ike_pol
set security ike gateway gw1 address 172.16.21.1
set security ike gateway gw1 local-identity user-at-hostname "srx1@example.com"
set security ike gateway gw1 remote-identity user-at-hostname "srx2@example.com"
set security ike gateway gw1 external-interface ge-0/0/1.0
```

### ??? ??

?? ?? ?? ????? ??? ??? ??? ??????. ?? ????? ??? ?? ??? CLI ??? ????? ?? ????? CLI ??? ??? ??????.

IKE(Internet Key Exchange) ??:

#### 1. IKE(Internet Key Exchange) 1?? ??? ?????.

```
[edit]
user@SRX1# set security ike proposal ike_prop authentication-method pre-shared-keys
user@SRX1# set security ike proposal ike_prop dh-group group2
user@SRX1# set security ike proposal ike_prop authentication-algorithm sha1
user@SRX1# set security ike proposal ike_prop encryption-algorithm 3des-cbc
```

#### 2. IKE(Internet Key Exchange) 1?? ??? ?????.

```
[edit]
user@SRX1# set security ike policy ike_pol mode main
```

```

user@SRX1# set security ike policy ike_pol proposals ike_prop
user@SRX1# set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"

```

### 3. IKE(Internet Key Exchange) 1?? 22222 ?? 222 22222. 22222 222 2222 ?? 22(NAT) 2222 IP222 222.

```

[edit security ike gateway gw1]
user@SRX1# set security ike gateway gw1 ike-policy ike_pol
user@SRX1# set security ike gateway gw1 address 172.16.21.1
user@SRX1# set security ike gateway gw1 local-identity user-at-hostname "srx1@example.com"
user@SRX1# set security ike gateway gw1 remote-identity user-at-hostname "srx2@example.com"
user@SRX1# set security ike gateway gw1 external-interface ge-0/0/1.0

```

??

?? 22222 show security ike 222 22222 222 22222. ?? 222 222 22222 22222 2222 2 ?? 222 22222 222 222222.

```

[edit]
user@SRX1# show security ike
proposal ike_prop {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
policy ike_pol {
    mode main;
    proposals ike_prop;
    pre-shared-key ascii-text "$9$xPn7-VwsgaJUHqp01IcSs2g"; ## SECRET-DATA
}
gateway gw1 {
    ike-policy ike_pol;
    address 172.16.21.1;
    local-identity user-at-hostname "srx1@example.com";
    remote-identity user-at-hostname "srx2@example.com";
    external-interface ge-0/0/1.0;
}

```

2222 222 22222 ?? 22222 commit?(?) 22222.

## SRX1? ?? IPsec ??

### CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security ipsec proposal ipsec_prop protocol esp
set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
set security ipsec policy ipsec_pol perfect-forward-secrecy keys group2
set security ipsec policy ipsec_pol proposals ipsec_prop
set security ipsec vpn vpn1 bind-interface st0.0
set security ipsec vpn vpn1 ike gateway gw1
set security ipsec vpn vpn1 ike ipsec-policy ipsec_pol
set security ipsec vpn vpn1 establish-tunnels immediately
```

??? ??

?? ?? ?? ????? ??? ???? ???? ?????. ?? ????? ??? ? ???? CLI ??? ????? ?? ????? CLI ??? ??? ??????.

IPsec ??:

#### 1. IPsec 2?? ??? ?????.

```
[edit]
user@SRX1# set security ipsec proposal ipsec_prop protocol esp
user@SRX1# set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
user@SRX1# set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
```

#### 2. IPsec 2?? ??? ?????.

```
[edit]
user@SRX1# set security ipsec policy ipsec_pol perfect-forward-secrecy keys group2
user@SRX1# set security ipsec policy ipsec_pol proposals ipsec_prop
```

### 3. IPsec VPN `?? ???? ?????.`

```
[edit]
user@SRX1# set security ipsec vpn vpn1 bind-interface st0.0
user@SRX1# set security ipsec vpn vpn1 ike gateway gw1
user@SRX1# set security ipsec vpn vpn1 ike ipsec-policy ipsec_pol
user@SRX1# set security ipsec vpn vpn1 establish-tunnels immediately
```

`??`

`?? ???? show security ipsec ???? ???? ???? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.`

```
[edit]
user@SRX1# show security ipsec
proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
}
policy ipsec_pol {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec_prop;
}
vpn vpn1 {
    bind-interface st0.0;
    ike {
        gateway gw1;
        ipsec-policy ipsec_pol;
    }
    establish-tunnels immediately;
}
```

`???? ???? ???? ? ? ???? commit?(?) ?????.`

**SRX2** `set security address-book book1 address Host2 10.1.21.0/24`

**CLI** `set`

`set security address-book book1 address Host2 10.1.21.0/24, set security address-book book2 address Host1 10.1.11.0/24 [edit] set security policies from-zone trust to-zone untrust policy to-SRX1 match source-address Host2`

```
set security address-book book1 address Host2 10.1.21.0/24
set security address-book book1 attach zone trust
set security address-book book2 address Host1 10.1.11.0/24
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy to-SRX1 match source-address Host2
set security policies from-zone trust to-zone untrust policy to-SRX1 match destination-address Host1
set security policies from-zone trust to-zone untrust policy to-SRX1 match application any
set security policies from-zone trust to-zone untrust policy to-SRX1 then permit
set security policies from-zone untrust to-zone trust policy from-SRX1 match source-address Host1
set security policies from-zone untrust to-zone trust policy from-SRX1 match destination-address Host2
set security policies from-zone untrust to-zone trust policy from-SRX1 match application any
set security policies from-zone untrust to-zone trust policy from-SRX1 then permit
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet address 10.1.21.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.31.1/24
set interfaces st0 unit 0 family inet address 10.1.100.2/24
set routing-options static route 172.16.11.1/32 next-hop 10.1.31.2
set routing-options static route 10.1.11.0/24 next-hop st0.0
```

**CLI** `set`

`set security address-book book1 address Host2 10.1.21.0/24, set security address-book book2 address Host1 10.1.11.0/24 [edit] set security policies from-zone trust to-zone untrust policy to-SRX1 match source-address Host2`

`set security policies from-zone trust to-zone untrust policy to-SRX1 match destination-address Host1`



1. VPN `10.1.21.0/24`, Host2 `10.1.31.0/24` `10.1.11.0/24`.

```
[edit]
user@SRX2# set interfaces ge-0/0/0 unit 0 family inet address 10.1.21.1/24
user@SRX2# set interfaces ge-0/0/1 unit 0 family inet address 10.1.31.1/24
user@SRX2# set interfaces st0 unit 0 family inet address 10.1.100.2/24
```

2. VPN `10.1.11.0/24` SRX2 `10.1.11.0/24` SRX1 `10.1.11.0/24`.

```
[edit]
user@SRX2# set routing-options static route 172.16.11.1/32 next-hop 10.1.31.2
user@SRX2# set routing-options static route 10.1.11.0/24 next-hop st0.0
```

3. `10.1.11.0/24`(untrust) `10.1.11.0/24` `10.1.11.0/24`.

```
[edit]
user@SRX2# set security zones security-zone untrust host-inbound-traffic system-services ike
user@SRX2# set security zones security-zone untrust host-inbound-traffic system-services ping
user@SRX2# set security zones security-zone untrust interfaces ge-0/0/1.0
user@SRX2# set security zones security-zone untrust interfaces st0.0
```

4. `10.1.11.0/24` `10.1.11.0/24` `10.1.11.0/24`.

```
[edit]
user@SRX2# set security zones security-zone trust host-inbound-traffic system-services all
user@SRX2# set security zones security-zone trust host-inbound-traffic protocols all
user@SRX2# set security zones security-zone trust interfaces ge-0/0/0.0
```

5. `10.1.11.0/24` `10.1.11.0/24` `10.1.11.0/24` `10.1.11.0/24`.

```
[edit]
user@SRX2# set security address-book book1 address Host2 10.1.21.0/24
user@SRX2# set security address-book book1 attach zone trust
user@SRX2# set security address-book book2 address Host1 10.1.11.0/24
user@SRX2# set security address-book book2 attach zone untrust
```



```

        family inet {
            address 10.1.100.2/24;
        }
    }
}

```

```

[edit]
user@SRX2# show routing-options
static {
    route 172.16.11.1/32 next-hop 10.1.31.2;
    route 10.1.11.0/24 next-hop st0.0;
}

```

```

[edit]
user@SRX2# show security
address-book {
    book1 {
        address Host2 10.1.21.0/24;
        attach {
            zone trust;
        }
    }
    book2 {
        address Host1 10.1.11.0/24;
        attach {
            zone untrust;
        }
    }
}
policies {
    from-zone trust to-zone untrust {
        policy to-SRX1 {
            match {
                source-address Host2;
                destination-address Host1;
                application any;
            }
            then {
                permit;
            }
        }
    }
}

```

```

    }
}
from-zone untrust to-zone trust {
    policy from-SRX1 {
        match {
            source-address Host1;
            destination-address Host2;
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone untrust {
        host-inbound-traffic {
            system-services {
                ike;
                ping;
            }
        }
        interfaces {
            ge-0/0/1.0;
            st0.0;
        }
    }
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
}
}

```

```
commit?() ?????.
```

## SRX2? ?? IKE(Internet Key Exchange) ??

### CLI ?? ??

```
? ?? ??? ?????, ?? ??? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?
? ???? ???? CLI? ??? ???? ???? ???? ???? ???? commit?() ?????.
```

```
set security ike proposal ike_prop authentication-method pre-shared-keys
set security ike proposal ike_prop dh-group group2
set security ike proposal ike_prop authentication-algorithm sha1
set security ike proposal ike_prop encryption-algorithm 3des-cbc
set security ike policy ike_pol mode main
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"
set security ike gateway gw1 ike-policy ike_pol
set security ike gateway gw1 address 172.16.11.1
set security ike gateway gw1 local-identity user-at-hostname "srx2@example.com"
set security ike gateway gw1 remote-identity user-at-hostname "srx1@example.com"
set security ike gateway gw1 external-interface ge-0/0/1.0
```

```
??? ??
```

```
?? ?? ? ???? ???? ???? ?????. ?? ???? ???? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.
```

IKE(Internet Key Exchange) ??:

#### 1. IKE(Internet Key Exchange) 1?? ???? ????.

```
[edit]
user@SRX2# set security ike proposal ike_prop authentication-method pre-shared-keys
user@SRX2# set security ike proposal ike_prop dh-group group2
user@SRX2# set security ike proposal ike_prop authentication-algorithm sha1
user@SRX2# set security ike proposal ike_prop encryption-algorithm 3des-cbc
```

#### 2. IKE(Internet Key Exchange) 1?? ???? ????.

```
[edit]
user@SRX2# set security ike policy ike_pol mode main
```

```
user@SRX2# set security ike policy ike_pol proposals ike_prop
user@SRX2# set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"
```

### 3. IKE(Internet Key Exchange) 1?? ???? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? SRX1? ?? IP?? ???.

```
[edit]
user@SRX2# set security ike gateway gw1 ike-policy ike_pol
user@SRX2# set security ike gateway gw1 address 172.16.11.1
user@SRX2# set security ike gateway gw1 local-identity user-at-hostname "srx2@example.com"
user@SRX2# set security ike gateway gw1 remote-identity user-at-hostname "srx1@example.com"
user@SRX2# set security ike gateway gw1 external-interface ge-0/0/1.0
```

??

```
?? ???? show security ike ??? ???? ???? ?????. ?? ??? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.
```

```
[edit]
user@SRX2# show security ike
proposal ike_prop {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
}
policy ike_pol {
    mode main;
    proposals ike_prop;
    pre-shared-key ascii-text "$9$mP5QF3/At0IE-VsYoa36/"; ## SECRET-DATA
}
gateway gw1 {
    ike-policy ike_pol;
    address 172.16.11.1;
    local-identity user-at-hostname "srx2@example.com";
    remote-identity user-at-hostname "srx1@example.com";
    external-interface ge-0/0/1.0;
}
```

```
???? ???? ???? ?? ???? commit?(?) ??????.
```

## SRX2? ?? IPsec ??

### CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???? ????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security ipsec proposal ipsec_prop protocol esp
set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
set security ipsec policy ipsec_pol perfect-forward-secrecy keys group2
set security ipsec policy ipsec_pol proposals ipsec_prop
set security ipsec vpn vpn1 bind-interface st0.0
set security ipsec vpn vpn1 ike gateway gw1
set security ipsec vpn vpn1 ike ipsec-policy ipsec_pol
set security ipsec vpn vpn1 establish-tunnels immediately
```

??? ??

?? ?? ?? ????? ??? ???? ???? ?????. ?? ????? ??? ?? ??? CLI ??? ????? ??/????? CLI ???/??? ??????.

IPsec ??:

#### 1. IPsec 2?? ??? ?????.

```
[edit]
user@SRX2# set security ipsec proposal ipsec_prop protocol esp
user@SRX2# set security ipsec proposal ipsec_prop authentication-algorithm hmac-sha1-96
user@SRX2# set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
```

#### 2. IPsec 2?? ??? ?????.

```
[edit]
user@SRX2# set security ipsec policy ipsec_pol perfect-forward-secrecy keys group2
user@SRX2# set security ipsec policy ipsec_pol proposals ipsec_prop
```

### 3. IPsec VPN `?? ???? ?????.`

```
[edit]
user@SRX2# set security ipsec vpn vpn1 bind-interface st0.0
user@SRX2# set security ipsec vpn vpn1 ike gateway gw1
user@SRX2# set security ipsec vpn vpn1 ike ipsec-policy ipsec_pol
user@SRX2# set security ipsec vpn vpn1 establish-tunnels immediately
```

`??`

`?? ???? show security ipsec ???? ???? ???? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.`

```
[edit]
user@SRX2# show security ipsec
proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
}
policy ipsec_pol {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec_prop;
}
vpn vpn1 {
    bind-interface st0.0;
    ike {
        gateway gw1;
        ipsec-policy ipsec_pol;
    }
    establish-tunnels immediately;
}
```

`???? ???? ???? ? ? ???? commit?(?) ?????.`



```
set security nat static rule-set rule1 from zone untrust
```

## CLI

```
set security nat static rule-set rule1 rule ipsec match source-address 172.16.11.1/32
set security nat static rule-set rule1 rule ipsec match destination-address 172.16.21.1/32
set security nat static rule-set rule1 rule ipsec then static-nat prefix 10.1.31.1/32
```

```
set security policies from-zone trust to-zone untrust policy allow-out match source-address any
set security policies from-zone trust to-zone untrust policy allow-out match destination-address any
set security policies from-zone trust to-zone untrust policy allow-out match application any
set security policies from-zone trust to-zone untrust policy allow-out then permit
set security policies from-zone untrust to-zone trust policy allow-out-in match source-address any
set security policies from-zone untrust to-zone trust policy allow-out-in match destination-address any
set security policies from-zone untrust to-zone trust policy allow-out-in match application any
set security policies from-zone untrust to-zone trust policy allow-out-in then permit
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet address 172.16.21.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.31.2/24
set routing-options static route 172.16.11.0/24 next-hop 172.16.21.2
```

```
set security nat static rule-set rule1 from zone untrust
set security nat static rule-set rule1 rule ipsec match source-address 172.16.11.1/32
set security nat static rule-set rule1 rule ipsec match destination-address 172.16.21.1/32
set security nat static rule-set rule1 rule ipsec then static-nat prefix 10.1.31.1/32
set security policies from-zone trust to-zone untrust policy allow-out match source-address any
set security policies from-zone trust to-zone untrust policy allow-out match destination-address any
set security policies from-zone trust to-zone untrust policy allow-out match application any
set security policies from-zone trust to-zone untrust policy allow-out then permit
set security policies from-zone untrust to-zone trust policy allow-out-in match source-address any
set security policies from-zone untrust to-zone trust policy allow-out-in match destination-address any
set security policies from-zone untrust to-zone trust policy allow-out-in match application any
set security policies from-zone untrust to-zone trust policy allow-out-in then permit
set security zones security-zone trust host-inbound-traffic system-services ping
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet address 172.16.21.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.31.2/24
set routing-options static route 172.16.11.0/24 next-hop 172.16.21.2
```

??

### in this section

● [SRX100 IKE\(Internet Key Exchange\) 100 100 100 | 672](#)

● [SRX100 IPsec 100 100 100 | 674](#)

- [SRX2?? IKE\(Internet Key Exchange\) 1?? ?? ?? | 676](#)
- [SRX2? ?? IPsec ?? ?? ?? | 678](#)
- [???-??? ??? ?? | 680](#)

??? ??? ???? ???? ???? ???? ???? ???? ??:

**SRX1?? IKE(Internet Key Exchange) 1?? ?? ??**

??

IKE(Internet Key Exchange) 1?? ??? ????.

??

?? ???? **show security ike security-associations** ??? ?????. ? ??? ?? ?? **show security ike security-associations detail** ??? ???? ???.

```
user@SRX1> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
302301  UP    84e8fc61d0750278 ea9a07ef032805b6 Main 172.16.21.1
```

```
user@SRX1> show security ike security-associations detail
IKE peer 172.16.21.1, Index 302301, Gateway Name: gw1
Role: Initiator, State: UP
Initiator cookie: 84e8fc61d0750278, Responder cookie: ea9a07ef032805b6
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 172.16.11.1:4500, Remote: 172.16.21.1:4500
Lifetime: Expires in 19657 seconds
Reauth Lifetime: Disabled
IKE Fragmentation: Disabled, Size: 0
Remote Access Client Info: Unknown Client
Peer ike-id: srx2@example.com
AAA assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : 3des-cbc
```



- `?? ?????(????? IKE ??? ???? ??)`
- `IKE(Internet Key Exchange) ?? ?? ??`
- `?? ?? ? ??`
- `1?? ?? ?? ??(? ?? ???? ???? ??)`

`show security ike security-associations ??? ?? ??(SA)? ?? ?? ??? ?????.`

- `??? ?? ? ??? ?????`
- `1?? ??`
- `??? ??(???? ???? ???? ??? ??? ???? ? ???? ? ???? ?)`
- `?? ??`

`?? ??? ??? ???? ???? ???? ?? ? ?????.`

- `??? ? ???? ??`
- `??? IPsec SA? ?`
- `?? ?? 2?? ?? ?`

**SRX1?? IPsec ?? ?? ??**

**??**

IPsec `??? ?????.`

**??**

`?? ???? show security ipsec security-associations ??? ?????. ? ??? ???? ?? show security ipsec security-associations detail ??? ????? ???.`

```
user@SRX1> show security ipsec security-associations
Total active tunnels: 1      Total Isec sas: 1
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
```

```
<131073 ESP:3des/sha1 fc5dbac4 2160/ unlim - root 4500 172.16.21.1
>131073 ESP:3des/sha1 45fed9d8 2160/ unlim - root 4500 172.16.21.1
```

```
user@SRX1> show security ipsec security-associations detail
```

```
ID: 131073 Virtual-system: root, VPN Name: vpn1
```

```
Local Gateway: 172.16.11.1, Remote Gateway: 172.16.21.1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Version: IKEv1
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.0
```

```
Port: 4500, Nego#: 7, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
```

```
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
```

```
Tunnel events:
```

```
Fri Jul 22 2022 11:07:40 -0700: IPSec SA rekey successfully completed (3 times)
```

```
Fri Jul 22 2022 08:38:41 -0700: IPSec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:38:41 -0700: User cleared IPSec SA from CLI (1 times)
```

```
Fri Jul 22 2022 08:38:41 -0700: IKE SA negotiation successfully completed (3 times)
```

```
Fri Jul 22 2022 08:38:26 -0700: IPSec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:38:26 -0700: User cleared IPSec SA from CLI (1 times)
```

```
Fri Jul 22 2022 08:38:25 -0700: IPSec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:38:24 -0700: User cleared IPSec SA from CLI (1 times)
```

```
Fri Jul 22 2022 08:37:37 -0700: IPSec SA negotiation successfully completed (1 times)
```

```
Direction: inbound, SPI: fc5dbac4, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 2153 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 1532 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 45fed9d8, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 2153 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 1532 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
show security ipsec security-associations [??] [??] [?] [??] [????].
```

- `?? ?????? 172.16.21.1 ??? ?????.`
- `IPsec SA ??? ? ??? ?? 4500? ????? ?????.`
- `SPI, ??(2 ??) ? ?? ??(?? KB? ?? ??)? ?????? ??????. 2160/unlim ?? 2160? ?? 2?? ??? ?????? ?? ??? ?? ? ?????? ??????. ?? ?????? ??????. 2?? ??? VPN? up? ? 1??? ????? ?? ??? 1?? ??? ?? ? ?????.`
- `VPN ????? Mon ??? ?????? ??????, ? SA?? ?????? ?????. VPN ?????? ????? ??, U? ?????? up ????? D? ??? ? down ?????? ??????.`
- `?? ???(vsys)? ?? ?????? ?? O? ??????.`

## SRX2?? IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

```

?? ???? show security ike security-associations ??? ??????. ? ??? ???? ?? show security ike security-
associations detail ??? ????? ????.
```

```
user@SRX2> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|---------|-------|------------------|------------------|------|----------------|
| 5567091 | UP    | 84e8fc61d0750278 | ea9a07ef032805b6 | Main | 172.16.11.1    |

```
user@SRX2> show security ike security-associations detail
IKE peer 172.16.11.1, Index 5567091, Gateway Name: gw1
  Role: Responder, State: UP
  Initiator cookie: 84e8fc61d0750278, Responder cookie: ea9a07ef032805b6
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.31.1:4500, Remote: 172.16.11.1:4500
  Lifetime: Expires in 18028 seconds
  Reauth Lifetime: Disabled
  IKE Fragmentation: Disabled, Size: 0
  Remote Access Client Info: Unknown Client
  Peer ike-id: srx1@example.com
```

```

AAA assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : 3des-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-2
Traffic statistics:
  Input  bytes   :           2352
  Output bytes   :           1780
  Input  packets :           14
  Output packets :            7
  Input  fragmentated packets: 0
  Output fragmentated packets: 0
IPSec security associations: 4 created, 3 deleted
Phase 2 negotiations in progress: 1

```

```

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 10.1.31.1:4500, Remote: 172.16.11.1:4500
Local identity: srx2@example.com
Remote identity: srx1@example.com
Flags: IKE SA is created

```

??

show security ike security-associations ??? ?? ?? IKE(Internet Key Exchange) 1?? SA? ??????. SA? ????? ??  
 ?? ??, 1?? ????? ?? ?? ?????, ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ????? ??????.

SA? ????? ?? ?? ?? ????? ??????.

- ??? - ? ?? ? IKE(Internet Key Exchange)? ?? ????? SA? ?? ????? ????? ?? ?? show security ike security-associations detail???? ? ?????.
- ?? ?? - ?? IP ??? ????? ?? 4500? ?? ? ??? ????? ????? ????? ??????.
- ?? ????? ??
  - ? - 1?? SA? ?????????.
  - ?? - 1?? SA? ????? ? ??? ?????.
  - ?? IKE(Internet Key Exchange) ID - ??? ????? ?????.
  - ?? ID ? ?? ID - ??? ??? ????? ?????.
- ?? - ??? ??? ????? ????? ?????.





```
<131073 ESP:3des/sha1 45fed9d8 1526/ unlim - root 4500 172.16.11.1
>131073 ESP:3des/sha1 fc5dbac4 1526/ unlim - root 4500 172.16.11.1
```

```
user@SRX2> show security ipsec security-associations detail
```

```
ID: 131073 Virtual-system: root, VPN Name: vpn1
```

```
Local Gateway: 10.1.31.1, Remote Gateway: 172.16.11.1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Version: IKEv1
```

```
DF-bit: clear, Copy-Outer-DSCP Disabled, Bind-interface: st0.0
```

```
Port: 4500, Nego#: 25, Fail#: 0, Def-Del#: 0 Flag: 0x600a29
```

```
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
```

```
Tunnel events:
```

```
Fri Jul 22 2022 11:07:40 -0700: IPsec SA negotiation successfully completed (4 times)
```

```
Fri Jul 22 2022 08:38:41 -0700: Initial-Contact received from peer. Stale IKE/IPsec SAs
cleared (1 times)
```

```
Fri Jul 22 2022 08:38:41 -0700: IKE SA negotiation successfully completed (5 times)
```

```
Fri Jul 22 2022 08:38:26 -0700: IPsec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:38:26 -0700: IPsec SA delete payload received from peer, corresponding
IPsec SAs cleared (1 times)
```

```
Fri Jul 22 2022 08:38:25 -0700: IPsec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:38:25 -0700: Initial-Contact received from peer. Stale IKE/IPsec SAs
cleared (1 times)
```

```
Fri Jul 22 2022 08:37:37 -0700: IPsec SA negotiation successfully completed (1 times)
```

```
Fri Jul 22 2022 08:37:37 -0700: IPsec SA delete payload received from peer, corresponding
IPsec SAs cleared (1 times)
```

```
Thu Jul 21 2022 17:57:09 -0700: Peer's IKE-ID validation failed during negotiation (1 times)
```

```
Thu Jul 21 2022 17:49:30 -0700: IKE SA negotiation successfully completed (4 times)
```

```
Direction: inbound, SPI: 45fed9d8, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 1461 seconds
```

```
Lifetime Remaining: Unlimited
```

```
Soft lifetime: Expires in 885 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: fc5dbac4, AUX-SPI: 0
```

```
, VPN Monitoring: -
```

```
Hard lifetime: Expires in 1461 seconds
```

```
Lifetime Remaining: Unlimited
```

```
Soft lifetime: Expires in 885 seconds
```

```
user@Host1> ping 10.1.21.2 count 10 rapid
PING 10.1.21.2 (10.1.21.2): 56 data bytes
```

```
!!!!!!!
--- 10.1.21.2 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max/stddev = 3.437/4.270/7.637/1.158 ms
```

```
user@SRX1> show security ipsec statistics
ESP Statistics:
  Encrypted bytes:      1360
  Decrypted bytes:      840
  Encrypted packets:    10
  Decrypted packets:    10
AH Statistics:
  Input bytes:          0
  Output bytes:         0
  Input packets:        0
  Output packets:       0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

??

?? Host1? Host2? ping? ? ???? ???? VPN? ???? ???? ?????.

SEE ALSO

- [IPsec ?? | 11](#)
- [?: ?? ?? VPN ?? | 328](#)

?: ????? ?? ??(NAT) ????? ?? ??? ? ???? ?? ?? ?? ?? VPN ??

in this section

[?? ?? | 682](#)

|   |          |
|---|----------|
| ● | ??   682 |
| ● | ??   689 |
| ● | ??   718 |

?? ???? ? ???? ? ? ???? ? ? ? ???? ? ? ?(NAT) ???? ? ???? ???? ? ? ? ? ? VPN? ???? ? ?  
? ?????.

?? ??

???? ? "IPsec ?" ??? 11?(?) ????.

??

? ???? ? ???? ???? VPN ???? ???? ???? ???? ???? ? ? ? ? ? VPN? ?????. ??? ???? VPN?  
???? ???? ???? ? ? ? ? ?.

? ???? ? ? ? ? ? ? ???? , ??? ? , ? ? , ? ? ? ? ?.

?? 43 ??? 683?(?) ? ???? ? ?(NAT) ???? ? ? ? ? ? VPN? ???? ? ????.



配置IKE，IPv4地址为13.168.11.1，IPsec 200，IKE(Internet Key Exchange) 100。配置NAT，使1.1.100.1/24能够通过IP 1.1.100.1/24访问互联网。

配置NAT，使104.100.684~107.100.686(2)能够通过互联网访问。

**104:** 配置NAT，使104.100.684~107.100.686(2)能够通过互联网访问。

| 名称           | 接口              | 配置                                                                                                                    |
|--------------|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| ge-0/0/0     | ge-0/0/0        | 12.168.99.100/24                                                                                                      |
|              | ge-0/0/1        | 10.1.99.1/24                                                                                                          |
| 10.2.99.0/24 | 10.2.99.0/24(2) | next hop 12.168.99.100                                                                                                |
|              | 1.1.100.0/24    | 12.168.99.100                                                                                                         |
| 10.2.99.0/24 | 10.2.99.0/24    | <ul style="list-style-type: none"> <li>10.2.99.0/24</li> <li>10.2.99.0/24</li> <li>ge-0/0/1.0 10.2.99.0/24</li> </ul> |
|              | untrust         | <ul style="list-style-type: none"> <li>ge-0/0/0.0 12.168.99.100</li> </ul>                                            |

**105:** 配置IKE(Internet Key Exchange) 100

| 名称       | 接口       | 配置                                                                                                                                     |
|----------|----------|----------------------------------------------------------------------------------------------------------------------------------------|
| ike_prop | ike_prop | <ul style="list-style-type: none"> <li>pre-shared-keys</li> <li>Diffie-Hellman group: group2</li> <li>md5</li> <li>3des-cbc</li> </ul> |

### ? 105: ???? ? IKE(Internet Key Exchange) 1?? ?? ?? ?? (Continued)

| ??     | ??      | ?? ?? ??                                                                                                                                                                                                                            |
|--------|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ??     | ike_pol | <ul style="list-style-type: none"> <li>• ??: main</li> <li>• ?? ??: ike_prop</li> <li>• IKE(Internet Key Exchange) 1?? ?? ?? ??: pre-shared-key ascii-text</li> </ul>                                                               |
| ?????? | gate    | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) ?? ??: ike_pol</li> <li>• ?? ??????: ge-0/0/1.0</li> <li>• ?????? ??: 1.1.100.23</li> <li>• ?? ?? ??????: chicago</li> <li>• ?? ?? ??????: sunnyvale</li> </ul> |

### ? 106: ???? ? IPSec 2?? ?? ?? ??

| ??  | ??         | ?? ?? ??                                                                                                                            |
|-----|------------|-------------------------------------------------------------------------------------------------------------------------------------|
| ??  | ipsec_prop | <ul style="list-style-type: none"> <li>• ??????: esp</li> <li>• ?? ??????: hmac-md5-96</li> <li>• ????? ??????: 3des-cbc</li> </ul> |
| ??  | ipsec_pol  | <ul style="list-style-type: none"> <li>• ?? ??: ipsec_prop</li> <li>• PFS(Perfect Forward Secrecy): group1</li> </ul>               |
| VPN | first_vpn  | <ul style="list-style-type: none"> <li>• IKE(Internet Key Exchange) ?????? ??: gate</li> <li>• IPsec ?? ??: ipsec_pol</li> </ul>    |





**108:**  , (Continued)

|  | untrust | <ul style="list-style-type: none"> <li>ge-0/0/0.0 .</li> </ul> |
|--|---------|----------------------------------------------------------------|

**109:**  IKE(Internet Key Exchange) 1

|  | ike_prop | <ul style="list-style-type: none"> <li>: pre-shared-keys</li> <li>Diffie-Hellman : group2</li> <li>: md5</li> <li>: 3des-cbc</li> </ul>                                                                         |
|--|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | ike_pol  | <ul style="list-style-type: none"> <li>: main</li> <li>: ike_prop</li> <li>IKE(Internet Key Exchange) 1 : pre-shared-key ascii-text</li> </ul>                                                                  |
|  | gate     | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) : ike_pol</li> <li>: ge-0/0/1.0</li> <li>: 1.1.100.22</li> <li>: DPD(Dead Peer Detection) </li> <li>: sunnyvale</li> <li>: chicago</li> </ul> |

# 图 110: 配置 IPsec 策略

| 配置项        | 配置值        | 配置说明                                                                                                               |
|------------|------------|--------------------------------------------------------------------------------------------------------------------|
| ipsec_prop | ipsec_prop | <ul style="list-style-type: none"> <li>加密算法: esp</li> <li>认证算法: hmac-md5-96</li> <li>加密模式: 3des-cbc</li> </ul>     |
| ipsec_pol  | ipsec_pol  | <ul style="list-style-type: none"> <li>策略名称: ipsec_prop</li> <li>PFS(Perfect Forward Secrecy): group1</li> </ul>   |
| VPN        | first_vpn  | <ul style="list-style-type: none"> <li>IKE(Internet Key Exchange) 配置: gate</li> <li>IPsec 策略: ipsec_pol</li> </ul> |

# 图 111: 配置 IPsec 策略

| 配置项                                    | 配置值  | 配置说明                                                                                                                                                                                     |
|----------------------------------------|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 配置 IPsec 策略 (untrust) 策略名称: ipsec_prop | pol1 | <ul style="list-style-type: none"> <li>策略名称:</li> <li>source-address</li> <li>destination-address</li> <li>认证算法: hmac-md5-96</li> <li>策略名称: permit tunnel ipsec-vpn first_vpn</li> </ul> |
| 配置 IPsec 策略 (untrust) 策略名称: ipsec_prop | pol1 | <ul style="list-style-type: none"> <li>策略名称:</li> <li>认证算法: hmac-md5-96</li> <li>策略名称: permit tunnel ipsec-vpn first_vpn</li> </ul>                                                      |



?????, ?? ?? ? ?? ?? ?? ??:

1. ??? ?????? ?? ????.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 12.168.99.100/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.1.99.1/24
```

2. ?? ?? ??? ????.

```
[edit]
user@host# set routing-options static route 10.2.99.0/24 next-hop 12.168.99.1
user@host# set routing-options static route 1.1.100.0/24 next-hop 12.168.99.1
```

3. ????? ?? ??? ????.

```
[edit ]
user@host# set security zones security-zone trust host-inbound-traffic protocols all
```

4. ?????? ????? ?? ??? ????.

```
[edit security zones security-zone trust]
user@host# set interfaces ge-0/0/1.0
```

5. ????? ?? ??? ??? ???? ????.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
```

6. ?????? ??????(untrust) ?? ??? ????.

```
[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/0.0
```

??

?? ???? show interfaces, show routing-options, show security zones ??? ???? ???? ?????. ?? ??? ???? ???? ????  
 ??? ? ???? ???? ???? ???? ?????.

```
[edit]
user@host# show interfaces
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 12.168.99.100/24;
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 10.1.99.1/24;
      }
    }
  }
}
```

```
[edit]
user@host# show routing-options
  static {
    route 10.2.99.0/24 next-hop 12.168.99.1;
    route 1.1.100.0/24 next-hop 12.168.99.1;
  }
```

```
[edit]
user@host# show security zones
  security-zone trust {
    host-inbound-traffic {
      system-services {
        all;
      }
    }
    protocols {
      all;
    }
  }
```

```

    }
    interfaces {
        ge-0/0/1.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
    }
    interfaces {
        ge-0/0/0.0;
    }
}
}

```

?? ?? ?? ?? commit?(?) ????.

### ??? IKE(Internet Key Exchange) ??

#### CLI ?? ??

? ?? ?? ?????, ?? ?? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ?? ???? ? ?? ? ? ???? [edit] ?  
 ? ???? ???? CLI? ??? ?? ?? ??, ?? ???? commit?(?) ????.

```

set security ike proposal ike_prop authentication-method pre-shared-keys
set security ike proposal ike_prop dh-group group2
set security ike proposal ike_prop authentication-algorithm md5
set security ike proposal ike_prop encryption-algorithm 3des-cbc
set security ike policy ike_pol mode aggressive
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"
set security ike gateway gate ike-policy ike_pol
set security ike gateway gate address 13.168.11.100
set security ike gateway gate external-interface ge-0/0/0.0
set security ike gateway gate local-identity hostname chicago

```

??? ??

?? ?? ? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ????.

IKE(Internet Key Exchange) ??:

1. IKE(Internet Key Exchange) 1?? ???? ????.

```
[edit security ike]
user@host# edit proposal ike_prop
```

2. IKE(Internet Key Exchange) ?? ?? ??? ????.

```
[edit security ike proposal ike_prop]
user@host# set authentication-method pre-shared-keys
```

3. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ????.

```
[edit security ike proposal ike_prop]
user@host# set dh-group group2
```

4. IKE(Internet Key Exchange) ?? ?? ????? ????.

```
[edit security ike proposal ike_prop]
user@host# set authentication-algorithm md5
```

5. IKE(Internet Key Exchange) ?? ??? ????? ????.

```
[edit security ike proposal ike_prop]
user@host# set encryption-algorithm 3des-cbc
```

6. IKE(Internet Key Exchange) 1?? ??? ????.

```
[edit security ike policy ]
user@host# edit policy ike_pol
```

7. IKE(Internet Key Exchange) 1?? ?? ??? ????.

```
[edit security ike policy ike_pol]
user@host# set mode aggressive
```

8. IKE(Internet Key Exchange) 100 100 100 10000.

```
[edit security ike policy ike_pol]
user@host# set proposals ike_prop
```

9. IKE(Internet Key Exchange) 100 100 100 1000 100000.

```
[edit security ike policy ike_pol pre-shared-key]
user@host# set ascii-text "$ABC123"
```

10. IKE(Internet Key Exchange) 100 100000 10000 10 1000000 100000.

```
[edit security ike ]
user@host# set gateway gate external-interface ge-0/0/0.0
```

11. IKE(Internet Key Exchange) 100 100000 1000 100000.

```
[edit security ike gateway gate]
set address 13.168.11.100
```

12. IKE(Internet Key Exchange) 100 100 1000 100000.

```
[edit security ike gateway gate]
set ike-policy ike_pol
```

13. 100 1000 100 local-identity1(1) 100000.

```
[edit security ike gateway gate]
user@host# set local-identity hostname chicago
```





```
set security ipsec vpn first_vpn ike ipsec-policy ipsec_pol
set security ipsec vpn first_vpn establish-tunnels immediately
```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

IPsec ??:

1. IPsec ??? ???? ????.

```
[edit]
user@host# edit security ipsec proposal ipsec_prop
```

2. IPsec ??? ?? ???? ????.

```
[edit security ipsec proposal ipsec_prop]
user@host# set protocol esp
```

3. IPsec ??? ?? ?? ???? ????.

```
[edit security ipsec proposal ipsec_prop]
user@host# set authentication-algorithm hmac-md5-96
```

4. IPsec ??? ?? ??? ???? ????.

```
[edit security ipsec proposal ipsec_prop]
user@host# set encryption-algorithm 3des-cbc
```

5. IPsec ??? ?? ??? ????.

```
[edit security ipsec policy ipsec_pol]
user@host# set proposals ipsec_prop
```

## 6. PFS(Perfect Forward Secrecy) group1? ???? IPsec 2?? ????.

```
[edit security ipsec policy ipsec_pol ]
user@host# set perfect-forward-secrecy keys group1
```

## 7. IKE(Internet Key Exchange) ???? ????.

```
[edit security ipsec]
user@host# set vpn first_vpn ike gateway gate
```

## 8. IPsec 2?? ???? ????.

```
[edit security ipsec]
user@host# set vpn first_vpn ike ipsec-policy ipsec_pol
```

??

?? ???? show security ipsec ??? ???? ???? ?????. ?? ???? ???? ???? ???? ???? ? ? ???? ???? ???? ????.

```
[edit]
user@host# show security ipsec
  proposal ipsec_prop {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm 3des-cbc;
  }
  policy ipsec_pol {
    perfect-forward-secrecy {
      keys group1;
    }
    proposals ipsec_prop;
  }
  vpn first_vpn {
    ike {
      gateway gate;
      ipsec-policy ipsec_pol;
    }
  }
```



## 2. `set policy pol1 match application any`

```
[edit security policies from-zone untrust to-zone trust]
user@host# set policy pol1 match application any
user@host# set policy pol1 then permit tunnel ipsec-vpn first_vpn
```

??

?? show security policies

```
[edit]
user@host# show security policies
  from-zone trust to-zone untrust {
    policy pol1 {
      match {
        source-address any;
        destination-address any;
        application any;
      }
      then {
        permit {
          tunnel {
            ipsec-vpn first_vpn;
          }
        }
      }
    }
  }
  from-zone untrust to-zone trust {
    policy pol1 {
      match {
        application any;
      }
      then {
        permit {
          tunnel {
            ipsec-vpn first_vpn;
          }
        }
      }
    }
  }
```

} }

1. `?? ?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet address 12.168.99.1/24
user@host# set ge-0/0/1 unit 0 family inet address 1.1.100.23/24
```

2. `?? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/0.0
```

```
[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/1.0
```

3. `?? ?? ? ? ? ? (NAT) ? ? ? ? ? ? ? ?`.

```
[edit security nat source rule-set ipsec]
user@host# set from zone trust
user@host# set to zone untrust
user@host# set rule 1 match source-address 0.0.0.0/0
user@host# set rule 1 then source-nat interface
```

4. `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy allow-all match source-address any
user@host# set from-zone trust to-zone untrust policy allow-all match destination-address any
user@host# set from-zone trust to-zone untrust policy allow-all match application any
user@host# set from-zone trust to-zone untrust policy allow-all then permit
user@host# set from-zone untrust to-zone trust policy allow-all match application any
user@host# set from-zone untrust to-zone trust policy allow-all then permit
```





```

    from-zone untrust to-zone trust {
        policy allow-all {
            match {
                application any;
            }
            then {
                permit;
            }
        }
    }
}

zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone untrust {
        host-inbound-traffic {
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
}

interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 12.168.99.1/24;
            }
        }
    }
    ge-0/0/1 {

```



1. `?? ???? ? ????.`

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet address 13.168.11.100/24
user@host# set interfaces ge-0/0/1 unit 0 family inet address 10.2.99.1/24
```

2. `?? ? ???? ????.`

```
[edit]
user@host# set routing-options static route 10.1.99.0/24 next-hop 13.168.11.1
user@host# set routing-options static route 1.1.100.0/24 next-hop 13.168.11.1
```

3. `????? ?????(untrust) ? ? ? ?.`

```
[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/0.0
```

4. `???? ? ? ? ?.`

```
[edit]
user@host# set security zones security-zone trust host-inbound-traffic protocols all
```

5. `????? ???? ? ? ? ?.`

```
[edit security zones security-zone trust]
user@host# set interfaces ge-0/0/1.0
```

6. `???? ? ? ? ? ? ? ? ?.`

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
```

??

?? ???? show interfaces, show routing-options ? show security zones ??? ???? ???? ?????. ?? ???? ???? ???? ????  
 ? ???? ? ???? ???? ???? ???? ?????.

```
[edit]
user@host# show interfaces
    ge-0/0/0 {
        unit 0 {
            family inet {
                address 13.168.11.100/24;
            }
        }
    }
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 10.2.99.1/24;
            }
        }
    }
}
```

```
[edit]
user@host# show routing-options
    static {
        route 10.1.99.0/24 next-hop 13.168.11.1;
        route 1.1.100.0/24 next-hop 13.168.11.1;
    }
```

```
[edit]
user@host# show security zones
    security-zone untrust {
        host-inbound-traffic {
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone trust {
```

```

    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

?? ?? ?? ?? commit?(?) ?????.

??? IKE(Internet Key Exchange) ??

CLI ?? ??

? ?? ?? ?????, ?? ?? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ?? ???? ? ?? ? ? ???? [edit] ?  
 ? ???? ???? CLI? ??? ?? ?? ??, ?? ???? commit?(?) ?????.

```

set security ike proposal ike_prop authentication-method pre-shared-keys
set security ike proposal ike_prop dh-group group2
set security ike proposal ike_prop authentication-algorithm md5
set security ike proposal ike_prop encryption-algorithm 3des-cbc
set security ike policy ike_pol mode aggressive
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "$ABC123"
set security ike gateway gate ike-policy ike_pol
set security ike gateway gate dynamic hostname chicago
set security ike gateway gate external-interface ge-0/0/0.0

```

??? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI / ??? ??? ?????.

IKE(Internet Key Exchange) ??:

1. IKE(Internet Key Exchange) ?? ?? ??? ?????.

```
[edit security ike proposal ike_prop]
user@host# set authentication-method pre-shared-key
```

2. IKE(Internet Key Exchange) ?? Diffie-Hellman ??? ?????.

```
[edit security ike proposal ike_prop]
user@host# set dh-group group2
```

3. IKE(Internet Key Exchange) ?? ?? ????? ?????.

```
[edit security ike proposal ike_prop]
user@host# set authentication-algorithm md5
```

4. IKE(Internet Key Exchange) ?? ??? ?????? ?????.

```
[edit security ike proposal ike_prop]
user@host# set encryption-algorithm 3des-cbc
```

5. IKE(Internet Key Exchange) 1?? ?? ?????.

```
[edit security ike]
user@host# edit policy ike_pol
```

6. IKE(Internet Key Exchange) 1?? ?? ??? ?????.

```
[edit security ike policy ike_pol]
user@host# set mode aggressive
```

7. IKE(Internet Key Exchange) ??? ?? ??? ?????.

```
[edit security ike policy ike_pol]
user@host# set proposals ike_prop
```



```

ike-policy ike_pol;
dynamic hostname chicago;
external-interface ge-0/0/0.0;
}

```

```

?? ?? ?? ?? ?? commit?(?) ??????.

```

## ?? IPsec ??

### CLI ?? ??

```

? ?? ?? ?????, ?? ?? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?
? ???? ???? CLI? ??? ?? ?? ??, ?? ???? commit?(?) ??????.

```

```

set security ipsec proposal ipsec_prop protocol esp
set security ipsec proposal ipsec_prop authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec_prop encryption-algorithm 3des-cbc
set security ipsec policy ipsec_pol perfect-forward-secrecy keys group1
set security ipsec policy ipsec_pol proposals ipsec_prop
set security ipsec vpn first_vpn ike gateway gate
set security ipsec vpn first_vpn ike ipsec-policy ipsec_pol

```

### ??? ??

```

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

```

IPsec ??:

#### 1. IPsec ??? ???? ????.

```

[edit]
user@host# edit security ipsec proposal ipsec_prop

```

#### 2. IPsec ??? ?? ???? ????.

```

[edit security security ipsec proposal ipsec_prop]
user@host# set protocol esp

```







```
set security policies from-zone untrust to-zone trust policy pol1 then permit tunnel ipsec-vpn
first_vpn
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ????? ???? ?? ???? CLI ??? ???? ??/ ???? CLI ??? ???? ??????.

?? ?? ??:

1. `???? ???? ??????(untrust) ???? ???? ???? ? ? ? ? ?`

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy pol1 match source-address any
user@host# set policy pol1 match destination-address any
user@host# set policy pol1 match application any
user@host# set policy pol1 then permit tunnel ipsec-vpn first_vpn
```

- 2.** ☐☐☐☐☐ (untrust) ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐

```
[edit security policies from-zone untrust to-zone trust]
user@host# set policy pol1 match application any
user@host# set policy pol1 then permit tunnel ipsec-vpn first_vpn
```

??

[illegible]

```
[edit]
user@host# show security policies
    from-zone trust to-zone untrust {
        policy pol1 {
            match {
                source-address any;
                destination-address any;
                application any;
            }
            then {
                permit {
                    tunnel {
```

```

        ipsec-vpn first_vpn;
    }
}
}
}
}
from-zone untrust to-zone trust {
    policy pol1 {
        match {
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn first_vpn;
                }
            }
        }
    }
}
}
}

```

```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

```

```

?? ?? ?? ?? ?? ??(NAT) ??

```

## CLI ?? ??

```

? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ?? ?? ?? ?? ?? ? ?? ?? ?? ?? [edit] ?
? ?? ?? ?? ?? CLI? ?? ?? ?? ??, ?? ?? ?? commit?(?) ?????.

```

```

set security nat source rule-set ipsec from zone trust
set security nat source rule-set ipsec to zone untrust
set security nat source rule-set ipsec rule 1 match source-address 0.0.0.0/0
set security nat source rule-set ipsec rule 1 then source-nat interface
set security policies from-zone trust to-zone untrust policy allow-all match source-address any
set security policies from-zone trust to-zone untrust policy allow-all match destination-address any
set security policies from-zone trust to-zone untrust policy allow-all match application any
set security policies from-zone trust to-zone untrust policy allow-all then permit
set security policies from-zone untrust to-zone trust policy allow-all match application any
set security policies from-zone untrust to-zone trust policy allow-all then permit
set security zones security-zone trust host-inbound-traffic system-services all

```

```

set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet address 13.168.11.1/24
set interfaces ge-0/0/1 unit 0 family inet address 1.1.100.22/24
set routing-options static route 0.0.0.0/0 next-hop 1.1.100.23

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

???? ?? ??(NAT)? ???? ???? ?? ??:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet address 13.168.11.1/24
user@host# set ge-0/0/1 unit 0 family inet address 1.1.100.22/24

```

2. ??? ????.

```

[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/0.0

```

```

[edit security zones security-zone untrust]
user@host# set interfaces ge-0/0/1.0

```

3. ??? ? ?(NAT)? ????.

```

[edit security nat source rule-set ipsec]
user@host# set from zone trust
user@host# set to zone untrust
user@host# set rule 1 match source-address 0.0.0.0/0
user@host# set rule 1 then source-nat interface

```

4. `?? ?? ?? ????.`

```
[edit security policies]
user@host# set from-zone trust to-zone untrust policy allow-all match source-address any
user@host# set from-zone trust to-zone untrust policy allow-all match destination-address any
user@host# set from-zone trust to-zone untrust policy allow-all match application any
user@host# set from-zone trust to-zone untrust policy allow-all then permit
user@host# set from-zone untrust to-zone trust policy allow-all match application any
user@host# set from-zone untrust to-zone trust policy allow-all then permit
```

5. `??? ??? ?????.`

```
[edit routing-options]
user@host# set static route 0.0.0.0/0 next-hop 1.1.100.23
```

??

?? ????? show security nat ??? ???? ???? ?????. ?? ??? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.

```
[edit]
user@host# show security nat
  nat {
    source {
      rule-set ipsec {
        from zone trust;
        to zone untrust;
        rule 1 {
          match {
            source-address 0.0.0.0/0;
          }
          then {
            source-nat {
              interface;
            }
          }
        }
      }
    }
  }
}
policies {
```

```

from-zone trust to-zone untrust {
    policy allow-all {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy allow-all {
        match {
            application any;
        }
        then {
            permit;
        }
    }
}
}
zones {
    security-zone trust {
        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone untrust {
        host-inbound-traffic {
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
}

```

```
    }
  }
}
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        address 13.168.11.1/24;
      }
    }
  }
  ge-0/0/1 {
    unit 0 {
      family inet {
        address 1.1.100.22/24;
      }
    }
  }
}
routing-options {
  static {
    route 0.0.0.0/0 next-hop 1.1.100.23;
  }
}
```

?? ?? ???? ? ???? commit?(?) ?????.

??

**in this section**

- [???? ? IKE\(Internet Key Exchange\) 1?? ?? ? | 719](#)
- [???? ? IPsec ?? ?? ? | 721](#)
- [???? ? IKE\(Internet Key Exchange\) 1?? ?? ? | 723](#)
- [???? ? IPsec ?? ?? ? | 725](#)

??? ?? ???? ???? ? ? ? ??:



?? ?? IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

?? ?????? ????? ?? 10.1.99.0 ?????? ?????? 10.2.99.0 ?????? ?????? ?????? ??????. ?? ?? VPN? ??, SRX ??? ??  
 ?? ??? ?? ?????? ??? ? ??????. IPsec ??? ??????, VPN ??? ?? ??? ?????? VPN? ?????? ?? ? ?? ?????? ??? ???  
 ? ?????? ?? ??????. ?? ??, 10.1.99.2?? 10.2.99.2? ping ??? ??????.

?? ????? show security ike security-associations ??? ??????. ?????? ??? ?? ? show security ike security-  
 associations index *index\_number* detail ??? ??????.

```
user@host> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode       | Remote Address |
|---------|-------|------------------|------------------|------------|----------------|
| 5649304 | UP    | c3193077d38e426f | 011f0ef28d928f4c | Aggressive | 13.168.11.     |

```
user@host> show security ike security-associations index 5649304 detail
```

IKE peer 13.168.11.100, Index 5649304, Gateway Name: gate

Role: Initiator, State: UP

Initiator cookie: c3193077d38e426f, Responder cookie: 011f0ef28d928f4c

Exchange type: Aggressive, Authentication method: Pre-shared-keys

Local: 12.168.99.100:4500, Remote: 13.168.11.100:4500

Lifetime: Expires in 26359 seconds

Reauth Lifetime: Disabled

IKE Fragmentation: Disabled, Size: 0

Remote Access Client Info: Unknown Client

Peer ike-id: 13.168.11.100

AAA assigned IP: 0.0.0.0

Algorithms:

Authentication : hmac-md5-96

Encryption : 3des-cbc

Pseudo random function: hmac-md5

Diffie-Hellman group : DH-group-2

Traffic statistics:

Input bytes : 1140

Output bytes : 1203

Input packets: 6

Output packets: 6



show security ike security-associations `???` `??` `??(SA)?` `??` `??` `???` `??????`.

- `???` `??` `?` `???` `?????`
- `1??` `??`
- `???` `??(???? ???? ???? ???? ???? ???? ? ???? ? ???? ?)`
- `??` `??`

`??` `???` `???` `???` `?????` `?????` `??` `?` `??????`.

- `???` `?` `???` `??`
- `???` IPsec SA `?` `?`
- `??` `??` `2??` `??` `?`

`????` `??` IPsec `??` `??` `??`

`??`

IPsec `???` `??????`.

`??`

`??` `????` show security ipsec security-associations `???` `??????`. `????` `???` `???` `??` `?` show security ipsec security-associations index *index\_number* detail `???` `??????`.

```
user@host> show security ipsec security-associations
```

```
Total active tunnels: 1      Total Isec sas: 1
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<2      ESP:3des/md5      aff3ac30 1103/ unlim -   root 4500  13.168.11.100
>2      ESP:3des/md5      40539d12 1103/ unlim -   root 4500  13.168.11.100
```

```
user@host> show security ipsec security-associations detail
```

```
ID: 2 Virtual-system: root, VPN Name: first_vpn
Local Gateway: 12.168.99.100, Remote Gateway: 13.168.11.100
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```

Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv1
DF-bit: clear, Copy-Outer-DSCP Disabled, Policy-name: pol1
Port: 4500, Nego#: 7, Fail#: 0, Def-Del#: 0 Flag: 0x600829
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
Tunnel events:
  Wed Apr 08 2020 19:13:53: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020
    : IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
  Wed Apr 08 2020 19:13:09: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020 19:13:09: User cleared IPSec SA from CLI (1 times)
  Wed Apr 08 2020 19:13:09: IKE SA negotiation successfully completed (5 times)
  Wed Apr 08 2020 19:12:18: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020 19:12:18: User cleared IPSec SA from CLI (1 times)
  Wed Apr 08 2020 19:12:12: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020 19:12:12: User cleared IPSec SA from CLI (1 times)
  Wed Apr 08 2020 19:06:52: Peer's IKE-ID validation failed during negotiation (2 times)
  Wed Apr 08 2020
    : Negotiation failed with error code NO_PROPOSAL_CHOSEN received from peer (2 times)
  Wed Apr 08 2020 19:05:26: Peer's IKE-ID validation failed during negotiation (1 times)
  Wed Apr 08 2020
    : Negotiation failed with error code NO_PROPOSAL_CHOSEN received from peer (1 times)
  Wed Apr 08 2020 19:04:26: Peer's IKE-ID validation failed during negotiation (1 times)
  Wed Apr 08 2020
    : Negotiation failed with error code NO_PROPOSAL_CHOSEN received from peer (1 times)
  Wed Apr 08 2020 19:03:26: Peer's IKE-ID validation failed during negotiation (1 times)
Direction: inbound, SPI: aff3ac30, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1093 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 453 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
  Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 40539d12, AUX-SPI: 0
, VPN Monitoring: -
  Hard lifetime: Expires in 1093 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 453 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
  Anti-replay service: counter-based enabled, Replay window size: 64

```



```
show security ike security-associations ??? ?? ?? IKE(Internet Key Exchange) 1?? SA? ?????. SA? ????? ??
?? ??, 1?? ???? ???? ?? ?????. ????? IKE(Internet Key Exchange) ?? ?? ?? ?? ?????? ???? ??????.
```

- `? ? ? - ? ? ? IKE(Internet Key Exchange)? ? ? ? ? SA? ? ? ? ? show security ike security-associations index detail? ? ? ? ?`.
- Remote address - `? IP ? ? ? ? ? 4500? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- `? ? ? ? ?`
- `? - 1?? SA? ? ? ? ? ? ? ?`.
- `? - 1?? SA? ? ? ? ? ? ? ? ? ? ? ? ? ?`.
- Peer IKE ID - `??? ? ID? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? chicago?`.

- ID ID - .
  - - .
- .
- (IKE )
  - IKE(Internet Key Exchange)
  - 
  - 1 ( )

show security ike security-associations (SA) .

- 
- 1
- ( )
- 

.

- 
- IPsec SA
- 2

IPsec

IPsec .

show security ipsec security-associations . show security ipsec security-associations index *index\_number* detail .

```
user@host> show security ipsec security-associations
```

```
Total active tunnels: 1      Total Ipsec sas: 1
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
```

```
<67108878 ESP:3des/md5 40539d12 939/ unlim - root 23434 1.1.100.23
>67108878 ESP:3des/md5 aff3ac30 939/ unlim - root 23434 1.1.100.23
```

```
user@host> show security ipsec security-associations detail
```

```
ID: 67108878 Virtual-system: root, VPN Name: first_vpn
Local Gateway: 13.168.11.100, Remote Gateway: 1.1.100.23
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv1
DF-bit: clear, Copy-Outer-DSCP Disabled, Policy-name: pol1
Port: 23434, Nego#: 8, Fail#: 0, Def-Del#: 0 Flag: 0x608829
Multi-sa, Configured SAs# 1, Negotiated SAs#: 1
Tunnel events:
  Wed Apr 08 2020 19:14:22: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020 19:14:15: User cleared IPSec SA from CLI (1 times)
  Wed Apr 08 2020 19:13:39: IPSec SA negotiation successfully completed (3 times)
  Wed Apr 08 2020 19:13:39: IKE SA negotiation successfully completed (4 times)
  Wed Apr 08 2020
  : IPSec SA delete payload received from peer, corresponding IPSec SAs cleared (1 times)
  Wed Apr 08 2020 19:10:39: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020 19:10:20: User cleared IPSec SA from CLI (1 times)
  Wed Apr 08 2020 19:10:08: IPSec SA negotiation successfully completed (1 times)
  Wed Apr 08 2020
  : Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
Direction: inbound, SPI: 40539d12, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 930 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 335 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: aff3ac30, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 930 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 335 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-md5-96, Encryption: 3des-cbc
Anti-replay service: counter-based enabled, Replay window size: 64
```



??

show security ipsec security-associations ??? ??? ?? ??? ?????.

- ?? ?????? ????? ?? ??(NAT) ??? 1.1.100.23???
- IPsec SA ??? ? ?? ?? ?? 4500? ????? ???, ?? NAT-T? ?????? ??????. (NAT-T? ?? 4500 ?? ?? ??? ? ?? ????? ??????)
- SPI, ??(? ??) ? ?? ??(?? KB? ?? ??)? ?????? ??????. 3571/ ??? ?? 2?? ??? 3571? ?? ?????, ?? ??? ????? ?? ?????? ??????. 2?? ??? VPN? up? ? 1??? ????? ?? ??? 1?? ??? ?? ? ?????.
- VPN ????? Mon ??? ?????? ??????, ? SA?? ?????? ?????. VPN ?????? ????? ??, U? ?????? up ????? D? ??? down ?????? ??????.
- ?? ???(vsys)? ?? ?????? ?? O? ??????.

## SEE ALSO

[IPsec ?? | 11](#)

[?? ?? IPsec VPN ?? | 327](#)

## ?: ?? ?????? VPN? ??? NAT-T ??

### in this section

- [?? ?? | 727](#)
- [?? | 728](#)
- [?? | 730](#)
- [?? | 746](#)

? ?? IKEv2 ?????? ????? ?? ??(NAT) ?????? ?? ?? ?? ?????? ?? ?? VPN? ?????? ??? ??????.

?? ??

? ??? ?????? ?????? ? ?????? ?? ??? ??? ?????.

- ?? ?????? ??? SRX ??? ??? 2?

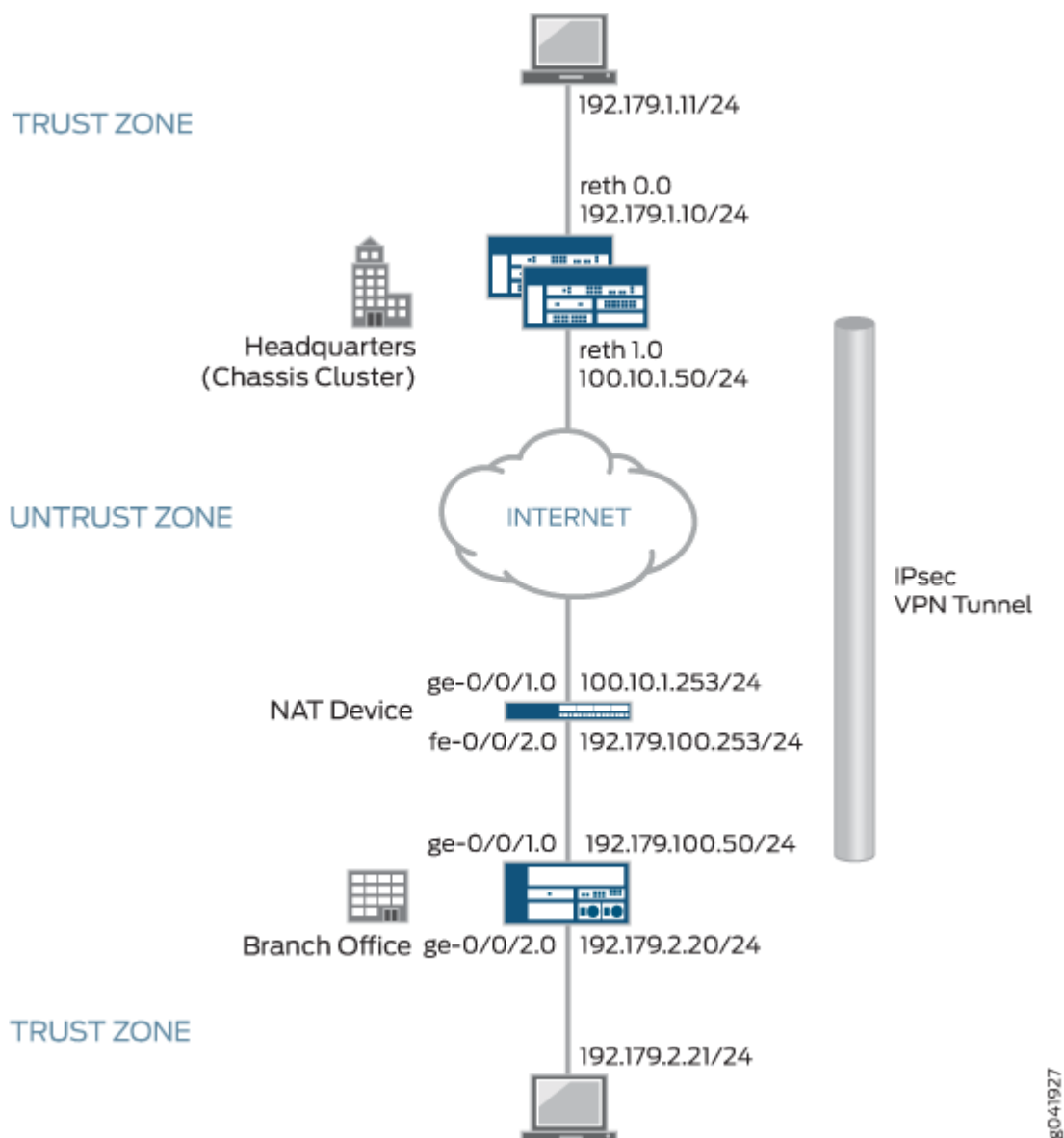
- `?? ?? (NAT)? ???? SRX ??? ? 1?`
- `??? ???? ???? ???? SRX ??? ? 1?`
- IKEv2 NAT-T `??? ? Junos OS ??? 12.1X46-D10 ? ? ?`

??

1 2222 222 222(IKEv2 222)2 22(IKEv2 222) 222 IPSec VPN2 222 2 22 22 2222 2222 22222. 222 2222 2222  
 22 22(NAT) 2222 22 2222. 222 222 222 2222 2222 2222 2 2 2222. 2222 22 222 22 2222 22 ID2 22222. 2 2  
 22 2222 22 22(NAT) 2222 222 22 22 22 22222 VPN2 222222.

44 729 NAT-Traversal (NAT-T) VPN

# ?? 44: ?? ????? VPN? ??? NAT-T



? ????? ?????? ????? ??? ????? IP ?? 192.179.100.50? ????? ?? ??(NAT) ?????? ?? ??? ??? 100.10.1.253??  
 ??????.

? ????? ?? ?? ??? ?????.

- ????? ?? ID? ????? ??? ?? ????? ID? ????? ???.
- ????? ?? 1?? ? 2?? ??? ????? ???.

? ????? ?? ????? ????? ?? ?? ??? ?? ?????? ??????, ?? ??? ?? ?? ? ????? ?? ??? ????? ???, ?? ?? ??? ??????.

??

## in this section

- [IKEv2 \(IKEv2\) ?? | 730](#)
- [\(NAT\) \(NAT\) ?? | 735](#)
- [\(IKEv2 \(IKEv2\) ?? | 739](#)

[IKEv2 \(IKEv2\) ??](#)

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ???? ???? ???? ???? ???? ???? ???? [edit] ?  
 ? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set interfaces ge-0/0/1 unit 0 family inet address 192.179.100.50/24
set interfaces ge-0/0/2 unit 0 family inet address 192.179.2.20/24
set interfaces st0 unit 0 family inet address 172.168.100.1/16
set routing-options static route 192.179.1.0/24 next-hop st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway HQ_GW ike-policy IKE_POL
set security ike gateway HQ_GW address 100.10.1.50
set security ike gateway HQ_GW local-identity hostname branch.example.net
set security ike gateway HQ_GW external-interface ge-0/0/1.0
set security ike gateway HQ_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
```

```

set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn HQ_VPN bind-interface st0.0
set security ipsec vpn HQ_VPN ike gateway HQ_GW
set security ipsec vpn HQ_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn HQ_VPN establish-tunnels immediately
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ?? ????.

??? ??? ???? ???? ????.

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 192.179.100.50/24
user@host# set ge-0/0/2 unit 0 family inet address 192.179.2.20/24
user@host# set st0 unit 0 family inet address 172.168.100.1/16

```

2. ??? ??? ????.

```

[edit routing-options]
user@host# set static route 192.179.1.0/24 next-hop st0.0

```

3. ??? ????.

```

[edit security zones security-zones trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/2.0
[edit security zones security-zones untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.0

```

## 4. 1?? ???? ?????.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy IKE_POL]
user@host# set proposals IKE_PROP
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security ike gateway HQ_GW]
user@host# set ike-policy IKE_POL
user@host# set address 100.10.1.50
user@host# set local-identity hostname branch.example.net
user@host# set external-interface ge-0/0/1.0
user@host# set version v2-only
```

## 5. 2?? ???? ?????.

```
[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy IPSEC_POL]
user@host# set proposals IPSEC_PROP
user@host# set perfect-forward-secrecy keys group5
[edit security ipsec vpn HQ_VPN]
user@host# set bind-interface st0.0
user@host# set ike gateway HQ_GW
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels immediately
```

## 6. ?? ???? ?????.

```
[edit security policies]
user@host# set default-policy permit-all
```

??

?? ???? show interfaces, show routing-options, show security zones, show security ike, show security ipsec ? show security policies ??? ???? ???? ?????. ??? ???? ???? ???? ???? ? ?? ?? ???? ???? ?????.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 192.179.100.50/24;
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family inet {
      address 192.179.2.20/24;
    }
  }
}
st0 {
  unit 0 {
    family inet {
      address 172.168.100.1/16;
    }
  }
}
[edit]
user@host# show routing-options
static {
  route 192.179.1.0/24 next-hop st0.0;
}
[edit]
user@host# show security zones
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
  }
  protocols {
    all;
  }
}
```

```

    }
}
interfaces {
    ge-0/0/2.0;
}
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.0;
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method pre-shared-keys;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    pre-shared-key ascii-text "$ABC123"
}
gateway HQ_GW{
    ike-policy IKE_POL;
    address 100.10.1.50;
    local-identity hostname branch.example.net;
    external-interface ge-0/0/1.0;
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;

```



```

    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}
vpn HQ_VPN {
    bind-interface st0.0;
    ike {
        gateway HQ_GW;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

?? ?? ?? ?? commit?(?) ??????.

```

```

???? ?? ??(NAT) ????? ??

```

## CLI ?? ??

```

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ??????? ?????, ????? ?? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```

```

set interfaces ge-0/0/1 unit 0 family inet address 100.10.1.253/24
set interfaces fe-0/0/2 unit 0 family inet address 192.179.100.253/24
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/2.0
set security nat source rule-set DYNAMIC from zone trust
set security nat source rule-set DYNAMIC to zone untrust

```

```
set security nat source rule-set DYNAMIC rule R2R3 match source-address 0.0.0.0/0
set security nat source rule-set DYNAMIC rule R2R3 then source-nat interface
set security policies default-policy permit-all
```

??? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

???? ?? ??(NAT)? ???? ?? ???? ???? ????.

### 1. ???? ????.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 100.10.1.253/24
user@host# set fe-0/0/2 unit 0 family inet address 192.179.100.253/24
```

### 2. ??? ????.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/2.0
```

### 3. ??? ? ?(NAT)? ????.

```
[edit security nat source rule-set DYNAMIC]
user@host# set from zone trust
user@host# set to zone untrust
user@host# set rule R2R3 match source-address 0.0.0.0/0
user@host# set rule R2R3 then source-nat interface
```



```

security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/2.0;
    }
}
[edit]
user@host# show security nat source
rule-set DYNAMIC {
    from zone untrust;
    to zone trust;
    rule R2R3 {
        match {
            source-address 0.0.0.0/0;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

?? ?? ?? ?? ?? commit?(?) ??.

```

```
?? ???? (IKEv2 ???) ??
```

CLI ?? ??

```
? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?
? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.
```

```
set chassis cluster reth-count 5
set chassis cluster redundancy-group 1 node 0 priority 220
set chassis cluster redundancy-group 1 node 1 priority 149
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/0/1 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-0/0/2 weight 255
set chassis cluster redundancy-group 1 interface-monitor ge-8/0/2 weight 255
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
set interfaces ge-0/0/2 gigether-options redundant-parent reth1
set interfaces ge-8/0/1 gigether-options redundant-parent reth0
set interfaces ge-8/0/2 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 192.179.1.10/24
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 100.10.1.50/24
set interfaces st0 unit 0 family inet address 172.168.100.2/16
set routing-options static route 192.179.2.0/24 next-hop st0.0
set routing-options static route 192.179.100.0/24 next-hop 100.10.1.253
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces reth1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces reth0.0
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text "$ABC123"
set security ike gateway Branch_GW ike-policy IKE_POL
set security ike gateway Branch_GW dynamic hostname branch.example.net
set security ike gateway Branch_GW dead-peer-detection optimized
set security ike gateway Branch_GW external-interface reth1.0
```

```

set security ike gateway Branch_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn Branch_VPN bind-interface st0.0
set security ipsec vpn Branch_VPN ike gateway Branch_GW
set security ipsec vpn Branch_VPN ike ipsec-policy IPSEC_POL
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

## 1. ??? ???? ? ???? ????.

```

[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 1 node 0 priority 220
user@host# set redundancy-group 1 node 1 priority 149
user@host# set redundancy-group 1 interface-monitor ge-0/0/1 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/0/1 weight 255
user@host# set redundancy-group 1 interface-monitor ge-0/0/2 weight 255
user@host# set redundancy-group 1 interface-monitor ge-8/0/2 weight 255

```

## 2. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/1 gigether-options redundant-parent reth0
user@host# set ge-0/0/2 gigether-options redundant-parent reth1
user@host# set ge-8/0/1 gigether-options redundant-parent reth0
user@host# set ge-8/0/2 gigether-options redundant-parent reth1
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 192.179.1.10/24
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 100.10.1.50/24
user@host# set st0 unit 0 family inet address 172.168.100.2/16

```

3. `???` `???` `?????`.

```
[edit routing-options]
user@host# set static route 192.179.2.0/24 next-hop st0.0
user@host# set static route 192.179.100.0/24 next-hop 100.10.1.253
```

4. `???` `?????`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic protocols all
user@host# set host-inbound-traffic system-services all
user@host# set interfaces st0.0
user@host# set interfaces reth1.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces reth0.0
```

5. `1??` `???` `?????`.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy IKE_POL]
user@host# set proposals IKE_PROP
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security ike gateway Branch_GW]
user@host# set ike-policy IKE_POL
user@host# set dynamic hostname branch.example.net
user@host# set dead-peer-detection optimized
user@host# set external-interface reth1.0
user@host# set version v2-only
```

6. `???` `???` `?????`.

```
[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
```





```

ge-0/0/2 {
    gigether-options {
        redundant-parent reth1;
    }
}
ge-8/0/1 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-8/0/2 {
    gigether-options {
        redundant-parent reth1;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 192.179.1.10/24;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 100.10.1.50/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 172.168.100.2/16;
        }
    }
}
[edit]

```

```

user@host# show routing-options
static {
    route 192.179.2.0/24 next-hop st0.0;
    route 192.179.100.0/24 next-hop 100.10.1.253;
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.0;
        reth1.0;
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method pre-shared-keys;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {

```

```

    proposals IKE_PROP;
    pre-shared-key ascii-text "$ABC123"
}
gateway Branch_GW {
    ike-policy IKE_POL;

    dynamic hostname branch.example.net;
    dead-peer-detection optimized;
    external-interface reth1.0;
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}
vpn Branch_VPN {
    bind-interface st0.0;
    ike {
        gateway Branch_GW;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

??

in this section

- [???? ?? IKE\(Internet Key Exchange\) 1?? ?? ?? | 746](#)
- [???? ?? IPsec ?? ?? ?? | 748](#)

??? ????? ????? ???? ??????.

???? ?? IKE(Internet Key Exchange) 1?? ?? ??

??

IKE(Internet Key Exchange) 1?? ??? ??????.

??

?? 0? ?? ????? show security ike security-associations ??? ??????. ????? ??? ??? ? show security ike security-associations detail ??? ??????.

```
user@host# show security ike security-associations
node0:
Index      State  Initiator cookie  Responder cookie  Mode    Remote Address
1367024684 UP    f82c54347e2f3fb1  020e28e1e4cae003  IKEv2    100.10.1.253
```

```
user@host# show security ike security-associations detail
node0:
IKE peer 100.10.1.253, Index 1367024684, Gateway Name: Branch_GW
  Location: FPC 5, PIC 0, KMD-Instance 2
  Role: Responder, State: UP
  Initiator cookie: f82c54347e2f3fb1, Responder cookie: 020e28e1e4cae003
  Exchange type: IKEv2, Authentication method: Pre-shared-keys
  Local: 100.10.1.50:4500, Remote: 100.10.1.253:2541
  Lifetime: Expires in 3593 seconds
  Peer ike-id: branch.example.net
  Xauth assigned IP: 0.0.0.0
```



show security ike security-associations `???` `??` `??(SA)` `?` `??` `??` `???` `???`.

- `???` `??` `?` `???` `???`
- `1??` `??`
- `???` `??(???? ???? ???? ???? ???? ???? ? ???? ? ???? ?)`
- `??` `??`

`??` `???` `???` `???` `???` `???` `??` `?` `???`.

- `???` `?` `???` `??`
- `???` IPsec SA `?` `?`
- `??` `??` `2??` `??` `?`

`???` `??` IPsec `??` `??` `??`

`??`

IPsec `???` `???`.

`??`

`??` `0?` `??` `???` **show security ipsec security-associations** `???` `???`. `???` `???` `???` `??` `?` **show security ipsec security-associations detail** `???` `???`.

```
user@host# show security ipsec security-associations
```

```
node0
```

```
Total active tunnels: 1
```

| ID        | Algorithm            | SPI      | Life:sec/kb | Mon | lsys | Port | Gateway      |
|-----------|----------------------|----------|-------------|-----|------|------|--------------|
| <77856771 | ESP:aes-cbc-256/sha1 | 4ad5af40 | 7186/unlim  | -   | root | 2541 | 100.10.1.253 |
| >77856771 | ESP:aes-cbc-256/sha1 | 5bb0a5ee | 7186/unlim  | -   | root | 2541 | 100.10.1.253 |

```
user@host# show security ipsec security-associations detail
```

```
node0
```

```
ID: 77856771 Virtual-system: root, VPN Name: Branch_VPN
Local Gateway: 100.10.1.50, Remote Gateway: 100.10.1.253
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
```







# 8

CHAPTER LABEL COVER PAGE

## ?? VPN

---

### in this chapter

- ?? VPNv1 | 752
  - ?? VPNv2 | 802
  - ?? VPNv2 ?? ???? | 860
-

# ?? VPNv1

summary

Junos OS? ?? VPNv1? ?? ?????? ? ??? ??????.

in this section

- ?? VPNv1 ?? | 752
- ?? VPNv1 ?? ?? | 760
- ?? VPNv1? IKE 1?? ?? ?? | 761
- ?? VPNv1? ?? IPsec SA ?? ?? | 762
- ?? VPNv1? ?? ?? ?? | 762
- ?? VPNv1? ?? Antireplay ????? | 763
- ?: ?? VPNv1 ?? ? ??? ?? | 763
- ?: ????? ? ??? ????? ?? ?? VPNv1 ??-?? ?? ? | 784
- ?: ????? ? ??? ????? ?? ?? VPNv1 ??-?? ?? ? | 786
- ?: ?? ?? ????????? ?? VPNv1 ?? | 789

?? VPN? ?????? ?????? ??? ???? ???? WAN? ?? IP ?????? ?? ??? ???? ???? ???? ? ???? ? ???? ??.

## ?? VPNv1 ??

in this section

- ?? VPNv1? ?? GDOI ????? ????? | 755
- ?? VPNv1 ?? ?? ?? | 755
- ?? VPNv1 ?? ? ??? ????? | 756
- ?? VPNv1 ??-?? ?? ????? | 757
- ?? VPNv1 ?? ?? ?? ?? | 757
- ?? VPNv1 ????? ???? ????? | 759

● [VPNv1 22-22 22222 22 2222 | 760](#)

IPsec SA(22 22)2 22 2 222 2222, 2 22 2222 2 22 2222 222 2222 VPN(22 222) 222 22 222 22222. 22  
VPN 2222 SA2 2 22 2222 22 22 2 22222. 22 VPNv12 IPsec 22222 2222 22 2222 222 2222 SA2 22222( 22  
[22 45 222 754](#)).





- [illegible]

?? VPNv1 ?? ? ???? ???? ?

?? VPN? ??? ?? ??????. ?? ??? ?? ??? ?????.

- [?] [?] [?] [?] [?] [?] [?]
- [?] [?] [?] [?]
- [?] SA [?] [?] [?] [?] [?] [?] [?] [?] [?] [?]

**SAT**

?? ???? ?? ???? ????? ???? ? ?????. ?? ?? ?????? ?? ???? ????? ? ? ?????.

[ 222 122 65,535 222 222 22 2222 22222, 22 22 2 22 222 22 22 22222, 222 222 22 2222 22 2 222  
 22 222 222 22 2222 222 2 2222

**VPN**

1. `?? ???? ???? ? ???? UDP ?? 848?? ? ?????. ?? ????? ???? ???? ? ???? IKE(Internet Key Exchange) 1?? ??? ???? ??. ??? ??? ? ? ? ???? ?????.`
2. `?? ? ??? ???? ? ???? GDOI groupkey-pull ??? ? ???? ? SA ? ? ????.`

3. `vpn group vpn group vpn group`.

4. `vpn group vpn SA vpn group vpn group`.

`vpn group vpn group(GDOI groupkey-push) vpn group vpn group SA vpn group vpn group. vpn group vpn group SA vpn group vpn group`  
`vpn group vpn group vpn group vpn group vpn group vpn group vpn group vpn group vpn group.`

`vpn group vpn group vpn group vpn group SA vpn group vpn group vpn group vpn group vpn group vpn group vpn group.`

## VPNv1 vpn-vpn vpn vpn

`vpn vpn vpn vpn vpn GDOI groupkey-push vpn vpn vpn vpn vpn. vpn vpn vpn vpn vpn vpn vpn vpn vpn GDOI`  
`groupkey-pull vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn.`

`vpn vpn vpn [edit security group-vpn server] vpn vpn server-member-communication vpn vpn vpn vpn. vpn vpn`  
`vpn vpn vpn.`

- `vpn vpn vpn vpn vpn vpn vpn vpn. 3des-cbc, aes-128-cbc, aes-192-cbc, aes-256-cbc vpn des-cbc vpn`  
`vpn vpn. vpn vpn vpn vpn.`
- `vpn vpn vpn vpn vpn vpn vpn vpn(md5 vpn sha1)vpn. vpn vpn vpn vpn.`
- `vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn.`
- `vpn vpn vpn vpn vpn vpn vpn vpn vpn. vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn, vpn vpn vpn vpn vpn vpn`  
`vpn vpn. vpn vpn 300vpn.`
- `KEK(vpn vpn)vpn vpn. vpn 3600vpn.`

`vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn, vpn vpn vpn vpn vpn vpn, vpn vpn vpn vpn vpn vpn`  
`vpn(vpn: vpn) vpn vpn vpn vpn vpn vpn vpn IP vpn vpn vpn vpn vpn. vpn vpn vpn vpn vpn vpn vpn vpn`  
`vpn vpn vpn vpn vpn vpn. GDOI vpn vpn vpn VPN(Internet Key Exchange) 1vpn SA vpn vpn vpn vpn vpn vpn`  
`vpn vpn vpn.`

`vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn show security group-vpn server registered-members vpn vpn vpn vpn`  
`vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn vpn. vpn vpn vpn vpn vpn vpn vpn vpn`  
`vpn show security group-vpn server registered-members vpn vpn vpn vpn vpn vpn. vpn vpn vpn vpn show security`  
`group-vpn server registered-members vpn vpn vpn vpn vpn vpn vpn vpn vpn. vpn vpn vpn vpn vpn vpn vpn`  
`vpn vpn vpn vpn vpn vpn.`

## VPNv1 vpn vpn vpn vpn

`vpn vpn vpn vpn vpn.`

?? ?

?? ??? VPN ??, ?? ??? ? ?? ? ?? ??? ????? ?? ??????? ?? ?????, ??? ????? ??????? ?? ??? ? ?? ??? ?? ?.

- KEK(Key Encryption Key) - ? ??? ????? ????? ? ?????, ??? ??? KEK ?????.
- ??? ??? ?(TEK) - ?? ?? ?? IPsec ??? ????? ????? ? ?????.

SA? ??? ? ???? ????? ?? ??? ?? ????? ?? ??? ??????, ??? ?? ?? VPN? ?? ?????? ?? ? ????.

??? ? ???

??? ?? ??? ??? ?? ??? ? ??? ? ???(GDOI groupkey-push) ????? ?? ? ????? SA ? ? ?? ??? ????? ?????, ? ?  
?? ????? SA? ????? ?? ?????, ??? ?? ?? ??? ? ???? ????? ? ??? ?? ??? ? ????.

?? ??? ? ???? ?????? ?? SA? ??? ?(? : ?? ?? ?? ?? ?) ????? ? ?? ????? ? ? ??? ????? ?????.

??? ?? ?????? ? ???? ????? ? ? ??? ????? ?? ??? ?? ??? ????? ???. ??? ??? ?? ????? ????? ? ???? ? ? ?  
? ???? ?????.

? ??? ????? ? ?? ??? ?????.

- ????? ? ??? ??? - ?? ??? ? ?? ????? ? ??? ????? ?? ??? ?????, ? ??? ????? ????? ????? ???? (ACK)? ??  
? ???, ??? ?????? ACK? ????? ???(? ??? ??? ?? ?) ??? ????? ??? ?? ??? ????? ?? ????? ?????, ??? ?  
? ?? ? ??? ??? ????? ?????.

?? ?? ??? ? ? retransmission-period ?? ?? number-of-retransmission ????? ACK? ????? ? ? ??? ? ? ? ?  
???? ?????.

- ????? ? ??? ??? - ?? ??? ??? ?? ??????? ???? ????? ?? ??? ? ??? ????? ??? ??? ?????, ??? ????? ? ?  
? ??? ? ???? ???? ?????, ??? ?? ??? ? ? ? ? ???? ? ? ????? ? ???? ???? ? ???? ? ???? ? ?  
?? ????? ?????? ????? ????.

?????? ?????? ??? ? ???? IP ????? ?????? ????? ??, ??? ????? ?????? ?????? ????? ?? ?? ? ?  
[????? ???? ???? ???? ???? ??????](#)

??? ? ??? ????? ???? ??? [edit security group-vpn server group] ??? ?? ? activation-time-delay ?? ?? ?  
lifetime-seconds ????? ?????, ??? ? lifetime-seconds minus 4\*(activation-time-delay)????.

KEK? ?? ?? lifetime-seconds ??? ??? ???? ????? 3600????, TEK? ?? lifetime-seconds IPsec ??? ?? ????  
?, ????? 3600????, ? (activation-time-delay ?) ??? ?? ? ???? ????? 15????, ? ? ?? lifetime-seconds ????? ?  
?? ??? ? ???? ????? ???? , ?? 3540????3600 minus 4\*15.activation-time-delay



???)

?? ???? ?? ???? ???? ? SA ?? ?? ?? ???? ???? ???? GDOI groupkey-pull ??? ???? ???? ?  
 ??, ? ?? ???? ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 time-delay? ???? lifetime-seconds ? ???? ???? ? ???? ???? ???? ???? 3600 - 3\*15 ?? 3555????.

?? ???? ???? ???? ???? ???? ? ????.

- ???? ???? ???? ???? ???? ???? ???? ????.
- ?? ???? ? ???? ???? ???? ???? ???? TEK ???? ????.

? ???

??? ???? ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ??? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

???? ???? ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

??? ???? ???? ? ???? SA? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

?? VPNv1 ???? ???? ???? ???? ???? VPNv1 ???? ???? ???? ???? ?(TEK)? ???? ? ???? groupkey-pull . ???? ?  
 VPNv1 ???? ???? TEK ? ???? ???? ???? TEK? ???? ???? ???? ????.

- ?? VPNv1 ???? ? ???? TEK? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ???? ???? VPNv1 ???? ???? ???? ???? ? activation-time-delay ?? TEK? ???? ???? (15?).
- ?? VPNv1 ???? ???? TEK? ???? ???? ???? ???? ???? groupkey-push TEK? ???? ???? ???? ???? ???? ?  
 ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

?? VPNv1 ???? TEK ???? ???? 2? ???? ???? ???? TEK? activation-time-delay ????.

?? VPNv1 ???? ???? ???? ???? ???? ?

?? ???? ???? ???? ???? ???? VPNv1 ???? ???? ???? ???? 300?) ???? ???? ???? ???? ???? ?  
 ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

???? ???? ???? groupkey-push ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?  
 ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ?

???? ???? ???? ???? ???? ?





## ?? VPNv1? ?? IPsec SA ?? ??

??? ??? 1?? ????? ????? ??? ??? ? 2??? ??????. 2?? ??? ?? ?? ????? ?????? ??? ?? ??? ????? IPsec SA? ??????. ?? VPN? ?? IPsec SA ??? ?? VPN? ?? ??? ??????, ?? ??? ?? ?? ??? SA? ??? ??? ?????.

?? VPNv1? ?? 2?? IPsec ??? ?? ??? ?????.

- SA? ??? ?? ?????, ?? ? ??? ?????? ?? ??????. IPsec SA ??? [edit security group-vpn server ipsec] ??? proposal *?? ??*????? ?? ????? ??????.
- ??? ????? ?? ??????. ?? ??? SA? ?? ????? ????(????, ?? ??, ?? ??, ?? ?? ? ?? ??)?? ??????. ?? ??? [edit security group-vpn server group] ??? ?? ?? ????? ipsec-sa ????? ??????.
- ?? ???, ?? ??(?? ??? ike-gateway ???) ? ??? ??? ????? ? ????? ?????? ????? ?? ? IKE(Internet Key Exchange)?????. ?? ? IKE(Internet Key Exchange)? [edit security group-vpn member] ??? ?? ?? ????? ipsec vpn ??? ??????.

## ?? VPNv1? ?? ?? ??

?? ??? ??? ??? ?????? ?? SA ? ?? ??????. ??? ??? ?? ?? ??? ??? IPsec SA ??? ??? ? ??????. ??? ??? ?? ??? ?? SA? ?? ?? ??? ????? ?? ??????. ?? ??? ??? SA? ?? SA? ??? ?? ? ??? ??? ?? ??? ?? ??????.

VPN ????? ??? ?????? ?????? ? ?? SA ? ?? ?? ??? ??????. ?? ??? ?????, ?? ??, ?? ??, ?? ?? ? ?? ??? ?????? ?? ????? ?? ????? ??????.

??? ?? ??(???? ?? ??, ?? ??, ?? ??, ?? ?? ? ????? ??? ?????)? ?? ??? ?? ??? ? ?????. ??? ?? ??? ?? ??? ?????? ????? ?????? ?? ??? ??????. ? ?? ??? ?? ?? ? ??? ?????? ???.

?? ?????? ?????? ?????? ?? ??? ??? ?????? ?? ??? ?????? ???. ????? ??? ?? ??? ??? ??? ?? ??? ??????. ????? ? ? ??? ?????? ?? ??? ?????? ???.

- ?? ??? ??? ?? ??? ?? ??? ??? ?? ?? ?? ??? ???.
- ?? ??? ??? ?? ??, ?? ?? ? ?????? ?? ??? ??? ?? ????? ???.

???? ??? ?? ??? ?? ?????? ???.

?? ??? ?? from-zone ? to-zone ?????? ?? ?? ??? ??? ??? ? ?????. Junos OS? ?? ?? ??? ? ??? ?????? ?? ?? ?? ?? ??? ??????.

??? ??? ?? ?? ?? ??? ?? ??? ??? ?? ?? ?? ??? ?? ? ?? ????? ?????.

- ?? ??? ?????? ?? ?????? ??? ?? ??? ?????? ?? ?? ??? ?????? ?????.



● 781

SA IPsec VPNv1

??

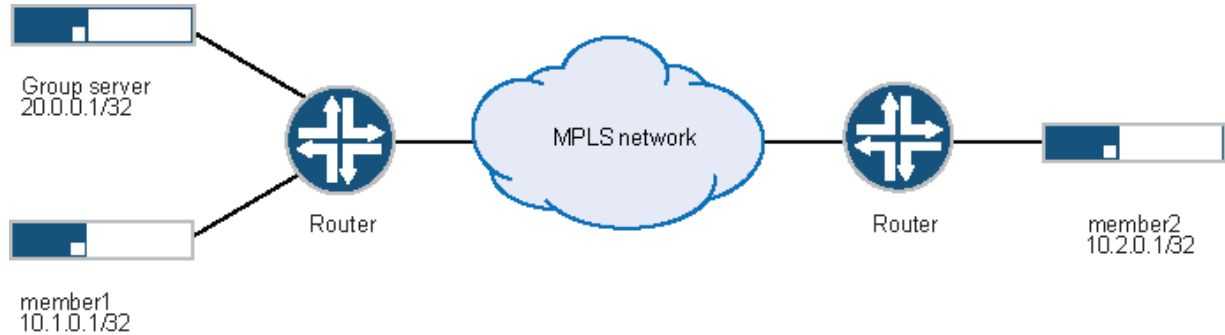
??:

- 
- 

??

VPN(member1 member2) IP 20.0.0.1

46: ??



VPN SA 1 SA VPN IKE(Internet Key Exchange) 1

??

- p1—10.1.0.0/16 10.2.0.0/16
- p2—10.2.0.0/16 10.1.0.0/16
- p3—10.1.1.1/32

member1 10.0.0.0/8 member1

```
member2 [redacted] 10.1.0.0/16[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] 10.1.0.0/16[redacted] [redacted] [redacted] [redacted] [redacted] [redacted]. [redacted] SA [redacted] p2[redacted] member2[redacted] [redacted].
```

??

**in this section**

- ?? ?? ?? | 765
- Member1 ?? | 769
- Member2 ?? | 774

?? ?? ??

CLI

```
? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ?????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.
```

```
set interfaces lo0 unit 0 family inet address 20.0.0.1/32
set security group-vpn server ike proposal srv-prop authentication-method pre-shared-keys
set security group-vpn server ike proposal srv-prop dh-group group2
set security group-vpn server ike proposal srv-prop authentication-algorithm sha1
set security group-vpn server ike proposal srv-prop encryption-algorithm 3des-cbc
set security group-vpn server ike policy srv-pol mode main
set security group-vpn server ike policy srv-pol proposals srv-prop
set security group-vpn server ike policy srv-pol pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike gateway gw1 ike-policy srv-pol
set security group-vpn server ike gateway gw1 address 10.1.0.1
set security group-vpn server ike gateway gw2 ike-policy srv-pol
set security group-vpn server ike gateway gw2 address 10.2.0.1
set security group-vpn server ipsec proposal group-prop authentication-algorithm hmac-sha1-96
set security group-vpn server ipsec proposal group-prop encryption-algorithm 3des-cbc
set security group-vpn server ipsec proposal group-prop lifetime-seconds 3600
set security group-vpn server group grp1 group-id 1
set security group-vpn server group grp1 ike-gateway gw1
set security group-vpn server group grp1 ike-gateway gw2
set security group-vpn server group grp1 anti-replay-time-window 120
set security group-vpn server group grp1 server-address 20.0.0.1
```

```

set security group-vpn server group grp1 ipsec-sa group-sa proposal group-prop
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 source 10.1.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 destination
10.2.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 protocol 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 source 10.2.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 destination
10.1.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 protocol 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 source 10.1.1.1/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 destination
239.1.1.1/32
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 protocol 0

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ??????.

?? ??? ?????? ??? ??????.

1. ?????? ??? ??? ??????.

```

[edit]
user@host# edit interfaces
user@host# set lo0 unit 0 family inet address 20.0.0.1/32

```

2. IKE(Internet Key Exchange) 1?? SA? ??????(? ??? ?? ??? ??? 1?? SA? ????? ?).

```

[edit security group-vpn server ike proposal srv-prop]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm 3des-cbc

```



### 3. IKE(Internet Key Exchange) `?? ???? ? ???? ????.`

```
[edit security group-vpn server ike]
user@host# set policy srv-pol mode main proposals srv-prop pre-shared-key ascii-text "$ABC123"
user@host# set gateway gw1 ike-policy srv-pol address 10.1.0.1
user@host# set gateway gw2 ike-policy srv-pol address 10.2.0.1
```

### 4. `?? SA ?? ????.`

```
[edit security group-vpn server ipsec proposal group-prop]
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm 3des-cbc
user@host# set lifetime-seconds 3600
```

### 5. `?? ??? ? IKE(Internet Key Exchange) ????? ????.`

```
[edit security group-vpn server group grp1]
user@host# set group-id 1
user@host# set ike-gateway gw1
user@host# set ike-gateway gw2
user@host# set anti-replay-time-window 120 server-address 20.0.0.1
```

### 6. `?? ? ??? ????.`

```
[edit security group-vpn server group grp1]
user@host# set server-member-communication communication-type unicast encryption-algorithm
aes-128-cbc sig-hash-algorithm md5 certificate "srv-cert"
```

### 7. `?? ????? ???? ? ? ? ????.`

```
[edit security group-vpn server group grp1 ipsec-sa group-sa]
user@host# set proposal group-prop match-policy p1 source 10.1.0.0/16 destination 10.2.0.0/16
source-port 0 destination-port 0 protocol 0
user@host# set proposal group-prop match-policy p2 source 10.2.0.0/16 destination 10.1.0.0/16
source-port 0 destination-port 0 protocol 0
user@host# set proposal group-prop match-policy p3 source 10.1.1.1/16 destination
239.1.1.1/32 source-port 0 destination-port 0 protocol 0
```

??

?? ???? show security group-vpn server ??? ???? ???? ?????. ??? ??? ???? ???? ???? ? ?? ?? ???? ???? ????  
?.

```
[edit]
user@host# show security group-vpn server
ike {
  proposal srv-prop {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
  }
  policy srv-pol {
    mode main;
    proposals srv-prop;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
  }
  gateway gw1 {
    ike-policy srv-pol;
    address 10.1.0.1;
  }
  gateway gw2 {
    ike-policy srv-pol;
    address 10.2.0.1;
  }
}
ipsec {
  proposal group-prop {
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
  }
}
group grp1 {
  group-id 1;
  ike-gateway gw1;
  ike-gateway gw2;
  anti-replay-time-window 120;
  server-address 20.0.0.1;
  ipsec-sa group-sa {
```



```

set security group-vpn member ike gateway g1 address 20.0.0.1
set security group-vpn member ike gateway g1 local-address 10.1.0.1
set security group-vpn member ipsec vpn v1 ike-gateway g1
set security group-vpn member ipsec vpn v1 group-vpn-external-interface ge-0/1/0
set security group-vpn member ipsec vpn v1 group 1
set security address-book book1 address 10_subnet 10.0.0.0/8
set security address-book book1 attach zone trust
set security address-book book2 address 10_subnet 10.0.0.0/8
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy scope1 match source-address
10_subnet
set security policies from-zone trust to-zone untrust policy scope1 match destination-address
10_subnet
set security policies from-zone trust to-zone untrust policy scope1 match application any
set security policies from-zone trust to-zone untrust policy scope1 then permit tunnel ipsec-
group-vpn v1
set security policies from-zone untrust to-zone trust policy scope1 match source-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope1 match destination-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope1 match application any
set security policies from-zone untrust to-zone trust policy scope1 then permit tunnel ipsec-
group-vpn v1

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

member1? ???? ???? ????.

1. 1?? SA? ?????(? ??? ?? ??? ??? 1?? SA? ???? ?).

```

[edit security group-vpn member ike proposal prop1]
user@member1# set authentication-method pre-shared-keys
user@member1# set dh-group group2
user@member1# set authentication-algorithm sha1
user@member1# set encryption-algorithm 3des-cbc

```

## 2. IKE(Internet Key Exchange) ??? ???? ?? ?????? ??????.

```
[edit security group-vpn member ike]
user@member1# set policy pol1 mode main proposals prop1 pre-shared-key ascii-text "$ABC123"
user@member1# set gateway g1 ike-policy pol1 address 20.0.0.1 local-address 10.1.0.1
```

3. member1? ?? ?? ???, IKE(Internet Key Exchange) ????? ? ?????? ??????.

```
[edit security group-vpn member ipsec]
user@member1# set vpn v1 group 1 ike-gateway g1 group-vpn-external-interface ge-0/1/0
```

?? ?? ???? ???? ? ? ???? MPLS ????? ? ???? ????? 1400??? ?? ? ? ? ?(MTU) ?? ????  
 ?? ?????. set *interface* mtu ?? ? ? ???? MTU ?? ? ????.

**4.**                         .

```
[edit security address-book book1]
user@member1# set address 10_subnet 10.0.0.0/8
user@member1# set attach zone trust
```

```
[edit security address-book book2]
user@member1# set address 10_subnet 10.0.0.0/8
user@member1# set attach zone untrust
```

5. [ ] [ ] 10.0.0.0/8 [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ].

```
[edit security policies from-zone trust to-zone untrust]
user@member1# set policy scope1 match source-address 10_subnet destination-address 10_subnet
application any
user@member1# set policy scope1 then permit tunnel ipsec-group-vpn v1
```

6. [ ] [ ] 10.0.0.0/8 [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ].

```
[edit security policies from-zone untrust to-zone trust]
user@member1# set policy scope1 match source-address 10_subnet destination-address 10_subnet
application any
user@member1# set policy scope1 then permit tunnel ipsec-group-vpn v1
```

??

?? ???? show security group-vpn member ? show security policies ??? ???? ???? ?????. ??? ??? ???? ???? ???? , ?  
 ?? ?? ???? ???? ????.

```
[edit]
user@member1# show security group-vpn member
ike {
  proposal prop1 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
  }
  policy pol1 {
    mode main;
    proposals prop1;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
  }
  gateway g1 {
    ike-policy pol1;
    address 20.0.0.1;
    local-address 10.1.0.1;
  }
}

ipsec {
  vpn v1 {
    ike-gateway g1;
    group-vpn-external-interface ge-0/1/0;
    group 1;
  }
}
```

```
[edit]
user@member1# show security policies
from-zone trust to-zone trust {
  policy default-permit {
    match {
      source-address any;
      destination-address any;
      application any;
```

```

    }
    then {
        permit;
    }
}
}

from-zone trust to-zone untrust {
    policy scope1 {
        match {
            source-address 10_subnet;
            destination-address 10_subnet;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v1;
                }
            }
        }
    }
    policy default-permit {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}

from-zone untrust to-zone trust {
    policy scope1 {
        match {
            source-address 10_subnet;
            destination-address 10_subnet;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v1;
                }
            }
        }
    }
}

```





```

set security address-book book1 attach zone trust
set security address-book book2 address 10_subnet 10.0.0.0/8
set security address-book book2 address 10_1_0_0_16 10.1.0.0/16
set security address-book book2 address multicast_net 239.0.0.0/8
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy deny2 match source-address
10_1_0_0_16
set security policies from-zone trust to-zone untrust policy deny2 match destination-address any
set security policies from-zone trust to-zone untrust policy deny2 match application any
set security policies from-zone trust to-zone untrust policy deny2 then reject
set security policies from-zone trust to-zone untrust policy scope2 match source -address
10_subnet
set security policies from-zone trust to-zone untrust policy scope2 match destination-address
10_subnet
set security policies from-zone trust to-zone untrust policy scope2 match application any
set security policies from-zone trust to-zone untrust policy scope2 then permit tunnel ipsec-
group-vpn v2
set security policies from-zone trust to-zone untrust policy multicast-scope2 match source-
address 10_subnet
set security policies from-zone trust to-zone untrust policy multicast-scope2 match destination-
address multicast-net
set security policies from-zone trust to-zone untrust policy multicast-scope2 match application
any
set security policies from-zone trust to-zone untrust policy multicast-scope2 then permit tunnel
ipsec-group-vpn v2
set security policies from-zone untrust to-zone trust policy deny2 match source-address any set
security policies from-zone untrust to-zone trust policy multicast-scope2 ma tch application any
set security policies from-zone untr
set security policies from-zone untrust to-zone trust policy deny2 match destination-address
10_1_0_0_16
set security policies from-zone untrust to-zone trust policy deny2 match application any
set security policies from-zone untrust to-zone trust policy deny2 then reject
set security policies from-zone untrust to-zone trust policy scope2 match source-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope2 match destination-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope2 match application any
set security policies from-zone untrust to-zone trust policy scope2 then permit tunnel ipsec-
group-vpn v2
set security policies from-zone untrust to-zone trust policy multicast-scope2 match source-
address 10_subnet
set security policies from-zone untrust to-zone trust policy multicast-scope2 match destination-
address multicast-net

```

```
set security policies from-zone untrust to-zone trust policy multicast-scope2 match application
any
set security policies from-zone untrust to-zone trust policy multicast-scope2 then permit tunnel
ipsec-group-vpn v2
```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ???? ?????.

member2? ?????:

1. 1?? SA? ????(? ???? ???? ???? 1?? SA? ???? ?).

```
[edit security group-vpn member ike proposal prop2]
user@member2# set authentication-method pre-shared-keys
user@member2# set dh-group group2
user@member2# set authentication-algorithm sha1
user@member2# set encryption-algorithm 3des-cbc
```

2. IKE(Internet Key Exchange) ??? ???? ? ???? ????.

```
[edit security group-vpn member ike]
user@member2# set policy pol2 mode main proposals prop2 pre-shared-key ascii-text "$ABC123"
user@member2# set gateway g2 ike-policy pol2 address 20.0.0.1 local-address 10.2.0.1
```

3. member2? ?? ?? ??, IKE(Internet Key Exchange) ???? ? ???? ????.

```
[edit security group-vpn member ipsec]
user@member2# set vpn v2 group 1 ike-gateway g2 group-vpn-external-interface ge-0/1/0
```

?? ??? ???? ???? ? ? ???? MPLS ???? ? ???? ???? 1400??? ???? ? ? ??(MTU) ??? ????  
 ?? ?????. set *interface* mtu ?? ?? ???? MTU ??? ????.

4. ???? ???? ???? ? ????.

```
[edit security address-book book1]
user@member2# set address 10_subnet 10.0.0.0/8
user@member2# set address 10_1_0_0_16 10.1.0.0/16
```

```
user@member2# set address multicast_net 239.0.0.0/8
user@member2# set attach zone trust
```

5. `?? ???? ???? ??? ? ? ???? ?????.`

```
[edit security address-book book2]
user@member2# set address 10_subnet 10.0.0.0/8
user@member2# set address 10_1_0_0_16 10.1.0.0/16
user@member2# set address multicast_net 239.0.0.0/8
user@member2# set attach zone untrust
```

6. `???? ???? 10.1.0.0/16? ???? ???? ???? ???? ? ? ? ????.`

```
[edit security policies from-zone trust to-zone untrust]
user@member2# set policy deny2 match source-address 10_1_0_0_16 destination-address any
application any
user@member2# set policy deny2 then reject
user@member2# set policy scope2 match source-address 10_subnet destination-address 10_subnet
application any
user@member2# set policy scope2 then permit tunnel ipsec-group-vpn v2
user@member2# set policy multicast-scope2 match source-address 10_subnet destination-address
multicast-net application any
user@member2# set policy multicast-scope2 then permit tunnel ipsec-group-vpn v2
```

7. `??? ? ? ???? 10.1.0.0/16? ? ???? ???? ??? ? ? ???? ? ? ? ????.`

```
[edit security policies from-zone untrust to-zone trust]
user@member2# set policy deny2 match source-address any destination-address 10_1_0_0_16
application any
user@member2# set policy deny2 then reject
user@member2# set policy scope2 match source-address 10_subnet destination-address 10_subnet
application any
user@member2# set policy scope2 then permit tunnel ipsec-group-vpn v2
user@member2# set policy multicast-scope2 match source-address 10_subnet destination-address
multicast-net application any
user@member2# set policy multicast-scope2 then permit tunnel ipsec-group-vpn v2
```

??

?? ???? show security group-vpn member ? show security policies ??? ???? ???? ?????. ??? ??? ???? ???? ???? , ?  
 ?? ?? ???? ???? ?????.

```
[edit]
user@member2# show security group-vpn member
ike {
  proposal prop2 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
  }
  policy pol2 {
    mode main;
    proposals prop2;
    pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
  }
  gateway g2 {
    ike-policy pol2;
    address 20.0.0.1;
    local-address 10.2.0.1;
  }
}

ipsec {
  vpn v2 {
    ike-gateway g2;
    group-vpn-external-interface ge-0/1/0;
    group 1;
  }
}
```

```
[edit]
user@member2# show security policies
from-zone trust to-zone trust {
  policy default-permit {
    match {
      source-address any;
      destination-address any;
      application any;
```

```

    }
    then {
        permit;
    }
}
}

from-zone trust to-zone untrust {
    policy deny2 {
        match {
            source-address 10_1_0_0_16;
            destination-address any;
            application any;
        }
        then {
            reject;
        }
    }
    policy scope2 {
        match {
            source-address 10_subnet;
            destination-address 10_subnet;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v2;
                }
            }
        }
    }
    policy multicast-scope2 {
        match {
            source-address 10_subnet;
            destination-address multicast-net;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v2;
                }
            }
        }
    }
}

```

```

    }
}
policy default-permit {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
}
from-zone untrust to-zone trust {
    policy deny2 {
        match {
            source-address any;
            destination-address 10_1_0_0_16;
            application any;
        }
        then {
            reject;
        }
    }
    policy scope2 {
        match {
            source-address 10_subnet;
            destination-address 10_subnet;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v2;
                }
            }
        }
    }
    policy multicast-scope2 {
        match {
            source-address 10_subnet;
            destination-address multicast-net;
            application any;

```

```
    }
    then {
        permit {
            tunnel {
                ipsec-group-vpn v2;
            }
        }
    }
}
policy default-deny {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        deny;
    }
}
}
```

##### ???? ???? commit?(?) ??????.

??

**in this section**

Member1? ?? ?? ?? ?? | 781

Member2? ?? ?? ?? ?? | 782

??? ??? ?????? ?????? ??? ??? ??????.

**Member1? ?? ?? ?? ??**

??

member1? ??? ?? ??? ???.

??

?? ??? member1? ?? ????? ? ?? ????? ??? ????? show security dynamic-policies .

```

user@member1> show security dynamic-policies
Policy: scope1-0001, action-type: permit, State: enabled, Index: 1048580,AI: disabled, Scope
Policy: 4
  Policy Type: Dynamic
  Sequence number: 1
  From zone: untrust, To zone: trust
  Source addresses: 10.1.0.0/16
  Destination addresses: 10.2.0.0/16
  Application: Unknown
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
  Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586
Policy: scope1-0001, action-type: permit, State: enabled, Index: 1048581,AI: disabled, Scope
Policy: 5
  Policy Type: Dynamic
  Sequence number: 2
  From zone: trust, To zone: untrust
  Source addresses: 10.1.0.0/16
  Destination addresses: 10.2.0.0/16
  Application: Unknown
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
    Source port range: [0-0]
    Destination port range: [0-0]
  Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586

```

??

member1? ????? ????? ????? ?? ??? ????? ?? ?? ??? ??? ?????? ?? p3? member1? ????? ?????.

**Member2?** ?? ?? ?? ??

??

??? 2? ??? ?? ??? ???.



??

?? ??? member2? ?? ????? ? ?? ????? ??? ????? show security dynamic-policies .

```
user@member2> show security dynamic-policies
```

```
Policy: scope2-0001, action-type: permit, State: enabled, Index: 1048580,AI: disabled, Scope
```

```
Policy: 4
```

```
Policy Type: Dynamic
```

```
Sequence number: 1
```

```
From zone: untrust, To zone: trust
```

```
Source addresses: 10.1.0.0/16
```

```
Destination addresses: 10.2.0.0/16
```

```
Application: Unknown
```

```
IP protocol: 0, ALG: 0, Inactivity timeout: 0
```

```
Source port range: [0-0]
```

```
Destination port range: [0-0]
```

```
Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586
```

```
Policy: scope2-0001, action-type: permit, State: enabled, Index: 1048580,AI: disabled, Scope
```

```
Policy: 4
```

```
Policy Type: Dynamic
```

```
Sequence number: 1
```

```
From zone: untrust, To zone: trust
```

```
Source addresses: 10.1.1.1/32
```

```
Destination addresses: 239.1.1.1/32
```

```
Application: Unknown
```

```
IP protocol: 0, ALG: 0, Inactivity timeout: 0
```

```
Source port range: [0-0]
```

```
Destination port range: [0-0]
```

```
Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586
```

```
Policy: scope2-0001, action-type: permit, State: enabled, Index: 1048581,AI: disabled, Scope
```

```
Policy: 5
```

```
Policy Type: Dynamic
```

```
Sequence number: 2
```

```
From zone: trust, To zone: untrust
```

```
Source addresses: 10.2.0.0/16/0
```

```
Destination addresses: 10.1.0.0/16
```

```
Application: Unknown
```

```
IP protocol: 0, ALG: 0, Inactivity timeout: 0
```

```
Source port range: [0-0]
```

```
Destination port range: [0-0]
```

```
Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586
```

```
Policy: scope2-0001, action-type: permit, State: enabled, Index: 1048581,AI: disabled, Scope
```

```
Policy: 5
  Policy Type: Dynamic
  Sequence number: 2
  From zone: trust, To zone: untrust
  Source addresses: 10.1.1.1/32
  Destination addresses: 239.1.1.1/32
  Application: Unknown
    IP protocol: 0, ALG: 0, Inactivity timeout: 0
      Source port range: [0-0]
      Destination port range: [0-0]
  Tunnel: INSTANCE-gvpn_133955586, Type: IPSec, Index: 133955586
```

??

```

[??] [?] p2(10.1.0.0/16[?] 10.2.0.0/16[?] [?])? member2? [??] deny2 [?] [??] [??] [??] member2? [??]
[??].

```

```
?: ? ? ? ? ? ? ? ? ? ? ? ? VPNv1 ? ? - ? ? ? ? ? ?
```

in this section

- | 784  
 ●   | 785  
 ●   | 785  
 ●   | 786

[illegible]

?? ??

□□□□ □□:

- IKE(Internet Key Exchange) 1?? ???? ?? ?? ? ???? ?????.
- 2?? IPsec SA? ?? ?? ? ???? ?????.
- ?? ???? ??? g1 ?????.

??

? ???? group g1? ?? ???? ?? ?? ?? ?? ???? ????.

- ??? ?? ???? ???? ? ???? ???? ????.
- 3DES-CBC? ???? ?? ?? ???? ???? ? ????.
- SHA1? ???? ???? ????.

???? ?? ???? , KEK ?? ? ???? ????.

??

in this section

● ?? | 785

??

??? ??

?? ?? ?? ???? ???? ???? ???? ???? . ??? ??? ?? ???? CLI ??? ?? ????.

?? ??? ???? ???? ???? ????.

1. ?? ??? ????.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set communications-type unicast
```

2. ??? ???? ????.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set encryption-algorithm 3des-cbc
```



??

? ???? group g1? ?? ???? ?? ?? ???? ???? ?????.

- ??? ?????? ?? 226.1.1.1 ? ?????? ge-0/0/1.0? ?? ?? ???? ???? ? ???? ???? ????.
- 3DES-CBC? ???? ?? ?? ???? ???? ? ????.
- SHA1? ???? ???? ????.

???? ?? ???? , KEK ?? ? ???? ????.

??

in this section

● ?? | 787

??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ???? , ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
? ???? ???? CLI? ???? ?? ?? ?? , ?? ???? commit?(?) ????.

```
set security group-vpn server group g1 server-member-communication communication-type multicast
set security group-vpn server group g1 server-member-communication multicast-group 226.1.1.1
set security group-vpn server group g1 server-member-communication multicast-outgoing-interface
ge-0/0/1.0
set security group-vpn server group g1 server-member-communication encryption-algorithm 3des-cbc
set security group-vpn server group g1 server-member-communication sig-hash-algorithm sha1
```

??? ??

?? ?? ?? ???? ???? ???? ?????. ??? ??? *?? ???? CLI ???? ???? ????.*

????? ? ???? ???? ?? ?? ???? ?? ??? ????.

1. `?? ??? ??????`.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set communication-type multicast
```

2. `????? ??? ??????`.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set multicast-group 226.1.1.1
```

3. `??? ?????? ????? ? ? ?????? ??????`.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set multicast-outgoing-interface ge-0/0/1.0
```

4. `??? ?????? ??????`.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set encryption-algorithm 3des-cbc
```

5. `??? ??? ??????`.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set sig-hash-algorithm sha1
```

`??`

```
?? ????? show security group-vpn server group g1 server-member-communication ??? ????? ??? ??????. ??? ??? ???
????? ???, ? ?? ?? ??? ????? ??????
```

```
[edit]
user@host# show security group-vpn server group g1 server-member-communication
communication-type multicast;
multicast-group 226.1.1.1;
multicast-outgoing-interface ge-0/0/1.0;
```

```
encryption-algorithm 3des-cbc;  
sig-hash-algorithm sha1;
```

commit( )

in this section

[| 789](#)

show security group-vpn server group g1 server-member-communication

SEE ALSO

|                                                       |
|-------------------------------------------------------|
| <a href="#">: IKE(Internet Key Exchange) ID</a>       |
| <a href="#">IKE(Internet Key Exchange) IPsec   94</a> |

**VPNv1**

in this section

[| 790](#)





??

in this section

● ?? | 791

??

## CLI ?? ??

?? ?? ???? ?????, ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?  
 ? ???? ???? CLI? ???? ???? ???? ???? ???? ???? ???? commit?(?) ???? ????.

```
set interfaces lo0 unit 0 family inet address 20.0.0.1/32
set interfaces ge-0/1/0 unit 0 family inet address 10.1.0.1/32
set security group-vpn member ike proposal prop1 authentication-method pre-shared-keys
set security group-vpn member ike proposal prop1 dh-group group2
set security group-vpn member ike proposal prop1 authentication-algorithm sha1
set security group-vpn member ike proposal prop1 encryption-algorithm 3des-cbc
set security group-vpn member ike policy pol1 mode main
set security group-vpn member ike policy pol1 proposals prop1
set security group-vpn member ike policy pol1 pre-shared-key ascii-text "$9$c1gr K8-
VYZUHX7UHqmF3Sre"
set security group-vpn member ike gateway g1 ike-policy pol1
set security group-vpn member ike gateway g1 address 20.0.0.1
set security group-vpn member ike gateway g1 local-address 10.1.0.1
set security group-vpn member ipsec vpn v1 ike-gateway g1
set security group-vpn member ipsec vpn v1 group-vpn-external-interface ge-0/1/0
set security group-vpn member ipsec vpn v1 group 1
set security group-vpn server ike proposal srv-prop authentication-method pre-shared-keys
set security group-vpn server ike proposal srv-prop dh-group group2
set security group-vpn server ike proposal srv-prop authentication-algorithm sha1
set security group-vpn server ike proposal srv-prop encryption-algorithm 3des-cbc
set security group-vpn server ike policy srv-pol mode main
set security group-vpn server ike policy srv-pol proposals srv-prop
set security group-vpn server ike policy srv-pol pre-shared-key ascii-text "$9$c 1grK8-
VYZUHX7UHqmF3Sre"
set security group-vpn server ike gateway gw1 ike-policy srv-pol
set security group-vpn server ike gateway gw1 address 10.1.0.1
```

```

set security group-vpn server ike gateway gw2 ike-policy srv-pol
set security group-vpn server ike gateway gw2 address 10.2.0.1
set security group-vpn server ipsec proposal group-prop authentication-algorithm hmac-sha1-96
set security group-vpn server ipsec proposal group-prop encryption-algorithm 3des-cbc
set security group-vpn server ipsec proposal group-prop lifetime-seconds 3600
set security group-vpn server group grp1 group-id 1
set security group-vpn server group grp1 ike-gateway gw1
set security group-vpn server group grp1 ike-gateway gw2
set security group-vpn server group grp1 anti-replay-time-window 120
set security group-vpn server group grp1 server-address 20.0.0.1
set security group-vpn server group grp1 server-member-communication communication-type unicast
set security group-vpn server group grp1 server-member-communication encryption-algorithm
aes-128-cbc
set security group-vpn server group grp1 server-member-communication sig-hash-algorithm md5
set security group-vpn server group grp1 server-member-communication certificate srv-cert
set security group-vpn server group grp1 ipsec-sa group-sa proposal group-prop
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 source 10.1.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 destination
10.2.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p1 protocol 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 source 10.2.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 destination
10.1.0.0/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p2 protocol 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 source 10.1.1.1/16
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 destination
239.1.1.1/32
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 source-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 destination-port 0
set security group-vpn server group grp1 ipsec-sa group-sa match-policy p3 protocol 0
set security group-vpn co-location
set security group-vpn member ipsec vpn v1 ike-gateway g1
set security group-vpn member ipsec vpn v1 group-vpn-external-interface ge-0/1/0
set security address-book book1 address 10_subnet 10.0.0.0/8
set security address-book book1 attach zone trust
set security address-book book2 address 10_subnet 10.0.0.0/8
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy scope1 match source-address
10_subnet

```

```

set security policies from-zone trust to-zone untrust policy scope1 match destination-address
10_subnet
set security policies from-zone trust to-zone untrust policy scope1 match application any
set security policies from-zone trust to-zone untrust policy scope1 then permit tunnel ipsec-
group-vpn v1
set security policies from-zone untrust to-zone trust policy scope1 match source-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope1 match destination-address
10_subnet
set security policies from-zone untrust to-zone trust policy scope1 match application any
set security policies from-zone untrust to-zone trust policy scope1 then permit tunnel ipsec-
group-vpn v1

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ???? ?????.

?? ??? ?????? ???? ?? VPN? ?????? ???? ?????.

1. ?????? ??? ???? ????.

```

[edit interfaces]
user@host# set lo0 unit 0 family inet address 20.0.0.1/32

```

2. member1? MPLS ?????? ???? ? ???? ?????? ?????.

```

[edit interfaces]
user@host# set ge-0/1/0 unit 0 family inet address 10.1.0.1/32

```

3. ?????? ?? VPN ?????? ?????.

```

[edit security group-vpn]
user@host# set co-location

```

4. ??? ?? IKE(Internet Key Exchange) 1?? SA? ??????(? ??? ?? ??? ??? 1?? SA? ????? ?).

```

[edit security group-vpn server ike proposal srv-prop]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group2

```

```
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm 3des-cbc
```

5. IKE(Internet Key Exchange) `???` `???` `??` `???` `???` `???`.

```
[edit security group-vpn server ike]
user@host# set policy srv-pol proposals srv-prop mode main pre-shared-key ascii-text
"$9$c1grK8-VYZUHX7UHqmF3Sre"
user@host# set gateway gw1 ike-policy srv-pol address 10.1.0.1
user@host# set gateway gw2 ike-policy srv-pol address 10.2.0.1
```

6. `???` `??` `2??` SA `???` `???`.

```
[edit security group-vpn server ipsec proposal group-prop]
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm 3des-cbc
user@host# set lifetime-seconds 3600
```

7. `???` `??` `???`, IKE(Internet Key Exchange) `???`, `???` `???` `??` `??` `???` `???`.

```
[edit security group-vpn server group grp1]
user@host# set group-id 1 anti-replay-time-window 120 server-address 20.0.0.1
user@host#set ike-gateway gw1
user@host#set ike-gateway gw2
```

8. `??` `?` `???` `???` `???`.

```
[edit security group-vpn server group grp1]
user@host# set server-member-communication communication-type unicast encryption-algorithm
aes-128-cbc sig-hash-algorithm md5 certificate "srv-cert"
```

9. `??` `???` `???` `??` `???` `???`.

```
[edit security group-vpn server group grp1 ipsec-sa group-sa ]
user@host# set proposal group-prop match-policy p1 source 10.1.0.0/16 destination
10.2.0.0/16 source-port 0 destination-port 0 protocol 0
user@host# set proposal group-prop match-policy p2 source 10.2.0.0/16 destination
10.1.0.0/16 source-port 0 destination-port 0 protocol 0
```

```
user@host# set proposal group-prop match-policy p3 source 10.1.1.1/16 destination
239.1.1.1/32 source-port 0 destination-port 0 protocol 0
```

10. `set security group-vpn member ike proposal prop1`.

```
[edit security group-vpn member ike proposal prop1]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm 3des-cbc
```

11. `set security group-vpn member ike proposal prop1`.

```
[edit security group-vpn member ike]
user@host# set policy pol1 mode main proposals prop1 pre-shared-key ascii-text "$9$c1grK8-
VYZUHX7UHqmF3Sre"
user@host# set gateway g1 ike-policy pol1 address 20.0.0.1 local-address 10.1.0.1
```

12. `set security group-vpn member ike proposal prop1`, IKE(Internet Key Exchange) `set security group-vpn member ike proposal prop1`.

```
[edit security group-vpn member ipsec]
user@host# set vpn v1 group 1 ike-gateway g1 group-vpn-external-interface ge-0/1/0
```

13. `set security address-book book1`.

```
[edit security address-book book1]
user@member1# set address 10_subnet 10.0.0.0/8
user@member1# set attach zone trust
```

```
[edit security address-book book2]
user@member1# set address 10_subnet 10.0.0.0/8
user@member1# set attach zone untrust
```

- [illegible]

```
[edit security policies from-zone trust to-zone untrust]
user@member1# set policy scope1 match source-address 10_subnet destination-address
10_subnet application any
user@member1# set policy scope1 then permit tunnel ipsec-group-vpn v1
```

- [illegible]

```
[edit security policies from-zone untrust to-zone trust]
user@member1# set policy scope1 match source-address 10_subnet destination-address
10_subnet application any
user@member1# set policy scope1 then permit tunnel ipsec-group-vpn v1
```

??

```

?? ???? ? show security policies ??? ???? show security group-vpn ??? ?????. ??? ??? ??? ????? ??, ? ? ? ?
??? ????? ?????.

```

□□□ □□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□ □□□ □□□□□.

```
[edit]
user@host# show security group-vpn
member {
    ike {
        proposal prop1 {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
        }
        policy pol1 {
            mode main;
            proposals prop1;
            pre-shared-key ascii-text "$9$c1grK8-VYZUHX7UHqmF3Sre"; ## SECRET-DATA
        }
        gateway g1 {
            ike-policy pol1;
            address 20.0.0.1;
            local-address 10.1.0.1;
```

```

    }
}
ipsec {
    vpn v1 {
        ike-gateway g1;
        group-vpn-external-interface ge-0/1/0;
        group 1;
    }
}
}
server {
    ike {
        proposal srv-prop {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
        }
        policy srv-pol {
            mode main;
            proposals srv-prop;
            pre-shared-key ascii-text "$9$c1grK8-VYZUHX7UHqmF3Sre"; ## SECRET-DATA
        }
        gateway gw1 {
            ike-policy srv-pol;
            address 10.1.0.1;
        }
        gateway gw2 {
            ike-policy srv-pol;
            address 10.2.0.1;
        }
    }
    ipsec {
        proposal group-prop {
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 3600;
        }
    }
    group grp1 {
        group-id 1;
        ike-gateway gw1;
        ike-gateway gw2;
    }
}

```

```

    anti-replay-time-window 120;
    server-address 20.0.0.1;
    server-member-communication {
        communication-type unicast;
        encryption-algorithm aes-128-cbc;
        sig-hash-algorithm md5;
        certificate srv-cert;
    }
    ipsec-sa group-sa {
        proposal group-prop;
        match-policy p1 {
            source 10.1.0.0/16;
            destination 10.2.0.0/16;
            source-port 0;
            destination-port 0;
            protocol 0;
        }
        match-policy p2 {
            source 10.2.0.0/16;
            destination 10.1.0.0/16;
            source-port 0;
            destination-port 0;
            protocol 0;
        }
        match-policy p3 {
            source 10.1.1.1/16;
            destination 239.1.1.1/32;
            source-port 0;
            destination-port 0;
            protocol 0;
        }
    }
}
}
co-location;

```

```

[edit]
user@host# show security policies
from-zone trust to-zone trust {
    policy default-permit {
        match {

```



```

        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
}
from-zone trust to-zone untrust {
    policy scope1 {
        match {
            source-address 10_subnet;
            destination-address 10_subnet;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-group-vpn v1;
                }
            }
        }
    }
}
policy default-permit {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit;
    }
}
}
from-zone untrust to-zone trust {
    policy default-deny {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {

```



??

?? ????? show security group-vpn registered-members ??? ?????.

**IKE? ?? ?? VPN ?? ?? ?? ??**

??

**IKE? ?? ?? VPN ??? SA? ??????**

??

?? ????? show security group-vpn server ike security-associations ??? ?????.

**IPsec? ?? ?? VPN ?? ?? ?? ??**

??

**IPsec? ?? ?? VPN ??? SA? ??????**

??

?? ????? show security group-vpn server ipsec security-associations ??? ?????.

**IKE? ?? ?? VPN ?? ?? ?? ??**

??

**IKE? ?? ?? VPN ??? SA? ??????**

??

?? ????? show security group-vpn member ike security-associations ??? ?????.

**IPsec? ?? ?? VPN ?? ?? ?? ??**

??

**IPsec? ?? ?? VPN ??? SA? ??????**



- ? : ? ? ? ? ? ? ? ? ? ? ? ? ? ? VPNv2 ? ? - ? ? ? ? ?  
? | 858

[illegible]

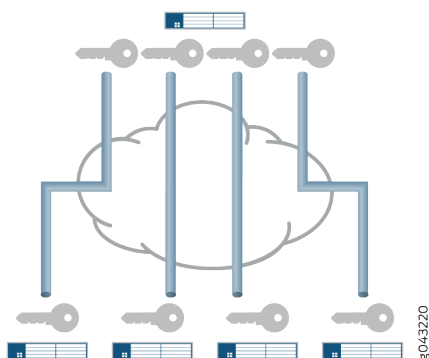
?? VPNv2 ??

in this section

- ?? VPNv2 ?? GDOI ???? ???? | 804
- ?? VPNv2 ?? ? ??? ???? | 804
- ?? VPNv2 ?? ?? ???? | 805
- ?? VPNv2 ?? ?? ?? ???? | 806
- ?? VPNv2 ?? ?? ?? | 806

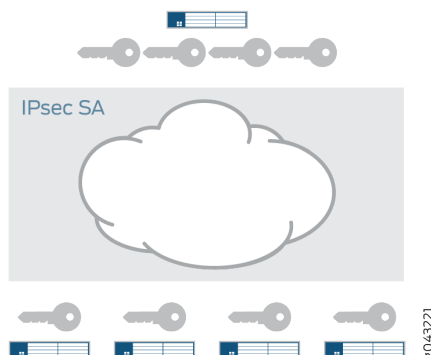
IPsec SA(?? ??)?? ? ? ??? ?????, ? ?? ????? ? ?? ??? ??? ??? ??? VPN(?? ???) ??? ? ? ??? ??????. ??  
VPN ????? SA? ? ?? ????? ?? ? ? ?????? ( ?? ?? 48 ??? 803).

48: [redacted] [redacted] SA



VPNv2 IPsec 49 804. VPNv2 IP any-to-any.

#### 49: SA



VPNv2 SRX Junos OS VPN RFC 6407, *GDOI(Group Domain of Interpretation)* RFC 6407.

#### VPNv2 GDOI

VPNv2 RFC 6407, *GDOI( Group Domain of Interpretation)* RFC SA GDOI SA, .

GDOI UDP 848. ISAKMP(Internet Security Association and Key Management Protocol) IKE IPsec SA 1 GDOI ISAKMP SA .

VPNv2 1 ISAKMP SA ISAKMP GDOI SA IPsec GDOI ISAKMP Phase 1 SA .

GDOI .

- groupkey-pull SA groupkey-pull .
- groupkey-push SA SA .

#### VPNv2

VPNv2 (GCKS) GCKS .

GCKS 22 22 222 22 222 22222.

- 22 222 222 22222.
- 222 22 22222.
- 22222 2 22 SA 2 22 2222. 22 222 22 SA 2 22 222 2222 22 2222 2222 222222.

22 222 22 222 2222 222 2 2222. 22 22 22222 22 222 2222 2 2 2222.

2 222 122 4,294,967,295 222 222 22 2222 22222. 22 22 2 22 222 22 2222 22 22 22222. 222 222 22 2222 22 2 222 222 222 22 22222.

222 22 VPNv2 22 2 22 222 22 2222 22222.

1. 22 222 2222 222 2 222 UDP 22 84822 22 22222.
2. 22 222 2222 22 2222 22 222 IKE(Internet Key Exchange) SA 22222. 22 22222 222 2222 22 222 IKE(Internet Key Exchange) 122 222 2222 222. 222 222 22 22 2 222 22222.
3. 22 2 222 2222, 22 22222 GDOI groupkey-pull 222 22 2222 222 22 2222 22 22 SA 22 22222.
4. 222 222 222 222 2222 22222.
5. 22 222 22 SA 22 2222 222 22222.

222 2 222(GDOI groupkey-push) 2222 22 22 22222 SA 2 2 22 222 2222. 222 SA 2222 22 2 222 2222 2222 2 22 22 2222 222222 2 222 22 222 2 222 22222.

222 222 2 222 22222 2 22 222 22(ack) 2222 22222. 222 22222 ack 2222 2222 22 22, 2 222 2222 222 retransmission-period 222 222222(2222 102). 222 number-of-retransmission 2(2222 22) 2222 222 22 22, 222 22 2 22222 2222 22222. 222 222 22 IKE(Internet Key Exchange) SA 22222.

22 222 22 SA 22 22222 2 22222 2 22 2222 22 2 222 2222 2222.

## 22 VPNv2 22 22 2222

22 VPNv2 222 RFC 6407, *GDOI(Group Domain of Interpretation)* 22222 22 VPNv2 2222 22222.

222 22 VPNv222 2222 2222.

- SNMP222.
- Cisco GET VPN 222 222 22222.
- 122 IKE(Internet Key Exchange) 222 22 PKI 22.
- 22 222 2222 22 22, 22 2 222 222 222 222 222 22222.
- 22 22222 222 22 22.

- 配置 J-Web 。
- 。

VPNv2 IP 地址 (NAT) 。

## VPNv2 配置

配置 GDOI groupkey-push ( ) 。

GDOI groupkey-pull 配置 。

配置 [edit security group-vpn server] server-member-communication 。

- 配置 (sha-256 sha-384) 。
- aes-128-cbc, aes-192-cbc aes-256-cbc 。
- 配置 。
- KEK( ) 3600 。
- 配置 groupkey-push ( ) ( ) 。

配置 show security group-vpn server registered-members 。

## VPNv2 配置

配置 。

配置

配置 VPN , 配置 。

- KEK(Key Encryption Key) - GDOI groupkey-push(SA ) 。
- (TEK) - IPsec 。

SA 配置 。







?? ???? IKE(Internet Key Exchange) ?? ? ?? ???? ?? ???? IKE(Internet Key Exchange) ?? ? ?? ???? ???? ????.  
?? ???? ? ?? ???? ?? IKE(Internet Key Exchange) ???? ???? ???? ???? ???? IKE(Internet Key Exchange) ??  
??? ???? ?? 4?? ?? ???? ???? ? ????.

**?? VPNv2? ?? IPsec SA ?? ?????**

??? ??? 1?? ???? ???? ???? ???? ?, ?? ?? ???? ???? ???? ?? ?? ???? ???? IPsec SA? ?????. ??  
VPNv2? ?? IPsec SA ???? ?? VPN? ?? ???? ?????, ?? ???? ?? ?? ???? SA? ???? ???? ????.

?? VPNv2? ?? IPsec ???? ?? ???? ????.

- ?? ???? SA? ???? ?? ???? , ?? ? ???? ???? ?? IPsec ???? ?????. IPsec SA ???? [edit security group-vpn server ipsec] ???? ?? ???? proposal ?? ???? ????.
- ?? ???? ?? ???? , ?? ??(?? ???? ike-gateway ??) ? ???? ?? ???? ???? ? ???? ???? ???? ???? ? ? IKE(Internet Key Exchange)? ?????. ?? ? IKE(Internet Key Exchange)? [edit security group-vpn member ipsec] ???? ?? ? ? ???? vpn ???? ????.

SEE ALSO

| [?? VPNv2 ?? ???? ???? | 860](#)

**?? VPNv2 ???? ???? ?????**

in this section

- [?? ???? ???? ?? | 810](#)
- [?? ???? ???? IPsec ?? | 810](#)
- [?? ???? \(Fail-Close\) | 810](#)
- [Exclude ? Fail-Open ?? | 810](#)
- [IPsec ?? ? ???? ?? ?? | 810](#)

?? ???? IPsec SA(Security Association) ? ?? ???? ???? ???? ?????. ??? ???? ?? ?? ???? ???? IPsec SA ???? ?  
??. ?? ?? ???? ???? SA? ?? SA? ???? ?? ? ?? ???? ???? IPsec ???? ?? ????.



- [illegible]

## SEE ALSO

VPNv2 867

**?? VPNv2 ?? ??? ???? ???? ???? ?**

? ?? ??? ? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

- **?? ?? ? ? SPI(Security Parameter Index) ? ? ESP(Encapsulating Security Payload) ??? ?????.**
- **??? IPsec ??? ? ? ? ? IPsec ??? ????.**

2 222 2 2222 22222 22 22222 22 2222 222222 22222 2 22222, 22 2222 222222 22 22222 GDOI groupkey-pull 222 22222 2  
 2 22222 222 SA2 22222222. 22 SPI 222 22 DoS 222 222 222 222222 22 22, 22 2222 22222 2222 22 2222 2 222  
 2. 222 22222 22222 22 10, 20, 40, groupkey-pull 80, 160 2 3202 2222 222 22 222222.

```
? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? ? ? [edit security group-vpn member ipsec vpn vpn-name] ?  
? ? ? ? ? ? (?) ? ? ? ? ? ? recovery-probe.
```

?? VPNv2 ?????? ???? ?

Antireplay? ??? ???? ???? ?? ???? ???? ???? ? ?? IPsec ??????. Antireplay? ??? ?? ????? ?????.

```
? IPsec ???? ???? ???? ??. ?? ??? ??? ?????? ??? anti-replay-time-window ? ?? ??? ??????. ????? ?  
???? ?? ?????.
```

```
?? VPNv2 ???? ???? ?? ???? NTP? ???? ?? ????.
```

```

#####  ???  #####  ???  #####  vSRX  ??  ???  #####  #####  ??  ???  ??  #####  ???  ?  ??  ???  ???  ?  #####
anti-replay-time-window . ??  ???  IPsec  ???  #####  #####  #####  ??  ??  #####  show security group-vpn member ipsec
statistics D3P  ???  #####, NTP?  #####  #####  #####,  ???  ??  ??  ??  #####  anti-replay-time-window .

```

SEE ALSO

[VPNv1 Antireplay](#) | [763](#)

**VPNv2**

in this section

• [VPNv2](#) | [812](#)

• [VPNv2](#) | [813](#)

• [VPNv2](#) | [814](#)

• [VPNv2](#) | [849](#)

VPNv2 (GCKS) VPNv2

VPNv2

VPNv2

- VPNv2 Junos OS 15.1X49-D30 SRX vSRX SRX vSRX VPNv2
- VPNv2 Junos OS 15.1X49-D30 SRX vSRX 2. VPNv2
- VPNv2 Junos OS 15.1R2 MX 2. VPNv2

VPNv2, NTP

VPNv2 VPNv2

??

in this section

813

?? VPNv2 1?? 4?? 2?? SRX ?? vSRX ??, ?? 2? ?? MX ?? VPN SA? ?? ?? ?? ??.

?? VPN SA? 1?? SA? ?? ???. ?? ?? VPN ?? ?? ?? ?? ?? IKE(Internet Key Exchange) 1 ?? ?? ??.

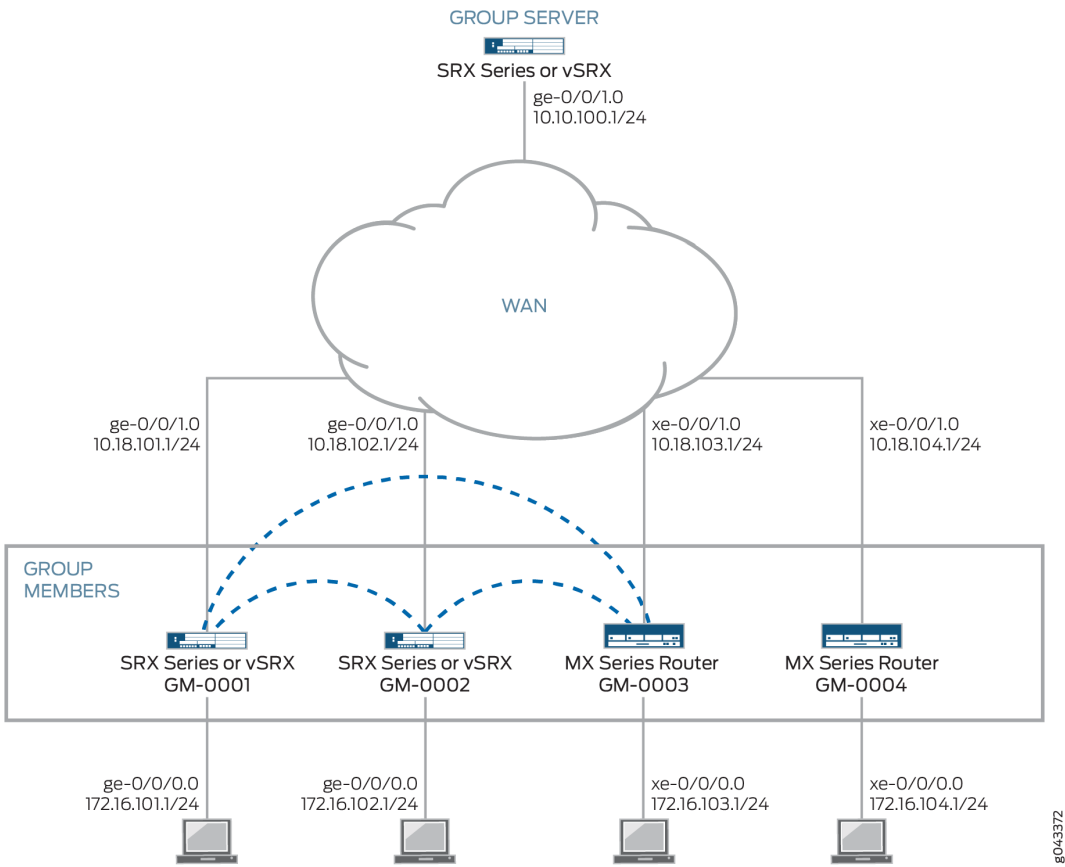
?? ?? ?? ?? ?? ???. ? ?? GROUP\_ID-0001?? ?? 1???. ?? ?? ?? ? SA? ?? 172.16.0.0/12 ?? ?? ?? ??.

SRX ?? vSRX ?? ?? IPsec ?? LAN ?? ??(?? ??)??, WAN ?? ??(?? ??)?? ? ?? ?? LAN? WAN ? ? ? ? ? ? ? ?.

???

50 814 ?(?) ? ? ? ? ? ? ? ?.

50: SRX (SRX Series or vSRX) MX (MX Series Router) VPNv2



??

in this section

- [?? ?? ?? | 815](#)
- [?? ?? GM-0001 ??\(SRX ??? ???? ?? vSRX ?? ???? ?????\) | 822](#)
- [?? ?? GM-0002 ??\(SRX ??? ???? ?? vSRX ?? ???? ?????\) | 830](#)
- [?? ?? ?? GM-0003 \(MX ??? ?????\) | 837](#)
- [?? ?? ?? GM-0004 \(MX ??? ?????\) | 843](#)



?? ?? ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ??????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.10.100.1/24
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then reject
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces ge-0/0/1.0
set routing-options static route 10.18.101.0/24 next-hop 10.10.100.254
set routing-options static route 10.18.102.0/24 next-hop 10.10.100.254
set routing-options static route 10.18.103.0/24 next-hop 10.10.100.254
set routing-options static route 10.18.104.0/24 next-hop 10.10.100.254
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy GMs mode main
set security group-vpn server ike policy GMs proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy GMs pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike gateway GM-0001 ike-policy GMs
set security group-vpn server ike gateway GM-0001 address 10.18.101.1
set security group-vpn server ike gateway GM-0001 local-address 10.10.100.1
set security group-vpn server ike gateway GM-0002 ike-policy GMs
set security group-vpn server ike gateway GM-0002 address 10.18.102.1
set security group-vpn server ike gateway GM-0002 local-address 10.10.100.1
set security group-vpn server ike gateway GM-0003 ike-policy GMs
```

```

set security group-vpn server ike gateway GM-0003 address 10.18.103.1
set security group-vpn server ike gateway GM-0003 local-address 10.10.100.1
set security group-vpn server ike gateway GM-0004 ike-policy GMs
set security group-vpn server ike gateway GM-0004 address 10.18.104.1
set security group-vpn server ike gateway GM-0004 local-address 10.10.100.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0001
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0002
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0003
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0004
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0005
set security group-vpn server group GROUP_ID-0001 anti-replay-time-window 1000
set security group-vpn server group GROUP_ID-0001 server-member-communication communication-type
unicast
set security group-vpn server group GROUP_ID-0001 server-member-communication encryption-
algorithm aes-256-cbc
set security group-vpn server group GROUP_ID-0001 server-member-communication lifetime-seconds
7200
set security group-vpn server group GROUP_ID-0001 server-member-communication sig-hash-algorithm
sha-256
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-
L3600
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 source
172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1
destination 172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 protocol
0

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?? VPNv2 ?? ?? ??:

[illegible]

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.10.100.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/1.0
[edit security policies]
user@host# set global policy 1000 match source-address any
user@host# set global policy 1000 match destination-address any
user@host# set global policy 1000 match application any
user@host# set global policy 1000 match from-zone any
user@host# set global policy 1000 match to-zone any
user@host# set global policy 1000 then reject
user@host# set global policy 1000 then log session-init
user@host# set global policy 1000 then count
user@host# set default-policy deny-all
```

**2.**                 .

```
[edit routing-options]
user@host# set static route 10.18.101.0/24 next-hop 10.10.100.254
user@host# set static route 10.18.102.0/24 next-hop 10.10.100.254
user@host# set static route 10.18.103.0/24 next-hop 10.10.100.254
user@host# set static route 10.18.104.0/24 next-hop 10.10.100.254
```

### 3. IKE(Internet Key Exchange) ??, ?? ? ?????? ??????.

```
[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set authentication-algorithm sha-256
user@host# set dh-group group14
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy GMs]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "ABC123"
[edit security group-vpn server ike gateway GM-0001]
```

```

user@host# set ike-policy GMs
user@host# set address 10.18.101.1
user@host# set local-address 10.10.100.1
[edit security group-vpn server ike gateway GM-0002]
user@host# set ike-policy GMs
user@host# set address 10.18.102.1
user@host# set local-address 10.10.100.1
[edit security group-vpn server ike gateway GM-0003]
user@host# set ike-policy GMs
user@host# set address 10.18.103.1
user@host# set local-address 10.10.100.1
[edit security group-vpn server ike gateway GM-0004]
user@host# set ike-policy GMs
user@host# set address 10.18.104.1
user@host# set local-address 10.10.100.1

```

#### 4. IPsec `???` `??????`.

```

[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600 VPN Group

```

#### 5. `???` `??????`.

```

[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set ike-gateway GM-0001
user@host# set ike-gateway GM-0002
user@host# set ike-gateway GM-0003
user@host# set ike-gateway GM-0004
user@host# set anti-replay-time-window 1000

```

#### 6. `?? ?` `???` `??????`.

```

[edit security group-vpn server group GROUP_ID-0001 server-member-communication]
user@host# set communication-type unicast
user@host# set encryption-algorithm aes-256-cbc

```

```
user@host# set lifetime-seconds 7200
user@host# set sig-hash-algorithm sha-256
```

**7.**      .

```
[edit security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001]
user@host# set proposal AES256-SHA256-L3600
user@host# set match-policy 1 source 172.16.0.0/12
user@host# set match-policy 1 destination 172.16.0.0/12
user@host# set match-policy 1 protocol 0
```

??

```

?? ???? show interfaces, show routing-options ? show security ??? ???? ???? ?????. ?? ???? ???? ???? ???? ????
? ?? ???? ???? ???? ?????.

```

```
[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet {
            address 10.10.100.1/24;
        }
    }
}

[edit]
user@host# show routing-options
static {
    route 10.18.101.0/24 next-hop 10.10.100.254;
    route 10.18.102.0/24 next-hop 10.10.100.254;
    route 10.18.103.0/24 next-hop 10.10.100.254;
    route 10.18.104.0/24 next-hop 10.10.100.254;
}

[edit]
user@host# show security
group-vpn {
    server {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
```

```

        authentication-algorithm sha-256;
        dh-group group14;
        encryption-algorithm aes-256-cbc;
    }
    policy GMs {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway GM-0001 {
        ike-policy GMs;
        address 10.18.101.1;
        local-address 10.10.100.1;
    }
    gateway GM-0002 {
        ike-policy GMs;
        address 10.18.102.1;
        local-address 10.10.100.1;
    }
    gateway GM-0003 {
        ike-policy GMs;
        address 10.18.103.1;
        local-address 10.10.100.1;
    }
    gateway GM-0004 {
        ike-policy GMs;
        address 10.18.104.1;
        local-address 10.10.100.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
    ike-gateway GM-0001;
    ike-gateway GM-0002;
    ike-gateway GM-0003;

```

```

ike-gateway GM-0004;
anti-replay-time-window 1000;
server-member-communication {
    communication-type unicast;
    lifetime-seconds 7200;
    encryption-algorithm aes-256-cbc;
    sig-hash-algorithm sha-256;
}
ipsec-sa GROUP_ID-0001 {
    proposal AES256-SHA256-L3600;
    match-policy 1 {
        source 172.16.0.0/12;
        destination 172.16.0.0/12;
        protocol 0;
    }
}
}
}
}
policies {
    global {
        policy 1000 {
            match {
                source-address any;
                destination-address any;
                application any;
                from-zone any;
                to-zone any;
            }
            then {
                reject;
                log {
                    session-init;
                }
                count;
            }
        }
    }
}
default-policy {
    deny-all;
}
}
zones {

```

```

security-zone GROUPVPN {
    host-inbound-traffic {
        system-services {
            ike;
            ssh;
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

```

```

?? ?? ???? ???? ???? commit?(?) ??????.

```

```

?? ?? GM-0001 ??(SRX ??? ???? ?? vSRX ?? ???? ?????)

```

## CLI ?? ??

```

? ?? ???? ?????, ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?
? ???? ???? CLI? ???? ???? ???? ???? ???? ???? commit?(?) ??????.

```

```

set interfaces ge-0/0/0 unit 0 description To_LAN
set interfaces ge-0/0/0 unit 0 family inet address 172.16.101.1/24
set interfaces ge-0/0/1 unit 0 description To_KeySrv
set interfaces ge-0/0/1 unit 0 family inet address 10.18.101.1/24
set security zones security-zone LAN host-inbound-traffic system-services ike
set security zones security-zone LAN host-inbound-traffic system-services ssh
set security zones security-zone LAN host-inbound-traffic system-services ping
set security zones security-zone LAN interfaces ge-0/0/0.0
set security zones security-zone WAN host-inbound-traffic system-services ike
set security zones security-zone WAN host-inbound-traffic system-services ssh
set security zones security-zone WAN host-inbound-traffic system-services ping
set security zones security-zone WAN interfaces ge-0/0/1.0
set security address-book global address 172.16.0.0/12 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match application any
set security policies from-zone LAN to-zone WAN policy 1 then permit
set security policies from-zone LAN to-zone WAN policy 1 then log session-init
set security policies from-zone WAN to-zone LAN policy 1 match source-address 172.16.0.0/12

```



```

set security policies from-zone WAN to-zone LAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match application any
set security policies from-zone WAN to-zone LAN policy 1 then permit
set security policies from-zone WAN to-zone LAN policy 1 then log session-init
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then reject
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set routing-options static route 10.18.102.0/24 next-hop 10.18.101.254
set routing-options static route 10.18.103.0/24 next-hop 10.18.101.254
set routing-options static route 10.18.104.0/24 next-hop 10.18.101.254
set routing-options static route 172.16.101.0/24 next-hop 10.18.101.254
set routing-options static route 172.16.102.0/24 next-hop 10.18.101.254
set routing-options static route 172.16.103.0/24 next-hop 10.18.101.254
set routing-options static route 172.16.104.0/24 next-hop 10.18.101.254
set routing-options static route 10.10.100.0/24 next-hop 10.18.101.254
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy KeySrv mode main
set security group-vpn member ike policy KeySrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy KeySrv pre-shared-key ascii-text "$ABC123"
set security group-vpn member ike gateway KeySrv ike-policy KeySrv
set security group-vpn member ike gateway KeySrv server-address 10.10.100.1
set security group-vpn member ike gateway KeySrv local-address 10.18.101.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway KeySrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group-vpn-external-interface ge-0/0/1.0
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 recovery-probe
set security ipsec-policy from-zone LAN to-zone WAN ipsec-group-vpn GROUP_ID-0001

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?? VPNv2 ??? ???? ???? ????.

1. ?????, ?? ?? ? ?? ???? ????.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_LAN
user@host# set ge-0/0/0 unit 0 family inet address 172.16.101.1/24
user@host# set ge-0/0/1 unit 0 description To_KeySrv
user@host# set ge-0/0/1 unit 0 family inet address 10.18.101.1/24
[edit security zones security-zone LAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/0.0
[edit security]
user@host# set address-book global address 172.16.0.0/12 172.16.0.0/12
[edit security zones security-zone WAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/1.0
[edit security policies from-zone LAN to-zone WAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set then log session-init
[edit security policies from-zone WAN to-zone LAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set then log session-init
[edit security policies]
user@host# set global policy 1000 match source-address any
user@host# set global policy 1000 match destination-address any
user@host# set global policy 1000 match application any
user@host# set global policy 1000 match from-zone any
user@host# set global policy 1000 match to-zone any
```

```

user@host# set global policy 1000 match then reject
user@host# set global policy 1000 match then log session-init
user@host# set global policy 1000 match then count
user@host# set default-policy deny-all

```

## 2. `?? ??? ?????`.

```

[edit routing-options]
user@host# set static route 10.18.102.0/24 next-hop 10.18.101.254
user@host# set static route 10.18.103.0/24 next-hop 10.18.101.254
user@host# set static route 10.18.104.0/24 next-hop 10.18.101.254
user@host# set static route 172.16.101.0/24 next-hop 10.18.101.254
user@host# set static route 172.16.102.0/24 next-hop 10.18.101.254
user@host# set static route 172.16.103.0/24 next-hop 10.18.101.254
user@host# set static route 172.16.104.0/24 next-hop 10.18.101.254
user@host# set static route 10.10.100.0/24 next-hop 10.18.101.254

```

## 3. IKE(Internet Key Exchange) `??, ?? ? ?????? ??????`.

```

[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set authentication-algorithm sha-256
user@host# set dh-group group14
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy KeySrv ]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn member ike gateway KeySrv]
user@host# set ike-policy KeySrv
user@host# set server-address 10.10.100.1
user@host# set local-address 10.18.101.1

```

## 4. IPsec SA `??????`.

```

[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway KeySrv
user@host# set group-vpn-external-interface ge-0/0/1.0

```

```
user@host# set group 1
user@host# set recovery-probe
```

## 5. IPsec `???` `???`.

```
[edit security ipsec-policy from-zone LAN to-zone WAN]
user@host# set ipsec-group-vpn GROUP_ID-0001
```

`??`

`??` `???` show interfaces, show routing-options `?` show security `???` `???` `???` `???`. `??` `???` `???` `???` `???` `???`  
`?` `??` `???` `???` `???` `???` `???`.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_LAN;
    family inet {
      address 172.16.101.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_KeySrv;
    family inet {
      address 10.18.101.1/24;
    }
  }
}
[edit]
user@host# show routing-options
static {
  route 10.18.102.0/24 next-hop 10.18.101.254;
  route 10.18.103.0/24 next-hop 10.18.101.254;
  route 10.18.104.0/24 next-hop 10.18.101.254;
  route 172.16.101.0/24 next-hop 10.18.101.254;
  route 172.16.102.0/24 next-hop 10.18.101.254;
  route 172.16.103.0/24 next-hop 10.18.101.254;
```

```

    route 172.16.104.0/24 next-hop 10.18.101.254;
    route 10.10.100.0/24 next-hop 10.18.101.254;
}
[edit]
user@host# show security
address-book {
    global {
        address 172.16.0.0/12 172.16.0.0/12;
    }
}
group-vpn {
    member {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                dh-group group14;
                authentication-algorithm sha-256;
                encryption-algorithm aes-256-cbc;
            }
            policy KeySrv {
                mode main;
                proposals PSK-SHA256-DH14-AES256;
                pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
            }
            gateway KeySrv {
                ike-policy KeySrv;
                server-address 10.10.100.1;
                local-address 10.18.101.1;
            }
        }
    }
    ipsec {
        vpn GROUP_ID-0001 {
            ike-gateway KeySrv;
            group-vpn-external-interface ge-0/0/1.0;
            group 1;
            recovery-probe;
        }
    }
}
ipsec-policy {
    from-zone LAN to-zone WAN {
        ipsec-group-vpn GROUP_ID-0001;
    }
}

```

```

    }
}
policies {
    from-zone LAN to-zone WAN {
        policy 1 {
            match {
                source-address 172.16.0.0/12;
                destination-address 172.16.0.0/12;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
            }
        }
    }
}
from-zone WAN to-zone LAN {
    policy 1 {
        match {
            source-address 172.16.0.0/12;
            destination-address 172.16.0.0/12;
            application any;
        }
        then {
            permit;
            log {
                session-init;
            }
        }
    }
}
global {
    policy 1000 {
        match {
            source-address any;
            destination-address any;
            application any;
            from-zone any;
            to-zone any;
        }
        then {

```

```

        reject;
        log {
            session-init;
        }
        count;
    }
}
}
default-policy {
    deny-all;
}
}
zones {
    security-zone LAN {
        host-inbound-traffic {
            system-services {
                ike;
                ssh;
                ping;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone WAN {
        host-inbound-traffic {
            system-services {
                ike;
                ssh;
                ping;
            }
        }
        interfaces {
            ge-0/0/1.0;
        }
    }
}
}

```

?? ?? ?? ?? ?? commit?(?) ??.

?? ?? GM-0002 ??(SRX ??? ??? ?? vSRX ?? ??? ????)

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set interfaces ge-0/0/0 unit 0 description To_LAN
set interfaces ge-0/0/0 unit 0 family inet address 172.16.102.1/24
set interfaces ge-0/0/1 unit 0 description To_KeySrv
set interfaces ge-0/0/1 unit 0 family inet address 10.18.102.1/24
set security zones security-zone LAN host-inbound-traffic system-services ike
set security zones security-zone LAN host-inbound-traffic system-services ssh
set security zones security-zone LAN host-inbound-traffic system-services ping
set security zones security-zone LAN interfaces ge-0/0/0.0
set security zones security-zone WAN host-inbound-traffic system-services ike
set security zones security-zone WAN host-inbound-traffic system-services ssh
set security zones security-zone WAN host-inbound-traffic system-services ping
set security zones security-zone WAN interfaces ge-0/0/1.0
set security address-book global address 172.16.0.0/12 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match application any
set security policies from-zone LAN to-zone WAN policy 1 then permit
set security policies from-zone LAN to-zone WAN policy 1 then log session-init
set security policies from-zone WAN to-zone LAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match application any
set security policies from-zone WAN to-zone LAN policy 1 then permit
set security policies from-zone WAN to-zone LAN policy 1 then log session-init
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then reject
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set routing-options static route 10.18.101.0/24 next-hop 10.18.102.254
set routing-options static route 10.18.103.0/24 next-hop 10.18.102.254
set routing-options static route 10.18.104.0/24 next-hop 10.18.102.254
```



```

set routing-options static route 172.16.101.0/24 next-hop 10.18.102.254
set routing-options static route 172.16.102.0/24 next-hop 10.18.102.254
set routing-options static route 172.16.103.0/24 next-hop 10.18.102.254
set routing-options static route 172.16.104.0/24 next-hop 10.18.102.254
set routing-options static route 10.10.100.0/24 next-hop 10.18.102.254
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy KeySrv mode main
set security group-vpn member ike policy KeySrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy KeySrv pre-shared-key ascii-text "$ABC123"
set security group-vpn member ike gateway KeySrv ike-policy KeySrv
set security group-vpn member ike gateway KeySrv server-address 10.10.100.1
set security group-vpn member ike gateway KeySrv local-address 10.18.102.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway KeySrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group-vpn-external-interface ge-0/0/1.0
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 recovery-probe
set security ipsec-policy from-zone LAN to-zone WAN ipsec-group-vpn GROUP_ID-0001

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

?? VPNv2 ??? ???? ???? ????.

1. ?????, ?? ?? ? ?? ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_LAN
user@host# set ge-0/0/0 unit 0 family inet address 172.16.102.1/24
user@host# set ge-0/0/1 unit 0 description To_KeySrv
user@host# set ge-0/0/1 unit 0 family inet address 10.18.101.1/24
[edit security zones security-zone LAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/0.0

```

```

[edit security zones security-zone WAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/1.0
[edit security]
user@host# set address-book global address 172.16.0.0/12 172.16.0.0/12
[edit security policies from-zone LAN to-zone WAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set then log session-init
[edit security policies from-zone WAN to-zone LAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set then log session-init
[edit security policies]
user@host# set global policy 1000 match source-address any
user@host# set global policy 1000 match destination-address any
user@host# set global policy 1000 match application any
user@host# set global policy 1000 match from-zone any
user@host# set global policy 1000 match to-zone any
user@host# set global policy 1000 match then reject
user@host# set global policy 1000 match then log session-init
user@host# set global policy 1000 match then count
user@host# set default-policy deny-all

```

## 2. `set` `static` `route` `next-hop`.

```

[edit routing-options]
user@host# set static route 10.18.101.0/24 next-hop 10.18.102.254
user@host# set static route 10.18.103.0/24 next-hop 10.18.102.254
user@host# set static route 10.18.104.0/24 next-hop 10.18.102.254
user@host# set static route 172.16.101.0/24 next-hop 10.18.102.254
user@host# set static route 172.16.102.0/24 next-hop 10.18.102.254
user@host# set static route 172.16.103.0/24 next-hop 10.18.102.254
user@host# set static route 172.16.104.0/24 next-hop 10.18.102.254
user@host# set static route 10.10.100.0/24 next-hop 10.18.102.254

```

### 3. IKE(Internet Key Exchange) `??, ?? ?` `?????? ?????`.

```
[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set authentication-algorithm sha-256
user@host# set dh-group group14
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy KeySrv ]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn member ike gateway KeySrv]
user@host# set ike-policy KeySrv
user@host# set server-address 10.10.100.1
user@host# set local-address 10.18.102.1
```

### 4. IPsec SA `??????`.

```
[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway KeySrv
user@host# set group-vpn-external-interface ge-0/0/1.0
user@host# set group 1
user@host# set recovery-probe
```

### 5. IPsec `???` `??????`.

```
[edit security ipsec-policy from-zone LAN to-zone WAN]
user@host# set ipsec-group-vpn GROUP_ID-0001
```

`??`

`??` `?????` show interfaces, show routing-options `?` show security `???` `?????` `???` `??????`, `??` `????` `???` `?????` `?????` `???`  
`?` `??` `????` `?????` `???` `????????`.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        description To_LAN;
```

```

        family inet {
            address 172.16.102.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        description To_KeySrv;
        family inet {
            address 10.18.102.1/24;
        }
    }
}
[edit]
user@host# show routing-options
static {
    route 10.18.101.0/24 next-hop 10.18.102.254;
    route 10.18.103.0/24 next-hop 10.18.102.254;
    route 10.18.104.0/24 next-hop 10.18.102.254;
    route 172.16.101.0/24 next-hop 10.18.102.254;
    route 172.16.102.0/24 next-hop 10.18.102.254;
    route 172.16.103.0/24 next-hop 10.18.102.254;
    route 172.16.104.0/24 next-hop 10.18.102.254;
    route 10.10.100.0/24 next-hop 10.18.102.254;
}
[edit]
user@host# show security
address-book {
    global {
        address 172.16.0.0/12 172.16.0.0/12;
    }
}
group-vpn {
    member {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                dh-group group14;
                authentication-algorithm sha-256;
                encryption-algorithm aes-256-cbc;
            }
            policy KeySrv {
                mode main;
            }
        }
    }
}

```

```

        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway KeySrv {
        ike-policy KeySrv;
        server-address 10.10.100.1;
        local-address 10.18.102.1;
    }
}
ipsec {
    vpn GROUP_ID-0001 {
        ike-gateway KeySrv;
        group-vpn-external-interface ge-0/0/1.0;
        group 1;
        recovery-probe;
    }
}
}
}
policies {
    from-zone LAN to-zone WAN {
        policy 1 {
            match {
                source-address 172.16.0.0/12;
                destination-address 172.16.0.0/12;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
            }
        }
    }
    from-zone WAN to-zone LAN {
        policy 1 {
            match {
                source-address 172.16.0.0/12;
                destination-address 172.16.0.0/12;
                application any;
            }
            then {

```

```

        permit;
        log {
            session-init;
        }
    }
}
global {
    policy 1000 {
        match {
            source-address any;
            destination-address any;
            application any;
            from-zone any;
            to-zone any;
        }
        then {
            reject;
            log {
                session-init;
            }
            count;
        }
    }
}
default-policy {
    deny-all;
}
}
zones {
    security-zone LAN {
        host-inbound-traffic {
            system-services {
                ike;
                ssh;
                ping;
            }
        }
        interfaces {
            ge-0/0/0.0;
        }
    }
    security-zone WAN {

```

```

    host-inbound-traffic {
        system-services {
            ike;
            ssh;
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
}

```

?? ?? ?? ?? ?? commit?(?) ??????.

?? ?? ?? GM-0003 (MX ?? ??)

CLI ?? ??

? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ????? ?? ?? ?? ?? ? ?? ?? ?? ?? [edit] ?  
 ? ?? ?? ?? CLI? ?? ?? ?? ??, ?? ?? ?? commit?(?) ??????.

```

set interfaces xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet address 10.18.103.1/24
set interfaces xe-0/0/2 unit 0 family inet address 172.16.103.1/24
set interfaces ms-0/2/0 unit 0 family inet
set routing-options static route 10.18.101.0/24 next-hop 10.18.103.254
set routing-options static route 10.18.102.0/24 next-hop 10.18.103.254
set routing-options static route 10.18.104.0/24 next-hop 10.18.103.254
set routing-options static route 172.16.101.0/24 next-hop 10.18.103.254
set routing-options static route 172.16.102.0/24 next-hop 10.18.103.254
set routing-options static route 172.16.103.0/24 next-hop 10.18.103.254
set routing-options static route 172.16.104.0/24 next-hop 10.18.103.254
set routing-options static route 10.10.100.0/24 next-hop 10.18.103.254
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256

```

```

set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-cbc
set security group-vpn member ike policy KeySrv mode main
set security group-vpn member ike policy KeySrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy KeySrv pre-shared-key ascii-text "$ABC123"
set security group-vpn member ike gateway KeySrv ike-policy KeySrv
set security group-vpn member ike gateway KeySrv server-address 10.10.100.1
set security group-vpn member ike gateway KeySrv local-address 10.18.103.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway KeySrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 match-direction output
set security group-vpn member ipsec vpn GROUP_ID-0001 tunnel-mtu 1400
set security group-vpn member ipsec vpn GROUP_ID-0001 df-bit clear
set services service-set GROUP_ID-0001 interface-service service-interface ms-0/2/0.0
set services service-set GROUP_ID-0001 ipsec-group-vpn GROUP_ID-0001
set firewall family inet service-filter GroupVPN-KS term inbound-ks from destination-address 10.10.100.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address 10.10.100.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address 10.10.100.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from source-address 172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from destination-address 172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 then service

```

???

?? VPNv2 ???

1. ???

[edit interfaces]

```
user@host# set xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-filter GroupVPN-KS
```

```
user@host# set xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-filter GroupVPN-KS
```

```
user@host# set xe-0/0/1 unit 0 family inet address 10.18.103.1/24
```



```

user@host# set xe-0/0/2 unit 0 family inet address 172.16.103.1/24
user@host# set ms-0/2/0 unit 0 family inet

```

## 2. `set static route`.

```

[edit routing-options]
user@host# set static route 10.18.101.0/24 next-hop 10.18.103.254
user@host# set static route 10.18.102.0/24 next-hop 10.18.103.254
user@host# set static route 10.18.104.0/24 next-hop 10.18.103.254
user@host# set static route 172.16.101.0/24 next-hop 10.18.103.254
user@host# set static route 172.16.102.0/24 next-hop 10.18.103.254
user@host# set static route 172.16.103.0/24 next-hop 10.18.103.254
user@host# set static route 172.16.104.0/24 next-hop 10.18.103.254
user@host# set static route 10.10.100.0/24 next-hop 10.18.103.254

```

## 3. IKE(Internet Key Exchange) `set security group-vpn member ike`.

```

[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256 ]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy KeySrv ]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn member ike gateway KeySrv]
user@host# set ike-policy KeySrv
user@host# set server-address 10.10.100.1
user@host# set local-address 10.18.103.1

```

## 4. IPsec SA `set security group-vpn member ipsec`.

```

[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway KeySrv
user@host# set group 1
user@host# set match-direction output
user@host# set tunnel-mtu 1400
user@host# set df-bit clear

```

5. `set term inbound-ks`.

```
[edit firewall family inet service-filter GroupVPN-KS]
user@host# set term inbound-ks from destination-address 10.10.100.1/32
user@host# set term inbound-ks from source-address 10.10.100.1/32
user@host# set term inbound-ks then skip
user@host# set term outbound-ks from destination-address 10.10.100.1/32
user@host# set term outbound-ks then skip
user@host# set term GROUP_ID-0001 from source-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 from destination-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 then service
```

6. `set ipsec-group-vpn`.

```
[edit services service-set GROUP_ID-0001]
user@host# set interface-service service-interface ms-0/2/0.0
user@host# set ipsec-group-vpn GROUP_ID-0001
```

??

?? `show interfaces`, `show routing-options`, `show security`, `show services` ? `show firewall` ??? ???? ???? ?????.

?? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.

```
[edit]
user@host# show interfaces
xe-0/0/1 {
  unit 0 {
    family inet {
      service {
        input {
          service-set GROUP_ID-0001 service-filter GroupVPN-KS;
        }
        output {
          service-set GROUP_ID-0001 service-filter GroupVPN-KS;
        }
      }
      address 10.18.103.1/24;
    }
  }
}
```

```

xe-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.103.1/24;
        }
    }
}
ms-0/2/0 {
    unit 0 {
        family inet;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.18.101.0/24 next-hop 10.18.103.254;
    route 10.18.102.0/24 next-hop 10.18.103.254;
    route 10.18.104.0/24 next-hop 10.18.103.254;
    route 172.16.101.0/24 next-hop 10.18.103.254;
    route 172.16.102.0/24 next-hop 10.18.103.254;
    route 172.16.103.0/24 next-hop 10.18.103.254;
    route 172.16.104.0/24 next-hop 10.18.103.254;
}
[edit]
user@host# show security
group-vpn {
    member {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                dh-group group14;
                authentication-algorithm sha-256;
                encryption-algorithm aes-256-cbc;
            }
            policy KeySrv {
                mode main;
                proposals PSK-SHA256-DH14-AES256;
                pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
            }
            gateway KeySrv {
                ike-policy KeySrv;
                local-address 10.18.103.1;
                server-address 10.10.101.1;
            }
        }
    }
}

```

```

    }
}
ipsec {
    vpn GROUP_ID-0001 {
        ike-gateway KeySrv
        group 1;
        match-direction output;
        tunnel-mtu 1400;
        df-bit clear;
    }
}
}
[edit]
user@host# show services
service-set GROUP_ID-0001 {
    interface-service {
        service-interface ms-0/2/0.0;
    }
    ipsec-group-vpn GROUP_ID-0001;
}
[edit]
user@host# show firewall
family inet {
    service-filter GroupVPN-KS {
        term inbound-ks {
            from {
                destination-address {
                    10.10.100.1/32;
                }
                source-address {
                    10.10.100.1/32;
                }
            }
            then skip;
        }
        term outbound-ks {
            from {
                destination-address {
                    10.10.100.1/32;
                }
            }
            then skip;
        }
    }
}

```

```

    }
    term GROUP_ID-0001 {
        from {
            source-address {
                172.16.0.0/12;
            }
            destination-address {
                172.16.0.0/12;
            }
        }
        then service;
    }
}
}

```

?? ?? ?? GM-0004 (MX ??? ????)

CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ??? ????? ???? , ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```

set interfaces xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet address 10.18.104.1/24
set interfaces xe-0/0/2 unit 0 family inet address 172.16.104.1/24
set interfaces ms-0/2/0 unit 0 family inet
set routing-options static route 10.18.101.0/24 next-hop 10.18.104.254
set routing-options static route 10.18.102.0/24 next-hop 10.18.104.254
set routing-options static route 10.18.103.0/24 next-hop 10.18.104.254
set routing-options static route 172.16.101.0/24 next-hop 10.18.104.254
set routing-options static route 172.16.102.0/24 next-hop 10.18.104.254
set routing-options static route 172.16.103.0/24 next-hop 10.18.104.254
set routing-options static route 172.16.104.0/24 next-hop 10.18.104.254
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256

```

```

set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy SubSrv mode main
set security group-vpn member ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy SubSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn member ike gateway SubSrv ike-policy SubSrv
set security group-vpn member ike gateway SubSrv server-address 10.17.101.1
set security group-vpn member ike gateway SubSrv server-address 10.17.102.1
set security group-vpn member ike gateway SubSrv server-address 10.17.103.1
set security group-vpn member ike gateway SubSrv server-address 10.17.104.1
set security group-vpn member ike gateway SubSrv local-address 10.18.104.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway SubSrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 match-direction output
set security group-vpn member ipsec vpn GROUP_ID-0001 tunnel-mtu 1400
set security group-vpn member ipsec vpn GROUP_ID-0001 df-bit clear
set services service-set GROUP_ID-0001 interface-service service-interface ms-0/2/0.0
set services service-set GROUP_ID-0001 ipsec-group-vpn GROUP_ID-0001
set firewall family inet service-filter GroupVPN-KS term inbound-ks from destination-address
10.10.100.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.10.100.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.101.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.102.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.103.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.104.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from source-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from destination-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 then service

```

?? ??

?? VPNv2 ??? ???? ???? ????.

1. `xe-0/0/1` `xe-0/0/2`.

```
[edit interfaces]
user@host# set xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet address 10.18.104.1/24
user@host# set xe-0/0/2 unit 0 family inet address 172.16.104.1/24
user@host# set ms-0/2/0 unit 0 family inet
```

2. `10.18.101.0/24` `10.18.102.0/24`.

```
[edit routing-options]
user@host# set static route 10.18.101.0/24 next-hop 10.18.104.254
user@host# set static route 10.18.102.0/24 next-hop 10.18.104.254
user@host# set static route 10.18.103.0/24 next-hop 10.18.104.254
user@host# set static route 172.16.101.0/24 next-hop 10.18.104.254
user@host# set static route 172.16.102.0/24 next-hop 10.18.104.254
user@host# set static route 172.16.103.0/24 next-hop 10.18.104.254
user@host# set static route 172.16.104.0/24 next-hop 10.18.104.254
```

3. IKE(Internet Key Exchange) `10.10.100.1` `10.18.104.1`.

```
[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256 ]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy KeySrv ]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn member ike gateway KeySrv]
user@host# set ike-policy KeySrv
user@host# set server-address 10.10.100.1
user@host# set local-address 10.18.104.1
```

4. IPsec SA `GROUP_ID-0001`.

```
[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway KeySrv
user@host# set group 1
user@host# set match-direction output
user@host# set tunnel-mtu 1400
user@host# set df-bit clear
```

5. `GROUP_ID-0001` `GROUP_ID-0001`.

```
[edit firewall family inet service-filter GroupVPN-KS]
user@host# set term inbound-ks from destination-address 10.10.101.1/32
user@host# set term inbound-ks from source-address 10.10.101.1/32
user@host# set term inbound-ks then skip
user@host# set term outbound-ks from destination-address 10.17.101.1/32
user@host# set term outbound-ks from destination-address 10.17.102.1/32
user@host# set term outbound-ks from destination-address 10.17.103.1/32
user@host# set term outbound-ks from destination-address 10.17.104.1/32
user@host# set term outbound-ks then skip
user@host# set term GROUP_ID-0001 from source-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 from destination-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 then service
```

6. `GROUP_ID-0001` `GROUP_ID-0001`.

```
[edit services service-set GROUP_ID-0001]
user@host# set interface-service service-interface ms-0/2/0.0
user@host# set ipsec-group-vpn GROUP_ID-0001
```

`??`

`??` `GROUP_ID-0001` show interfaces, show routing-options, show security, show services `?` show firewall `GROUP_ID-0001` `GROUP_ID-0001` `GROUP_ID-0001`.

```
[edit]
user@host# show interfaces
xe-0/0/1 {
  unit 0 {
```



```

        family inet {
            service {
                input {
                    service-set GROUP_ID-0001 service-filter GroupVPN-KS;
                }
                output {
                    service-set GROUP_ID-0001 service-filter GroupVPN-KS;
                }
            }
            address 10.18.104.1/24;
        }
    }
}
xe-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.104.1/24;
        }
    }
}
ms-0/2/0 {
    unit 0 {
        family inet;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.18.101.0/24 next-hop 10.18.104.254;
    route 10.18.102.0/24 next-hop 10.18.104.254;
    route 10.18.103.0/24 next-hop 10.18.104.254;
    route 172.16.101.0/24 next-hop 10.18.104.254;
    route 172.16.102.0/24 next-hop 10.18.104.254;
    route 172.16.103.0/24 next-hop 10.18.104.254;
    route 172.16.104.0/24 next-hop 10.18.104.254;
}
[edit]
user@host# show security
group-vpn {
    member {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
            }
        }
    }
}

```

```

        dh-group group14;
        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
    }
    policy KeySrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway KeySrv {
        ike-policy KeySrv;
        local-address 10.18.104.1;
        server-address 10.17.101.1;
    }
}
ipsec {
    vpn GROUP_ID-0001 {
        ike-gateway KeySrv
        group 1;
        match-direction output;
        tunnel-mtu 1400;
        df-bit clear;
    }
}
}
[edit]
user@host# show services
service-set GROUP_ID-0001 {
    interface-service {
        service-interface ms-0/2/0.0;
    }
    ipsec-group-vpn GROUP_ID-0001;
}
[edit]
user@host# show firewall
family inet {
    service-filter GroupVPN-KS {
        term inbound-ks {
            from {
                destination-address {
                    10.10.100.1/32;
                }
            }
        }
    }
}

```

```

        source-address {
            10.10.100.1/32;
        }
    }
    then skip;
}
term outbound-ks {
    from {
        destination-address {
            10.17.101.1/32;
            10.17.102.1/32;
            10.17.103.1/32;
            10.17.104.1/32;
        }
    }
    then skip;
}
term GROUP_ID-0001 {
    from {
        source-address {
            172.16.0.0/12;
        }
        destination-address {
            172.16.0.0/12;
        }
    }
    then service;
}
}
}

```

??

#### in this section

- [?? ?? ?? ?? | 850](#)
- [?? ?? ?? ?? ?? ?? | 851](#)
- [?? ?? ?? ?? VPN SA ?? | 851](#)
- [?? ?? ?? ?? VPN SA ?? | 852](#)

- [?? ???? IPsec SA ?? | 854](#)
- [?? ???? ?? IPsec SA ?? | 855](#)
- [?? ?? ??\(SRX ??? ???? ?? vSRX ?? ??? ?? ??? ??\) | 857](#)

??? ???? ???? ???? ????.

?? ?? ?? ??

??

?? ???? ???? ???? ???? ????.

??

?? ???? ???? ? show security group-vpn server registered-membersshow security group-vpn server registered-members detail ??? ????.

```
user@host> show security group-vpn server registered-members
Group: GROUP_ID-0001, Group Id: 1
Total number of registered members: 2
Member Gateway      Member IP      Last Update      Vsys
GM-0001             10.18.101.1   Thu Nov 19 2015 16:31:09 root
GM-0003             10.18.103.1   Thu Nov 19 2015 16:29:47 root
```

```
user@host> show security group-vpn server registered-members detail
GGroup: GROUP_ID-0001, Group Id: 1
Total number of registered members: 2

Member gateway: GM-0001, Member IP: 10.18.101.1, Vsys: root
Last Update: Thu Nov 19 2015 16:31:09
Stats:
Pull Succeeded      : 2
Pull Failed         : 0
Push Sent           : 0
Push Acknowledged   : 0
Push Unacknowledged : 0
```

Member gateway: GM-0003, Member IP: 10.18.103.1, Vsys: root

Last Update: Thu Nov 19 2015 16:29:47

Stats:

|                     |     |
|---------------------|-----|
| Pull Succeeded      | : 1 |
| Pull Failed         | : 0 |
| Push Sent           | : 0 |
| Push Acknowledged   | : 0 |
| Push Unacknowledged | : 0 |

?? ?? ??????? ??

??

?? ?? ????? ??????? ??????.

??

?? ????? ?? ??? ??? ????? show security group-vpn server statistics .

user@host> **show security group-vpn server statistics**

Group: GROUP\_ID-0001, Group Id: 1

Stats:

|                              |     |
|------------------------------|-----|
| Pull Succeeded               | : 4 |
| Pull Failed                  | : 0 |
| Pull Exceed Member Threshold | : 0 |
| Push Sent                    | : 0 |
| Push Acknowledged            | : 0 |
| Push Unacknowledged          | : 0 |

?? ????? ?? **VPN SA** ??

??

?? ????? ?? **VPN SA** ??????.

??

?? ???? ?? ??? ? show security group-vpn server kek security-associations detail ??? ??????show security group-vpn server kek security-associations.

```
user@host> show security group-vpn server kek security-associations
```

```
Index   Life:sec Initiator cookie Responder cookie GroupId
738879  1206      a471513492db1e13  24045792a4b3dd64  1
```

```
user@host> show security group-vpn server kek security-associations detail
```

```
Index 738879, Group Name: GROUP_ID-0001, Group Id: 1
```

```
Initiator cookie: a471513492db1e13, Responder cookie: 24045792a4b3dd64
```

```
Authentication method: RSA
```

```
Lifetime: Expires in 1204 seconds, Activated
```

```
Rekey in 694 seconds
```

```
Algorithms:
```

```
Sig-hash          : sha256
```

```
Encryption        : aes256-cbc
```

```
Traffic statistics:
```

```
Input bytes      : 0
```

```
Output bytes     : 0
```

```
Input packets    : 0
```

```
Output packets   : 0
```

```
Server Member Communication: Unicast
```

```
Retransmission Period: 10, Number of Retransmissions: 2
```

```
Group Key Push sequence number: 0
```

```
PUSH negotiations in progress: 0
```

?? ???? ?? ?? VPN SA ??

??

?? ???? ?? VPN SA? ??????.

??

?? ???? SRX ??? ???? ?? vSRX ?? ???? ?? ???? ? show security group-vpn member kek security-associations  
detail ??? ????show security group-vpn member kek security-associations.

```
user@host> show security group-vpn member kek security-associations
Index   Server Address  Life:sec  Initiator cookie  Responder cookie  GroupId
5455810 10.10.100.1     1093     a471513492db1e13 24045792a4b3dd64 1
```

```
user@host> show security group-vpn member kek security-associations detail
```

```
Index 5455810, Group Id: 1
Group VPN Name: GROUP_ID-0001
Local Gateway: 10.18.101.1, GDOI Server: 10.10.100.1
Initiator cookie: a471513492db1e13, Responder cookie: 24045792a4b3dd64
Lifetime: Expires in 1090 seconds
Group Key Push Sequence number: 0
```

Algorithms:

```
Sig-hash          : hmac-sha256-128
Encryption        : aes256-cbc
```

Traffic statistics:

```
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
```

Stats:

```
Push received      : 0
Delete received    : 0
```

?? ???? MX ??? ? ???? show security group-vpn member kek security-associations ? show security group-vpn  
member kek security-associations detail ??? ????.

```
user@host> show security group-vpn member kek security-associations
Index   Server Address  Life:sec  Initiator cookie  Responder cookie  GroupId
488598 10.10.100.1     963      a471513492db1e13 24045792a4b3dd64 1
```

```
user@host> show security group-vpn member kek security-associations detail
```

```
Index 488598, Group Id: 1
Group VPN Name: GROUP_ID-0001
```

```
Local Gateway: 10.18.103.1, GDOI Server: 10.10.100.1
Initiator cookie: a471513492db1e13, Responder cookie: 24045792a4b3dd64
Lifetime: Expires in 961 seconds
Group Key Push Sequence number: 0

Algorithms:
  Sig-hash      : hmac-sha256-128
  Encryption    : aes256-cbc
Traffic statistics:
  Input bytes   : 0
  Output bytes  : 0
  Input packets: 0
  Output packets: 0
Stats:
  Push received      : 0
  Delete received    : 0
```

?? ???? IPsec SA ??

??

?? ???? IPsec SA? ?????.

??

?? ???? ? ? show security group-vpn server ipsec security-associations detail ??? ????show security group-vpn server ipsec security-associations.

```
user@host> show security group-vpn server ipsec security-associations
Group: GROUP_ID-0001, Group Id: 1
Total IPsec SAs: 1
IPsec SA      Algorithm      SPI      Lifetime
GROUP_ID-0001 ESP:aes-256/sha256 1c548e4e 1156
```

```
user@host> show security group-vpn server ipsec security-associations detail
Group: GROUP_ID-0001, Group Id: 1
Total IPsec SAs: 1
IPsec SA: GROUP_ID-0001
  Protocol: ESP, Authentication: sha256, Encryption: aes-256
  Anti-replay: D3P enabled
```



```
SPI: 1c548e4e
Lifetime: Expires in 1152 seconds, Activated
Rekey in 642 seconds
Policy Name: 1
  Source: 172.16.0.0/12
  Destination: 172.16.0.0/12
  Source Port: 0
  Destination Port: 0
  Protocol: 0
```

?? ???? ?? IPsec SA ??

??

?? ???? IPsec SA? ??????.

??

?? ???? SRX ??? ???? ?? vSRX ?? ??? ?? ??? ? show security group-vpn member ipsec security-associations detail ??? ??????show security group-vpn member ipsec security-associations.

```
user@host> show security group-vpn member ipsec security-associations
Total active tunnels: 1
ID      Server      Port Algorithm      SPI      Life:sec/kb  GId lsys
<>49152 10.10.100.1  848  ESP:aes-256/sha256-128 1c548e4e 1073/ unlim 1 root
```

```
user@host> show security group-vpn member ipsec security-associations detail
Virtual-system: root Group VPN Name: GROUP_ID-0001
Local Gateway: 10.18.101.1, GDOI Server: 10.10.100.1
Group Id: 1
Routing Instance: default
Recovery Probe: Enabled
DF-bit: clear
Stats:
  Pull Succeeded      : 4
  Pull Failed         : 3
  Pull Timeout        : 3
  Pull Aborted        : 0
  Push Succeeded      : 6
  Push Failed         : 0
```

```

Server Failover      : 0
Delete Received     : 0
Exceed Maximum Keys(4) : 0
Exceed Maximum Policies(10): 0
Unsupported Algo     : 0

```

Flags:

```
Rekey Needed: no
```

List of policies received from server:

Tunnel-id: 49152

Source IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Destination IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Direction: bi-directional, SPI: 1c548e4e

Protocol: ESP, Authentication: sha256-128, Encryption: aes-256

Hard lifetime: Expires in 1070 seconds, Activated

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 931 seconds

Mode: Tunnel, Type: Group VPN, State: installed

Anti-replay service: D3P enabled

?? ???? MX ??? ?? ??? show security group-vpn member ipsec security-associations ? show security group-vpn member ipsec security-associations detail ??? ?????.

```
user@host> show security group-vpn member ipsec security-associations
```

```
Total active tunnels: 1
```

| ID      | Server      | Port | Algorithm              | SPI      | Life:sec/kb | GId   | lsys   |
|---------|-------------|------|------------------------|----------|-------------|-------|--------|
| <>10001 | 10.10.100.1 | 848  | ESP:aes-256/sha256-128 | 1c548e4e | 947/        | unlim | 1 root |

```
user@host> show security group-vpn member ipsec security-associations detail
```

```
Virtual-system: root Group VPN Name: GROUP_ID-0001
```

```
Local Gateway: 10.18.103.1, GDOI Server: 10.10.100.1
```

```
Group Id: 1
```

```
Rule Match Direction: output, Tunnel-MTU: 1400
```

```
Routing Instance: default
```

```
DF-bit: clear
```

Stats:

```

Pull Succeeded      : 2
Pull Failed         : 0
Pull Timeout        : 1
Pull Aborted        : 0

```

```

Push Succeeded      : 2
Push Failed         : 0
Server Failover     : 0
Delete Received     : 0
Exceed Maximum Keys(4) : 0
Exceed Maximum Policies(1): 0
Unsupported Algo     : 0

```

#### Flags:

```
Rekey Needed: no
```

#### List of policies received from server:

```
Tunnel-id: 10001
```

```
Source IP: ipv4_subnet(any:0,[0..7]=172.16.0.0/12)
```

```
Destination IP: ipv4_subnet(any:0,[0..7]=172.16.0.0/12)
```

```
Direction: bi-directional, SPI: 1c548e4e
```

```
Protocol: ESP, Authentication: sha256-128, Encryption: aes-256
```

```
Hard lifetime: Expires in 945 seconds, Activated
```

```
Lifetime Remaining: Unlimited
```

```
Soft lifetime: Expires in 840 seconds
```

```
Mode: Tunnel, Type: Group VPN, State: installed
```

```
Anti-replay service: D3P enabled
```

```
?? ?? ??(SRX ??? ???? ?? vSRX ?? ???? ?? ???? ??)
```

```
??
```

```
SRX ??? ???? ?? vSRX ?? ???? ?? ???? ?? ???? ?????.
```

```
??
```

```
?? ???? ?? ???? show security group-vpn member policy ??? ?????.
```

```
user@host> show security group-vpn member policy
```

```
Group VPN Name: GROUP_ID-0001, Group Id: 1
```

```
From-zone: LAN, To-zone: WAN
```

```
Tunnel-id: 49152, Policy type: Secure
```

```
Source      : IP <172.16.0.0 - 172.31.255.255>, Port <0 - 65535>, Protocol <0>
```

```
Destination : IP <172.16.0.0 - 172.31.255.255>, Port <0 - 65535>, Protocol <0>
```

```
Tunnel-id: 63488, Policy type: Fail-close
```

```
Source      : IP <0.0.0.0 - 255.255.255.255>, Port <0 - 65535>, Protocol <0>
Destination: IP <0.0.0.0 - 255.255.255.255>, Port <0 - 65535>, Protocol <0>
```

## SEE ALSO

?? ???? ?? VPNv2?? ?? VPN ??

?: ? ? ? ? ? ? ? ? ? ? ? ? ? ? VPNv2 ? ? - ? ? ? ? ? ?

in this section

- | 858  
 ●   | 858  
 ●   | 859  
 ●   | 859

[illegible]

?? ??

□□□□ □□:

- IKE(Internet Key Exchange) 1?? ???? ?? ?? ?? ? ????? ?????.
- IPsec SA? ?? ?? ?? ? ????? ?????.
- ?? ????? ??? g1 ?????.

??

group g1

- `???` `??` `????` `??????` `?` `???` `????` `????`.
- AES-128-CBC? `????` `??` `??` `????` `??????` `?` `??????`.
- SHA-256? `????` `???` `??????`.

???? KEK ?? ? ?????????.

??

in this section

● ?? | 859

??

??? ??

?? ?? ?? ?????? ??? ???? ???????. ??? ??? ?? ????? CLI ??? ??? ???????.

?? ??? ??? ?????? ??? ??????.

1. ?? ??? ??????.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set communications-type unicast
```

2. ??? ?????? ??????.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set encryption-algorithm aes-128-cbc
```

3. ??? ??? ??????.

```
[edit security group-vpn server group g1 server-member-communication]
user@host# set sig-hash-algorithm sha-256
```

??

??? ??? ?????? ?????? ??? ?????? show security group-vpn server group g1 server-member-communication .

SEE ALSO

|                                                     |
|-----------------------------------------------------|
| <a href="#">??: ?? VPNv1 ?? ? ??? ??   763</a>      |
| <a href="#">?: ?? ?? ???????? ?? VPNv1 ??   789</a> |

?? ??

|                                   |
|-----------------------------------|
| VPN ??? ?????                     |
| <a href="#">VPN ?? ???   1360</a> |

?? VPNv2 ?? ?????

summary

?? VPNv2 ?? ?????? ?? ?????? ? ??? ??????.

in this section

- [?? VPNv2 ?? ????? ????? | 860](#)
- [?? VPNv2 ?? ????? ?? ?? ????? | 864](#)
- [?? VPNv2 ?? ????? ??? ????? | 865](#)
- [?? VPNv2 ?? ?????? ?? ?? ????? | 867](#)
- [???? ?? VPNv2 ??? ?? VPNv2 ?? ?????? ?????? ? | 870](#)
- [?: ?? VPNv2 ?? ????? ? ??? ?? | 871](#)

?? VPNv2 ?? ?????? ?? ?????/? ??(GCKS) ????? ?????? ?? ?? VPN ?????? ?? ?? ??? ?????.

?? VPNv2 ?? ????? ?????

in this section

- [?? ?? ? ?? ?? | 861](#)
- [?? ?????? ?? ??? ??Group Member Registration with Server Clusters | 863](#)

- Dead Peer Detection(?? ?? ??) | 863
- ?? ?? | 864

GDOI(Group Domain of Interpretation) ?????? ?? ?????/? ??(GCKS)? ?? VPN ?? ??(SA)? ?????? ?? ?? ??  
?? ?? ?????? ??????. ?? ??? GCKS?? ????? ?? SA ? ?? ?????? ?????? ???????. GCKS? ?????? ?? ??? ?? ?????? ??  
? ??????. ?? VPNv2 ?? ?????? GCKS ?????? ?????? ?? ?? VPN ?????? ?? ?? ??? ??????. ?? VPNv2 ?? ?????? ??  
????, ?? ? ?? ??? ??? ? ?????.

?? VPNv2 ?? ?????? ?? ??? SRX ??? ?? ?? vSRX ?? ??? ?????? ?????? ???. ?? VPNv2 ?? ?????? ??? ??  
???? ?? ?????? ?? ??? GCKS? ?? ?????? ?????.

?? ?? ? ?? ??

?? VPNv2 ?? ?????? ??? ?? ??? ?? 4?? ??? ?? ??? ??????. ?????? ?? ??? ?? VPNv2 ?????? ?????? ??? SA ? ?  
?? ?? ??????. ?????? ??? ? ??? ?? 51 ??? 862?? ?? ?? ?????? ?? ? ?????.



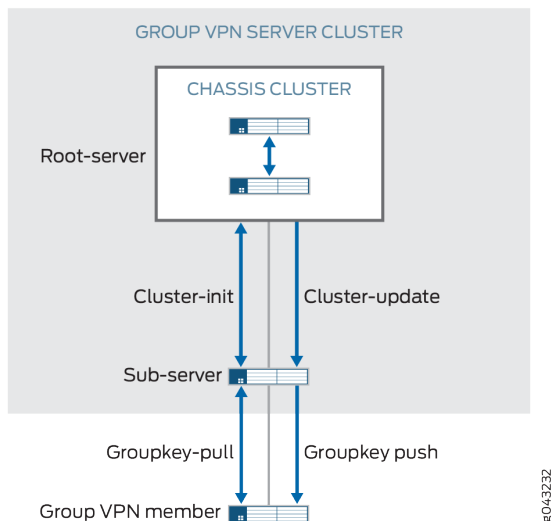








## ?? 52: ?? VPNv2 ?? ???? ???



### Cluster-Init ??

?? ??? SA ? ??? ? ??? ?? ?? ?? ??? ???? ???? (cluster-init) ??? ?????. ?? ??? ?? ?? SA ??? ?? ??? ?? ??? ???? cluster-init .

?? ?? ?? ??? ??? ?? ?? VPNv2 ??? ?? ??? ??? ? ???? groupkey-pull . ? ??? groupkey-pull ?? ?? VPNv2 ??? ?? ??? SA? ?? ??? ? ????.

?? ??? ??? ?? ?? ?? ??? ??? ???? cluster-init .

- ?? ??? ???? ?????. ?? ?? ?? ?? ?? ?????. ?? ?? ?? ?? ??? IKE SA? ?? ?? ?? ??? ?? ??? ?? IKE SA? ?????. ?? ?? cluster-init ?? ?? ??? SA? ?? ??? ?? ?? ??? ?? ??? ????.
- SA? ??? ?? ????.
- cluster-update ?? SA? ???? ???? ????.
- ?? ?? ?? ??? ????.

??? cluster-init ???? ?? ??? 5??? ?? ??? ??? ????.

### ???? ???? ???

??? groupkey-push ?? ?? SA? ???? ?? ?? ????/? ?? (GCKS)? ?? SA? ?? ???? ???? ?? ???? ???? ? ?? ?? ?? ? ???? ?????. ? ??? ???? GCKS? ???? ???? ?? ?? ????.

SA? ?? ? ??? ?? ??? ? ?? ??? ???? ?? cluster-update ?? ?? ?? SA ???? ?????. ?? ???? a? cluster-update ???? ?, ?? ??? SA? ???? a groupkey-push ? ?? ??? SA ??? ?? ???? ????.



**Figure 113: VPNv2 Configuration (Continued)**

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|------|
| ?? ??  | ?? ? VPNv2 ? ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | ?? VPNv2 ? ? ? ? ? |      |
|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | ?? ?               | ?? ? |
| ?? ? ? | ?? ? ? ? '?? ?' ? ? ? ? , ? ? ? ? IKE(Internet Key Exchange) SA ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? |                    |      |

113: 22 222 22 VPNv2 222 222 22 (Continued)

| 22 22 | 222 22 VPNv2 22 22                              | 22 VPNv2 22 2222 22                                                                          |                 |
|-------|-------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------|
|       |                                                 | 22 22                                                                                        | 22 22           |
| 2222  | 22 KEK SA? 222222 222 22<br>22. KEK SA? 222222. | 22 2222 2222 22222. KEK SA<br>? 222222, 22 2222<br>IKE(Internet Key<br>Exchange) SA? 222222. | KEK SA? 222222. |

IPsec SA:

|       |                                                                                                                                            |                                                         |                                    |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|------------------------------------|
| 222   | 2 TEK SA? 222222. 222 22<br>2 TEK SA? 22222222.                                                                                            | 2 TEK SA? 222222, 2 TEK<br>SA? 22 2222 22222.           | 22 2222 22222 22222.               |
| 22    | 2 22 TEK ? 2222 ? 222222.<br>22 2222 22222 22 TEK? 22 ?<br>2222 ? 2222 2222222 22222 22<br>2222 2222 2222 delete<br>groupkey-push? 222222. | 22 2222 22222 22 2222 2222 ?<br>2222. TEK? 22 22222222. | 22 2222 22222 TEK? 22 22222<br>22. |
| 22222 | TEK? 22 22222222. 2 TEK<br>SA? 222222 2222 22222.                                                                                          | 22 2222 2222 22222. TEK? ?<br>? 22222222.               | TEK? 22 22222222.                  |

114 222 869 22 22 VPNv2 22 22222 22 2222 2222 22222 22222.

22 22 222222 22 2222 2222 22222 22222.

114: 22 VPNv2 22 22222 22 2222 22

| 22 22222 22 22                                               | 22 VPNv2 22 22222                                                                               |       |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------|
|                                                              | 22 22                                                                                           | 22 22 |
| IKE(Internet Key<br>Exchange) 22, 22 22 22<br>2222(22222 22) | 2222 22 22 2222 22222. 22 22 2222 22 2222 22 2222 22 IKE(Internet Key Exchange) SA? 22222<br>2. |       |

### Figure 114: VPNv2 Peer Configuration (Continued)

| Peer Name                                                               | VPNv2 Peer Configuration                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                         | Peer IP                                                                                                                                                                                                                                                                                 | Peer Port                                                                                                                                                                                                                                                                              |
| Peer Name:                                                              |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                        |
| Peer IP                                                                 | Peer IP.                                                                                                                                                                                                                                                                                | Peer Port 'Peer IP' Peer Port. Peer IP Peer Port<br>IKE(Internet Key Exchange) SA Peer Port. Peer Port<br>Peer TEK Peer KEK Peer Peer Port. Peer Peer Peer Peer Peer Peer<br>Peer Peer Peer Peer cluster-init .                                                                        |
| Peer Port<br>Peer Peer Peer Peer Peer Peer Peer<br>Peer Peer Peer Peer. | Peer Peer "Peer IP" Peer Port. Peer IP Peer Port<br>IKE(Internet Key Exchange) SA Peer Port<br>Peer Peer Peer TEK Peer KEK Peer Peer Port. Peer Peer<br>Peer Peer Peer Peer Peer Peer. Peer Peer Peer IKE(Internet<br>Key Exchange) SA Peer Port. Peer Peer Peer<br>Peer cluster-init . | TEK Peer Peer Peer Peer. KEK Peer Peer Peer Peer. Peer Peer<br>Peer Peer Peer. Peer Peer Peer Peer.                                                                                                                                                                                    |
| Peer Port                                                               | Peer.                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                        |
| Peer Port                                                               | Peer Peer Peer Peer Peer Peer. Peer IKE(Internet Key<br>Exchange) SA Peer Port.                                                                                                                                                                                                         | Peer Peer Peer Peer. KEK Peer Peer. TEK Peer Peer. Peer<br>IKE(Internet Key Exchange) SA Peer Port.                                                                                                                                                                                    |
| Peer Peer Peer                                                          | Peer.                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                        |
| Peer Peer Peer Peer                                                     | Peer Peer "Peer IP" Peer Port. Peer Peer Peer TEK Peer<br>KEK Peer Peer Port. Peer Peer Peer Peer Peer Peer. Peer<br>Peer Peer IKE(Internet Key Exchange) SA<br>Peer Peer Port. Peer Peer Peer TEK Peer KEK Peer Port.                                                                  | Peer Peer Peer IKE(Internet Key Exchange) SA<br>Peer Port. Peer Peer Peer TEK Peer KEK Peer Peer Port. Peer Peer<br>Peer Peer Peer Peer Peer Peer. Peer Peer Peer Peer Peer Peer. Peer Peer<br>IKE(Internet Key Exchange) SA Peer Port. Peer Peer Peer<br>Peer TEK Peer KEK Peer Port. |

### VPNv2 Peer Configuration VPNv2 Peer Configuration

Peer Peer Peer VPNv2 Peer Peer VPNv2 Peer Peer Peer Peer Peer Peer Peer Peer Peer.







- 22 2222 222 root-server 22 2 22 222 22 22222 22 IKE 222222 222222.

22 222 22 2222 222 22222 22222 2222. 2 222 22 222 22 222 222222 22 22222 2 22 222 222222. 22 22 2222 222 2222 22222.

2 22 22222:

- 2 22 IKE(Internet Key Exchange) 222 222222. RootSrv 22 222 22 122 SA2 2222 2 22222 GMs , 2 22 222 22 1 22 SA2 2222 2 222222.

22 22 22 22 222 22 22 22, 22 222 22 22 22 122 SA2 2222 2 222222. 222 22 22 22 222 222 222222. 22 222 2 IKE(Internet Key Exchange) 222 RootSrv 22 222 22 22 22 22 222 222 22 22 22 2222 22 IKE(Internet Key Exchange) 222 GMs 22 222 22 22 22 22 222 222 22 22 22 2222 2222.

- IKE(Internet Key Exchange) 222222 22 222 DPD2 222222. 22 2 22 222 22 IKE(Internet Key Exchange) 2 22222 222222.

- 22 2222 222 22 sub-server 22 222 22 22222 22 IKE 222222 222222.

2 22 2222 22 222 222222.

- IKE(Internet Key Exchange) 222 SubSrv 22 222 22 122 SA2 2222 2 222222.

- IKE(Internet Key Exchange) 222222 22222 22 222 222 222222.

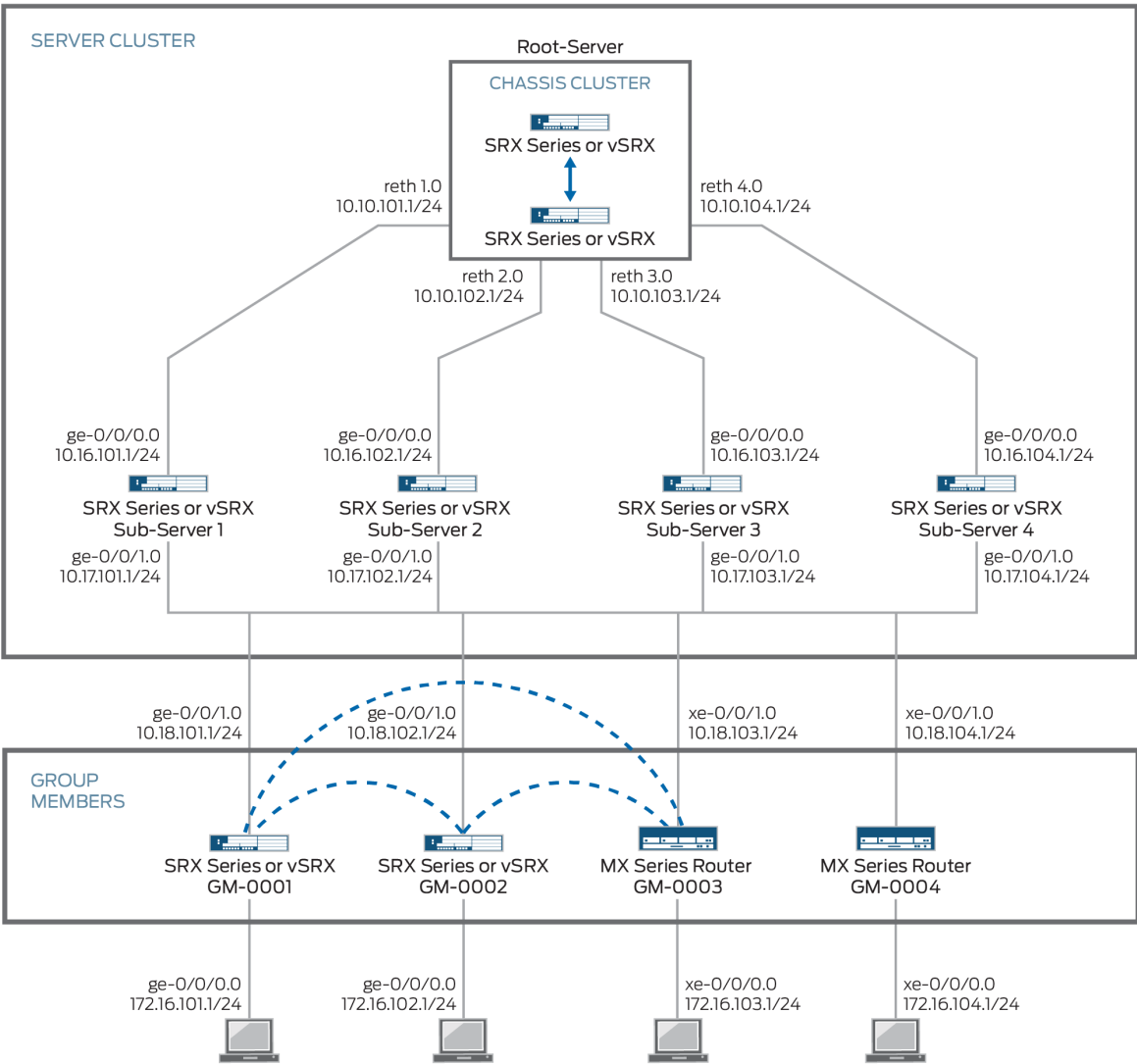
SRX 222 222 22 vSRX 22 222 22 22222 LAN 222 22 22(22 222)22, WAN 222 22 22(22 222)22 2222 222 22 IPsec 222 222222. LAN2 WAN 22 22 2222 222222 22 222 222222.

22 222 22 22 2222 222 22 2222 2222 2222. 2 222 22 222 GROUP\_ID-000122 22 2222 1222. 222 222 22 22 2 SA2 22 172.16.0.0/12 222 2222222 2 2222 222222 222222.

22222

22 53 222 874 2(2) 2 222 222 222 2222 22222 222222.

53: SRX vSRX MX VPNv2



8043373

??

in this section

- 875
- 884
- 892
- 900

- [?? ?? ?? 4 | 908](#)
- [GM-0001 ??\(SRX ??? ???? ?? vSRX ?? ??? ?????\) | 916](#)
- [GM-0002 ??\(SRX ??? ???? ?? vSRX ?? ??? ?????\) | 923](#)
- [GM-0003 ??\(MX ??? ?????\) | 930](#)
- [GM-0004 ??\(MX ??? ?????\) | 936](#)

?? ?? ??

## CLI ?? ??

? ?? ??? ??????, ?? ??? ????? ???? ???? ?? ?? ?? ???? ????? ?????, ????? ???? ????? ? ??? ???? ???? [edit] ?  
 ? ????? ???? CLI? ??? ???? ???? ???? ???? ???? commit?(?) ??????.

```
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 description To_SubSrv01
set interfaces reth1 unit 0 family inet address 10.10.101.1/24
set interfaces reth2 redundant-ether-options redundancy-group 1
set interfaces reth2 unit 0 description To_SubSrv02
set interfaces reth2 unit 0 family inet address 10.10.102.1/24
set interfaces reth3 redundant-ether-options redundancy-group 1
set interfaces reth3 unit 0 description To_SubSrv03
set interfaces reth3 unit 0 family inet address 10.10.103.1/24
set interfaces reth4 redundant-ether-options redundancy-group 1
set interfaces reth4 unit 0 description To_SubSrv04
set interfaces reth4 unit 0 family inet address 10.10.104.1/24
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces reth1.0
set security zones security-zone GROUPVPN interfaces reth2.0
set security zones security-zone GROUPVPN interfaces reth3.0
set security zones security-zone GROUPVPN interfaces reth4.0
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
```

```

set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set chassis cluster reth-count 5
set chassis cluster redundancy-group 1 node 0 priority 254
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 254
set chassis cluster redundancy-group 0 node 1 priority 1
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy SubSrv mode main
set security group-vpn server ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy SubSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike gateway SubSrv01 ike-policy SubSrv
set security group-vpn server ike gateway SubSrv01 address 10.16.101.1
set security group-vpn server ike gateway SubSrv01 dead-peer-detection always-send
set security group-vpn server ike gateway SubSrv01 local-address 10.10.101.1
set security group-vpn server ike gateway SubSrv02 ike-policy SubSrv
set security group-vpn server ike gateway SubSrv02 address 10.16.102.1
set security group-vpn server ike gateway SubSrv02 dead-peer-detection always-send
set security group-vpn server ike gateway SubSrv02 local-address 10.10.102.1
set security group-vpn server ike gateway SubSrv03 ike-policy SubSrv
set security group-vpn server ike gateway SubSrv03 address 10.16.103.1
set security group-vpn server ike gateway SubSrv03 dead-peer-detection always-send
set security group-vpn server ike gateway SubSrv03 local-address 10.10.103.1
set security group-vpn server ike gateway SubSrv04 ike-policy SubSrv
set security group-vpn server ike gateway SubSrv04 address 10.16.104.1
set security group-vpn server ike gateway SubSrv04 dead-peer-detection always-send
set security group-vpn server ike gateway SubSrv04 local-address 10.10.104.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000
set security group-vpn server group GROUP_ID-0001 server-cluster server-role root-server
set security group-vpn server group GROUP_ID-0001 server-cluster ike-gateway SubSrv01

```

```

set security group-vpn server group GROUP_ID-0001 server-cluster ike-gateway SubSrv02
set security group-vpn server group GROUP_ID-0001 server-cluster ike-gateway SubSrv03
set security group-vpn server group GROUP_ID-0001 server-cluster ike-gateway SubSrv04
set security group-vpn server group GROUP_ID-0001 server-cluster retransmission-period 10
set security group-vpn server group GROUP_ID-0001 anti-replay-time-window 1000
set security group-vpn server group GROUP_ID-0001 server-member-communication communication-type
unicast
set security group-vpn server group GROUP_ID-0001 server-member-communication encryption-
algorithm aes-256-cbc
set security group-vpn server group GROUP_ID-0001 server-member-communication lifetime-seconds
7200
set security group-vpn server group GROUP_ID-0001 server-member-communication sig-hash-algorithm
sha-256
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-
L3600
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 source
172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1
destination 172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 protocol
0

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

?? ??? ???? ???? ????.

1. ?? ?? ? ?? ???? ????.

```

[edit interfaces]
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 description To_SubSrv01
user@host# set reth1 unit 0 family inet address 10.10.101.1/24
user@host# set reth2 redundant-ether-options redundancy-group 1
user@host# set reth2 unit 0 description To_SubSrv02
user@host# set reth2 unit 0 family inet address 10.10.102.1/24
user@host# set reth3 redundant-ether-options redundancy-group 1
user@host# set reth3 unit 0 description To_SubSrv03
user@host# set reth3 unit 0 family inet address 10.10.103.1/24
user@host# set reth4 redundant-ether-options redundancy-group 1
user@host# set reth4 unit 0 description To_SubSrv04

```

```

user@host# set reth4 unit 0 family inet address 10.10.104.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces reth1.0
user@host# set interfaces reth2.0
user@host# set interfaces reth3.0
user@host# set interfaces reth4.0
[edit security policies global]
user@host# set policy 1000 match source-address any
user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit security policies]
user@host# set default-policy deny-all

```

## 2. `set chassis cluster`.

```

[edit chassis cluster]
user@host# set reth-count 5
user@host# set redundancy-group 1 node 0 priority 254
user@host# set redundancy-group 1 node 1 priority 1
user@host# set redundancy-group 0 node 0 priority 254
user@host# set redundancy-group 0 node 1 priority 1

```

## 3. IKE(Internet Key Exchange) `set security group-vpn server ike proposal`.

```

[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy SubSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"

```



```

[edit security group-vpn server ike gateway SubSrv01]
user@host# set ike-policy SubSrv
user@host# set address 10.16.101.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.10.101.1
[edit security group-vpn server ike gateway SubSrv02]
user@host# set ike-policy SubSrv
user@host# set address 10.16.102.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.10.102.1
[edit security group-vpn server ike gateway SubSrv03]
user@host# set ike-policy SubSrv
user@host# set address 10.16.103.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.10.103.1
[edit security group-vpn server ike gateway SubSrv04]
user@host# set ike-policy SubSrv
user@host# set address 10.16.104.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.10.104.1

```

#### 4. IPsec SA `???`.

```

[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600

```

#### 5. VPN `???`.

```

[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set server-cluster server-role root-server
user@host# set server-cluster ike-gateway SubSrv01
user@host# set server-cluster ike-gateway SubSrv02
user@host# set server-cluster ike-gateway SubSrv03
user@host# set server-cluster ike-gateway SubSrv04
user@host# set server-cluster retransmission-period 10
user@host# set anti-replay-time-window 1000
user@host# set server-member-communication communication-type unicast

```



```

}
reth3 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        description To_SubSrv03;
        family inet {
            address 10.10.103.1/24;
        }
    }
}
reth4 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        description To_SubSrv04;
        family inet {
            address 10.10.104.1/24;
        }
    }
}
[edit]
user@host# show chassis cluster
reth-count 5;
redundancy-group 1 {
    node 0 priority 254;
    node 1 priority 1;
}
redundancy-group 0 {
    node 0 priority 254;
    node 1 priority 1;
}
[edit]
user@host# show security
group-vpn {
    server {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                authentication-algorithm sha-256;
                dh-group group14;
            }
        }
    }
}

```

```

        encryption-algorithm aes-256-cbc;
    }
    policy SubSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
    gateway SubSrv01 {
        ike-policy SubSrv;
        address 10.16.101.1;
        dead-peer-detection always-send;
        local-address 10.10.101.1;
    }
    gateway SubSrv02 {
        ike-policy SubSrv;
        address 10.16.102.1;
        dead-peer-detection always-send;
        local-address 10.10.102.1;
    }
    gateway SubSrv03 {
        ike-policy SubSrv;
        address 10.16.103.1;
        dead-peer-detection always-send;
        local-address 10.10.103.1;
    }
    gateway SubSrv04 {
        ike-policy SubSrv;
        address 10.16.104.1;
        dead-peer-detection always-send;
        local-address 10.10.104.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
    server-cluster {

```



```

    }
    default-policy {
        deny-all;
    }
}
zones {
    security-zone GROUPVPN {
        host-inbound-traffic {
            system-services {
                ike;
                ssh;
                ping;
            }
        }
        interfaces {
            reth1.0;
            reth2.0;
            reth3.0;
            reth4.0;
        }
    }
}
}

```

```

?? ?? ?? ?? ?? commit?(?) ??????.

```

```

?? ?? 1 ??

```

**CLI ?? ??**

```

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```

```

set interfaces ge-0/0/0 unit 0 description To_RootSrv
set interfaces ge-0/0/0 unit 0 family inet address 10.16.101.1/24
set interfaces ge-0/0/1 unit 0 description To_WAN
set interfaces ge-0/0/1 unit 0 family inet address 10.17.101.1/24
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces ge-0/0/0.0
set security zones security-zone GROUPVPN interfaces ge-0/0/1.0
set security policies global policy 1000 match source-address any

```

```

set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy RootSrv mode main
set security group-vpn server ike policy RootSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy RootSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike policy GMs mode main
set security group-vpn server ike policy GMs proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy GMs pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn server ike gateway RootSrv ike-policy RootSrv
set security group-vpn server ike gateway RootSrv address 10.10.101.1
set security group-vpn server ike gateway RootSrv dead-peer-detection always-send
set security group-vpn server ike gateway RootSrv local-address 10.16.101.1
set security group-vpn server ike gateway GM-0001 ike-policy GMs
set security group-vpn server ike gateway GM-0001 address 10.18.101.1
set security group-vpn server ike gateway GM-0001 local-address 10.17.101.1
set security group-vpn server ike gateway GM-0002 ike-policy GMs
set security group-vpn server ike gateway GM-0002 address 10.18.102.1
set security group-vpn server ike gateway GM-0002 local-address 10.17.101.1
set security group-vpn server ike gateway GM-0003 ike-policy GMs
set security group-vpn server ike gateway GM-0003 address 10.18.103.1
set security group-vpn server ike gateway GM-0003 local-address 10.17.101.1
set security group-vpn server ike gateway GM-0004 ike-policy GMs
set security group-vpn server ike gateway GM-0004 address 10.18.104.1
set security group-vpn server ike gateway GM-0004 local-address 10.17.101.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000

```

```
set security group-vpn server group GROUP_ID-0001 server-cluster server-role sub-server
set security group-vpn server group GROUP_ID-0001 server-cluster ike-gateway RootSrv
set security group-vpn server group GROUP_ID-0001 server-cluster retransmission-period 10
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0001
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0002
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0003
set security group-vpn server group GROUP_ID-0001 ike-gateway GM-0004
set security group-vpn server group GROUP_ID-0001 anti-replay-time-window 1000
set security group-vpn server group GROUP_ID-0001 server-member-communication communication-type
unicast
set security group-vpn server group GROUP_ID-0001 server-member-communication encryption-
algorithm aes-256-cbc
set security group-vpn server group GROUP_ID-0001 server-member-communication lifetime-seconds
7200
set security group-vpn server group GROUP_ID-0001 server-member-communication sig-hash-algorithm
sha-256
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-
L3600
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 source
172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1
destination 172.16.0.0/12
set security group-vpn server group GROUP_ID-0001 ipsec-sa GROUP_ID-0001 match-policy 1 protocol
0
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ??? /? /??? CLI /??? /??? ??????.

?? VPNv2 ?? ?????? ?? ???? ???? ???? ???? ????.

- 1.** □□□□□, □□ □□ ? □□ □□□ □□□□□.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_RootSrv
user@host# set ge-0/0/0 unit 0 family inet address 10.16.101.1/24
user@host# set ge-0/0/1 unit 0 description To_WAN
user@host# set ge-0/0/1 unit 0 family inet address 10.17.101.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
```



```

user@host# set interfaces ge-0/0/0.0
user@host# set interfaces ge-0/0/1.0
[edit security policies global]
user@host# set policy 1000 match source-address any
user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit security policies]
user@host# set default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy RootSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn server ike policy GMs]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn server ike gateway RootSrv]
user@host# set ike-policy RootSrv
user@host# set address 10.10.101.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.16.101.1
[edit security group-vpn server ike gateway GM-0001]
user@host# set ike-policy GMs
user@host# set address 10.18.101.1
user@host# set local-address 10.17.101.1
[edit security group-vpn server ike gateway GM-0002]
user@host# set ike-policy GMs
user@host# set address 10.18.102.1
user@host# set local-address 10.17.101.1

```

```
[edit security group-vpn server ike gateway GM-0003]
user@host# set ike-policy GMs
user@host# set address 10.18.103.1
user@host# set local-address 10.17.101.1
[edit security group-vpn server ike gateway GM-0004]
user@host# set ike-policy GMs
user@host# set address 10.18.104.1
user@host# set local-address 10.17.101.1
```

### 3. IPsec SA `???` `??????`.

```
[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600
```

### 4. VPN `???` `??????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set server-cluster server-role sub-server
user@host# set server-cluster ike-gateway RootSrv
user@host# set server-cluster retransmission-period 10
user@host# set ike-gateway GM-0001
user@host# set ike-gateway GM-0002
user@host# set ike-gateway GM-0003
user@host# set ike-gateway GM-0004
user@host# set anti-replay-time-window 1000
user@host# set server-member-communication communication-type unicast
user@host# set server-member-communication encryption-algorithm aes-256-cbc
user@host# set server-member-communication lifetime-seconds 7200
user@host# set server-member-communication sig-hash-algorithm sha-256
user@host# set ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-L3600
```

### 5. `??` `???` `??????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 source 172.16.0.0/12
```

```

user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 destination 172.16.0.0/12
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 protocol 0

```

??

?? ???? ? show security ??? ???? show interfaces??? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ? ? ? ????.

```

[edit]
user@host# show interfaces
ge-0/0/0 {
    unit 0 {
        description To_RootSrv;
        family inet {
            address 10.16.101.1/24;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        description To_WAN;
        family inet {
            address 10.17.101.1/24;
        }
    }
}
[edit]
user@host# show security
group-vpn {
    server {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                authentication-algorithm sha-256;
                dh-group group14;
                encryption-algorithm aes-256-cbc;
            }
            policy RootSrv {
                mode main;
                proposals PSK-SHA256-DH14-AES256;
                pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
            }
        }
    }
}

```

```

    }
    policy GMs {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway RootSrv {
        ike-policy RootSrv;
        address 10.10.101.1;
        dead-peer-detection always-send;
        local-address 10.16.101.1;
    }
    gateway GM-0001 {
        ike-policy GMs;
        address 10.18.101.1;
        local-address 10.17.101.1;
    }
    gateway GM-0002 {
        ike-policy GMs;
        address 10.18.102.1;
        local-address 10.17.101.1;
    }
    gateway GM-0003 {
        ike-policy GMs;
        address 10.18.103.1;
        local-address 10.17.101.1;
    }
    gateway GM-0004 {
        ike-policy GMs;
        address 10.18.104.1;
        local-address 10.17.101.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
}

```

```

server-cluster {
    server-role sub-server;
    ike-gateway RootSrv;
    retransmission-period 10;
}
ike-gateway GM-0001;
ike-gateway GM-0002;
ike-gateway GM-0003;
ike-gateway GM-0004;
anti-replay-time-window 1000;
server-member-communication {
    communication-type unicast;
    lifetime-seconds 7200;
    encryption-algorithm aes-256-cbc;
    sig-hash-algorithm sha-256;
}
ipsec-sa GROUP_ID-0001 {
    proposal AES256-SHA256-L3600;
    match-policy 1 {
        source 172.16.0.0/12;
        destination 172.16.0.0/12;
        protocol 0;
    }
}
}
}
}
}
policies {
    global {
        policy 1000 {
            match {
                source-address any;
                destination-address any;
                application any;
                from-zone any;
                to-zone any;
            }
            then {
                deny;
                log {
                    session-init;
                }
                count;
            }
        }
    }
}

```

```

    }
  }
}
default-policy {
  deny-all;
}
}
zones {
  security-zone GROUPVPN {
    host-inbound-traffic {
      system-services {
        ike;
        ssh;
        ping;
      }
    }
    interfaces {
      ge-0/0/0.0;
      ge-0/0/1.0;
    }
  }
}
}

```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

?? ?? 2 ??

**CLI ?? ??**

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set interfaces ge-0/0/0 unit 0 description To_RootSrv
set interfaces ge-0/0/0 unit 0 family inet address 10.16.102.1/24
set interfaces ge-0/0/1 unit 0 description To_WAN
set interfaces ge-0/0/1 unit 0 family inet address 10.17.102.1/24
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces ge-0/0/0.0
set security zones security-zone GROUPVPN interfaces ge-0/0/1.0
set security policies global policy 1000 match source-address any

```

```

set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy RootSrv mode main
set security group-vpn server ike policy RootSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy RootSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike policy GMs mode main
set security group-vpn server ike policy GMs proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy GMs pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn server ike gateway RootSrv ike-policy RootSrv
set security group-vpn server ike gateway RootSrv address 10.10.102.1
set security group-vpn server ike gateway RootSrv dead-peer-detection always-send
set security group-vpn server ike gateway RootSrv local-address 10.16.102.1
set security group-vpn server ike gateway GM-0001 ike-policy GMs
set security group-vpn server ike gateway GM-0001 address 10.18.101.1
set security group-vpn server ike gateway GM-0001 local-address 10.17.102.1
set security group-vpn server ike gateway GM-0002 ike-policy GMs
set security group-vpn server ike gateway GM-0002 address 10.18.102.1
set security group-vpn server ike gateway GM-0002 local-address 10.17.102.1
set security group-vpn server ike gateway GM-0003 ike-policy GMs
set security group-vpn server ike gateway GM-0003 address 10.18.103.1
set security group-vpn server ike gateway GM-0003 local-address 10.17.102.1
set security group-vpn server ike gateway GM-0004 ike-policy GMs
set security group-vpn server ike gateway GM-0004 address 10.18.104.1
set security group-vpn server ike gateway GM-0004 local-address 10.17.102.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000

```

- [illegible]

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_RootSrv
user@host# set ge-0/0/0 unit 0 family inet address 10.16.102.1/24
user@host# set ge-0/0/1 unit 0 description To_WAN
user@host# set ge-0/0/1 unit 0 family inet address 10.17.102.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
```



```

user@host# set interfaces ge-0/0/0.0
user@host# set interfaces ge-0/0/1.0
[edit security policies global]
user@host# set policy 1000 match source-address any
user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit security policies]
user@host# set default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy RootSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn server ike policy GMs]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn server ike gateway RootSrv]
user@host# set ike-policy RootSrv
user@host# set address 10.10.102.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.16.102.1
[edit security group-vpn server ike gateway GM-0001]
user@host# set ike-policy GMs
user@host# set address 10.18.101.1
user@host# set local-address 10.17.102.1
[edit security group-vpn server ike gateway GM-0002]
user@host# set ike-policy GMs
user@host# set address 10.18.102.1
user@host# set local-address 10.17.102.1

```

```
[edit security group-vpn server ike gateway GM-0003]
user@host# set ike-policy GMs
user@host# set address 10.18.103.1
user@host# set local-address 10.17.102.1
[edit security group-vpn server ike gateway GM-0004]
user@host# set ike-policy GMs
user@host# set address 10.18.104.1
user@host# set local-address 10.17.102.1
```

### 3. IPsec SA `???` `?????`.

```
[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600
```

### 4. VPN `???` `?????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set server-cluster server-role sub-server
user@host# set server-cluster ike-gateway RootSrv
user@host# set server-cluster retransmission-period 10
user@host# set ike-gateway GM-0001
user@host# set ike-gateway GM-0002
user@host# set ike-gateway GM-0003
user@host# set ike-gateway GM-0004
user@host# set anti-replay-time-window 1000
user@host# set server-member-communication communication-type unicast
user@host# set server-member-communication encryption-algorithm aes-256-cbc
user@host# set server-member-communication lifetime-seconds 7200
user@host# set server-member-communication sig-hash-algorithm sha-256
```

### 5. `??` `???` `?????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 source 172.16.0.0/12
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 destination 172.16.0.0/12
```

```

user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 protocol 0
user@host# set ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-L3600

```

??

?? ???? show interfaces ? show security ??? ???? ???? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ????  
 ??????.

```

[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_RootSrv;
    family inet {
      address 10.16.102.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_WAN;
    family inet {
      address 10.17.102.1/24;
    }
  }
}
[edit]
user@host# show security
group-vpn {
  server {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        authentication-algorithm sha-256;
        dh-group group14;
        encryption-algorithm aes-256-cbc;
      }
      policy RootSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
      }
    }
  }
}

```

```

    }
    policy GMs {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway RootSrv {
        ike-policy RootSrv;
        address 10.10.102.1;
        dead-peer-detection always-send;
        local-address 10.16.102.1;
    }
    gateway GM-0001 {
        ike-policy GMs;
        address 10.18.101.1;
        local-address 10.17.102.1;
    }
    gateway GM-0002 {
        ike-policy GMs;
        address 10.18.102.1;
        local-address 10.17.102.1;
    }
    gateway GM-0003 {
        ike-policy GMs;
        address 10.18.103.1;
        local-address 10.17.102.1;
    }
    gateway GM-0004 {
        ike-policy GMs;
        address 10.18.104.1;
        local-address 10.17.102.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
}

```

```

server-cluster {
    server-role sub-server;
    ike-gateway RootSrv;
    retransmission-period 10;
}
ike-gateway GM-0001;
ike-gateway GM-0002;
ike-gateway GM-0003;
ike-gateway GM-0004;
anti-replay-time-window 1000;
server-member-communication {
    communication-type unicast;
    lifetime-seconds 7200;
    encryption-algorithm aes-256-cbc;
    sig-hash-algorithm sha-256;
}
ipsec-sa GROUP_ID-0001 {
    proposal AES256-SHA256-L3600;
    match-policy 1 {
        source 172.16.0.0/12;
        destination 172.16.0.0/12;
        protocol 0;
    }
}
}
}
}
}
policies {
    global {
        policy 1000 {
            match {
                source-address any;
                destination-address any;
                application any;
                from-zone any;
                to-zone any;
            }
            then {
                deny;
                log {
                    session-init;
                }
                count;
            }
        }
    }
}

```

```

    }
  }
}
default-policy {
  deny-all;
}
}
zones {
  security-zone GROUPVPN {
    host-inbound-traffic {
      system-services {
        ike;
        ssh;
        ping;
      }
    }
    interfaces {
      ge-0/0/0.0;
      ge-0/0/1.0;
    }
  }
}
}

```

?? ?? ?? ?? ?? commit?(?) ?????.

?? ?? 3 ??

**CLI ?? ??**

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ??????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set interfaces ge-0/0/0 unit 0 description To_RootSrv
set interfaces ge-0/0/0 unit 0 family inet address 10.16.103.1/24
set interfaces ge-0/0/1 unit 0 description To_WAN
set interfaces ge-0/0/1 unit 0 family inet address 10.17.103.1/24
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces ge-0/0/0.0
set security zones security-zone GROUPVPN interfaces ge-0/0/1.0
set security policies global policy 1000 match source-address any

```

```

set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy RootSrv mode main
set security group-vpn server ike policy RootSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy RootSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike policy GMs mode main
set security group-vpn server ike policy GMs proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy GMs pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn server ike gateway RootSrv ike-policy RootSrv
set security group-vpn server ike gateway RootSrv address 10.10.103.1
set security group-vpn server ike gateway RootSrv dead-peer-detection always-send
set security group-vpn server ike gateway RootSrv local-address 10.16.103.1
set security group-vpn server ike gateway GM-0001 ike-policy GMs
set security group-vpn server ike gateway GM-0001 address 10.18.101.1
set security group-vpn server ike gateway GM-0001 local-address 10.17.103.1
set security group-vpn server ike gateway GM-0002 ike-policy GMs
set security group-vpn server ike gateway GM-0002 address 10.18.102.1
set security group-vpn server ike gateway GM-0002 local-address 10.17.103.1
set security group-vpn server ike gateway GM-0003 ike-policy GMs
set security group-vpn server ike gateway GM-0003 address 10.18.103.1
set security group-vpn server ike gateway GM-0003 local-address 10.17.103.1
set security group-vpn server ike gateway GM-0004 ike-policy GMs
set security group-vpn server ike gateway GM-0004 address 10.18.104.1
set security group-vpn server ike gateway GM-0004 local-address 10.17.103.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ????? ???? ?? ??? CLI ??? ???? ?? /? /???? CLI ??? /??? ??????.

?? VPNv2 ?? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

**1.** [ ][ ][ ][ ] , [ ][ ] [ ][ ] ? [ ][ ] [ ][ ][ ][ ].

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_RootSrv
user@host# set ge-0/0/0 unit 0 family inet address 10.16.103.1/24
user@host# set ge-0/0/1 unit 0 description To_WAN
user@host# set ge-0/0/1 unit 0 family inet address 10.17.103.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
```



```

user@host# set interfaces ge-0/0/0.0
user@host# set interfaces ge-0/0/1.0
[edit security policies global]
user@host# set policy 1000 match source-address any
user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit security policies]
user@host# set default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy RootSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn server ike policy GMs]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn server ike gateway RootSrv]
user@host# set ike-policy RootSrv
user@host# set address 10.10.103.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.16.103.1
[edit security group-vpn server ike gateway GM-0001]
user@host# set ike-policy GMs
user@host# set address 10.18.101.1
user@host# set local-address 10.17.103.1
[edit security group-vpn server ike gateway GM-0002]
user@host# set ike-policy GMs
user@host# set address 10.18.102.1
user@host# set local-address 10.17.103.1

```

```
[edit security group-vpn server ike gateway GM-0003]
user@host# set ike-policy GMs
user@host# set address 10.18.103.1
user@host# set local-address 10.17.103.1
[edit security group-vpn server ike gateway GM-0004]
user@host# set ike-policy GMs
user@host# set address 10.18.104.1
user@host# set local-address 10.17.103.1
```

### 3. IPsec SA `???` `??????`.

```
[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600
```

### 4. VPN `???` `??????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set server-cluster server-role sub-server
user@host# set server-cluster ike-gateway RootSrv
user@host# set server-cluster retransmission-period 10
user@host# set ike-gateway GM-0001
user@host# set ike-gateway GM-0002
user@host# set ike-gateway GM-0003
user@host# set ike-gateway GM-0004
user@host# set anti-replay-time-window 1000
user@host# set server-member-communication communication-type unicast
user@host# set server-member-communication encryption-algorithm aes-256-cbc
user@host# set server-member-communication lifetime-seconds 7200
user@host# set server-member-communication sig-hash-algorithm sha-256
```

### 5. `??` `???` `??????`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 source 172.16.0.0/12
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 destination 172.16.0.0/12
```

```

user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 protocol 0
user@host# set ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-L3600

```

??

?? ???? show interfaces ? show security ??? ???? ???? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ????  
 ??????.

```

[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_RootSrv;
    family inet {
      address 10.16.103.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_WAN;
    family inet {
      address 10.17.103.1/24;
    }
  }
}
[edit]
user@host# show security
group-vpn {
  server {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        authentication-algorithm sha-256;
        dh-group group14;
        encryption-algorithm aes-256-cbc;
      }
      policy RootSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
      }
    }
  }
}

```

```

    }
    policy GMs {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway RootSrv {
        ike-policy RootSrv;
        address 10.10.103.1;
        dead-peer-detection always-send;
        local-address 10.16.103.1;
    }
    gateway GM-0001 {
        ike-policy GMs;
        address 10.18.101.1;
        local-address 10.17.103.1;
    }
    gateway GM-0002 {
        ike-policy GMs;
        address 10.18.102.1;
        local-address 10.17.103.1;
    }
    gateway GM-0003 {
        ike-policy GMs;
        address 10.18.103.1;
        local-address 10.17.103.1;
    }
    gateway GM-0004 {
        ike-policy GMs;
        address 10.18.104.1;
        local-address 10.17.103.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
}

```

```

server-cluster {
    server-role sub-server;
    ike-gateway RootSrv;
    retransmission-period 10;
}
ike-gateway GM-0001;
ike-gateway GM-0002;
ike-gateway GM-0003;
ike-gateway GM-0004;
anti-replay-time-window 1000;
server-member-communication {
    communication-type unicast;
    lifetime-seconds 7200;
    encryption-algorithm aes-256-cbc;
    sig-hash-algorithm sha-256;
}
ipsec-sa GROUP_ID-0001 {
    proposal AES256-SHA256-L3600;
    match-policy 1 {
        source 172.16.0.0/12;
        destination 172.16.0.0/12;
        protocol 0;
    }
}
}
}
}
}
policies {
    global {
        policy 1000 {
            match {
                source-address any;
                destination-address any;
                application any;
                from-zone any;
                to-zone any;
            }
            then {
                deny;
                log {
                    session-init;
                }
                count;
            }
        }
    }
}

```

```

    }
  }
}
default-policy {
  deny-all;
}
}
zones {
  security-zone GROUPVPN {
    host-inbound-traffic {
      system-services {
        ike;
        ssh;
        ping;
      }
    }
    interfaces {
      ge-0/0/0.0;
      ge-0/0/1.0;
    }
  }
}
}

```

?? ?? ?? ?? commit?(?) ?????.

?? ?? ?? 4

CLI ?? ??

? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? [edit] ?  
 ? ?? ?? ?? CLI? ?? ?? ?? ??, ?? ?? ?? commit?(?) ?????.

```

set interfaces ge-0/0/0 unit 0 description To_RootSrv
set interfaces ge-0/0/0 unit 0 family inet address 10.16.104.1/24
set interfaces ge-0/0/1 unit 0 description To_WAN
set interfaces ge-0/0/1 unit 0 family inet address 10.17.104.1/24
set security zones security-zone GROUPVPN host-inbound-traffic system-services ike
set security zones security-zone GROUPVPN host-inbound-traffic system-services ssh
set security zones security-zone GROUPVPN host-inbound-traffic system-services ping
set security zones security-zone GROUPVPN interfaces ge-0/0/0.0
set security zones security-zone GROUPVPN interfaces ge-0/0/1.0
set security policies global policy 1000 match source-address any

```

```

set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn server ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn server ike policy RootSrv mode main
set security group-vpn server ike policy RootSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy RootSrv pre-shared-key ascii-text "$ABC123"
set security group-vpn server ike policy GMs mode main
set security group-vpn server ike policy GMs proposals PSK-SHA256-DH14-AES256
set security group-vpn server ike policy GMs pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn server ike gateway RootSrv ike-policy RootSrv
set security group-vpn server ike gateway RootSrv address 10.10.104.1
set security group-vpn server ike gateway RootSrv dead-peer-detection always-send
set security group-vpn server ike gateway RootSrv local-address 10.16.104.1
set security group-vpn server ike gateway GM-0001 ike-policy GMs
set security group-vpn server ike gateway GM-0001 address 10.18.101.1
set security group-vpn server ike gateway GM-0001 local-address 10.17.104.1
set security group-vpn server ike gateway GM-0002 ike-policy GMs
set security group-vpn server ike gateway GM-0002 address 10.18.102.1
set security group-vpn server ike gateway GM-0002 local-address 10.17.104.1
set security group-vpn server ike gateway GM-0003 ike-policy GMs
set security group-vpn server ike gateway GM-0003 address 10.18.103.1
set security group-vpn server ike gateway GM-0003 local-address 10.17.104.1
set security group-vpn server ike gateway GM-0004 ike-policy GMs
set security group-vpn server ike gateway GM-0004 address 10.18.104.1
set security group-vpn server ike gateway GM-0004 local-address 10.17.104.1
set security group-vpn server ipsec proposal AES256-SHA256-L3600 authentication-algorithm hmac-
sha-256-128
set security group-vpn server ipsec proposal AES256-SHA256-L3600 encryption-algorithm aes-256-cbc
set security group-vpn server ipsec proposal AES256-SHA256-L3600 lifetime-seconds 3600
set security group-vpn server group GROUP_ID-0001 group-id 1
set security group-vpn server group GROUP_ID-0001 member-threshold 2000

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? /? /??? CLI ??? /??? ??????.

**VPNv2**

- 1.** [ ][ ][ ][ ] , [ ][ ] [ ][ ] ? [ ][ ] [ ][ ][ ][ ].

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_RootSrv
user@host# set ge-0/0/0 unit 0 family inet address 10.16.104.1/24
user@host# set ge-0/0/1 unit 0 description To_WAN
user@host# set ge-0/0/1 unit 0 family inet address 10.17.104.1/24
[edit security zones security-zone GROUPVPN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
```



```

user@host# set interfaces ge-0/0/0.0
user@host# set interfaces ge-0/0/1.0
[edit security policies global]
user@host# set policy 1000 match source-address any
user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit security policies]
user@host# set default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn server ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn server ike policy RootSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123"
[edit security group-vpn server ike policy GMs]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn server ike gateway RootSrv]
user@host# set ike-policy RootSrv
user@host# set address 10.10.104.1
user@host# set dead-peer-detection always-send
user@host# set local-address 10.16.104.1
[edit security group-vpn server ike gateway GM-0001]
user@host# set ike-policy GMs
user@host# set address 10.18.101.1
user@host# set local-address 10.17.104.1
[edit security group-vpn server ike gateway GM-0002]
user@host# set ike-policy GMs
user@host# set address 10.18.102.1
user@host# set local-address 10.17.104.1

```

```
[edit security group-vpn server ike gateway GM-0003]
user@host# set ike-policy GMs
user@host# set address 10.18.103.1
user@host# set local-address 10.17.104.1
[edit security group-vpn server ike gateway GM-0004]
user@host# set ike-policy GMs
user@host# set address 10.18.104.1
user@host# set local-address 10.17.104.1
```

### 3. IPsec SA `???`.

```
[edit security group-vpn server ipsec proposal AES256-SHA256-L3600]
user@host# set authentication-algorithm hmac-sha-256-128
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 3600
```

### 4. VPN `???`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set group-id 1
user@host# set member-threshold 2000
user@host# set server-cluster server-role sub-server
user@host# set server-cluster ike-gateway RootSrv
user@host# set server-cluster retransmission-period 10
user@host# set ike-gateway GM-0001
user@host# set ike-gateway GM-0002
user@host# set ike-gateway GM-0003
user@host# set ike-gateway GM-0004
user@host# set anti-replay-time-window 1000
user@host# set server-member-communication communication-type unicast
user@host# set server-member-communication encryption-algorithm aes-256-cbc
user@host# set server-member-communication lifetime-seconds 7200
user@host# set server-member-communication sig-hash-algorithm sha-256
```

### 5. `??`.

```
[edit security group-vpn server group GROUP_ID-0001]
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 source 172.16.0.0/12
user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 destination 172.16.0.0/12
```

```

user@host# set ipsec-sa GROUP_ID-0001 match-policy 1 protocol 0
user@host# set ipsec-sa GROUP_ID-0001 proposal AES256-SHA256-L3600

```

??

?? ???? show interfaces ? show security ??? ???? ???? ?????. ?? ???? ???? ???? ???? ? ? ? ???? ???? ????  
 ??????.

```

[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_RootSrv;
    family inet {
      address 10.16.104.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_WAN;
    family inet {
      address 10.17.104.1/24;
    }
  }
}
[edit]
user@host# show security
group-vpn {
  server {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        authentication-algorithm sha-256;
        dh-group group14;
        encryption-algorithm aes-256-cbc;
      }
      policy RootSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
      }
    }
  }
}

```

```

    }
    policy GMs {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway RootSrv {
        ike-policy RootSrv;
        address 10.10.104.1;
        dead-peer-detection always-send;
        local-address 10.16.104.1;
    }
    gateway GM-0001 {
        ike-policy GMs;
        address 10.18.101.1;
        local-address 10.17.104.1;
    }
    gateway GM-0002 {
        ike-policy GMs;
        address 10.18.102.1;
        local-address 10.17.104.1;
    }
    gateway GM-0003 {
        ike-policy GMs;
        address 10.18.103.1;
        local-address 10.17.104.1;
    }
    gateway GM-0004 {
        ike-policy GMs;
        address 10.18.104.1;
        local-address 10.17.104.1;
    }
}
ipsec {
    proposal AES256-SHA256-L3600 {
        authentication-algorithm hmac-sha-256-128;
        encryption-algorithm aes-256-cbc;
        lifetime-seconds 3600;
    }
}
group GROUP_ID-0001 {
    group-id 1;
    member-threshold 2000;
}

```

```

server-cluster {
    server-role sub-server;
    ike-gateway RootSrv;
    retransmission-period 10;
}
ike-gateway GM-0001;
ike-gateway GM-0002;
ike-gateway GM-0003;
ike-gateway GM-0004;
anti-replay-time-window 1000;
server-member-communication {
    communication-type unicast;
    lifetime-seconds 7200;
    encryption-algorithm aes-256-cbc;
    sig-hash-algorithm sha-256;
}
ipsec-sa GROUP_ID-0001 {
    proposal AES256-SHA256-L3600;
    match-policy 1 {
        source 172.16.0.0/12;
        destination 172.16.0.0/12;
        protocol 0;
    }
}
}
}
}
}
policies {
    global {
        policy 1000 {
            match {
                source-address any;
                destination-address any;
                application any;
                from-zone any;
                to-zone any;
            }
            then {
                deny;
                log {
                    session-init;
                }
                count;
            }
        }
    }
}

```

```

    }
  }
}
default-policy {
  deny-all;
}
}
zones {
  security-zone GROUPVPN {
    host-inbound-traffic {
      system-services {
        ike;
        ssh;
        ping;
      }
    }
    interfaces {
      ge-0/0/0.0;
      ge-0/0/1.0;
    }
  }
}
}

```

?? ?? ?? ?? commit?(?) ?????.

**GM-0001** ??(SRX ??? ?? vSRX ?? ?? ??)

**CLI** ?? ??

? ?? ??, ?? ?? ?? ?? ?? ?? ?? ??, ??? ?? ?? ?? [edit] ?  
 ? ??? CLI? ?? ?? ??, ?? ??? commit?(?) ?????.

```

set interfaces ge-0/0/0 unit 0 description To_LAN
set interfaces ge-0/0/0 unit 0 family inet address 172.16.101.1/24
set interfaces ge-0/0/1 unit 0 description To_SubSrv
set interfaces ge-0/0/1 unit 0 family inet address 10.18.101.1/24
set security zones security-zone LAN host-inbound-traffic system-services ike
set security zones security-zone LAN host-inbound-traffic system-services ssh
set security zones security-zone LAN host-inbound-traffic system-services ping
set security zones security-zone LAN interfaces ge-0/0/0.0
set security zones security-zone WAN host-inbound-traffic system-services ike
set security zones security-zone WAN host-inbound-traffic system-services ssh

```

```

set security zones security-zone WAN host-inbound-traffic system-services ping
set security zones security-zone WAN interfaces ge-0/0/1.0
set security address-book global address 172.16.0.0/12 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match application any
set security policies from-zone LAN to-zone WAN policy 1 then permit
set security policies from-zone LAN to-zone WAN policy 1 then log session-init
set security policies from-zone WAN to-zone LAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match application any
set security policies from-zone WAN to-zone LAN policy 1 then permit
set security policies from-zone WAN to-zone LAN policy 1 then log session-init
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy SubSrv mode main
set security group-vpn member ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy SubSrv pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn member ike gateway SubSrv ike-policy SubSrv
set security group-vpn member ike gateway SubSrv server-address 10.17.101.1
set security group-vpn member ike gateway SubSrv server-address 10.17.102.1
set security group-vpn member ike gateway SubSrv server-address 10.17.103.1
set security group-vpn member ike gateway SubSrv server-address 10.17.104.1
set security group-vpn member ike gateway SubSrv local-address 10.18.101.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway SubSrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group-vpn-external-interface ge-0/0/1.0
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1

```

```
set security group-vpn member ipsec vpn GROUP_ID-0001 recovery-probe
set security ipsec-policy from-zone LAN to-zone WAN ipsec-group-vpn GROUP_ID-0001
```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ???? ???? ?/? ???? CLI ?/? ?/? ????.

?? VPNv2 ???? ???? ????.

1. ?????, ?? ? ? ? ? ? ? ?.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_LAN
user@host# set ge-0/0/0 unit 0 family inet address 172.16.101.1/24
user@host# set ge-0/0/1 unit 0 description To_SubSrv
user@host# set ge-0/0/1 unit 0 family inet address 10.18.101.1/24
[edit security zones security-zone LAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/0.0
[edit security zones security-zone WAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/1.0
[edit security]
user@host# set address-book global address 172.16.0.0/12 172.16.0.0/12
[edit security policies from-zone LAN to-zone WAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set policy 1 then log session-init
[edit security policies from-zone WAN to-zone LAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set policy 1 then log session-init
[edit security policies global]
user@host# set policy 1000 match source-address any
```



```

user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit]
user@host# set security policies default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy SubSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn member ike gateway SubSrv]
user@host# set ike-policy SubSrv
user@host# set server-address 10.17.101.1
user@host# set server-address 10.17.102.1
user@host# set server-address 10.17.103.1
user@host# set server-address 10.17.104.1
user@host# set local-address 10.18.101.1

```

## 3. IPsec SA `set` `show`.

```

[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway SubSrv
user@host# set group-vpn-external-interface ge-0/0/1.0
user@host# set group 1
user@host# set recovery-probe

```

#### 4. IPsec `???` `??????`.

```
[edit security ipsec-policy from-zone LAN to-zone WAN]
user@host# set ipsec-group-vpn GROUP_ID-0001
```

`??`

`?? ???? show interfaces ? show security ??? ???? ???? ?????. ?? ??? ???? ???? ???? ? ? ? ???? ???? ???? ????.`

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_LAN;
    family inet {
      address 172.16.101.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_SubSrv;
    family inet {
      address 10.18.101.1/24;
    }
  }
}
[edit]
user@host# show security
address-book {
  global {
    address 172.16.0.0/12 172.16.0.0/12;
  }
}
group-vpn {
  member {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        dh-group group14;
```

```

        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
    }
    policy SubSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway SubSrv {
        ike-policy SubSrv;
        server-address [ 10.17.101.1 10.17.102.1 10.17.103.1 10.17.104.1 ];
        local-address 10.18.101.1;
    }
}
ipsec {
    vpn GROUP_ID-0001 {
        ike-gateway SubSrv;
        group-vpn-external-interface ge-0/0/1.0;
        group 1;
        recovery-probe;
    }
}
}
ipsec-policy {
    from-zone LAN to-zone WAN {
        ipsec-group-vpn GROUP_ID-0001;
    }
}
policies {
    from-zone LAN to-zone WAN {
        policy 1 {
            match {
                source-address 172.16.0.0/12;
                destination-address 172.16.0.0/12;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
            }
        }
    }
}

```

```

    }
}
from-zone WAN to-zone LAN {
    policy 1 {
        match {
            source-address 172.16.0.0/12;
            destination-address 172.16.0.0/12;
            application any;
        }
        then {
            permit;
            log {
                session-init;
            }
        }
    }
}
global {
    policy 1000 {
        match {
            source-address any;
            destination-address any;
            application any;
            from-zone any;
            to-zone any;
        }
        then {
            deny;
            log {
                session-init;
            }
            count;
        }
    }
}
default-policy {
    deny-all;
}
}
zones {
    security-zone LAN {
        host-inbound-traffic {
            system-services {

```

```

        ike;
        ssh;
        ping;
    }
}
interfaces {
    ge-0/0/0.0;
}
}
security-zone WAN {
    host-inbound-traffic {
        system-services {
            ike;
            ssh;
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
}
}

```

?? ?? ?? ?? ?? commit?(?) ?????.

**GM-0002 ??(SRX ??? ?? ? vSRX ?? ?? ????)**

**CLI ?? ??**

? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ??? ?? ?? ?? ? ?? ?? ?? ?? [edit] ?  
 ? ??? ?? CLI? ?? ?? ?? ??, ?? ??? commit?(?) ?????.

```

set interfaces ge-0/0/0 unit 0 description To_LAN
set interfaces ge-0/0/0 unit 0 family inet address 172.16.102.1/24
set interfaces ge-0/0/1 unit 0 description To_SubSrv
set interfaces ge-0/0/1 unit 0 family inet address 10.18.102.1/24
set security zones security-zone LAN host-inbound-traffic system-services ike
set security zones security-zone LAN host-inbound-traffic system-services ssh
set security zones security-zone LAN host-inbound-traffic system-services ping
set security zones security-zone LAN interfaces ge-0/0/0.0
set security zones security-zone WAN host-inbound-traffic system-services ike
set security zones security-zone WAN host-inbound-traffic system-services ssh

```

```

set security zones security-zone WAN host-inbound-traffic system-services ping
set security zones security-zone WAN interfaces ge-0/0/1.0
set security address-book global address 172.16.0.0/12 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone LAN to-zone WAN policy 1 match application any
set security policies from-zone LAN to-zone WAN policy 1 then permit
set security policies from-zone LAN to-zone WAN policy 1 then log session-init
set security policies from-zone WAN to-zone LAN policy 1 match source-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match destination-address 172.16.0.0/12
set security policies from-zone WAN to-zone LAN policy 1 match application any
set security policies from-zone WAN to-zone LAN policy 1 then permit
set security policies from-zone WAN to-zone LAN policy 1 then log session-init
set security policies global policy 1000 match source-address any
set security policies global policy 1000 match destination-address any
set security policies global policy 1000 match application any
set security policies global policy 1000 match from-zone any
set security policies global policy 1000 match to-zone any
set security policies global policy 1000 then deny
set security policies global policy 1000 then log session-init
set security policies global policy 1000 then count
set security policies default-policy deny-all
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy SubSrv mode main
set security group-vpn member ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy SubSrv pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn member ike gateway SubSrv ike-policy SubSrv
set security group-vpn member ike gateway SubSrv server-address 10.17.101.1
set security group-vpn member ike gateway SubSrv server-address 10.17.102.1
set security group-vpn member ike gateway SubSrv server-address 10.17.103.1
set security group-vpn member ike gateway SubSrv server-address 10.17.104.1
set security group-vpn member ike gateway SubSrv local-address 10.18.102.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway SubSrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group-vpn-external-interface ge-0/0/1.0
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1

```

```
set security group-vpn member ipsec vpn GROUP_ID-0001 recovery-probe
set security ipsec-policy from-zone LAN to-zone WAN ipsec-group-vpn GROUP_ID-0001
```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ??/ ????/ CLI ???/ ??/ ?????.

?? VPNv2 ??? ????? ??? ?????.

- 1.** □□□□□, □□ □□ □ □□ □□□ □□□□□.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 description To_LAN
user@host# set ge-0/0/0 unit 0 family inet address 172.16.102.1/24
user@host# set ge-0/0/1 unit 0 description To_SubSrv
user@host# set ge-0/0/1 unit 0 family inet address 10.18.102.1/24
[edit security zones security-zone LAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/0.0
[edit security zones security-zone WAN]
user@host# set host-inbound-traffic system-services ike
user@host# set host-inbound-traffic system-services ssh
user@host# set host-inbound-traffic system-services ping
user@host# set interfaces ge-0/0/1.0
[edit security]
user@host# set address-book global address 172.16.0.0/12 172.16.0.0/12
[edit security policies from-zone LAN to-zone WAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set policy 1 then log session-init
[edit security policies from-zone WAN to-zone LAN]
user@host# set policy 1 match source-address 172.16.0.0/12
user@host# set policy 1 match destination-address 172.16.0.0/12
user@host# set policy 1 match application any
user@host# set policy 1 then permit
user@host# set policy 1 then log session-init
[edit security policies global]
user@host# set policy 1000 match source-address any
```

```

user@host# set policy 1000 match destination-address any
user@host# set policy 1000 match application any
user@host# set policy 1000 match from-zone any
user@host# set policy 1000 match to-zone any
user@host# set policy 1000 then deny
user@host# set policy 1000 then log session-init
user@host# set policy 1000 then count
[edit]
user@host# set security policies default-policy deny-all

```

## 2. IKE(Internet Key Exchange) `set`, `show` `set` `show` `set` `show`.

```

[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy SubSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn member ike gateway SubSrv]
user@host# set ike-policy SubSrv
user@host# set server-address 10.17.101.1
user@host# set server-address 10.17.102.1
user@host# set server-address 10.17.103.1
user@host# set server-address 10.17.104.1
user@host# set local-address 10.18.102.1

```

## 3. IPsec SA `set` `show`.

```

[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway SubSrv
user@host# set group-vpn-external-interface ge-0/0/1.0
user@host# set group 1
user@host# set recovery-probe

```



#### 4. IPsec `???` `??????`.

```
[edit security ipsec-policy from-zone LAN to-zone WAN]
user@host# set ipsec-group-vpn GROUP_ID-0001
```

`??`

`?? ???? show interfaces ? show security ??? ???? ???? ?????. ?? ??? ???? ???? ???? ? ? ? ???? ???? ???? ???? ????.`

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    description To_LAN;
    family inet {
      address 172.16.102.1/24;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    description To_SubSrv;
    family inet {
      address 10.18.102.1/24;
    }
  }
}
[edit]
user@host# show security
address-book {
  global {
    address 172.16.0.0/12 172.16.0.0/12;
  }
}
group-vpn {
  member {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        dh-group group14;
```

```

        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
    }
    policy SubSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
    }
    gateway SubSrv {
        ike-policy SubSrv;
        server-address [ 10.17.101.1 10.17.102.1 10.17.103.1 10.17.104.1 ];
        local-address 10.18.102.1;
    }
}
ipsec {
    vpn GROUP_ID-0001 {
        ike-gateway SubSrv;
        group-vpn-external-interface ge-0/0/1.0;
        group 1;
        recovery-probe;
    }
}
}
}
ipsec-policy {
    from-zone LAN to-zone WAN {
        ipsec-group-vpn GROUP_ID-0001;
    }
}
policies {
    from-zone LAN to-zone WAN {
        policy 1 {
            match {
                source-address 172.16.0.0/12;
                destination-address 172.16.0.0/12;
                application any;
            }
            then {
                permit;
                log {
                    session-init;
                }
            }
        }
    }
}

```

```

    }
}
from-zone WAN to-zone LAN {
    policy 1 {
        match {
            source-address 172.16.0.0/12;
            destination-address 172.16.0.0/12;
            application any;
        }
        then {
            permit;
            log {
                session-init;
            }
        }
    }
}
global {
    policy 1000 {
        match {
            source-address any;
            destination-address any;
            application any;
            from-zone any;
            to-zone any;
        }
        then {
            deny;
            log {
                session-init;
            }
            count;
        }
    }
}
default-policy {
    deny-all;
}
}
zones {
    security-zone LAN {
        host-inbound-traffic {
            system-services {

```

```

        ike;
        ssh;
        ping;
    }
}
interfaces {
    ge-0/0/0.0;
}
}
security-zone WAN {
    host-inbound-traffic {
        system-services {
            ike;
            ssh;
            ping;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
}
}

```

?? ?? ?? ?? ?? commit?(?) ?????.

**GM-0003** ??(MX ??? ????)

**CLI** ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ??????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set interfaces xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
set interfaces xe-0/0/1 unit 0 family inet address 10.18.103.1/24
set interfaces xe-0/0/2 unit 0 family inet address 172.16.103.1/24
set interfaces ms-0/2/0 unit 0 family inet
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-method pre-
shared-keys
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 dh-group group14

```

```

set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 authentication-algorithm
sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy SubSrv mode main
set security group-vpn member ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy SubSrv pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn member ike gateway SubSrv ike-policy SubSrv
set security group-vpn member ike gateway SubSrv server-address 10.17.101.1
set security group-vpn member ike gateway SubSrv server-address 10.17.102.1
set security group-vpn member ike gateway SubSrv server-address 10.17.103.1
set security group-vpn member ike gateway SubSrv server-address 10.17.104.1
set security group-vpn member ike gateway SubSrv local-address 10.18.103.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway SubSrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 match-direction output
set security group-vpn member ipsec vpn GROUP_ID-0001 tunnel-mtu 1400
set security group-vpn member ipsec vpn GROUP_ID-0001 df-bit clear
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.101.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.102.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.103.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.104.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.101.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.102.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.103.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.104.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from source-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from destination-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 then service

```

```
set services service-set GROUP_ID-0001 interface-service service-interface ms-0/2/0.0
set services service-set GROUP_ID-0001 ipsec-group-vpn GROUP_ID-0001
```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ???? ???? ?/? ???? CLI ???? ???? ?????.

?? VPNv2 ???? ???? ???? ????.

## 1. ???? ????.

```
[edit interfaces]
user@host# set xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet address 10.18.103.1/24
user@host# set xe-0/0/2 unit 0 family inet address 172.16.103.1/24
user@host# set ms-0/2/0 unit 0 family inet
```

## 2. IKE(Internet Key Exchange) ??, ?? ? ???? ????.

```
[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy SubSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn member ike gateway SubSrv]
user@host# set ike-policy SubSrv
user@host# set server-address 10.17.101.1
user@host# set server-address 10.17.102.1
user@host# set server-address 10.17.103.1
user@host# set server-address 10.17.104.1
user@host# set local-address 10.18.103.1
```

### 3. IPsec SA[?] [?] [?] [?] [?].

```
[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway SubSrv
user@host# set group 1
user@host# set match-direction output
user@host# set tunnel-mtu 1400
user@host# set df-bit clear
```

[illegible]

```
[edit firewall family inet service-filter GroupVPN-KS]
user@host# set term inbound-ks from source-address 10.17.101.1/32
user@host# set term inbound-ks from source-address 10.17.102.1/32
user@host# set term inbound-ks from source-address 10.17.103.1/32
user@host# set term inbound-ks from source-address 10.17.104.1/32
user@host# set term inbound-ks then skip
user@host# set term outbound-ks from destination-address 10.17.101.1/32
user@host# set term outbound-ks from destination-address 10.17.102.1/32
user@host# set term outbound-ks from destination-address 10.17.103.1/32
user@host# set term outbound-ks from destination-address 10.17.104.1/32
user@host# set term outbound-ks then skip
user@host# set term GROUP_ID-0001 from source-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 from destination-address 172.16.0.0/12
user@host# set term GROUP_ID-0001 then service
```

**5.**                  .

```
[edit services service-set GROUP_ID-0001]
user@host# set interface-service service-interface ms-0/2/0.0
user@host# set ipsec-group-vpn GROUP_ID-0001
```

??

```

[?] [????] show interfaces, show security, show services [?] show firewall [??? [????? [??? [?????. [?] [??? [??? [????? [?]
[?] [??? [?] [??? [???? [??? [???????].

```

```
[edit]
user@host# show interfaces
```

```

xe-0/0/1 {
  unit 0 {
    family inet {
      service {
        input {
          service-set GROUP_ID-0001 service-filter GroupVPN-KS;
        }
        output {
          service-set GROUP_ID-0001 service-filter GroupVPN-KS;
        }
      }
      address 10.18.103.1/24;
    }
  }
}
xe-0/0/2 {
  unit 0 {
    family inet {
      address 172.16.103.1/24;
    }
  }
}
ms-0/2/0 {
  unit 0 {
    family inet;
  }
}
[edit]
user@host# show security
group-vpn {
  member {
    ike {
      proposal PSK-SHA256-DH14-AES256 {
        authentication-method pre-shared-keys;
        dh-group group14;
        authentication-algorithm sha-256;
        encryption-algorithm aes-256-cbc;
      }
      policy SubSrv {
        mode main;
        proposals PSK-SHA256-DH14-AES256;
        pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
      }
    }
  }
}

```



```

        gateway SubSrv {
            ike-policy SubSrv;
            server-address [ 10.17.101.1 10.17.102.1 10.17.103.1 10.17.104.1 ];
            local-address 10.18.103.1;
        }
    }
    ipsec {
        vpn GROUP_ID-0001 {
            ike-gateway SubSrv;
            group 1;
            match-direction output;
            tunnel-mtu 1400;
            df-bit clear;
        }
    }
}
[edit]
user@host# show services
service-set GROUP_ID-0001 {
    interface-service {
        service-interface ms-0/2/0.0;
    }
    ipsec-group-vpn GROUP_ID-0001;
}
[edit]
user@host# show firewall
family inet {
    service-filter GroupVPN-KS {
        term inbound-ks {
            from {
                source-address {
                    10.17.101.1/32;
                    10.17.102.1/32;
                    10.17.103.1/32;
                    10.17.104.1/32;
                }
            }
            then skip;
        }
        term outbound-ks {
            from {
                destination-address {

```



```

sha-256
set security group-vpn member ike proposal PSK-SHA256-DH14-AES256 encryption-algorithm aes-256-
cbc
set security group-vpn member ike policy SubSrv mode main
set security group-vpn member ike policy SubSrv proposals PSK-SHA256-DH14-AES256
set security group-vpn member ike policy SubSrv pre-shared-key ascii-text "$ABC123$ABC123"
set security group-vpn member ike gateway SubSrv ike-policy SubSrv
set security group-vpn member ike gateway SubSrv server-address 10.17.101.1
set security group-vpn member ike gateway SubSrv server-address 10.17.102.1
set security group-vpn member ike gateway SubSrv server-address 10.17.103.1
set security group-vpn member ike gateway SubSrv server-address 10.17.104.1
set security group-vpn member ike gateway SubSrv local-address 10.18.104.1
set security group-vpn member ipsec vpn GROUP_ID-0001 ike-gateway SubSrv
set security group-vpn member ipsec vpn GROUP_ID-0001 group 1
set security group-vpn member ipsec vpn GROUP_ID-0001 match-direction output
set security group-vpn member ipsec vpn GROUP_ID-0001 tunnel-mtu 1400
set security group-vpn member ipsec vpn GROUP_ID-0001 df-bit clear
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.101.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.102.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.103.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks from source-address
10.17.104.1/32
set firewall family inet service-filter GroupVPN-KS term inbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.101.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.102.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.103.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks from destination-address
10.17.104.1/32
set firewall family inet service-filter GroupVPN-KS term outbound-ks then skip
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from source-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 from destination-address
172.16.0.0/12
set firewall family inet service-filter GroupVPN-KS term GROUP_ID-0001 then service
set services service-set GROUP_ID-0001 interface-service service-interface ms-0/2/0.0
set services service-set GROUP_ID-0001 ipsec-group-vpn GROUP_ID-0001

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ???? CLI ??? ???? ?? ???? CLI ??? ?? ????.

?? VPNv2 ??? ???? ????.

### 1. ???? ????.

```
[edit interfaces]
user@host# set xe-0/0/1 unit 0 family inet service input service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet service output service-set GROUP_ID-0001 service-
filter GroupVPN-KS
user@host# set xe-0/0/1 unit 0 family inet address 10.18.104.1/24
user@host# set xe-0/0/2 unit 0 family inet address 172.16.104.1/24
user@host# set ms-0/2/0 unit 0 family inet
```

### 2. IKE(Internet Key Exchange) ??, ?? ? ???? ????.

```
[edit security group-vpn member ike proposal PSK-SHA256-DH14-AES256]
user@host# set authentication-method pre-shared-keys
user@host# set dh-group group14
user@host# set authentication-algorithm sha-256
user@host# set encryption-algorithm aes-256-cbc
[edit security group-vpn member ike policy SubSrv]
user@host# set mode main
user@host# set proposals PSK-SHA256-DH14-AES256
user@host# set pre-shared-key ascii-text "$ABC123$ABC123"
[edit security group-vpn member ike gateway SubSrv]
user@host# set ike-policy SubSrv
user@host# set server-address 10.17.101.1
user@host# set server-address 10.17.102.1
user@host# set server-address 10.17.103.1
user@host# set server-address 10.17.104.1
user@host# set local-address 10.18.104.1
```

### 3. IPsec SA ? ????.

```
[edit security group-vpn member ipsec vpn GROUP_ID-0001]
user@host# set ike-gateway SubSrv
user@host# set group 1
```



```

        service-set GROUP_ID-0001 service-filter GroupVPN-KS;
    }
    output {
        service-set GROUP_ID-0001 service-filter GroupVPN-KS;
    }
}
address 10.18.104.1/24;
}
}
}
xe-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.104.1/24;
        }
    }
}
ms-0/2/0 {
    unit 0 {
        family inet;
    }
}
[edit]
user@host# show security
group-vpn {
    member {
        ike {
            proposal PSK-SHA256-DH14-AES256 {
                authentication-method pre-shared-keys;
                dh-group group14;
                authentication-algorithm sha-256;
                encryption-algorithm aes-256-cbc;
            }
            policy SubSrv {
                mode main;
                proposals PSK-SHA256-DH14-AES256;
                pre-shared-key ascii-text "$ABC123$ABC123"; ## SECRET-DATA
            }
            gateway SubSrv {
                ike-policy SubSrv;
                server-address [ 10.17.101.1 10.17.102.1 10.17.103.1 10.17.104.1 ];
                local-address 10.18.104.1;
            }
        }
    }
}

```

```

    }
    ipsec {
        vpn GROUP_ID-0001 {
            ike-gateway SubSrv;
            group 1;
            match-direction output;
            tunnel-mtu 1400;
            df-bit clear;
        }
    }
}

[edit]
user@host# show services
service-set GROUP_ID-0001 {
    interface-service {
        service-interface ms-0/2/0.0;
    }
    ipsec-group-vpn GROUP_ID-0001;
}

[edit]
user@host# show firewall
family inet {
    service-filter GroupVPN-KS {
        term inbound-ks {
            from {
                source-address {
                    10.17.101.1/32;
                    10.17.102.1/32;
                    10.17.103.1/32;
                    10.17.104.1/32;
                }
            }
            then skip;
        }
        term outbound-ks {
            from {
                destination-address {
                    10.17.101.1/32;
                    10.17.102.1/32;
                    10.17.103.1/32;
                    10.17.104.1/32;
                }
            }
        }
    }
}

```

```
    }
    then skip;
  }
  term GROUP_ID-0001 {
    from {
      source-address {
        172.16.0.0/12;
      }
      destination-address {
        172.16.0.0/12;
      }
    }
    then service;
  }
}
```

?? ?? ?? ?? ?? commit?(?) ????.

??

**in this section**

- [?? ???? ?? ?? | 942](#)
- [SA? ???? ???? ?? | 946](#)
- [???? IKE\(Internet Key Exchange\) SA ?? | 949](#)
- [?? ? ?? ???? IPsec SA ?? | 951](#)
- [?? ??? ?? IPsec ?? ?? | 954](#)

??? ???? ???? ???? ????.

?? ???? ?? ??

??

?? ????? ???? ???? ?? ???? ?????. ??? ?? ???? ???? ???? ???? ????.



??

?? ???? ?? ???, show security group-vpn server server-cluster detail, ? show security group-vpn server statistics ??? ????show security group-vpn server server-cluster.

```
user@RootSrv> show security group-vpn server server-cluster
Group: GROUP_ID-0001, Group Id: 1
Role: Root-server, Version Number: 2,
  Peer Gateway      Peer IP      Role      Status
  SubSrv01          10.16.101.1  Sub-server Active
  SubSrv02          10.16.102.1  Sub-server Active
  SubSrv03          10.16.103.1  Sub-server Active
  SubSrv04          10.16.104.1  Sub-server Active
```

```
user@RootSrv> show security group-vpn server server-cluster detail
Group: GROUP_ID-0001, Group Id: 1
Role: Root-server, Version Number: 2

Peer gateway: SubSrv01
  Peer IP: 10.16.101.1, Local IP: 10.10.101.1, VR: default
  Role: Sub-server, Status: Active
  CLUSTER-INIT send:      0
  CLUSTER-INIT recv:      1
  CLUSTER-INIT success:    1
  CLUSTER-INIT fail:      0
  CLUSTER-INIT dup:       0
  CLUSTER-INIT abort:     0
  CLUSTER-INIT timeout:   0
  CLUSTER-UPDATE send:    2
  CLUSTER-UPDATE recv:    0
  CLUSTER-UPDATE success: 2
  CLUSTER-UPDATE fail:    0
  CLUSTER-UPDATE abort:   0
  CLUSTER-UPDATE timeout: 0
  CLUSTER-UPDATE pending: 0
  CLUSTER-UPDATE max retry reached: 0
  DPD send:               677
  DPD send fail:          0
  DPD ACK recv:           677
  DPD ACK invalid seqno:  0
  IPsec SA policy mismatch: 0
```

```

IPsec SA proposal mismatch:      0
KEK SA proposal mismatch:        0

```

Peer gateway: SubSrv02

Peer IP: 10.16.102.1, Local IP: 10.10.102.1, VR: default

Role: Sub-server, Status: Active

```

CLUSTER-INIT send:                0
CLUSTER-INIT recv:                1
CLUSTER-INIT success:             1
CLUSTER-INIT fail:                0
CLUSTER-INIT dup:                 0
CLUSTER-INIT abort:               0
CLUSTER-INIT timeout:             0
CLUSTER-UPDATE send:              2
CLUSTER-UPDATE recv:              0
CLUSTER-UPDATE success:           2
CLUSTER-UPDATE fail:              0
CLUSTER-UPDATE abort:             0
CLUSTER-UPDATE timeout:           0
CLUSTER-UPDATE pending:           0
CLUSTER-UPDATE max retry reached: 0
DPD send:                          676
DPD send fail:                    0
DPD ACK recv:                     676
DPD ACK invalid seqno:            0
IPsec SA policy mismatch:          0
IPsec SA proposal mismatch:        0
KEK SA proposal mismatch:          0

```

user@RootSrv> **show security group-vpn server statistics**

Group: GROUP\_ID-0001, Group Id: 1

Stats:

```

Pull Succeeded                    : 0
Pull Failed                      : 0
Pull Exceed Member Threshold     : 0
Push Sent                        : 0
Push Acknowledged                : 0
Push Unacknowledged              : 0

```

?? ???? ? ?? ???? show security group-vpn server server-cluster, show security group-vpn server server-cluster detail, ??? show security group-vpn server statistics ?????.

```
user@SubSrv01> show security group-vpn server server-cluster
```

Group: GROUP\_ID-0001, Group Id: 1

Role: Sub-server, Version Number: 2,

| Peer Gateway | Peer IP     | Role        | Status |
|--------------|-------------|-------------|--------|
| RootSrv      | 10.10.101.1 | Root-server | Active |

```
user@SubSrv01> show security group-vpn server server-cluster detail
```

Group: GROUP\_ID-0001, Group Id: 1

Role: Sub-server, Version Number: 2

Peer gateway: RootSrv

Peer IP: 10.10.101.1, Local IP: 10.16.101.1, VR: default

Role: Root-server, Status: Active

|                                   |     |
|-----------------------------------|-----|
| CLUSTER-INIT send:                | 1   |
| CLUSTER-INIT recv:                | 0   |
| CLUSTER-INIT success:             | 1   |
| CLUSTER-INIT fail:                | 0   |
| CLUSTER-INIT dup:                 | 0   |
| CLUSTER-INIT abort:               | 0   |
| CLUSTER-INIT timeout:             | 0   |
| CLUSTER-UPDATE send:              | 0   |
| CLUSTER-UPDATE recv:              | 2   |
| CLUSTER-UPDATE success:           | 2   |
| CLUSTER-UPDATE fail:              | 0   |
| CLUSTER-UPDATE abort:             | 0   |
| CLUSTER-UPDATE timeout:           | 0   |
| CLUSTER-UPDATE pending:           | 0   |
| CLUSTER-UPDATE max retry reached: | 0   |
| DPD send:                         | 812 |
| DPD send fail:                    | 0   |
| DPD ACK recv:                     | 812 |
| DPD ACK invalid seqno:            | 0   |
| IPsec SA policy mismatch:         | 0   |
| IPsec SA proposal mismatch:       | 0   |
| KEK SA proposal mismatch:         | 0   |

```
user@SubSrv01> show security group-vpn server statistics
```

Group: GROUP\_ID-0001, Group Id: 1

## Stats:

```

Pull Succeeded           : 4
Pull Failed              : 0
Pull Exceed Member Threshold : 0
Push Sent                : 8
Push Acknowledged        : 8
Push Unacknowledged      : 0

```

SA? ???? ???? ??

??

?? ??? ? ???? ???? SA? ???? ? ???? SA? ???? ????.

??

?? ???? ? ???? ? show security group-vpn server kek security-associations detail ??? ????show security group-vpn server kek security-associations.

```
user@RootSrv> show security group-vpn server kek security-associations
```

```

Index   Life:sec Initiator cookie Responder cookie GroupId
738885  2888     5742c24020056c6a d6d479543b56404c 1

```

```
user@RootSrv> show security group-vpn server kek security-associations detail
```

```
Index 738885, Group Name: GROUP_ID-0001, Group Id: 1
```

```
Initiator cookie: 5742c24020056c6a, Responder cookie: d6d479543b56404c
```

```
Authentication method: RSA
```

```
Lifetime: Expires in 2883 seconds, Activated
```

```
Rekey in 2373 seconds
```

## Algorithms:

```

Sig-hash      : sha256
Encryption    : aes256-cbc

```

## Traffic statistics:

```

Input bytes   : 0
Output bytes  : 0
Input packets : 0
Output packets: 0

```

```
Server Member Communication: Unicast
```

```
Retransmission Period: 10, Number of Retransmissions: 2
```

```
Group Key Push sequence number: 0
```

PUSH negotiations in progress: 0

```

?? ???? ? ?? ??? ? show security group-vpn server kek security-associations detail ??? ?????show security
group-vpn server kek security-associations.

```

```
user@SubSrv01> show security group-vpn server kek security-associations
```

| Index  | Life:sec | Initiator cookie | Responder cookie | GroupId |
|--------|----------|------------------|------------------|---------|
| 738885 | 1575     | 5742c24020056c6a | d6d479543b56404c | 1       |

```
user@SubSrv01> show security group-vpn server kek security-associations detail
```

Index 738879, Group Name: GROUP\_ID-0001, Group Id: 1

Initiator cookie: 114e4a214891e42f, Responder cookie: 4b2848d14372e5bd

Authentication method: RSA

Lifetime: Expires in 4186 seconds, Activated

Rekey in 3614 seconds

### Algorithms:

Sig-hash : sha256

```
Encryption      : aes256-cbc
```

Traffic statistics:

```
Input bytes : 0
```

```
Output bytes      :      0
```

```
Input packets: 0
```

Output packets: 0

Server Member Communication: Unicast

```
Retransmission Period: 10, Number of Retransmissions: 2
```

Group Key Push sequence number: 0

PUSH negotiations in progress: 0

```

[?] [?] [?] [?] [?] [?] show security group-vpn member kek security-associations [?] show security group-vpn member kek
security-associations detail [?] [?] [?] [?] [?] [?].

```

SRX [??] [??] [?] vSRX [?] [??] [?] [??] [?]:

```
user@GM-0001> show security group-vpn server kek security-associations
```

| Index   | Server Address | Life:sec | Initiator cookie | Responder cookie | GroupId |
|---------|----------------|----------|------------------|------------------|---------|
| 5455799 | 10.17.101.1    | 1466     | 5742c24020056c6a | d6d479543b56404c | 1       |

```
user@GM-0001> show security group-vpn server kek security-associations detail
```

```

Index 5455799, Group Id: 1
Group VPN Name: GROUP_ID-0001
Local Gateway: 10.18.101.1, GDOI Server: 10.17.101.1
Initiator cookie: 5742c24020056c6a, Responder cookie: d6d479543b56404c
Lifetime: Expires in 1464 seconds
Group Key Push Sequence number: 0

```

#### Algorithms:

```

Sig-hash          : hmac-sha256-128
Encryption        : aes256-cbc

```

#### Traffic statistics:

```

Input bytes  : 0
Output bytes : 0
Input packets: 0
Output packets: 0

```

#### Stats:

```

Push received      : 0
Delete received    : 0

```

MX **?? ???? ??**:

```
user@GM-0003> show security group-vpn member kek security-associations
```

| Index   | Server Address | Life:sec | Initiator cookie | Responder cookie | GroupId |
|---------|----------------|----------|------------------|------------------|---------|
| 5184329 | 10.17.101.1    | 1323     | 5742c24020056c6a | d6d479543b56404c | 1       |

```
user@GM-0003> show security group-vpn member kek security-associations detail
```

```

Index 5184329, Group Id: 1
Group VPN Name: GROUP_ID-0001
Local Gateway: 10.18.103.1, GDOI Server: 10.17.101.1
Initiator cookie: 5742c24020056c6a, Responder cookie: d6d479543b56404c
Lifetime: Expires in 1321 seconds
Group Key Push Sequence number: 0

```

#### Algorithms:

```

Sig-hash          : hmac-sha256-128
Encryption        : aes256-cbc

```

#### Traffic statistics:

```

Input bytes  : 0
Output bytes : 0
Input packets: 0
Output packets: 0

```

#### Stats:

|                 |   |   |
|-----------------|---|---|
| Push received   | : | 0 |
| Delete received | : | 0 |

?? IKE(Internet Key Exchange) SA ??

??

?? IKE SA(?? ??) ? ????.

??

?? ???? ?? ??? ? show security group-vpn server ike security-associations detail ??? ????show security group-vpn server ike security-associations.

```

user@RootSrv> show security group-vpn server ike security-associations

```

| Index  | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|--------|-------|------------------|------------------|------|----------------|
| 738880 | UP    | 2221001e980eb08b | 5af00708f5da289c | Main | 10.16.104.1    |
| 738881 | UP    | 59e8c1d328b1d9fd | d63e823fb8be1f22 | Main | 10.16.101.1    |
| 738883 | UP    | 9cb3a49c6771819e | 8df3be8c9ddeb2a7 | Main | 10.16.102.1    |
| 738882 | UP    | 9a8a75f05a1384c5 | c6d58696c896b730 | Main | 10.16.103.1    |

```

user@RootSrv> show security group-vpn server ike security-associations detail

```

IKE peer 10.16.101.1, Index 738881, Gateway Name: SubSrv01

Role: Responder, State: UP

Initiator cookie: 59e8c1d328b1d9fd, Responder cookie: d63e823fb8be1f22

Exchange type: Main, Authentication method: Pre-shared-keys

Local: 10.10.101.1:848, Remote: 10.16.101.1:848

Lifetime: Expires in 21890 seconds

Peer ike-id: 10.16.101.1

Xauth user-name: not available

Xauth assigned IP: 0.0.0.0

Algorithms:

|                        |   |                 |
|------------------------|---|-----------------|
| Authentication         | : | hmac-sha256-128 |
| Encryption             | : | aes256-cbc      |
| Pseudo random function | : | hmac-sha256     |
| Diffie-Hellman group   | : | DH-group-14     |

Traffic statistics:

|               |   |        |
|---------------|---|--------|
| Input bytes   | : | 150112 |
| Output bytes  | : | 153472 |
| Input packets | : | 1387   |

```

Output packets:          1387
Flags: IKE SA is created
IKE peer 10.16.102.1, Index 738883, Gateway Name: SubSrv02
Role: Responder, State: UP
Initiator cookie: 9cb3a49c6771819e, Responder cookie: 8df3be8c9ddeb2a7
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.10.102.1:848, Remote: 10.16.102.1:848
Lifetime: Expires in 21899 seconds
Peer ike-id: 10.16.102.1
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication          : hmac-sha256-128
Encryption               : aes256-cbc
Pseudo random function: hmac-sha256
Diffie-Hellman group    : DH-group-14
Traffic statistics:
Input  bytes   :          149788
Output bytes   :          153148
Input  packets:           1384
Output packets:           1384
Flags: IKE SA is created

```

?? ???? ? ?? ???? ? show security group-vpn server ike security-associations detail ??? ????show security group-vpn server ike security-associations.

```

user@SubSrv01> show security group-vpn server ike security-associations
Index   State Initiator cookie Responder cookie Mode      Remote Address
738878  UP    59e8c1d328b1d9fd d63e823fb8be1f22 Main      10.10.101.1

```

```

user@SubSrv01> show security group-vpn server ike security-associations detail
IKE peer 10.10.101.1, Index 738878, Gateway Name: RootSrv
Role: Initiator, State: UP
Initiator cookie: 59e8c1d328b1d9fd, Responder cookie: d63e823fb8be1f22
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.16.101.1:848, Remote: 10.10.101.1:848
Lifetime: Expires in 20589 seconds
Peer ike-id: 10.10.101.1
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:

```



```

Authentication      : hmac-sha256-128
Encryption          : aes256-cbc
Pseudo random function: hmac-sha256
Diffie-Hellman group : DH-group-14
Traffic statistics:
Input  bytes   :          181444
Output bytes   :          178084
Input  packets :           1646
Output packets :           1646
Flags: IKE SA is created

```

?? ? ?? ???? IPsec SA ??

??

?? ? ?? ???? IPsec SA(Security Association)? ?????.

??

?? ???? ? ???? ? show security group-vpn server ipsec security-associations detail ??? ?????.show security group-vpn server ipsec security-associations.

```

user@RootSrv> show security group-vpn server ipsec security-associations
Group: GROUP_ID-0001, Group Id: 1
Total IPsec SAs: 1
IPsec SA      Algorithm      SPI      Lifetime
GROUP_ID-0001  ESP:aes-256/sha256 dddef414      2773

user@RootSrv> show security group-vpn server ipsec security-associations detail
Group: GROUP_ID-0001, Group Id: 1
Total IPsec SAs: 1
IPsec SA: GROUP_ID-0001
Protocol: ESP, Authentication: sha256, Encryption: aes-256
Anti-replay: D3P enabled
SPI: dddef414
Lifetime: Expires in 1670 seconds, Activated
Rekey in 1160 seconds
Policy Name: 1
Source: 172.16.0.0/12
Destination: 172.16.0.0/12
Source Port: 0

```

Destination Port: 0

Protocol: 0

?? ???? ? ?? ???? ? show security group-vpn server ipsec security-associations detail ??? ????show security group-vpn server ipsec security-associations.

```
user@SubSrv01> show security group-vpn server ipsec security-associations
```

Group: GROUP\_ID-0001, Group Id: 1

Total IPsec SAs: 1

| IPsec SA      | Algorithm          | SPI      | Lifetime |
|---------------|--------------------|----------|----------|
| GROUP_ID-0001 | ESP:aes-256/sha256 | dddef414 | 1520     |

```
user@SubSrv01> show security group-vpn server ipsec security-associations detail
```

Group: GROUP\_ID-0001, Group Id: 1

Total IPsec SAs: 1

IPsec SA: GROUP\_ID-0001

Protocol: ESP, Authentication: sha256, Encryption: aes-256

Anti-replay: D3P enabled

SPI: dddef414

Lifetime: Expires in 1518 seconds, Activated

Rekey in 1230 seconds

Policy Name: 1

Source: 172.16.0.0/12

Destination: 172.16.0.0/12

Source Port: 0

Destination Port: 0

Protocol: 0

?? ???? ? ?? ???? ? show security group-vpn member ipsec security-associations ? show security group-vpn member ipsec security-associations detail ??? ???? ?

SRX ??? ???? ? vSRX ?? ???? ? ???? ? ??:

```
user@GM-0001> show security group-vpn member ipsec security-associations
```

Total active tunnels: 1

| ID      | Server      | Port | Algorithm              | SPI      | Life:sec/kb | GId | lsys |
|---------|-------------|------|------------------------|----------|-------------|-----|------|
| <>49152 | 10.17.101.1 | 848  | ESP:aes-256/sha256-128 | dddef414 | 1412/ unlim | 1   | root |

```
user@GM-0001> show security group-vpn member ipsec security-associations detail
```

Virtual-system: root Group VPN Name: GROUP\_ID-0001

Local Gateway: 10.18.101.1, GDOI Server: 10.17.101.1

Group Id: 1

Routing Instance: default

Recovery Probe: Enabled

DF-bit: clear

Stats:

```

Pull Succeeded      : 1
Pull Failed         : 0
Pull Timeout        : 0
Pull Aborted        : 0
Push Succeeded      : 2
Push Failed         : 0
Server Failover     : 0
Delete Received     : 0
Exceed Maximum Keys(4) : 0
Exceed Maximum Policies(10): 0
Unsupported Algo    : 0

```

Flags:

Rekey Needed: no

List of policies received from server:

Tunnel-id: 49152

Source IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Destination IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Direction: bi-directional, SPI: dddef414

Protocol: ESP, Authentication: sha256-128, Encryption: aes-256

Hard lifetime: Expires in 1409 seconds, Activated

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 1193 seconds

Mode: Tunnel, Type: Group VPN, State: installed

Anti-replay service: D3P enabled

MX `??` `???` `??`:

```
user@GM-0003> show security group-vpn member ipsec security-associations
```

Total active tunnels: 1

```

ID      Server      Port Algorithm      SPI      Life:sec/kb  GId lsys
<>10001 10.17.101.1    848   ESP:aes-256/sha256-128 dddef414 1308/ unlim 1 root

```

```
user@GM-0003> show security group-vpn member ipsec security-associations detail
```

Virtual-system: root Group VPN Name: GROUP\_ID-0001

Local Gateway: 10.18.103.1, GDOI Server: 10.17.101.1

Group Id: 1

Rule Match Direction: output, Tunnel-MTU: 1400

Routing Instance: default

DF-bit: clear

Stats:

|                            |   |   |
|----------------------------|---|---|
| Pull Succeeded             | : | 1 |
| Pull Failed                | : | 0 |
| Pull Timeout               | : | 0 |
| Pull Aborted               | : | 0 |
| Push Succeeded             | : | 2 |
| Push Failed                | : | 0 |
| Server Failover            | : | 0 |
| Delete Received            | : | 0 |
| Exceed Maximum Keys(4)     | : | 0 |
| Exceed Maximum Policies(1) | : | 0 |
| Unsupported Algo           | : | 0 |

Flags:

Rekey Needed: no

List of policies received from server:

Tunnel-id: 10001

Source IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Destination IP: ipv4\_subnet(any:0,[0..7]=172.16.0.0/12)

Direction: bi-directional, SPI: dddef414

Protocol: ESP, Authentication: sha256-128, Encryption: aes-256

Hard lifetime: Expires in 1305 seconds, Activated

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 1087 seconds

Mode: Tunnel, Type: Group VPN, State: installed

Anti-replay service: D3P enabled

?? ???? ?? IPsec ?? ??

??

SRX ???? ???? ?? vSRX ?? ???? ?? ???? IPsec ???? ?????.

MX ???? ?? ???? ? ???? ???? ? ????.

??

?? ???? SRX ??? ???? ?? vSRX ?? ???? ?? ???? ???? ???? show security group-vpn member policy .

```
user@GM-0001> show security group-vpn member policy
Group VPN Name: GROUP_ID-0001, Group Id: 1
From-zone: LAN, To-zone: WAN
Tunnel-id: 49152, Policy type: Secure
  Source      : IP <172.16.0.0 - 172.31.255.255>, Port <0 - 65535>, Protocol <0>
  Destination : IP <172.16.0.0 - 172.31.255.255>, Port <0 - 65535>, Protocol <0>

Tunnel-id: 63488, Policy type: Fail-close
  Source      : IP <0.0.0.0 - 255.255.255.255>, Port <0 - 65535>, Protocol <0>
  Destination : IP <0.0.0.0 - 255.255.255.255>, Port <0 - 65535>, Protocol <0>
```

SEE ALSO

?? VPNv2 ?? ?? | 807

---

??? ???? ?? VPNv2?? ?? VPN ??

?? ??

?? VPNv1 | 752

# 9

CHAPTER LABEL COVER PAGE

?? ?? ??

---

in this chapter

- ?? ?? VPN | 957
-

?? ? VPN ? SRX ??? ????? ? ? VPN? ????? ? ? ?  
 ??????.

?? ?? VPN ?? | 957

?? ?? ??? ??? ??? ??? | 963

?: ?? ?? VPN ?? ??? ?? ??? ??? ??? ?  
? | 965

?: IPv6 ??? ?? OSPFv3? ??? ADVPN ?  
? | 1017

ADVPN ?? ?? ??? ??? ? OSPF? ??? ??? ???  
? ? ??? ?? | 1053

ADVPN ??? ????? ??? | 1054

**QUESTION**

???? ???? ???? "ADVPN ???? ???? ?????" ??? 1054 ???? ?????.

?? ?? VPN ??

- ADVPN ???? | 958
- ??? ? | 958
- ? ? ? ? ? ? ? ? | 959
- ??? ? | 959
- ???? ? | 961
- PIM? ??? ?????? ? | 961
- ADVPN ? ? ? ? | 962

ADVPN(Auto Discovery VPN)은 모든 VPN 클라이언트가 ADVPN을 지원하는지 확인하고, ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.

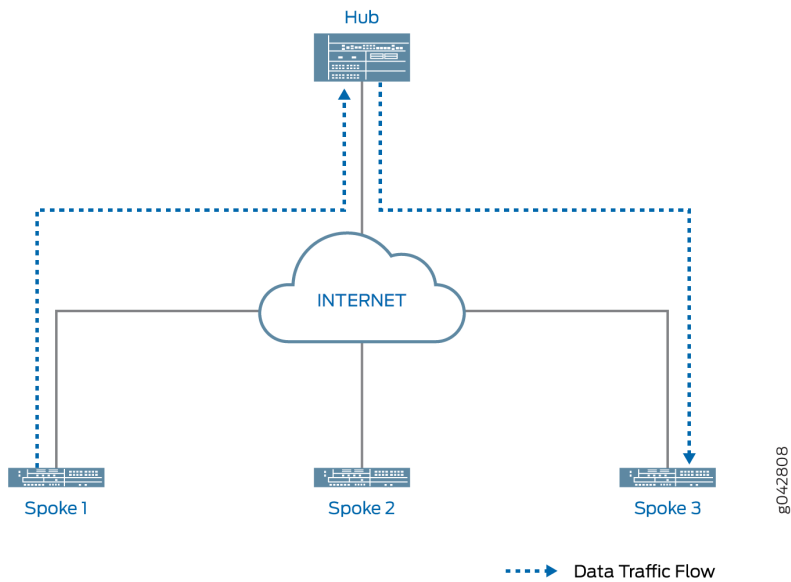
ADVPN 구성

ADVPN은 IKEv2 프로토콜을 사용하여 VPN 클라이언트가 ADVPN을 지원하는지 확인하고, ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다. ADVPN은 ADVPN\_SUPPORTED라는 속성을 사용하여 IKE 프로토콜을 사용하여 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.

구성

IPsec VPN 클라이언트가 ADVPN을 지원하는지 확인하고, ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다. [54](#) [958](#)은 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.

54: ADVPN 구성



ADVPN은 모든 VPN 클라이언트가 ADVPN을 지원하는지 확인하고, ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다. [1](#) [3](#)은 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.

ADVPN은 IKEv2 SA를 사용하여 VPN 클라이언트가 ADVPN을 지원하는지 확인하고, ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다. ADVPN은 ADVPN\_SUPPORTED라는 속성을 사용하여 IKE(Internet Key Exchange) 프로토콜을 사용하여 IPsec SA를 사용하여 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.

[55](#) [959](#)은 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다. [1](#) [3](#)은 ADVPN을 지원하는 클라이언트와 ADVPN을 지원하지 않는 클라이언트 간의 연결을 설정하는 프로세스입니다.





115: 115 115 115

| 115                               | 115/115 115 |
|-----------------------------------|-------------|
| 115 115 115                       | 115         |
| 115115115                         | 115         |
| 115 115115                        | 115         |
| 115 115 115                       | 115         |
| DF 115                            | 115         |
| 115115 115115                     | 115         |
| 115 115                           | 115115      |
| 115 115115115                     | 115         |
| 115115115 115                     | 115         |
| 115 IKE(Internet Key Exchange) ID | 115         |
| IKE 115                           | 115         |
| 115 115                           | 115         |
| 115 115                           | 115         |
| 115 ID                            | 115115      |
| NAT 115                           | 115         |















116: AutoVPN 1.2.2.2 ADVPN 2.2.2.2

|    |    |
|----|----|
| ?? | ?? |
|----|----|

IKE(Internet Key Exchange) 2.2:

|                       |             |
|-----------------------|-------------|
| ?? ??                 | RSA ??      |
| DH(Diffie-Hellman) ?? | group5      |
| ?? 2222               | sha1        |
| 222 2222              | AES-256-CBC |

IKE(Internet Key Exchange) 2.2:

|     |        |
|-----|--------|
| 222 | ?? 222 |
|-----|--------|

IKE(Internet Key Exchange) 2.2.2.2:

|    |       |
|----|-------|
| ?? | v2 ?? |
|----|-------|

IPsec 2.2:

|          |              |
|----------|--------------|
| 2222     | esp          |
| ?? 2222  | hmac-sha1-96 |
| 222 2222 | AES-256-CBC  |

IPsec 2.2:

|                                 |        |
|---------------------------------|--------|
| PFS(Perfect Forward Secrecy) ?? | group5 |
|---------------------------------|--------|

?? ? 2222 IKE(Internet Key Exchange) 2.2.2.2 VPN 2.2.2.2 ?? ? ?? ?? 22222. 117 222 968 ?? ?  
222 ?? ? 2222 ?? IKE(Internet Key Exchange) 2.2.2.2 ?? 2222.







```
set routing-options router-id 172.16.1.1
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate Suggester_Certificate_ID
set security ike gateway SUGGESTER_GW ike-policy IKE_POL
set security ike gateway SUGGESTER_GW dynamic distinguished-name wildcard O=XYZ, OU=Sales
set security ike gateway SUGGESTER_GW dynamic ike-user-type group-ike-id
set security ike gateway SUGGESTER_GW dead-peer-detection
set security ike gateway SUGGESTER_GW local-identity distinguished-name
set security ike gateway SUGGESTER_GW external-interface reth1.0
set security ike gateway SUGGESTER_GW local-address 11.1.1.1
set security ike gateway SUGGESTER_GW advpn partner disable
set security ike gateway SUGGESTER_GW advpn suggester
set security ike gateway SUGGESTER_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn SUGGESTER_VPN bind-interface st0.1
set security ipsec vpn SUGGESTER_VPN ike gateway SUGGESTER_GW
set security ipsec vpn SUGGESTER_VPN ike ipsec-policy IPSEC_POL
set security pki ca-profile advpn ca-identity advpn
set security pki ca-profile advpn enrollment url http://10.157.92.176:8080/scep/advpn/
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces st0.1
set security zones security-zone trust interfaces reth0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces reth1.0
set security policies default-policy permit-all
```

???

?? ?? ?? ???? ??? ??? ???? ?????. ?? ????? ??? ?? ??? CLI ??? ???? ?? ????? CLI ??? ???? ?????.

□□□□ □□□□□□.

1. `?? ?? ? ? ? ? ? ?`.

```
[edit interfaces]
user@host# set ge-0/0/3 gigether-options redundant-parent reth0
user@host# set ge-0/0/4 gigether-options redundant-parent reth1
user@host# set ge-7/0/3 gigether-options redundant-parent reth0
user@host# set ge-7/0/4 gigether-options redundant-parent reth1
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 10.1.1.1/24
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 11.1.1.1/24
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 172.16.1.1/24
```

2. `?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?`.

```
[edit protocols ospf]
user@host# set graceful-restart restart-duration 300
user@host# set graceful-restart notify-duration 300
user@host# set graceful-restart no-strict-lsa-checking
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 metric 10
user@host# set area 0.0.0.0 interface st0.1 retransmit-interval 1
user@host# set area 0.0.0.0 interface st0.1 dead-interval 40
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface reth0.0
[edit routing-options]
user@host# set graceful-restart
user@host# set static route 21.1.1.0/24 next-hop 11.1.1.2
user@host# set static route 31.1.1.0/24 next-hop 11.1.1.2
user@host# set router-id 172.16.1.1
```

3. `1 ? ? ? ? ? ? ? ? ? ?`.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
```

```
[edit security ike policy IKE_POL]
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate Suggester_Certificate_ID
[edit security ike gateway SUGGESTER_GW]
user@host# set ike-policy IKE_POL
user@host# set dynamic distinguished-name wildcard O=XYZ, OU=Sales
user@host# set dynamic ike-user-type group-ike-id
user@host# set dead-peer-detection
user@host# set local-identity distinguished-name
user@host# set external-interface reth1.0
user@host# set local-address 11.1.1.1
user@host# set advpn partner disable
user@host# set advpn suggester
user@host# set version v2-only
```

#### 4. `set security ipsec proposal`.

```
[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals IPSEC_PROP
[edit security isec vpn SUGGESTER_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway SUGGESTER_GW
user@host# set ike ipsec-policy IPSEC_POL
```

#### 5. `set security advpn ca-profile`.

```
[edit security pki]
user@host# set ca-profile advpn ca-identity advpn
user@host# set ca-profile advpn enrollment url http://10.157.92.176:8080/scep/advpn/
```

#### 6. `set security zones security-zone`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
```

```
user@host# set interfaces st0.1
user@host# set interfaces reth0.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces reth1.0
```

**7.**                     .

```
[edit security policies]
user@host# set default-policy permit-all
```

??

```

[?] [?][?][?], show protocols, , show security ikeshow routing-options, show security ipsec, show security pki, show
security zones? show security policies [?][?] [?][?][?] show interfaces[?][?] [?][?][?][?]. [?] [?][?] [?][?] [?][?][?] [?][?] [?] [?] [?]
[?] [?][?][?] [?][?] [?][?][?][?].

```

```
[edit]
user@host# show interfaces
ge-0/0/3 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-0/0/4 {
    gigether-options {
        redundant-parent reth1;
    }
}
ge-7/0/3 {
    gigether-options {
        redundant-parent reth0;
    }
}
ge-7/0/4 {
    gigether-options {
        redundant-parent reth1;
    }
}
```



```

reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 10.1.1.1/24;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 11.1.1.1/24;
        }
    }
}
st0 {
    unit 1 {
        multipoint;
        family inet {
            address 172.16.1.1/24;
        }
    }
}
[edit]
user@host# show protocols
ospf {
    graceful-restart {
        restart-duration 300;
        notify-duration 300;
        no-strict-lsa-checking;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            metric 10;
            retransmit-interval 1;
            dead-interval 40;
            demand-circuit;

```

```

        dynamic-neighbors;
    }
    interface reth0.0;
}
[edit]
user@host# show routing-options
graceful-restart;
static {
    route 21.1.1.0/24 next-hop 11.1.1.2;
    route 31.1.1.0/24 next-hop 11.1.1.2;
}
router-id 172.16.1.1;
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate Suggester_Certificate_ID;
    }
}
gateway SUGGESTER_GW {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard O=XYZ, OU=Sales;
        }
        ike-user-type group-ike-id;
    }
    dead-peer-detection {
    }
    local-identity distinguished-name;
    external-interface reth1.0
    local-address 11.1.1.1;
    advpn {
        partner {
            disable;

```

```

        }
        suggester {
    ]
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}
vpn SUGGESTER_VPN {
    bind-interface st0.1;
    ike {
        gateway SUGGESTER_GW;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security pki
ca-profile advpn {
    ca-identity advpn;
    enrollment {
        url http://10.157.92.176:8080/scep/advpn/;
    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;

```

```

    }
  }
  interfaces {
    st0.1;
    reth0.0;
  }
}
security-zone untrust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    reth1.0;
  }
}
[edit]
user@host# show security policies
  default-policy {
    permit-all;
  }

```

```

?? ?? ?? ?? commit?(?) ??????.

```

```

?? ??(??? 1)

```

## CLI ?? ??

```

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```

```

set interfaces ge-0/0/3 gigether-options redundant-parent reth0
set interfaces ge-0/0/4 gigether-options redundant-parent reth1
set interfaces ge-7/0/3 gigether-options redundant-parent reth0
set interfaces ge-7/0/4 gigether-options redundant-parent reth1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 25.1.1.1/24
set interfaces reth1 redundant-ether-options redundancy-group 1

```

```

set interfaces reth1 unit 0 family inet address 21.1.1.2/24
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet address 172.16.1.2/24
set protocols ospf graceful-restart restart-duration 300
set protocols ospf graceful-restart notify-duration 300
set protocols ospf graceful-restart no-strict-lsa-checking
set protocols ospf area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf area 0.0.0.0 interface st0.1 metric 15
set protocols ospf area 0.0.0.0 interface st0.1 retransmit-interval 1
set protocols ospf area 0.0.0.0 interface st0.1 dead-interval 40
set protocols ospf area 0.0.0.0 interface st0.1 demand-circuit
set protocols ospf area 0.0.0.0 interface st0.1 dynamic-neighbors
set protocols ospf area 0.0.0.0 interface reth0.0
set routing-options graceful-restart
set routing-options static route 11.1.1.0/24 next-hop 21.1.1.1
set routing-options static route 31.1.1.0/24 next-hop 21.1.1.1
set routing-options router-id 172.16.1.2
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate Partner1_Certificate_ID
set security ike gateway PARTNER_GW ike-policy IKE_POL
set security ike gateway PARTNER_GW address 11.1.1.1
set security ike gateway PARTNER_GW local-identity distinguished-name
set security ike gateway PARTNER_GW remote-identity distinguished-name container OU=Sales
set security ike gateway PARTNER_GW external-interface reth1
set security ike gateway PARTNER_GW local-address 21.1.1.2
set security ike gateway PARTNER_GW advpn suggerster disable
set security ike gateway PARTNER_GW advpn partner
set security ike gateway PARTNER_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn PARTNER_VPN bind-interface st0.1
set security ipsec vpn PARTNER_VPN ike gateway PARTNER_GW
set security ipsec vpn PARTNER_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn PARTNER_VPN establish-tunnels immediately
set security pki ca-profile advpn ca-identity advpn
set security pki ca-profile advpn enrollment url http://10.157.92.176:8080/scep/advpn/

```

```

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces st0.1
set security zones security-zone trust interfaces reth0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces reth1.0
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

??? 1? ?????.

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/3 gigether-options redundant-parent reth0
user@host# set ge-0/0/4 gigether-options redundant-parent reth1
user@host# set ge-7/0/3 gigether-options redundant-parent reth0
user@host# set ge-7/0/4 gigether-options redundant-parent reth1
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 25.1.1.1/24
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 21.1.1.2/24
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 172.16.1.2/24

```

2. ??? ???? ? ? ???? ????.

```

[edit protocols ospf]
user@host# set graceful-restart restart-duration 300
user@host# set graceful-restart notify-duration 300
user@host# set graceful-restart no-strict-lsa-checking
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 metric 15
user@host# set area 0.0.0.0 interface st0.1 retransmit-interval 1
user@host# set area 0.0.0.0 interface st0.1 dead-interval 40
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors

```

```

user@host# set protocols ospf area 0.0.0.0 interface reth0.0
[edit routing-options]
user@host# set graceful-restart
user@host# set static route 11.1.1.0/24 next-hop 21.1.1.1
user@host# set static route 31.1.1.0/24 next-hop 21.1.1.1
user@host# set router-id 172.16.1.2

```

### 3. 1?? ???? ?????.

```

[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy IKE_POL]
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate Partner1_Certificate_ID
[edit security ike gateway PARTNER_GW]
user@host# set ike-policy IKE_POL
user@host# set address 11.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=Sales
user@host# set external-interface reth1
user@host# set local-address 21.1.1.2
user@host# set advpn suggester disable
user@host# set advpn partner
user@host# set version v2-only

```

### 4. 2?? ???? ?????.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals IPSEC_PROP
[edit security isec vpn PARTNER_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway PARTNER_GW

```

```
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels immediately
```

**5.**                  .

```
[edit security pki]
user@host# set ca-profile advpn ca-identity advpn
user@host# set ca-profile advpn enrollment url http://10.157.92.176:8080/scep/advpn/
```

6.       .

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.1
user@host# set interfaces reth0.0

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces reth1.0
```

**7.**                    .

```
[edit security policies]
user@host# set default-policy permit-all
```

??

```
? ? ? ? ?, show protocols, , show security ikeshow routing-options, show security ipsec, show security pki, show
security zones? show security policies ? ? ? ? ? ? ? ? show interfaces? ? ? ? ? ? ? ?. ? ? ? ? ? ? ? ? ? ? ? ? ? ?
? ? ? ? ? ? ? ? ? ? ? ? ? ?.
```

```
[edit]
user@host# show interfaces
ge-0/0/3 {
    gigether-options {
        redundant-parent reth0;
    }
}
```



```

}
ge-0/0/4 {
    together-options {
        redundant-parent reth1;
    }
}
ge-7/0/3 {
    together-options {
        redundant-parent reth0;
    }
}
ge-7/0/4 {
    together-options {
        redundant-parent reth1;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 25.1.1.1/24;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 21.1.1.2/24;
        }
    }
}
st0 {
    unit 1 {
        multipoint;
        family inet {
            address 172.16.1.2/24;
        }
    }
}

```

```

}
[edit]
user@host# show protocols
ospf {
    graceful-restart {
        restart-duration 300;
        notify-duration 300;
        no-strict-lsa-checking;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            metric 15;
            retransmit-interval 1;
            dead-interval 40;
            demand-circuit;
            dynamic-neighbors;
        }
        interface reth0.0;
    }
}
[edit]
user@host# show routing-options
graceful-restart;
static {
    route 11.1.1.0/24 next-hop 21.1.1.1;
    route 31.1.1.0/24 next-hop 21.1.1.1;
}
router-id 172.16.1.2;
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate Partner1_Certificate_ID;
    }
}

```

```

gateway PARTNER_GW {
    ike-policy IKE_POL;
    address 11.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=Sales;
    external-interface reth1;
    local-address 21.1.1.2;
    advpn {
        suggester {
            disable;
        }
        partner {
        }
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}
vpn PARTNER_VPN {
    bind-interface st0.1;
    ike {
        gateway PARTNER_GW;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security pki
ca-profile advpn {
    ca-identity advpn;
    enrollment {
        url http://10.157.92.176:8080/scep/advpn/;
    }
}

```

```

    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        reth0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        reth1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

```

???(?? 2)

## CLI ??

?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ???? ???? ???? ???? [edit] ?  
 ? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set interfaces ge-0/0/2 unit 0 family inet address 31.1.1.2/24
set interfaces ge-0/0/4 unit 0 family inet address 36.1.1.1/24
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet address 172.16.1.3/24
set protocols ospf graceful-restart restart-duration 300
set protocols ospf graceful-restart notify-duration 300
set protocols ospf graceful-restart no-strict-lsa-checking
set protocols ospf area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf area 0.0.0.0 interface st0.1 metric 15
set protocols ospf area 0.0.0.0 interface st0.1 retransmit-interval 1
set protocols ospf area 0.0.0.0 interface st0.1 dead-interval 40
set protocols ospf area 0.0.0.0 interface st0.1 demand-circuit
set protocols ospf area 0.0.0.0 interface st0.1 dynamic-neighbors
set protocols ospf area 0.0.0.0 interface ge-0/0/4.0
set routing-options graceful-restart
set routing-options static route 11.1.1.0/24 next-hop 31.1.1.1
set routing-options static route 21.1.1.0/24 next-hop 31.1.1.1
set routing-options router-id 172.16.1.3
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group5
set security ike proposal IKE_PROP authentication-algorithm sha1
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate Partner2_Certificate_ID
set security ike gateway PARTNER_GW ike-policy IKE_POL
set security ike gateway PARTNER_GW address 11.1.1.1
set security ike gateway PARTNER_GW dead-peer-detection
set security ike gateway PARTNER_GW local-identity distinguished-name
set security ike gateway PARTNER_GW remote-identity distinguished-name container OU=Sales
set security ike gateway PARTNER_GW external-interface ge-0/0/2.0
set security ike gateway PARTNER_GW local-address 31.1.1.2
set security ike gateway PARTNER_GW advpn suggerter disable
set security ike gateway PARTNER_GW advpn partner
set security ike gateway PARTNER_GW version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
```

```

set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha1-96
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-cbc
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group5
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn PARTNER_VPN bind-interface st0.1
set security ipsec vpn PARTNER_VPN ike gateway PARTNER_GW
set security ipsec vpn PARTNER_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn PARTNER_VPN establish-tunnels immediately
set security pki ca-profile advpn ca-identity advpn
set security pki ca-profile advpn enrollment url http://10.157.92.176:8080/scep/advpn/
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/4.0
set security zones security-zone trust interfaces st0.1
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/2.0
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

??? 2? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/2 unit 0 family inet address 31.1.1.2/24
user@host# set ge-0/0/4 unit 0 family inet address 36.1.1.1/24
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 172.16.1.3/24

```

2. ??? ???? ? ? ? ? ? ?.

```

[edit protocols ospf]
user@host# set graceful-restart restart-duration 300
user@host# set graceful-restart notify-duration 300
user@host# set graceful-restart no-strict-lsa-checking
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 metric 15

```

```

user@host# set area 0.0.0.0 interface st0.1 retransmit-interval 1
user@host# set area 0.0.0.0 interface st0.1 dead-interval 40
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/4.0
[edit routing-options]
user@host# set graceful-restart
user@host# set static route 11.1.1.0/24 next-hop 31.1.1.1
user@host# set static route 21.1.1.0/24 next-hop 31.1.1.1
user@host# set router-id 172.16.1.3

```

### 3. 1?? ???? ?????.

```

[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy IKE_POL]
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate Partner2_Certificate_ID
[edit security ike gateway PARTNER_GW]
user@host# set ike-policy IKE_POL
user@host# set address 11.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=Sales
user@host# set external-interface ge-0/0/2.0
user@host# set local-address 31.1.1.2
user@host# set advpn suggester disable
user@host# set advpn partner
user@host# set version v2-only

```

### 4. 2?? ???? ?????.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals IPSEC_PROP

```





```

        unit 0 {
            family inet {
                address 31.1.1.2/24;
            }
        }
    }
}
ge-0/0/4{
    unit 0 {
        family inet {
            address 36.1.1.1/24;
        }
    }
}
st0 {
    unit 1 {
        multipoint;
        family inet {
            address 172.16.1.3/24;
        }
    }
}
[edit]
user@host# show protocols
ospf {
    graceful-restart {
        restart-duration 300;
        notify-duration 300;
        no-strict-lsa-checking;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            metric 15;
            retransmit-interval 1;
            dead-interval 40;
            demand-circuit;
            dynamic-neighbors;
        }
        interface ge-0/0/4.0;
    }
}
[edit]
user@host# show routing-options

```

```

graceful-restart;
static {
    route 11.1.1.0/24 next-hop 31.1.1.1;
    route 21.1.1.0/24 next-hop 31.1.1.1;
}
router-id 172.16.1.3;
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy IKE_POL {
    proposals IKE_PROP;
    certificate {
        local-certificate Partner2_Certificate_ID
    }
}
gateway PARTNER_GW {
    ike-policy IKE_POL;
    address 11.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=Sales;
    external-interface ge-0/0/2.0;
    local-address 31.1.1.2;
    advpn {
        suggester{
            disable;
        }
        partner {
        }
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}

```

```

policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals IPSEC_PROP;
}

vpn PARTNER_VPN {
    bind-interface st0.1;
    ike {
        gateway PARTNER_GW;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels immediately;
}

[edit]
user@host# show security pki
ca-profile advpn {
    ca-identity advpn;
    enrollment {
        url http://10.157.92.176:8080/scep/advpn/;
    }
}

[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/4.0;
        st0.1;
    }
}

security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
}

```

```
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/2.0;
    }
}
[edit]
user@host# show security policies
    default-policy {
        permit-all;
    }
```

commit ?(?)

??

in this section

?? ? | 994

?? ? | 1004

AutoVPN

?? ? ? ?

??

AutoVPN

??

show security ipsec security-associations

?? ???? ? ? ? ? ?.

```
user@host> show security ike security-associations
```

```
node1:
```

```
-----
Index   State Initiator cookie Responder cookie Mode           Remote Address
10957048 UP    2d58d8fbc396762d 46145be580c68be0 IKEv2          31.1.1.2
10957049 UP    fa05ee6d0f2cfb22 16f5ca836b118c0e IKEv2          21.1.1.2
```

```
user@host> show security ike security-associations detail
```

```
node1:
```

```
-----
IKE peer 31.1.1.2, Index 10957048, Gateway Name: SUGGESTER_GW
Auto Discovery VPN:
  Type: Static, Local Capability: Suggester, Peer Capability: Partner
  Suggester Shortcut Suggestions Statistics:
    Suggestions sent      :    0
    Suggestions accepted:    0
    Suggestions declined:    0
Role: Responder, State: UP
Initiator cookie: 2d58d8fbc396762d, Responder cookie: 46145be580c68be0
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 11.1.1.1:500, Remote: 31.1.1.2:500
Lifetime: Expires in 28196 seconds
Peer ike-id: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : aes256-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes  :      2030
  Output bytes :      2023
  Input packets:        4
  Output packets:       4
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1
```

```
Negotiation type: Quick mode, Role: Responder, Message ID: 0
```

```

Local: 11.1.1.1:500, Remote: 31.1.1.2:500
Local identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Remote identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Flags: IKE SA is created

```

IKE peer 21.1.1.2, Index 10957049, Gateway Name: SUGGESTER\_GW

Auto Discovery VPN:

Type: Static, Local Capability: Suggester, Peer Capability: Partner

Suggester Shortcut Suggestions Statistics:

Suggestions sent : 0

Suggestions accepted: 0

Suggestions declined: 0

Role: Responder, State: UP

Initiator cookie: fa05ee6d0f2cfb22, Responder cookie: 16f5ca836b118c0e

Exchange type: IKEv2, Authentication method: RSA-signatures

Local: 11.1.1.1:500, Remote: 21.1.1.2:500

Lifetime: Expires in 28219 seconds

Peer ike-id: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

Xauth user-name: not available

Xauth assigned IP: 0.0.0.0

Algorithms:

Authentication : hmac-sha1-96

Encryption : aes256-cbc

Pseudo random function: hmac-sha1

Diffie-Hellman group : DH-group-5

Traffic statistics:

Input bytes : 2030

Output bytes : 2023

Input packets: 4

Output packets: 4

IPSec security associations: 2 created, 0 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0

Local: 11.1.1.1:500, Remote: 21.1.1.2:500

Local identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US

Remote identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

Flags: IKE SA is created

```

user@host> show security ipsec security-associations
node1:

```

```

-----
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<201326593 ESP:aes-cbc-256/sha1 44ccf265 2999/ unlim - root 500 31.1.1.2
>201326593 ESP:aes-cbc-256/sha1 a9d301b0 2999/ unlim - root 500 31.1.1.2
<201326594 ESP:aes-cbc-256/sha1 98a2b155 3022/ unlim - root 500 21.1.1.2
>201326594 ESP:aes-cbc-256/sha1 de912bcd 3022/ unlim - root 500 21.1.1.2

```

```

user@host> show security ipsec security-associations detail

```

```

node1:

```

```

-----
ID: 201326593 Virtual-system: root, VPN Name: SUGGESTER_VPN
Local Gateway: 11.1.1.1, Remote Gateway: 31.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 2, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
Tunnel events:
  Tue Jan 13 2015 12:57:48 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Jan 13 2015 12:57:48 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Jan 13 2015 12:57:48 -0800: IKE SA negotiation successfully completed (1 times)
Direction: inbound, SPI: 44ccf265, AUX-SPI: 0
Hard lifetime: Expires in 2991 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2414 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: a9d301b0, AUX-SPI: 0
Hard lifetime: Expires in 2991 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2414 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64

ID: 201326594 Virtual-system: root, VPN Name: SUGGESTER_VPN
Local Gateway: 11.1.1.1, Remote Gateway: 21.1.1.2

```

```

Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 3, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
Tunnel events:
  Tue Jan 13 2015 12:58:11 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Jan 13 2015 12:58:11 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Jan 13 2015 12:58:11 -0800: IKE SA negotiation successfully completed (1 times)
Direction: inbound, SPI: 98a2b155, AUX-SPI: 0
  Hard lifetime: Expires in 3014 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2436 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: de912bcd, AUX-SPI: 0
  Hard lifetime: Expires in 3014 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2436 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64

```

```

user@host> show route protocol ospf
inet.0: 28 destinations, 28 routes (27 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

25.1.1.0/24      *[OSPF/10] 00:00:27, metric 11
                  > to 172.16.1.2 via st0.1
36.1.1.0/24      *[OSPF/10] 00:00:27, metric 11
                  > to 172.16.1.3 via st0.1
172.16.1.2/32    *[OSPF/10] 00:00:27, metric 10
                  > to 172.16.1.2 via st0.1
172.16.1.3/32    *[OSPF/10] 00:00:27, metric 10
                  > to 172.16.1.3 via st0.1

```



```
224.0.0.5/32      *[OSPF/10] 00:00:48, metric 1
                  MultiRecv
```

```
user@host> show ospf neighbor
```

| Address    | Interface | State | ID         | Pri | Dead |
|------------|-----------|-------|------------|-----|------|
| 172.16.1.3 | st0.1     | Full  | 172.16.1.3 | 128 | -    |
| 172.16.1.2 | st0.1     | Full  | 172.16.1.2 | 128 | -    |

```
?? 1? ?? ??? ?????.
```

```
user@host> show security ike security-associations
node0:
-----
Index   State Initiator cookie Responder cookie Mode      Remote Address
578872  UP     fa05ee6d0f2cfb22 16f5ca836b118c0e IKEv2     11.1.1.1
```

```
user@host> show security ike security-associations detail
node0:
-----
IKE peer 11.1.1.1, Index 578872, Gateway Name: PARTNER_GW
Auto Discovery VPN:
Type: Static, Local Capability: Partner, Peer Capability: Suggester
Partner Shortcut Suggestions Statistics:
  Suggestions received:    0
  Suggestions accepted:    0
  Suggestions declined:    0
Role: Initiator, State: UP
Initiator cookie: fa05ee6d0f2cfb22, Responder cookie: 16f5ca836b118c0e
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 21.1.1.2:500, Remote: 11.1.1.1:500
Lifetime: Expires in 28183 seconds
Peer ike-id: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : aes256-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-5
```

## Traffic statistics:

```

Input bytes :          2023
Output bytes :          2030
Input packets:          4
Output packets:         4

```

IPSec security associations: 2 created, 0 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 0

Local: 21.1.1.2:500, Remote: 11.1.1.1:500

Local identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

Remote identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US

Flags: IKE SA is created

```
user@host> show security ipsec security-associations
```

node0:

```

-----
Total active tunnels: 1
ID   Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<67108866 ESP:aes-cbc-256/sha1 de912bcd 2985/ unlim - root 500 11.1.1.1
>67108866 ESP:aes-cbc-256/sha1 98a2b155 2985/ unlim - root 500 11.1.1.1

```

```
user@host> show security ipsec security-associations detail
```

node0:

```

-----
ID: 67108866 Virtual-system: root, VPN Name: PARTNER_VPN
Local Gateway: 21.1.1.2, Remote Gateway: 11.1.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29
Tunnel events:
  Tue Jan 13 2015 12:58:11 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Jan 13 2015 12:58:11 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Jan 13 2015 12:58:11 -0800: IKE SA negotiation successfully completed (1 times)
Direction: inbound, SPI: de912bcd, AUX-SPI: 0
Hard lifetime: Expires in 2980 seconds

```

```

Lifetimes Remaining: Unlimited
Soft lifetime: Expires in 2358 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 98a2b155, AUX-SPI: 0
Hard lifetime: Expires in 2980 seconds
Lifetimes Remaining: Unlimited
Soft lifetime: Expires in 2358 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64

```

```

user@host> show route protocol ospf
inet.0: 29 destinations, 29 routes (28 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.1.1.0/24      *[OSPF/10] 00:11:46, metric 16
                  > to 172.16.1.1 via st0.1
36.1.1.0/24      *[OSPF/10] 00:11:46, metric 26
                  > to 172.16.1.1 via st0.1
172.16.1.1/32    *[OSPF/10] 00:11:46, metric 15
                  > to 172.16.1.1 via st0.1
172.16.1.3/32    *[OSPF/10] 00:11:46, metric 25
                  > to 172.16.1.1 via st0.1
224.0.0.5/32     *[OSPF/10] 00:16:52, metric 1
                  MultiRecv

```

```

user@host> show ospf neighbor

```

| Address    | Interface | State | ID         | Pri | Dead |
|------------|-----------|-------|------------|-----|------|
| 172.16.1.1 | st0.1     | Full  | 172.16.1.1 | 128 | -    |

?? 2? ?? ??? ?????.

```
user@host> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode  | Remote Address |
|---------|-------|------------------|------------------|-------|----------------|
| 2299162 | UP    | 2d58d8fbc396762d | 46145be580c68be0 | IKEv2 | 11.1.1.1       |

```
user@host> show security ike security-associations detail
```

IKE peer 11.1.1.1, Index 2299162, Gateway Name: PARTNER\_GW

Auto Discovery VPN:

Type: Static, Local Capability: Partner, Peer Capability: Suggester

Partner Shortcut Suggestions Statistics:

Suggestions received: 0

Suggestions accepted: 0

Suggestions declined: 0

Role: Initiator, State: UP

Initiator cookie: 2d58d8fbc396762d, Responder cookie: 46145be580c68be0

Exchange type: IKEv2, Authentication method: RSA-signatures

Local: 31.1.1.2:500, Remote: 11.1.1.1:500

Lifetime: Expires in 28135 seconds

Peer ike-id: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US

Xauth user-name: not available

Xauth assigned IP: 0.0.0.0

Algorithms:

Authentication : hmac-sha1-96

Encryption : aes256-cbc

Pseudo random function: hmac-sha1

Diffie-Hellman group : DH-group-5

Traffic statistics:

Input bytes : 2023

Output bytes : 2030

Input packets: 4

Output packets: 4

IPSec security associations: 2 created, 0 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 0

Local: 31.1.1.2:500, Remote: 11.1.1.1:500

Local identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

```
Remote identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Flags: IKE SA is created
```

```
user@host> show security ipsec security-associations
```

```
Total active tunnels: 1
```

```
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<67108866 ESP:aes-cbc-256/sha1 a9d301b0 2936/ unlim - root 500 11.1.1.1
>67108866 ESP:aes-cbc-256/sha1 44ccf265 2936/ unlim - root 500 11.1.1.1
```

```
user@host> show security ipsec security-associations detail
```

```
ID: 67108866 Virtual-system: root, VPN Name: PARTNER_VPN
```

```
Local Gateway: 31.1.1.2, Remote Gateway: 11.1.1.1
```

```
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
```

```
Version: IKEv2
```

```
DF-bit: clear, Bind-interface: st0.1
```

```
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29
```

```
Tunnel events:
```

```
Tue Jan 13 2015 12:57:48 -0800: IPSec SA negotiation successfully completed (1 times)
```

```
Tue Jan 13 2015 12:57:48 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
```

```
Tue Jan 13 2015 12:57:48 -0800: IKE SA negotiation successfully completed (1 times)
```

```
Direction: inbound, SPI: a9d301b0, AUX-SPI: 0
```

```
Hard lifetime: Expires in 2933 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2311 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 44ccf265, AUX-SPI: 0
```

```
Hard lifetime: Expires in 2933 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2311 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
user@host> show route protocol ospf
```

```
inet.0: 36 destinations, 36 routes (35 active, 0 holddown, 1 hidden)
```

| Address    | Interface | State | ID         | Pri | Dead |
|------------|-----------|-------|------------|-----|------|
| 172.16.1.1 | st0.1     | Full  | 172.16.1.1 | 128 | -    |

```
show security ike security-associations ???? ? ? IKE(Internet Key Exchange) 1?? SA? ??????. show security  
ipsec security-associations ???? ? ? IKE 2?? SA? ??????. ????? ? ????? ??? ? ?? ?? ??? ??????. ? ????? ???  
?? ? ? ??? ?????.
```

[illegible]

```

[?] show route protocol ospf OSPF [?] [?] [?] [?] [?] [?]. [?] show ospf neighbor OSPF [?] [?] [?] [?]
[?] [?] [?].

```

**???** **?** **????** **??** **??**

??

[illegible]

??

?? ???? ???? show security ike security-associations, show security ipsec security-associations, show route protocol ospf, ? show ospf neighbor ??? ?????.

??? ???? ???? ???? ????.

```
user@host> show security ike security-associations
node0:
-----
Index   State Initiator cookie Responder cookie Mode      Remote Address
10957048 UP    2d58d8fbc396762d 46145be580c68be0 IKEv2     31.1.1.2
10957049 UP    fa05ee6d0f2cfb22 16f5ca836b118c0e IKEv2     21.1.1.2
```

```
user@host> show security ike security-associations detail
node0:
-----
IKE peer 31.1.1.2, Index 10957048, Gateway Name: SUGGESTER_GW
Auto Discovery VPN:
  Type: Static, Local Capability: Suggester, Peer Capability: Partner
  Suggester Shortcut Suggestions Statistics:
    Suggestions sent      :    1
    Suggestions accepted:    1
    Suggestions declined:    0
  Role: Responder, State: UP
  Initiator cookie: 2d58d8fbc396762d, Responder cookie: 46145be580c68be0
  Exchange type: IKEv2, Authentication method: RSA-signatures
  Local: 11.1.1.1:500, Remote: 31.1.1.2:500
  Lifetime: Expires in 27781 seconds
  Peer ike-id: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
  Xauth user-name: not available
  Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication      : hmac-sha1-96
  Encryption          : aes256-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes  :          260
  Output bytes :          548
  Input packets:           3
```

Output packets: 3  
 IPsec security associations: 0 created, 0 deleted  
 Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0  
 Local: 11.1.1.1:500, Remote: 31.1.1.2:500  
 Local identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US  
 Remote identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US  
 Flags: IKE SA is created

IKE peer 21.1.1.2, Index 10957049, Gateway Name: SUGGESTER\_GW

Auto Discovery VPN:

Type: Static, Local Capability: Suggester, Peer Capability: Partner

Suggester Shortcut Suggestions Statistics:

Suggestions sent : 1  
 Suggestions accepted: 1  
 Suggestions declined: 0

Role: Responder, State: UP

Initiator cookie: fa05ee6d0f2cfb22, Responder cookie: 16f5ca836b118c0e

Exchange type: IKEv2, Authentication method: RSA-signatures

Local: 11.1.1.1:500, Remote: 21.1.1.2:500

Lifetime: Expires in 27804 seconds

Peer ike-id: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

Xauth user-name: not available

Xauth assigned IP: 0.0.0.0

Algorithms:

Authentication : hmac-sha1-96  
 Encryption : aes256-cbc  
 Pseudo random function: hmac-sha1  
 Diffie-Hellman group : DH-group-5

Traffic statistics:

Input bytes : 244  
 Output bytes : 548  
 Input packets: 3  
 Output packets: 3

IPsec security associations: 0 created, 0 deleted

Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0  
 Local: 11.1.1.1:500, Remote: 21.1.1.2:500  
 Local identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US



```
Remote identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Flags: IKE SA is created
```

```
user@host> show security ipsec security-associations
```

```
node0:
```

```
-----
s Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<201326593 ESP:aes-cbc-256/sha1 44ccf265 2584/ unlim - root 500 31.1.1.2
>201326593 ESP:aes-cbc-256/sha1 a9d301b0 2584/ unlim - root 500 31.1.1.2
<201326594 ESP:aes-cbc-256/sha1 98a2b155 2607/ unlim - root 500 21.1.1.2
>201326594 ESP:aes-cbc-256/sha1 de912bcd 2607/ unlim - root 500 21.1.1.2
```

```
user@host> show security ipsec security-associations detail
```

```
node0:
```

```
-----
ID: 201326593 Virtual-system: root, VPN Name: SUGGESTER_VPN
Local Gateway: 11.1.1.1, Remote Gateway: 31.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x608a29
Tunnel events:
  Tue Jan 13 2015 13:09:48 -0800: Bind-interface's address received. Information updated (1
times)
  Tue Jan 13 2015 13:09:48 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
Direction: inbound, SPI: 44ccf265, AUX-SPI: 0
  Hard lifetime: Expires in 2578 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2001 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: a9d301b0, AUX-SPI: 0
  Hard lifetime: Expires in 2578 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2001 seconds
```

```

Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64

```

```
ID: 201326594 Virtual-system: root, VPN Name: SUGGESTER_VPN
```

```

Local Gateway: 11.1.1.1, Remote Gateway: 21.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x608a29

```

```
Tunnel events:
```

```
Tue Jan 13 2015 13:09:48 -0800: Bind-interface's address received. Information updated (1 times)
```

```
Tue Jan 13 2015 13:09:48 -0800: Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)
```

```
Direction: inbound, SPI: 98a2b155, AUX-SPI: 0
```

```
Hard lifetime: Expires in 2601 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2023 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: de912bcd, AUX-SPI: 0
```

```
Hard lifetime: Expires in 2601 seconds
```

```
Lifesize Remaining: Unlimited
```

```
Soft lifetime: Expires in 2023 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
user@host> show route protocol ospf
```

```
inet.0: 28 destinations, 28 routes (27 active, 0 holddown, 1 hidden)
```

```
Restart Complete
```

```
+ = Active Route, - = Last Active, * = Both
```

```
25.1.1.0/24      *[OSPF/10] 00:04:49, metric 11
```

```
> to 172.16.1.2 via st0.1
```

```
36.1.1.0/24      *[OSPF/10] 00:04:49, metric 11
```

```
> to 172.16.1.3 via st0.1
```

```
172.16.1.2/32    *[OSPF/10] 00:04:49, metric 10
```

```

> to 172.16.1.2 via st0.1
172.16.1.3/32      *[OSPF/10] 00:04:49, metric 10
> to 172.16.1.3 via st0.1
224.0.0.5/32      *[OSPF/10] 00:05:10, metric 1
MultiRecv

```

```

user@host> show ospf neighbor

```

| Address    | Interface | State | ID         | Pri | Dead |
|------------|-----------|-------|------------|-----|------|
| 172.16.1.3 | st0.1     | Full  | 172.16.1.3 | 128 | -    |
| 172.16.1.2 | st0.1     | Full  | 172.16.1.2 | 128 | -    |

?? 1? ?? ??? ?????.

```

user@host> show security ike security-associations

```

| Index  | State | Initiator cookie | Responder cookie | Mode  | Remote Address |
|--------|-------|------------------|------------------|-------|----------------|
| 578872 | UP    | fa05ee6d0f2cfb22 | 16f5ca836b118c0e | IKEv2 | 11.1.1.1       |
| 578873 | UP    | 895e4d9c7c5da7a4 | 17de7f18b45139b4 | IKEv2 | 31.1.1.2       |

```

user@host> show security ike security-associations detail
node0:
-----
IKE peer 11.1.1.1, Index 578872, Gateway Name: PARTNER_GW
Auto Discovery VPN:
Type: Static, Local Capability: Partner, Peer Capability: Suggester
Partner Shortcut Suggestions Statistics:
Suggestions received: 1
Suggestions accepted: 1
Suggestions declined: 0
Role: Initiator, State: UP
Initiator cookie: fa05ee6d0f2cfb22, Responder cookie: 16f5ca836b118c0e
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 21.1.1.2:500, Remote: 11.1.1.1:500
Lifetime: Expires in 27906 seconds
Peer ike-id: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication : hmac-sha1-96
Encryption : aes256-cbc

```

```

Pseudo random function: hmac-sha1
Diffie-Hellman group   : DH-group-5
Traffic statistics:
Input bytes   :           2495
Output bytes  :           2274
Input packets :             6
Output packets:             7
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

```

```

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 21.1.1.2:500, Remote: 11.1.1.1:500
Local identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Remote identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Flags: IKE SA is created

```

```

IKE peer 31.1.1.2, Index 578873, Gateway Name: PARTNER_GW
Auto Discovery VPN:
Type: Shortcut, Local Capability: Partner, Peer Capability: Partner
Role: Initiator, State: UP
Initiator cookie: 895e4d9c7c5da7a4, Responder cookie: 17de7f18b45139b4
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 21.1.1.2:500, Remote: 31.1.1.2:500
Lifetime: Expires in 28787 seconds
Peer ike-id: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption           : aes256-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input bytes   :           1855
Output bytes  :           1990
Input packets :             2
Output packets:             2
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

```

```

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 21.1.1.2:500, Remote: 31.1.1.2:500
Local identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

```

Remote identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US  
 Flags: IKE SA is created

```
user@host> show security ipsec security-associations
```

```
node0:
```

```
-----
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<67108866 ESP:aes-cbc-256/sha1 de912bcd 2709/ unlim - root 500 11.1.1.1
>67108866 ESP:aes-cbc-256/sha1 98a2b155 2709/ unlim - root 500 11.1.1.1
<67108868 ESP:aes-cbc-256/sha1 75d0177b 3590/ unlim - root 500 31.1.1.2
>67108868 ESP:aes-cbc-256/sha1 e4919d73 3590/ unlim - root 500 31.1.1.2
```

```
user@host> show security ipsec security-associations detail
```

```
node0:
```

```
-----
ID: 67108866 Virtual-system: root, VPN Name: PARTNER_VPN
Local Gateway: 21.1.1.2, Remote Gateway: 11.1.1.1
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29
Tunnel events:
  Tue Jan 13 2015 12:58:11 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Jan 13 2015 12:58:11 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Jan 13 2015 12:58:11 -0800: IKE SA negotiation successfully completed (1 times)
Direction: inbound, SPI: de912bcd, AUX-SPI: 0
  Hard lifetime: Expires in 2701 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2079 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 98a2b155, AUX-SPI: 0
  Hard lifetime: Expires in 2701 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2079 seconds
```

```

Mode: Tunnel(0 0), Type: dynamic, State: installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
Anti-replay service: counter-based enabled, Replay window size: 64

```

```
ID: 67108868 Virtual-system: root, VPN Name: PARTNER_VPN
```

```

Local Gateway: 21.1.1.2, Remote Gateway: 31.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Auto Discovery VPN:

```

```
Type: Shortcut, Shortcut Role: Initiator
```

```
Version: IKEv2
```

```
DF-bit: clear, Bind-interface: st0.1
```

```
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x40608a29
```

```
Tunnel events:
```

```
Tue Jan 13 2015 13:12:52 -0800: IPsec SA negotiation successfully completed (1 times)
```

```

Tue Jan 13 2015 13:12:52 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)

```

```
Tue Jan 13 2015 13:12:52 -0800: IKE SA negotiation successfully completed (1 times)
```

```
Direction: inbound, SPI: 75d0177b, AUX-SPI: 0
```

```
Hard lifetime: Expires in 3582 seconds
```

```
Lifetime Remaining: Unlimited
```

```
Soft lifetime: Expires in 2959 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
Direction: outbound, SPI: e4919d73, AUX-SPI: 0
```

```
Hard lifetime: Expires in 3582 seconds
```

```
Lifetime Remaining: Unlimited
```

```
Soft lifetime: Expires in 2959 seconds
```

```
Mode: Tunnel(0 0), Type: dynamic, State: installed
```

```
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
```

```
Anti-replay service: counter-based enabled, Replay window size: 64
```

```
user@host> show route protocol ospf
```

```
inet.0: 29 destinations, 29 routes (28 active, 0 holddown, 1 hidden)
```

```
Restart Complete
```

```
+ = Active Route, - = Last Active, * = Both
```

```

10.1.1.0/24          *[OSPF/10] 00:03:29, metric 16
                    > to 172.16.1.1 via st0.1

```

```
36.1.1.0/24          *[OSPF/10] 00:00:35, metric 16
```

```

> to 172.16.1.3 via st0.1
172.16.1.1/32    *[OSPF/10] 00:03:29, metric 15
> to 172.16.1.1 via st0.1
172.16.1.3/32    *[OSPF/10] 00:00:35, metric 15
> to 172.16.1.3 via st0.1
224.0.0.5/32     *[OSPF/10] 00:20:22, metric 1
MultiRecv

```

```
user@host> show ospf neighbor
```

| Address    | Interface | State | ID         | Pri | Dead |
|------------|-----------|-------|------------|-----|------|
| 172.16.1.3 | st0.1     | Full  | 172.16.1.3 | 128 | -    |
| 172.16.1.1 | st0.1     | Full  | 172.16.1.1 | 128 |      |

```
?? 2? ?? ??? ?????.
```

```
user@host> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode  | Remote Address |
|---------|-------|------------------|------------------|-------|----------------|
| 2299162 | UP    | 2d58d8fbc396762d | 46145be580c68be0 | IKEv2 | 11.1.1.1       |
| 2299163 | UP    | 895e4d9c7c5da7a4 | 17de7f18b45139b4 | IKEv2 | 21.1.1.2       |

```
user@host> show security ike security-associations detail
```

```
IKE peer 11.1.1.1, Index 2299162, Gateway Name: PARTNER_GW
```

```
Auto Discovery VPN:
```

```
Type: Static, Local Capability: Partner, Peer Capability: Suggester
```

```
Partner Shortcut Suggestions Statistics:
```

```
Suggestions received: 1
```

```
Suggestions accepted: 1
```

```
Suggestions declined: 0
```

```
Role: Initiator, State: UP
```

```
Initiator cookie: 2d58d8fbc396762d, Responder cookie: 46145be580c68be0
```

```
Exchange type: IKEv2, Authentication method: RSA-signatures
```

```
Local: 31.1.1.2:500, Remote: 11.1.1.1:500
```

```
Lifetime: Expires in 27835 seconds
```

```
Peer ike-id: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
```

```
Xauth user-name: not available
```

```
Xauth assigned IP: 0.0.0.0
```

```
Algorithms:
```

```
Authentication : hmac-sha1-96
```

```
Encryption : aes256-cbc
```

```

Pseudo random function: hmac-sha1
Diffie-Hellman group   : DH-group-5
Traffic statistics:
Input  bytes   :           2571
Output bytes   :           2290
Input  packets :             7
Output packets :             7
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local: 31.1.1.2:500, Remote: 11.1.1.1:500
Local identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Remote identity: DC=XYZ, CN=suggester, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
Flags: IKE SA is created

```

```

IKE peer 21.1.1.2, Index 2299163, Gateway Name: PARTNER_GW
Auto Discovery VPN:
Type: Shortcut, Local Capability: Partner, Peer Capability: Partner
Role: Responder, State: UP
Initiator cookie: 895e4d9c7c5da7a4, Responder cookie: 17de7f18b45139b4
Exchange type: IKEv2, Authentication method: RSA-signatures
Local: 31.1.1.2:500, Remote: 21.1.1.2:500
Lifetime: Expires in 28739 seconds
Peer ike-id: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US
Xauth user-name: not available
Xauth assigned IP: 0.0.0.0
Algorithms:
Authentication      : hmac-sha1-96
Encryption          : aes256-cbc
Pseudo random function: hmac-sha1
Diffie-Hellman group : DH-group-5
Traffic statistics:
Input  bytes   :           2066
Output bytes   :           1931
Input  packets :             3
Output packets :             3
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 31.1.1.2:500, Remote: 21.1.1.2:500
Local identity: DC=XYZ, CN=partner2, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US

```



Remote identity: DC=XYZ, CN=partner1, OU=Sales, O=XYZ, L=NewYork, ST=NY, C=US  
 Flags: IKE SA is created

```
user@host> show security ipsec security-associations
```

Total active tunnels: 2

| ID        | Algorithm            | SPI      | Life:sec/kb | Mon   | lsys | Port     | Gateway  |
|-----------|----------------------|----------|-------------|-------|------|----------|----------|
| <67108866 | ESP:aes-cbc-256/sha1 | a9d301b0 | 2638/       | unlim | -    | root 500 | 11.1.1.1 |
| >67108866 | ESP:aes-cbc-256/sha1 | 44ccf265 | 2638/       | unlim | -    | root 500 | 11.1.1.1 |
| <67108868 | ESP:aes-cbc-256/sha1 | e4919d73 | 3542/       | unlim | -    | root 500 | 21.1.1.2 |
| >67108868 | ESP:aes-cbc-256/sha1 | 75d0177b | 3542/       | unlim | -    | root 500 | 21.1.1.2 |

```
user@host> show security ipsec security-associations detail
```

ID: 67108866 Virtual-system: root, VPN Name: PARTNER\_VPN

Local Gateway: 31.1.1.2, Remote Gateway: 11.1.1.1

Local Identity: ipv4\_subnet(any:0,[0..7]=0.0.0.0/0)

Remote Identity: ipv4\_subnet(any:0,[0..7]=0.0.0.0/0)

Version: IKEv2

DF-bit: clear, Bind-interface: st0.1

Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x8608a29

Tunnel events:

Tue Jan 13 2015 12:57:48 -0800: IPSec SA negotiation successfully completed (1 times)

Tue Jan 13 2015 12:57:48 -0800: Tunnel is ready. Waiting for trigger event or peer to trigger negotiation (1 times)

Tue Jan 13 2015 12:57:48 -0800: IKE SA negotiation successfully completed (1 times)

Direction: inbound, SPI: a9d301b0, AUX-SPI: 0

Hard lifetime: Expires in 2632 seconds

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 2010 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: 44ccf265, AUX-SPI: 0

Hard lifetime: Expires in 2632 seconds

Lifetime Remaining: Unlimited

Soft lifetime: Expires in 2010 seconds

Mode: Tunnel(0 0), Type: dynamic, State: installed

Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)

Anti-replay service: counter-based enabled, Replay window size: 64

ID: 67108868 Virtual-system: root, VPN Name: PARTNER\_VPN

```

Local Gateway: 31.1.1.2, Remote Gateway: 21.1.1.2
Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Auto Discovery VPN:
  Type: Shortcut, Shortcut Role: Responder
Version: IKEv2
DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 0x40608aa9
Tunnel events:
  Tue Jan 13 2015 13:12:52 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Jan 13 2015 13:12:52 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Jan 13 2015 13:12:52 -0800: IKE SA negotiation successfully completed (1 times)
Direction: inbound, SPI: e4919d73, AUX-SPI: 0
  Hard lifetime: Expires in 3536 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2958 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 75d0177b, AUX-SPI: 0
  Hard lifetime: Expires in 3536 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2958 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (256 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64

```

```

user@host> show route protocol ospf
inet.0: 36 destinations, 36 routes (35 active, 0 holddown, 1 hidden)
Restart Complete
+ = Active Route, - = Last Active, * = Both

10.1.1.0/24      *[OSPF/10] 00:03:55, metric 16
                 > to 172.16.1.1 via st0.1
25.1.1.0/24      *[OSPF/10] 00:01:02, metric 16
                 > to 172.16.1.2 via st0.1
172.16.1.1/32    *[OSPF/10] 00:03:55, metric 15
                 > to 172.16.1.1 via st0.1
172.16.1.2/32    *[OSPF/10] 00:01:02, metric 15
                 > to 172.16.1.2 via st0.1

```



?? ??

? ??? ????? ????? ? ?????? ?? ??? ??? ?????.

- ADVPN ?? ? ????? ????? SRX ??? ??? 3?
- ????? kmd ?????? ????? ?? Junos OS ??? 18.1R1 ?? ???.
- ????? iked ?????? ????? ?? Junos OS ??? 24.2R1 ?? ???.

???? ??:

- ?? ????? ?? ??? ??? ? ?? ??(CA)? ??? ??? ?(?; ?? ?? ??)? ?????.

VPN ??? ?? ??? ????? ? ????? ?? ??? ?????? ?? ? ?? ??? ???.

??

in this section

| 1020

? ????? ADVPN ??? ??? ? ?? ????? ?? ?? ??? ?? ???.

? ????? ? ?? ??? SCEP(?? ??? ?? ?????)? ????? ? ?????? ??? ?????? ?????. ????? ?????? ?? ??? OU(?? ?? ??) ? "SLT"? ????? ?????, ??? OU ??? ? "SLT"? ????? ?? IKE ID? ?????.

???? ?? ? IPsec VPN ??? ????? ?? ??? ? ?? ?? ??? ??? ?????? ????? ? ????. ADVPN ??? ?? ????? ??? 1? ? ? 2?? IKE ?? ??? ??? ?? ??? ???. ? 118 ??? 1018 ?(?) ? ??? ??? ??? ?????.

? 118: ADPN ?? ? ??? ?? OSPFv3 ??? ?? 1?? ? 2?? ??

|                                |            |
|--------------------------------|------------|
| ??                             | ??         |
| IKE(Internet Key Exchange) ??: |            |
| ?? ??                          | RSA ??? ?? |
| DH(Diffie-Hellman) ??          | 19         |

118: ADPN 2 2 2 2 OSPFv3 2 2 1 2 2 2 2 (Continued)

|         |             |
|---------|-------------|
| 2       | 2           |
| 2 2 2 2 | SHA-384     |
| 2 2 2 2 | AES 256 CBC |

IKE(Internet Key Exchange) 2:

|   |     |
|---|-----|
| 2 | 2 2 |
|---|-----|

IPsec 2:

|               |             |
|---------------|-------------|
| 2 2 2         | ESP         |
| 2 2 2 2 2 (2) | 3000        |
| 2 2 2 2 2 2   | AES 256 GCM |

IPsec 2:

|                                |    |
|--------------------------------|----|
| PFS(Perfect Forward Secrecy) 2 | 19 |
|--------------------------------|----|

2 2 2 2 2 2 2 2 2 (CA) 2 2 2 2.

119 2 2 1019 2 2 2 2 2 2 2 2 2 2 2 2.

119: 2 2 2 2 2 2 ADVPN OSPFv3 2

|   |   |       |
|---|---|-------|
| 2 | 2 | 2 2 2 |
|---|---|-------|

IKE(Internet Key Exchange) 2 2 2 2:

|        |   |                  |
|--------|---|------------------|
| 2 IP 2 | 2 | 2001:db8:2000::1 |
|--------|---|------------------|

**119: 119 1 119 1191 119 ADVPN OSPFv3 119 (Continued)**

| 119                               | 119                                                           | 119 1191                                 |
|-----------------------------------|---------------------------------------------------------------|------------------------------------------|
| 119 IKE(Internet Key Exchange) ID | OU(119 119 119) 1191 1191 SLT 1 119 1191 119 1191 DN(119 119) | 119 11911 DNDN on the hub's certificate  |
| 119 IKE(Internet Key Exchange) ID | 119 11911 DNDN on the hub's certificate                       | 1191 11911 DN                            |
| 119 1191111                       | 1191                                                          | 1191 1: ge-0/0/0.0<br>1191 2: ge-0/0/0.0 |
| VPN:                              |                                                               |                                          |
| 1191 1191111                      | st0.1                                                         | st0.1                                    |
| 119 119                           | (11911 119)                                                   | 119 establish-tunnels                    |

119 1191 1020 1(1) 1 1191111 119 119 1191 1191111.

**120: OSPFv3 1191 119 1 119**

| 119               | 1191 1                           | 1191 2                           |
|-------------------|----------------------------------|----------------------------------|
| st0.1 1191111     | 2001:db8:9000::2/64              | 2001:db8:9000::3/64              |
| 119 11911 1191111 | (ge-0/0/1.0) 2001:db8:4000::1/64 | (ge-0/0/1.0) 2001:db8:6000::1/64 |
| 1191 1191111      | (ge-0/0/0.0) 2001:db8:3000::2/64 | (ge-0/0/0.0) 2001:db8:5000::2/64 |

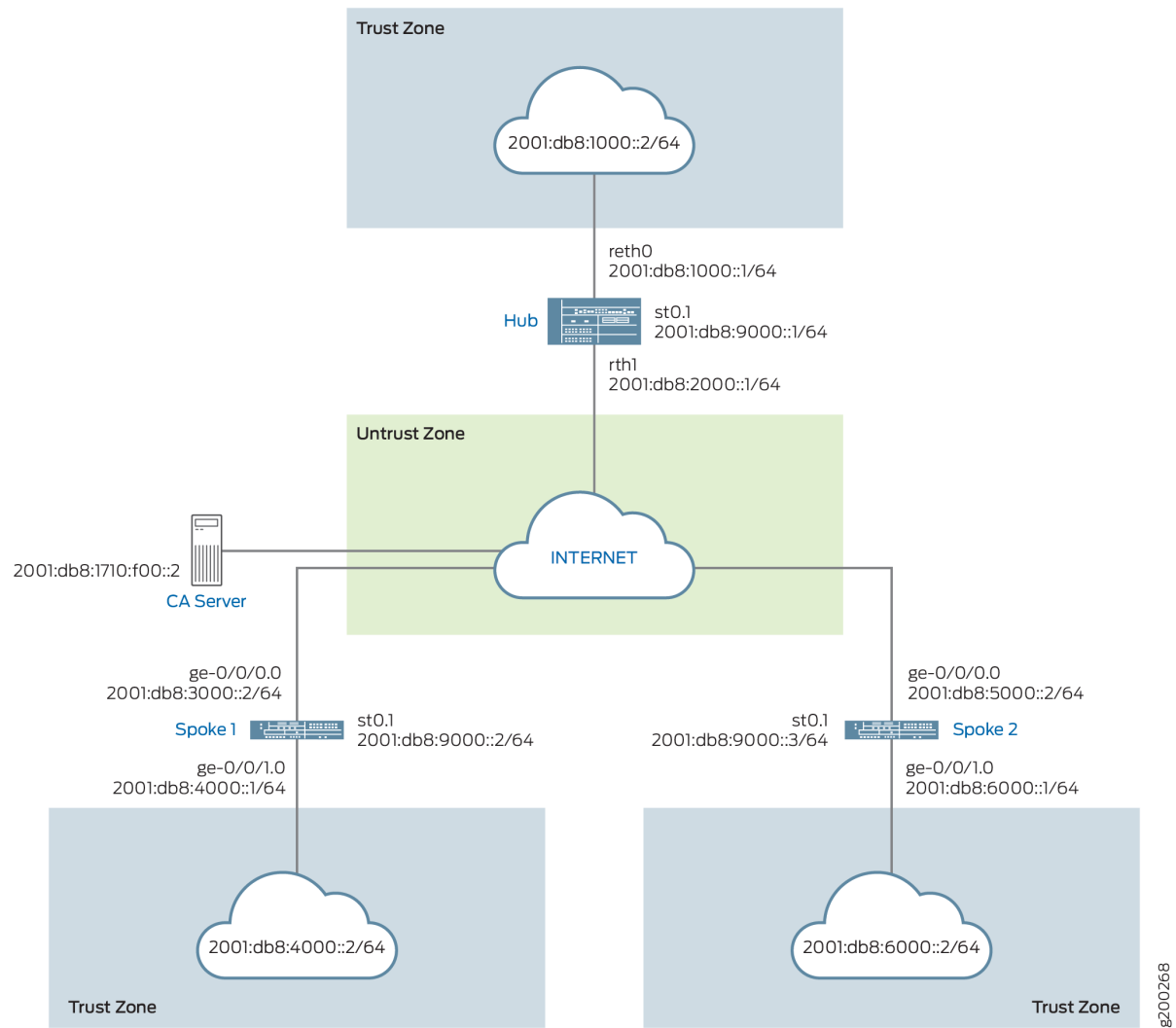
119 1191111 119 1191 1191 VPN 1191 119 1191111.

1 1191111 119 1191111 1191111 119 119 1191 119 1191111 1191111. 119 11911 119 119 1 1191111 119 11911 1191111 11911. 119 119 11911 1191111111.

1191111

119 61 1191 1021 119 1 11911 ADVPN 119 11911 SRX 11911 1191111 119 1191111.

61: OSPFv3 ADVPN



??

in this section

- SCEP? ???? ?? ???? ??Enroll Device Certificates with SCEP | 1022
- ?? ?? | 1027
- ???? ?? 1 | 1036
- ???? 2 ?? | 1043





5. `?? ???? ?????`.

```

user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2012 09:39
  Not after: 11- 6-2013 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
  6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

`??? ??``??? 1?? SCEP? ???? ???? ???? ?????:`

1. CA `ca1`.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

2. CA `ca1` `ca1`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
ca1 ca1 yes CA ca1 ca1.
```

3. `ca1` `ca1`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `ca1` `ca1` `ca1`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
```

5. `ca1` `ca1` `ca1`.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
```

???

1. CA? ?????.

2. CA [ ][ ][ ][ ] [ ][ ][ ][ ].

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

????? ???? yes CA ???? ????.

3. ? ??? ????.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. ?? ???? ????.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke2@example.net ip-address 10.3.3.1 subject
DC=example.net,CN=spoke2,OU=SLT,O=example,L=Tumkur,ST=KA,C=IN challenge-password <password>
```

5. ?? ???? ????.

```
user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40bb71d400000000258f
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Tumkur, Common name: spoke2, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
Alternate subject: "spoke2@example.net", example.net, 10.3.3.1
Validity:
  Not before: 11- 6-2012 10:02
  Not after: 11- 6-2013 10:12
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:b6:2e:e2:da:e6:ac:57:e4:5d:ff:de:f6:89
  27:d6:3e:1b:4a:3f:b2:2d:b3:d3:61:ed:ed:6a:07:d9:8a:d2:24:03
  77:1a:fe:84:e1:12:8a:2d:63:6e:bf:02:6b:15:96:5a:4f:37:a0:46
  44:09:96:c0:fd:bb:ab:79:2c:5d:92:bd:31:f0:3b:29:51:ce:89:8e
  7c:2b:02:d0:14:5b:0a:a9:02:93:21:ea:f9:fc:4a:e7:08:bc:b1:6d
  7c:f8:3e:53:58:8e:f1:86:13:fe:78:b5:df:0b:8e:53:00:4a:46:11
  58:4a:38:e9:82:43:d8:25:47:7d:ef:18:f0:ef:a7:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
```

```

http://ca-server1/CertEnroll/CASERVER1.crl
file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  1a:6d:77:ac:fd:94:68:ce:cf:8a:85:f0:39:fc:e0:6b:fd:fe:b8:66 (sha1)
  00:b1:32:5f:7b:24:9c:e5:02:e6:72:75:9e:a5:f4:77 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

?? ???? ???? OU(?? ?? ??) SLT???. ??? IKE(Internet Key Exchange) ???? ???? ???? ???? ???? ???? ???? ou=SLT .

?? ??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
 ? ???? ???? CLI ? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```

set chassis cluster reth-count 2
set chassis cluster node 0
set chassis cluster node 1
set chassis cluster redundancy-group 0 node 0 priority 254
set chassis cluster redundancy-group 0 node 1 priority 1
set chassis cluster redundancy-group 1 node 0 priority 254
set chassis cluster redundancy-group 1 node 1 priority 1
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate HUB
set security ike gateway IKE_GWA_1 ike-policy IKE_POL
set security ike gateway IKE_GWA_1 dynamic distinguished-name wildcard OU=SLT
set security ike gateway IKE_GWA_1 dynamic ike-user-type group-ike-id

```

```

set security ike gateway IKE_GWA_1 dead-peer-detection always-send
set security ike gateway IKE_GWA_1 dead-peer-detection interval 10
set security ike gateway IKE_GWA_1 dead-peer-detection threshold 3
set security ike gateway IKE_GWA_1 local-identity distinguished-name
set security ike gateway IKE_GWA_1 external-interface reth1
set security ike gateway IKE_GWA_1 advpn partner disable
set security ike gateway IKE_GWA_1 version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPNA_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPNA_1 ike gateway IKE_GWA_1
set security ipsec vpn IPSEC_VPNA_1 ike ipsec-policy IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces reth1.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces reth0.0
set interfaces ge-0/0/0 gigether-options redundant-parent reth1
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
set interfaces ge-7/0/0 gigether-options redundant-parent reth1
set interfaces ge-7/0/1 gigether-options redundant-parent reth0
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet
set interfaces reth0 unit 0 family inet6 address 2001:db8:1000::1/64
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet
set interfaces reth1 unit 0 family inet6 address 2001:db8:2000::1/64
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet6 address 2001:db8:9000::1/64
set routing-options rib inet6.0 static route 2001:db8:3000::0/64 next-hop 2001:db8:2000::2
set routing-options rib inet6.0 static route 2001:db8:5000::0/64 next-hop 2001:db8:2000::2
set protocols ospf3 area 0.0.0.0 interface reth0.0
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? ???? ???? ????.

### 1. ???? ????.

```
[edit interfaces]
user@host# set ge-0/0/0 gigether-options redundant-parent reth1
user@host# set ge-0/0/1 gigether-options redundant-parent reth0
user@host# set ge-7/0/0 gigether-options redundant-parent reth1
user@host# set ge-7/0/1 gigether-options redundant-parent reth0
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet
user@host# set reth0 unit 0 family inet6 address 2001:db8:1000::1/64
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet
user@host# set reth1 unit 0 family inet6 address 2001:db8:2000::1/64
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet6 address 2001:db8:9000::1/64
```

### 2. ??? ???? ????.

```
[edit protocols ospf3]
user@host# set ospf3 area 0.0.0.0 interface reth0.0
user@host# set ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:3000::0/64 next-hop 2001:db8:2000::2
user@host# set rib inet6.0 static route 2001:db8:5000::0/64 next-hop 2001:db8:2000::2
```

### 3. 1?? ??? ????.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
```

```

user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate HUB
[edit security ike gateway IKE_GWA_1]
user@host# set ike-policy IKE_POL
user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set ike-user-type group-ike-id
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set external-interface reth1
user@host# set version v2-only

```

#### 4. `set ipsec proposal`.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPNA_1]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GWA_1
user@host# set ike ipsec-policy IPSEC_POL

```

#### 5. `set host-inbound-traffic`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces reth1.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces reth0.0

```





```

}
ge-0/0/1 {
    gigether-options {
        redundant-parent reth0;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet;
        family inet6 {
            address 2001:db8:1000::1/64;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet;
        family inet6 {
            address 2001:db8:2000::1/64;
        }
    }
}
st0 {
    unit 1 {
        multipoint;
        family inet6 {
            address 2001:db8:9000::1/64 {
                primary;
            }
        }
    }
}
[edit]
user@host# show protocols
ospf3 {
    area 0.0.0.0 {
        interface st0.1 {

```

```

        interface-type p2mp;
        demand-circuit;
        dynamic-neighbors;
    }
    interface ge-0/0/1.0;
    interface reth0.0;
}
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 2001:db8:3000::/64 next-hop 2001:db8:2000::2;
        route 2001:db8:5000::/64 next-hop 2001:db8:2000::2;
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate HUB;
    }
}
gateway IKE_GWA_1 {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
        ike-user-type group-ike-id;
    }
    dead-peer-detection {
        always-send;
        interval 10;
    }
}

```

```

        threshold 3;
    }
    local-identity distinguished-name;
    external-interface reth1;
    advpn {
        partner {
            disable;
        }
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPNA_1 {
    bind-interface st0.1;
    ike {
        gateway IKE_GWA_1;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
}
interfaces {

```

```

        st0.1;
        reth1.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        reth0.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

```

commit?()

```

?? ? 1

CLI    

```
? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? ? CLI? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? ?.
```

```

set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE1
set security ike gateway IKE_GW_SPOKE_1 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_1 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_1 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_1 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_1 external-interface ge-0/0/0.0
set security ike gateway IKE_GW_SPOKE_1 advpn suggerter disable
set security ike gateway IKE_GW_SPOKE_1 version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike gateway IKE_GW_SPOKE_1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_1 establish-tunnels immediately
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all

```

```

set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet6 address 2001:db8:9000::2/64
set routing-options rib inet6.0 static route 2001:db8:2000::0/64 next-hop 2001:db8:3000::1
set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ? ???? CLI ??? ? ????.

??? 1? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet6 address 2001:db8:9000::2/64

```

2. ??? ???? ????.

```

[edit protocols ospf3]
set area 0.0.0.0 interface ge-0/0/1.0
set area 0.0.0.0 interface st0.1 interface-type p2mp
set area 0.0.0.0 interface st0.1 dynamic-neighbors
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:3000::1

```

## 3. 1?? ???? ?????.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE1
[edit security ike gateway IKE_GW_SPOKE_1]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0.0
user@host# set advpn suggerter disable
user@host# set version v2-only
```

## 4. 2?? ???? ?????.

```
[edit security ipsec proposal IPSEC_PROPI]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPN_SPOKE_1]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GW_SPOKE_1
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels immediately
```



5. `?? ????.`

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/0.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0
```

6. `?? ?? ??? ????.`

```
[edit security policies]
user@host# set default-policy permit-all
```

7. CA `???? ????.`

```
[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable
```

`??`

`?? ???? , show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show security policies? show security pki ??? ???? show interfaces??? ?????. ??? ??? ???? ???? ???? , ? ?? ? ???? ? ???? ????.`

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet6 {
```

```

        address 2001:db8:3000::2/64;
    }
}
ge-0/0/1 {
    unit 0 {
        family inet6 {
            address 2001:db8:4000::1/64;
        }
    }
}
st0 {
    unit 1 {
        multipoint;
        family inet6 {
            address 2001:db8:9000::2/64;
        }
    }
}
[edit]
user@host# show protocols
ospf3 {
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            dynamic-neighbors;
        }
        interface ge-0/0/1.0;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 2001:db8:2000::/64 next-hop [ 2001:db8:3000::1 2001:db8:5000::1 ];
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;

```

```

    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE1;
    }
}
gateway IKE_GW_SPOKE_1 {
    ike-policy IKE_POL;
    address 2001:db8:2000::1;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=SLT;
    external-interface ge-0/0/0.0;
    advpn {
        suggester {
            disable;
        }
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPN_SPOKE_1 {
    bind-interface st0.1;

```

```

ike {
    gateway IKE_GW_SPOKE_1;
    ipsec-policy IPSEC_POL;
}
establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {

```

???

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ?????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE2
set security ike gateway IKE_GW_SPOKE_2 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_2 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_2 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_2 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_2 external-interface ge-0/0/0.0
```

```

set security ike gateway IKE_GW_SPOKE_2 advpn suggerter disable
set security ike gateway IKE_GW_SPOKE_2 version v2-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_2 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike gateway IKE_GW_SPOKE_2
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_2 establish-tunnels immediately
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/1.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
set interfaces st0 unit 1 family inet6 address 2001:db8:9000::3/64
set routing-options rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ???? ?? ???? CLI ??? ???? ??????.

??? 2? ??????.

1. ?????? ??????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
user@host# set st0 unit 1 family inet6 address 2001:db8:9000::3/64

```

2. `?? ???? ????.`

```
[edit protocols ospf3]
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/1.0
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
```

3. `1?? ??? ?????.`

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE2
[edit security ike gateway IKE_GW_SPOKE_2]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0.0
user@host# set advpn suggester disable
user@host# set version v2-only
```

4. `2?? ??? ?????.`

```
[edit security ipsec proposal IPSEC_PROPI]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
```

```

user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPN_SPOKE_2]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GW_SPOKE_2
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels immediately

```

5. `???` `??????`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/0.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0

```

6. `??` `??` `???` `??????`.

```

[edit security policies]
user@host# set default-policy permit-all

```

7. CA `????` `??????`.

```

[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable

```



??

?? ???? , show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show security policies? show security pki ??? ???? show interfaces??? ?????. ??? ???? ???? ???? ???? , ? ?? ???? ? ???? ?????.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet6 {
      address 2001:db8:5000::2/64;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:6000::1/64;
    }
  }
}
st0 {
  unit 1 {
    family inet6 {
      address 2001:db8:9000::3/64;
    }
  }
}
[edit]
user@host# show protocols
ospf3 {
  area 0.0.0.0 {
    interface st0.1 {
      interface-type p2mp;
      dynamic-neighbors;
    }
    interface ge-0/0/1.0;
  }
}
[edit]
user@host# show routing-options
```

```

rib inet6.0 {
    static {
        route 2001:db8:2000::/64 next-hop [ 2001:db8:3000::1 2001:db8:5000::1 ];
    }
}
[edit]
user@host# show security ike
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE2;
    }
}
gateway IKE_GW_SPOKE_2 {
    ike-policy IKE_POL;
    address 2001:db8:2000::1;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=SLT;
    external-interface ge-0/0/0.0;
    advpn {
        suggester {
            disable
        }
    }
    version v2-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;

```

```

    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPN_SPOKE_2 {
    bind-interface st0.1;
    ike {
        gateway IKE_GW_SPOKE_2;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {

```

```

        ge-0/0/1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

commit( ) .

??

#### in this section

- [IKE\(Internet Key Exchange\) ?? | 1051](#)
- [IPsec ?? | 1051](#)
- [IPsec ? ? ? ? | 1052](#)
- [OSPFv3 ?? | 1052](#)

?? ???? ???? ????.

## IKE(Internet Key Exchange) ?? ??

??

IKE ??? ?????.

??

?? ????? show security ike sa ??? ?????.

```
user@host> show security ike sa
```

| Index   | State | Initiator cookie          | Responder cookie          | Mode | Remote Address   |
|---------|-------|---------------------------|---------------------------|------|------------------|
| 4295070 | UP    | 2001:db8:1ad4ba7a115fa229 | 2001:db8:32e6382a058bb296 | Main | 2001:db8:3000::2 |
| 295069  | UP    | 2001:db8:88a1520c20cbbe04 | 2001:db8:7fa4c8e365393c48 | Main | 2001:db8:5000::2 |

??

show security ike sa ??? ?? ?? IKE(Internet Key Exchange) 1?? SA? ?????. SA? ????? ?? ?? ??, 1?? ??? ??  
 ? ?? ?????, ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ??????. 1?? ?? ?? ??? ?????? ??  
 ?? ???.

## IPsec ?? ??

??

IPsec ??? ?????.

??

?? ????? show security ipsec sa ??? ?????.

```
user@host> show security ipsec sa
```

Total active tunnels: 2      Total Ipsec sas: 2

| ID        | Algorithm            | SPI      | Life:sec/kb | Mon   | lsys | Port     | Gateway          |
|-----------|----------------------|----------|-------------|-------|------|----------|------------------|
| <67108881 | ESP:aes-gcm-256/None | 3dba3f80 | 2979/       | unlim | -    | root 500 | 2001:db8:5000::2 |
| >67108881 | ESP:aes-gcm-256/None | 46746d5d | 2979/       | unlim | -    | root 500 | 2001:db8:5000::2 |

```
<67108882 ESP:aes-gcm-256/None 16dceb60 2992/ unlim - root 500 2001:db8:3000::2
>67108882 ESP:aes-gcm-256/None 681209c2 2992/ unlim - root 500 2001:db8:3000::2
```

??

show security ipsec sa [redacted] IKE [redacted] SA [redacted]. SA [redacted] [redacted] [redacted], [redacted] [redacted] [redacted] [redacted]. [redacted]  
IKE(Internet Key Exchange) [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

## IPsec ☐ ☐ ☐ ☐ ☐

??

IPsec [?] ? [??] [????].

??

```
?? ???? show security ipsec next-hop-tunnels ??? ?????.
```

```

user@host> show security ipsec next-hop-tunnels

Next-hop gateway          interface  IPSec VPN name Flag IKE-ID
XAUTH username
2001:db8:9000::2          st0.1     IPSEC_VPNA_1   Auto C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available
2001:db8:9000::3          st0.1     IPSEC_VPNA_1   Auto C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
2001:db8::5668:ad10:fcd8:10c8 st0.1     IPSEC_VPNA_1   Auto C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
2001:db8::5668:ad10:fcd8:112f st0.1     IPSEC_VPNA_1   Auto C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available

```

??

```

[?] ? [??????] [??] [??????] IP [?] st0 [???]. next hop? [??] IPSec VPN [??] [?????] [???].

```

## OSPFv3

??

OSPFv3? ??? ????? IP ??? st0 ????? ????

??

?? ???? show ospf3 neighbor interface ??? ?????.

```
user@host> show ospf3 neighbor interface
ID                               Interface           State  Pri  Dead
2001:db8:9000:2   st0.1               Full   128  -
Neighbor-address 2001:db8::5668:ad10:fcd8:110e

2001:db8:20:54:49.693          INFO    ${ret} = ID      Interface  State Pri Dead
2001:db8:9000:3   st0.1               Full   128  -
Neighbor-address 2001:db8::5668:ad10:fcd8:110e
```

SEE ALSO

| [?: ?? ?? VPN ??](#) | 453

ADVPN ?? ?? ??? ??? ? OSPF? ??? ??? ? ???? ? ???? ??

in this section

● [??](#) | 1053

● [???](#) | 1054

??

??

OSPF? ??? ?????? ?? ?? ??? ???????? ? ?? 9?? ?? ? ?????, ????? ?? ?? ??? ???????? ?? 10?? ?? ? ?????.





Feature Explorer

| release heading in release-history | desc heading in release-history                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 24.2R1                             | iked <a href="#">?????</a> <a href="#">????</a> <a href="#">?????</a> <a href="#">??</a> ADVPN? <a href="#">?????</a> IPv6 <a href="#">???</a> <a href="#">??</a> <a href="#">???</a> Junos OS <a href="#">???</a> 24.2R1? <a href="#">?????????</a> .                               |
| 24.2R1                             | iked <a href="#">??????</a> <a href="#">?????</a> <a href="#">?????</a> <a href="#">??</a> ADVPN? <a href="#">??</a> <a href="#">??????</a> <a href="#">????(IPv4 ??)?</a> <a href="#">??</a> <a href="#">???</a> Junos OS <a href="#">???</a> 24.2R1? <a href="#">?????????</a> .   |
| 23.4R1                             | iked <a href="#">??????</a> <a href="#">?????</a> <a href="#">?????</a> <a href="#">??</a> ADVPN? <a href="#">??</a> <a href="#">????</a> Junos OS <a href="#">???</a> 23.4R1? <a href="#">?????????</a> .                                                                           |
| 19.2R1                             | Junos OS <a href="#">???</a> 19.2R1 <a href="#">??</a> P2MP <a href="#">???</a> <a href="#">?????</a> PIM ? kmd <a href="#">???????????</a> IPsec VPN? PIM ? <a href="#">???</a> p2mp <a href="#">??????</a> <a href="#">???</a> <a href="#">???</a> ADVPN? <a href="#">??????</a> . |
| 18.1R1                             | Junos OS <a href="#">???</a> 18.1R1?? ADVPN? kmd <a href="#">??????</a> <a href="#">??</a> IPv6? <a href="#">??????</a> .                                                                                                                                                            |

?? ??

## IPv6 IPsec VPN

# 10

CHAPTER LABEL COVER PAGE

## AutoVPN

---

### in this chapter

- [?? ? ???? ?????? AutoVPN | 1057](#)
-

# ?? ? ??? ???? AutoVPN

## summary

AutoVPN? ?? ???? SRX ??? ???? AutoVPN? ???? ?  
?? ?? ????.

## in this section

- [AutoVPN ?? | 1058](#)
- [AutoVPN ??? ??? ?? ?? | 1063](#)
- [AutoVPN ?? ?? | 1066](#)
- [?: iBGP? ??? ?? AutoVPN ?? | 1067](#)
- [?: IPv6 ???? ?? iBGP? ???? ?? AutoVPN ?  
? | 1103](#)
- [?: iBGP ? ECMP? ??? AutoVPN ?? | 1140](#)
- [?: iBGP ? Active-Backup ??? ??? AutoVPN ?  
? | 1172](#)
- [?: OSPF? ??? ?? AutoVPN ?? | 1208](#)
- [?: IPv6 ???? ?? OSPFv3? ???? AutoVPN ?  
? | 1241](#)
- [?: ??? ???? ???? AutoVPN ??? ?? ??? ?  
? | 1277](#)
- [?: AutoVPN ? ??? ???? ?? VPN ?? ??? ?  
? | 1298](#)
- [?: ?? ?? ?? ???? AutoVPN ?? | 1326](#)
- [P2MP ???? ???? ?? ?? | 1330](#)
- [???? AutoVPN ?? | 1332](#)

AutoVPN? ?? ???(???? ?)? ?? ?? ??? ?? ?? ?? ??? ?? IPsec VPN ?????(??)? ?????. AutoVPN? ???? ?  
??? ???? ?? ? ??? ???? ??? ??? ? ???.

[?? ???? ???? ? ???? ? ???? ? ???? ????.](#)

???? ???? ??? "???? AutoVPN ??" ??? 1332 ???? ????.

- ?? ?? ?? | 1058
- ?? | 1059
- ?? ? ?? | 1060
- PIM? ???? ???? ?? | 1061
- AutoVPN ?? ?? ?? | 1062
- ??? ???? ?? AutoVPN ?? | 1062

?? ?? ??

- Point-to-point `?? - ????` [edit interfaces st0 unit x] `?? ???? ?? st0 ????? point-to-point ????.`
- Point-to-multipoint `?? - ? ?? multipoint ??? AutoVPN ??? ???? [edit interfaces st0 unit x] ?? ???? ???? ???? ???? st0 ?????? ???? ???? ?? ???? ???? IP ??? ???? st0 ????? ???? ???? ???? ????.`

## 122: AutoVPN Point-to-Point ? Point-to-Multipoint ?? ?? ?? ??

|                                                                             |                                                                            |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <p>?? ? ?? ?</p> <p>IKEv1 ? IKEv2 ? ????.</p> <p>IPv4 ? IPv6 ???? ????.</p> | <p>?? ? ???? ?</p> <p>IKEv1 ? IKEv2 ? ????.</p> <p>IPv4 ? IPv6 ? ????.</p> |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------|

## 122: AutoVPN Point-to-Point ? Point-to-Multipoint ?? ?? ?? ?? (Continued)

|                                   |                                     |
|-----------------------------------|-------------------------------------|
| <p>?? ? ?? ?</p>                  | <p>?? ? ???? ?</p>                  |
| <p>?? ??</p>                      | <p>?? ?? ?(OSPF, OSPFv3 ? iBGP)</p> |
| <p>?? ?? ?</p>                    | <p>?? ?? ?</p>                      |
| <p>?? ???? SRX ?? ? ? ???? ?.</p> | <p>? ??? SRX ?? ???? ?.</p>         |

??

AutoVPN[?] [??] [?] [??] [?] [?] [?] [?] [??] [??] [??] [??] [??].

AutoVPN 22 2 22222 2222 22 2222 22 X.509 PKI(Public Key Infrastructure) 22222 2222 2 22222. 2222 2222 22  
IKE(Internet Key Exchange) 2222 2222 22222 2222 22222 22 22 2222 222222 22222 2222 2 22222. 2222 22222 22 2222 2  
2 22 2222 2222 2 22222. "AutoVPN 2222 2222 22 2222(?)" 2222 1063 22222222.

?? ? ?? ???? AutoVPN? ?????.

- AutoVPN [?] PSK: [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?].

```
[?] PSK[?] [?][?] PSK([?, [?] ?] PSK)[?] [?]. [?] PSK[?] [?] ?[?] [?] [?] [?] PSK[?] [?][?], [?] ? [?] [?] [?] [?] [?] [?] [?] PSK[?] ?? [?]??. ? [?] ?? ?? [?] [?] [?] [?] [?] [?] IKE ID[?] ?? ?? 1? IKE ID  
user1@juniper.netuser2@juniper.net [?] ?? [?] 2? [?][?][?][?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] HUB_GW [?][?][?] [?] [?] [?] PSK[?] ?? [?]?.ThisIsMySecretPreSharedkey
```

**1** : 79e4ea39f5c06834a3c4c031e37c6de24d46798a

**2:** 3db8385746f3d1e639435a882579a9f28464e5c7

[?], [??] [???] ID[?] [????] [????] [??] [??] [??] [????] [??] [??] [??] [????] [??] [??] [??] [????].

Auto-VPN PSK? ?? pre-shared-key ? ??? seeded-pre-shared-key ??? ? ????.

- [illegible]

#####.

- **##/### ## ## :** **?(?)** ##### ## ## pre-shared-key-type PSK# ### #####. VPN ##### ## IKE ## ## ?  
? ##### ## ## #####.

VPN ##### ## ## ##### ? ## IKE PSK# ##### ## CLI ## pre-sharedkey *ascii-text* ## pre-  
shared-key *hexadecimal*.

VPN ##### ## ##### ## ## ##### general-ikeid IKE ID ### ## [edit security ike gateway *gateway\_name*  
dynamic] ? ####. ? ### ##### ## ## ## VPN ##### ## IKE ID ### #####. *general-ikeid*?(?) #####.

iked ##### SPC3 ## ? vSRX ## ##(### ##)? junos-ike ## SRX5000 ## ## IKE ### #####.

**? 123: AutoVPN PSK ??**

| IKE(Internet Key Exchange) ??                      | iked ##### SPC3 ## ? vSRX ## ##### SRX5000 ?? |        |
|----------------------------------------------------|-----------------------------------------------|--------|
|                                                    | ## PSK                                        | ##-PSK |
| IKEv2                                              | ?                                             | ?      |
| IKEv2 (##- ##)remote-id                            | ?                                             | ?      |
| IKEv1 #####                                        | ?                                             | ?      |
| IKEv1 ##### (##/ ##)any-remote-<br>idgeneral-ikeid | ?                                             | ?      |
| IKEv1 ## ##                                        | ?                                             | ###    |
| IKEv1 ## ##(any-remote-id/ ?<br>?)general-ikeid    | ?                                             | ###    |

"?: ## ##" ### **1326** ##### AutoVPN ##.

## ? ##

AutoVPN? CLI? ##### SRX ### ##### ? ? #####. ## SRX ### ##### AutoVPN ### ##### ? #####. ## ?  
? ##### ## ## SRX ### ##### ## #####.



- P2MP `???????? ?????? ping? ??? ? ?????`.
- PIM? `?????? IGMP? ?????? ??????? P2MP ?????????? ????? ?????`.

P2MP [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] "P2MP [REDACTED] [REDACTED] [REDACTED] [REDACTED]" [REDACTED] 1330 [REDACTED].

# AutoVPN ☐ ☐ ☐

?? ??? AutoVPN?? ???? ????.

- `?? ?? VPN? ???? ????.`
- `RIP ?? ??? ????? AutoVPN ???? ???? ????.`
- `?? ?? ?? ?? ?? ?? ? IKE(Internet Key Exchange)? ???? ????.`
- `???? ???? ?? NHTB(Next-Hop Tunnel Binding) ??? ???? ????.`
- `IPv6 multicast? ???? ????.`
- `?? IKE(Internet Key Exchange) ID ??? ??? IP ??? IKE(Internet Key Exchange) ID? ??? ? ????.`
- `?? IKE ID ??? ??? ???? ?? IKE ID? ??? ?? ?????? ??? ?? IKE ?????? ??? ??? ???.`

AutoVPN

AutoVPN [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted]:

- VPN [redacted] [redacted] [redacted] [redacted] [redacted].
- VPN [redacted] SRX [redacted] [redacted] [redacted] [redacted].
- [redacted] [redacted] VPN[redacted] [redacted] [redacted] [redacted] [redacted].
- [redacted] [redacted] [redacted] [redacted] AutoVPN[redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

???? ? ??? ????? ?? ?? ??????? ????? AutoVPN ?????? ??? ??? ? IKE(Internet Key Exchange) ??? ?? IPv6 ?  
 ?? ?????.

??-??? ??? ????? ?? ? ???? *RRI(Reverse Route Insertion)*? ??? ?? ?? ??(ARI)? ????? ??? ????? ??? ???  
 ? ??? ??????. ?? ?? ARI ??? ??? ?????? ?? ? ? ?????? ??? ? ?????.

?? ???? ? AutoVPN? IKEv1 ? IKEv2 ??? ?? ? ? ???? ?? ??(st0) ?????? ??? ? ????.

?? ??? ????? ??? ????? ??? ? st0 ?????? ????? ?????.

AutoVPN

- `?? ??? ?????? ??? ? ??? ????? st0 ?????? ?? ??? ?????? ????? ?????.`



- Auto Discovery VPN ? IKEv2 ?? ????? ? ??? ????? ?? AutoVPN?? ??? ? ?????.
- ????? SRX ??? ????? ?? ? ?????, ??? ??? ?? ????? ?????.
- IKEv2?? ? SRX ??? ????? ?? SA ????? ?? ??? ????? ?? ? ?????, ?? SRX ??? ?????? ?????? ??? ??? ?? ?
- ? SRX ??? ?????? ??? ?????? ?? ?? ?? ?? ?????? ??? ? ?????, ?? ? ?????? SRX ??? ?????? ??? ?????? ?

## SEE ALSO

AutoVPN 1063

VPN | 578

?: ?? ?? VPN?? ??? ??? ?? | 584

# AutoVPN

**in this section**

?? ? IKE(Internet Key Exchange) ID ?? | 1063

1065

AutoVPN [redacted] [redacted] [redacted] [redacted] [redacted] X.509 PKI [redacted] [redacted] [redacted] [redacted]. [redacted] [redacted] show security pki local-certificate detail [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

? ???? ???? ???? ???? ??? ???? ??? ? ???? ?? ???? ???? ?? ?????.

??? ?? IKE(Internet Key Exchange) ID ??

?? IKE ID ??? ????? ?? ??? ?????? ????? IKE ??? ??? ? ?????, ? ????? X.509 ????? ?? ?? ?? ?? ?? ?? ?? ?? ??  
? ????? ID?? ?? ????? ????? ?? ? ?????? ???. ??? ??? ?? ??? ??? IKE ??? ?? ??????.

```

22 22, 2222 IKE ID example.net 2 2222 222 22 device1.example.net, device2.example.net, 2 2222 222 2 2222
device3.example.net. 2 2222 2222 222 22 222 222 22 example.net 22 22 222 222 22 ID? 2222 222(2:
device1.example.net). 2 222 22 2222 IKE ID 222222 2 222 22 ID? 22222. IKE 22 22 2222 IKE ID? 222 222 22
IKE ID? 22 22 222 22222 2 22222. 222 2222 2222 22222.

```

□□□ □□□ □□ □□□ □□ □ □□□ □ □□□□.

- `???.???.???.???.???.???.???.???.(?:example.net)???`.
- `?????.???.???.? ?????? ?? ?? ?? ??(?:@example.net)???`.
- `???? ?????, ?????? ?? ?? ? ? ?????? ?? ??? ??????. ?? ????? ASN.1(`Abstract Syntax Notation One`) DN(??`  
`??) ??? ??? ??? ?????? ?? ?? ??? ??????. ????, ?? ?? ??, ??, ?/?/? ?? ?? ??? ??? ? ?????.`

???? ?? ???? ???? ???? IKE(Internet Key Exchange) ID? ???? ?? ??? ???? ID ??? ??? ? ????.

- `???? - ??? ???? ? ???? ???? ? ???? ???? ? ???? ???? IKE ID? ?????, ? ? ???? ? ? ???? ? ? ?  
????(?: ou=eng,ou=sw). ??? ? ???? ???? ????.`
- `?????—??? ???? ? ???? ???? ? ???? ? ???? ???? IKE ID? ?????, ????? ???? ???? ? ? ????  
?(?: ou=eng ? ? ou=sw ? ? ? ou=eng,ou=sw). ??? ???? ???? ????.`

?? ????? ???? ?? ?? ???? ?? ???? ???? example.net ????? ?? IKE(Internet Key Exchange) ID? ??????.

```
[edit]
security {
  ike {
    policy common-cert-policy {
      proposals common-ike-proposal;
      certificate {
        local-certificate hub-local-certificate;
      }
    }
  }
  gateway common-gateway-to-all-spoke-peer {
    ike-policy common-cert-policy;
    dynamic {
      hostname example.net;
      ike-user-type group-ike-id;
    }
    external-interface fe-0/0/2;
  }
}
}
```

```
[?] [??] [?(?) example.net [? [????] [????] [??] [?] [??? [?] [????], [????] [?] X.509 [????] [?] [??] [??] [?] example.net [?] [?] [??] [??] [??] [?] IP[?] [????] [??]. [?] [????] IKE IP [????] [??] [?] IP[?] [????] [??].
```



## AutoVPN 配置

配置 AutoVPN 配置。AutoVPN 配置。AutoVPN 配置。

AutoVPN 配置。

1. CA 配置。
  - CA 配置。
2. st0 配置 point-to-multipoint 配置。
3. IKE(Internet Key Exchange) 配置。
4. IKE(Internet Key Exchange) ID 配置 IKE(Internet Key Exchange) 配置。
5. IPsec 配置 VPN 配置。
6. 配置。

SRX AutoVPN 配置。

1. CA 配置。
  - 配置。
2. st0 配置 point-to-multipoint 配置。
3. IKE(Internet Key Exchange) 配置 IKE(Internet Key Exchange) 配置。
4. IKE(Internet Key Exchange) ID 配置 ID 配置 IKE(Internet Key Exchange) 配置。
5. IPsec 配置 IPsec 配置。
6. 配置。

配置 Junos OS 配置 SRX 配置。配置 Junos OS 配置。

## SEE ALSO

[配置 3 VPN 配置](#)

?: iBGP? ??? ?? AutoVPN ??

in this section

- [?? ??](#) | 1067
- [??](#) | 1067
- [??](#) | 1071
- [??](#) | 1099

? ?????? AutoVPN ??? ?? ?? ?????? ??? ?? ? ?? ?????? ?? ?????? ?? ?? ??? ???? ?????? ??? ?? ????. ? ?????? VPN  
??? ?? ??? ?????? iBGP? ?????? ??? ?? ??? ??????.

?? ?? ?? ??? ??? ?? " ??" [???? 1078](#) ? '1?? ?? ??' ??? ?????? ??? ??????, " spoke1" [???? 1086](#) ? ?????? spoke1  
? ??????, " spoke2? [????? spoke2](#)" [???? 1093](#) ? ??????.

?? ??

? ??? ?????? ?????? ? ?????? ?? ??? ???? ??????.

- AutoVPN ?? ? ?????? ?????? SRX ??? ??? 3?
- AutoVPN? ?????? Junos OS [???? 12.1X44-D10](#) ??

????? ??:

- ?? ?????? ?? ??? ???? ? ?? ??(CA)? ?????? ??(?: ?? ?? ??)? ??????.

VPN ??? ?? ??? ?????? ? ?????? ?? ??? ???? ?? ? ?? ??? ????. ?? ??? ?????? ?? ?? ??? ?? ??? ?? [??? ???](#)  
[? ???](#) ??????.

??

in this section

- [????](#) | 1070

? ?????? AutoVPN ??? ??? ? ?? ?????? ?? ?? ??? ?? ???.

在配置向导中，选择 SCEP(证书颁发机构) 并选择证书颁发机构。选择证书颁发机构时，选择 OU(组织) 并选择 "SLT" 证书颁发机构。选择 OU 并选择 "SLT" 证书颁发机构。选择 IKE ID 并选择。

在配置向导中，选择 IPsec VPN 并选择证书颁发机构。选择证书颁发机构时，选择 AutoVPN 并选择 1。选择 2 并选择 IKE 并选择证书颁发机构。选择 124 并选择 1068 并选择。

124: AutoVPN 配置向导 1 2 3 4

|   |   |
|---|---|
| 1 | 2 |
|---|---|

IKE(Internet Key Exchange) 配置:

|                      |             |
|----------------------|-------------|
| 1                    | RSA 2048    |
| DH(Diffie-Hellman) 2 | 2           |
| 3                    | SHA-1       |
| 4                    | AES 128 CBC |

IKE(Internet Key Exchange) 配置:

|   |   |
|---|---|
| 1 | 2 |
|---|---|

IPsec 配置:

|   |             |
|---|-------------|
| 1 | ESP         |
| 2 | HMAC MD5 96 |
| 3 | DES CBC     |

IPsec 配置:

|                                |    |
|--------------------------------|----|
| PFS(Perfect Forward Secrecy) 1 | 14 |
|--------------------------------|----|

在配置向导中，选择 CA 并选择。



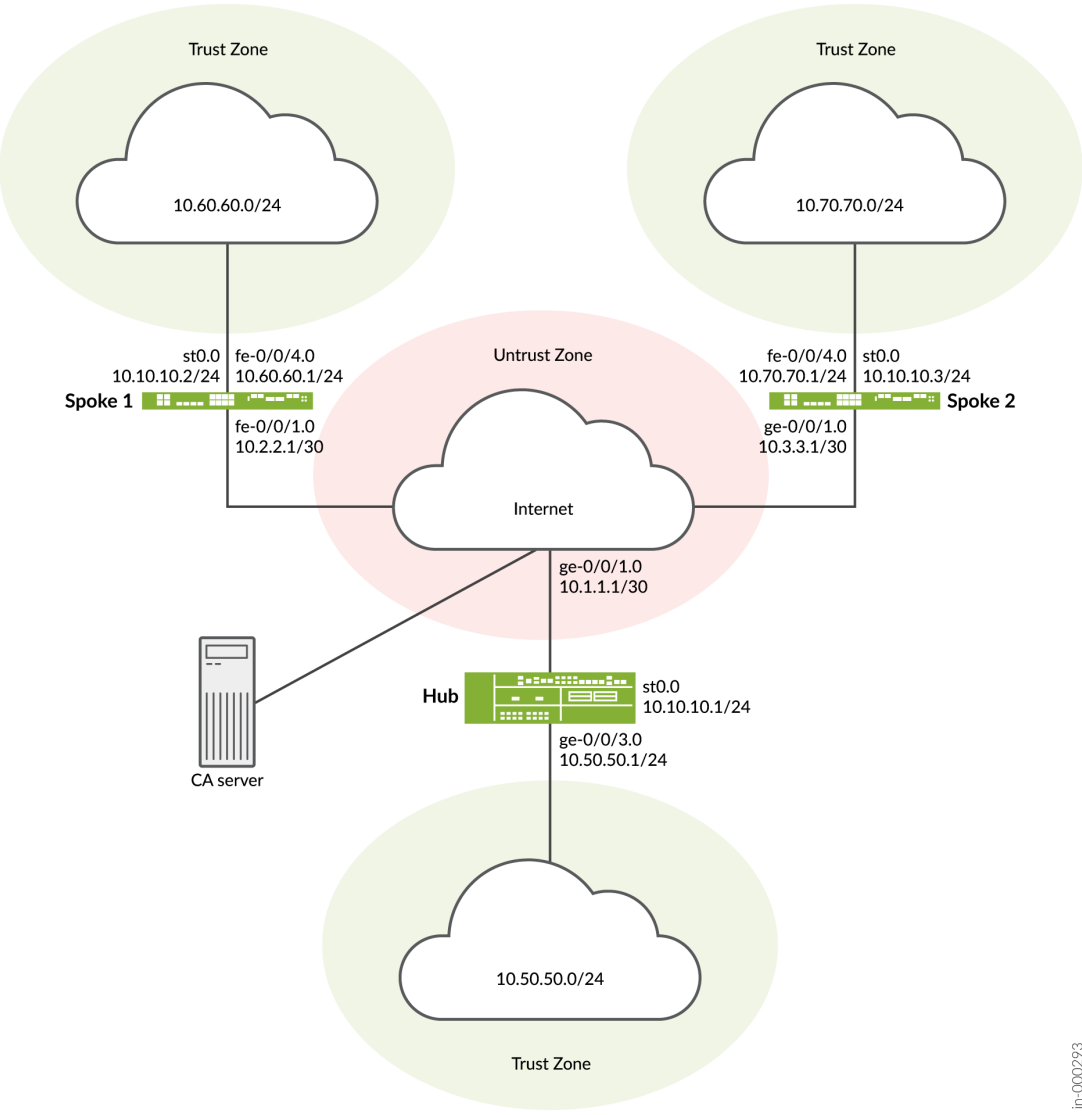
?? ????? ?? ??? ??? VPN ??? ?? ?????.

? ????? ?? ????? ????? ?? ?? ??? ?? ?????? ??????. ?? ??? ?? ?? ? ????? ?? ??? ????? ????. ?? ?? ??? ??????.

???

?? 63 ??? 1070 ?? ? ??? AutoVPN? ?? ??? SRX ??? ????? ?? ?????.

?? 63: iBGP? ??? ?? AutoVPN ??







3. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
```

5. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> show security pki local-certificate detail
```

Certificate identifier: Local1

Certificate version: 3

Serial number: 40a6d5f300000000258d

Issuer:

Common name: CASERVER1, Domain component: net, Domain component: internal

Subject:

Organization: example, Organizational unit: SLT, Country: IN, State: KA,

Locality: Bengaluru, Common name: hub, Domain component: example.net

Subject string:

C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub

Alternate subject: "hub@example.net", example.net, 10.1.1.1

Validity:

Not before: 11- 6-2012 09:39

Not after: 11- 6-2013 09:49

Public key algorithm: rsaEncryption(1024 bits)

30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76

01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3

2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b

34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da

90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8

ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82

6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01

Signature algorithm: sha1WithRSAEncryption

Distribution CRL:

http://ca-server1/CertEnroll/CASERVER1.crl

file://\ca-server1\CertEnroll\CASERVER1.crl

```
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started
```

???

??? 1?? SCEP? ???? ???? ???? ?????:

### 1. CA? ?????.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

### 2. CA ???? ????.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

????? ???? yes CA ???? ????.

### 3. ? ???? ????.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

### 4. ?? ???? ????.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
```

**5.**           .

```

user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
Alternate subject: "spoke1@example.net", example.net, 10.2.2.1
Validity:
  Not before: 11- 6-2012 09:40
  Not after: 11- 6-2013 09:50
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d8:45:09:77:cd:36:9a:6f:58:44:18:91:db
  b0:c7:8a:ee:c8:d7:a6:d2:e2:e7:20:46:2b:26:1a:92:e2:4e:8a:ce
  c9:25:d9:74:a2:81:ad:ea:e0:38:a0:2f:2d:ab:a6:58:ac:88:35:f4
  90:01:08:33:33:75:2c:44:26:f8:25:18:97:96:e4:28:de:3b:35:f2
  4a:f5:92:b7:57:ae:73:4f:8e:56:71:ab:81:54:1d:75:88:77:13:64
  1b:6b:01:96:15:0a:1c:54:e3:db:f8:ec:ec:27:5b:86:39:c1:09:a1
  e4:24:1a:19:0d:14:2c:4b:94:a4:04:91:3f:cb:ef:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  b6:24:2a:0e:96:5d:8c:4a:11:f3:5a:24:89:7c:df:ea:d5:c0:80:56 (sha1)
  31:58:7f:15:bb:d4:66:b8:76:1a:42:4a:8a:16:b3:a9 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

1. CA `?????`.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

2. CA `???? ?????`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
????? ???? yes CA ???? ????.
```

3. `? ??? ?????`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `?? ???? ?????`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke2@example.net ip-address 10.3.3.1 subject
DC=example.net,CN=spoke2,OU=SLT,O=example,L=Tumkur,ST=KA,C=IN challenge-password <password>
```

5. `?? ???? ?????`.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
Serial number: 40bb71d400000000258f
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Tumkur, Common name: spoke2, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
```

Alternate subject: "spoke2@example.net", example.net, 10.3.3.1

Validity:

Not before: 11- 6-2012 10:02

Not after: 11- 6-2013 10:12

Public key algorithm: rsaEncryption(1024 bits)

30:81:89:02:81:81:00:b6:2e:e2:da:e6:ac:57:e4:5d:ff:de:f6:89

27:d6:3e:1b:4a:3f:b2:2d:b3:d3:61:ed:ed:6a:07:d9:8a:d2:24:03

77:1a:fe:84:e1:12:8a:2d:63:6e:bf:02:6b:15:96:5a:4f:37:a0:46

44:09:96:c0:fd:bb:ab:79:2c:5d:92:bd:31:f0:3b:29:51:ce:89:8e

7c:2b:02:d0:14:5b:0a:a9:02:93:21:ea:f9:fc:4a:e7:08:bc:b1:6d

7c:f8:3e:53:58:8e:f1:86:13:fe:78:b5:df:0b:8e:53:00:4a:46:11

58:4a:38:e9:82:43:d8:25:47:7d:ef:18:f0:ef:a7:02:03:01:00:01

Signature algorithm: sha1WithRSAEncryption

Distribution CRL:

http://ca-server1/CertEnroll/CASERVER1.crl

file://\ca-server1\CertEnroll\CASERVER1.crl

Fingerprint:

1a:6d:77:ac:fd:94:68:ce:cf:8a:85:f0:39:fc:e0:6b:fd:fe:b8:66 (sha1)

00:b1:32:5f:7b:24:9c:e5:02:e6:72:75:9e:a5:f4:77 (md5)

Auto-re-enrollment:

Status: Disabled

Next trigger time: Timer not started

?? ???? ???? OU(?? ?? ??) SLT???. ??? IKE(Internet Key Exchange) ???? ???? ???? ???? ???? ???? ???? ???? ou=SLT .

?? ??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/30
set interfaces ge-0/0/3 unit 0 family inet address 10.50.50.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.1/24
set policy-options policy-statement lan_nw from interface ge-0/0/3.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.1
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp cluster 10.2.3.4
```

```

set protocols bgp group ibgp peer-as 65010
set policy-options policy-statement lan_nw from interface ge-0/0/3.0
set policy-options policy-statement lan_nw then accept
set policy-options policy-statement bgp_nh_self term 1 from protocol bgp
set policy-options policy-statement bgp_nh_self term 1 then next-hop self
set policy-options policy-statement bgp_nh_self term 1 then accept
set protocols bgp group ibgp export bgp_nh_self
set protocols bgp group ibgp allow 10.10.10.0/24
set routing-options static route 10.2.2.0/30 next-hop 10.1.1.2
set routing-options static route 10.3.3.0/30 next-hop 10.1.1.2
set routing-options autonomous-system 65010
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway hub-to-spoke-gw ike-policy ike-policy1
set security ike gateway hub-to-spoke-gw dynamic distinguished-name wildcard OU=SLT
set security ike gateway hub-to-spoke-gw dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw local-identity distinguished-name
set security ike gateway hub-to-spoke-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn bind-interface st0.0
set security ipsec vpn hub-to-spoke-vpn ike gateway hub-to-spoke-gw
set security ipsec vpn hub-to-spoke-vpn ike ipsec-policy vpn-policy1
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? ???? ???? ????.

### 1. ???? ????.

```
[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.1.1.1/30
user@host# set ge-0/0/3 unit 0 family inet address 10.50.50.1/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.1/24
```

### 2. ??? ???? ????.

```
[edit policy-options]
user@host# set policy-statement lan_nw from interface ge-0/0/3.0
user@host# set policy-statement lan_nw then accept
user@host# set policy-statement bgp_nh_self term 1 from protocol bgp
user@host# set policy-statement bgp_nh_self term 1 then next-hop self
user@host# set policy-statement bgp_nh_self term 1 then accept
[edit protocols bgp]
user@host# set group ibgp type internal
user@host# set group ibgp local-address 10.10.10.1
user@host# set group ibgp export lan_nw
user@host# set group ibgp cluster 10.2.3.4
user@host# set group ibgp peer-as 65010
user@host# set group ibgp allow 10.10.10.0/24
user@host# set group ibgp export bgp_nh_self
[edit routing-options]
user@host# set static route 10.2.2.0/30 next-hop 10.1.1.2
user@host# set static route 10.3.3.0/30 next-hop 10.1.1.2
user@host# set autonomous-system 65010
```

### 3. 1?? ???? ????.

??? ??? ?? ?? ?? ?? ???? ???? ??? ?? ????.

- ike ??? [edit security ike proposal ike-proposal] ?? ??? authentication-method rsa-signatures authentication-method pre-shared-keys.

??? ?? ??? ??? ??(?? IKE)? ????.



- `ike [??] [edit security ike policy policy-name] [??] [??] certificate local-certificate Local|pre-shared-key  
ascii-text key.`

- `?? ?? set pre-shared-key ascii-text juniper123???`

?? ? ? ? ? ? ?( ? ? IKE) ? ? ? ? ? ?.

- ike(Internet Key Exchange) [edit security ike gateway hub-to-spoke-gw] [?? [??]]

- `??` dynamic hostname *domain-name*`????`dynamic distinguished-name wildcard OU=SLT.

- `?? ?? set dynamic hostname juniper.net???.`

```

? set dynamic ike-user-type group-ike-id ?(?) ?
? set dynamic general-ikeid ? ??.

```

- `[[local-identity hostname hub-hostname[[local-identity distinguished-name.`

- `?? ?? set local-identity hostname hub.juniper.net.`

```
? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? inet ip-address ? ? ? ? set local-identity inet  
192.168.1.100.
```

?? ? ? ? ?( ? IKE)? ? ? ? ? ?.

```
[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway hub-to-spoke-gw]
user@host# set ike-policy ike-policy1
user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/1.0
```

4. 2?? ???? ?????.

```
[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
```

```

user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn hub-to-spoke-vpn]
user@host# set bind-interface st0.0
user@host# set ike gateway hub-to-spoke-gw
user@host# set ike ipsec-policy vpn-policy1

```

5. `set security ipsec vpn hub-to-spoke-vpn`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/3.0

```

6. `set security ipsec vpn hub-to-spoke-vpn`.

```

[edit security policies]
user@host# set default-policy permit-all

```

7. CA `set security pki ca-profile ca-profile1` PSK `set security pki ca-profile ca-profile1`.

```

[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable

```

??

?? ???? , show policy-options, , show routing-optionsshow protocols, show security ike, show security ipsec, show security zones, ? show security policiesshow security pki ??? ???? show interfaces??? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.1.1.1/30;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.50.50.1/24;
    }
  }
}
st0 {
  unit 0 {
    multipoint;
    family inet {
      address 10.10.10.1/24;
    }
  }
}
[edit]
user@host# show policy-options
policy-statement bgp_nh_self {
  term 1 {
    from protocol bgp;
    then {
      next-hop self;
      accept;
    }
  }
}
policy-statement lan_nw {
```

```

    from interface ge-0/0/3.0;
    then accept;
}
[edit]
user@host# show protocols
bgp {
    group ibgp {
        type internal;
        local-address 10.10.10.1;
        export lan_nw;
        cluster 10.2.3.4;
        peer-as 65010;
        allow 10.10.10.0/24;
        export bgp_nh_self;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.2.2.0/30 next-hop 10.1.1.2;
    route 10.3.3.0/30 next-hop 10.1.1.2;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
gateway hub-to-spoke-gw {
    ike-policy ike-policy1;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;

```

```

        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/1.0;
}
[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn hub-to-spoke-vpn {
    bind-interface st0.0;
    ike {
        gateway hub-to-spoke-gw;
        ipsec-policy vpn-policy1;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.0;
        ge-0/0/1.0;
    }
}
security-zone trust {

```

```

        host-inbound-traffic {
            system-services {
                all;
            }
            protocols {
                all;
            }
        }
        interfaces {
            ge-0/0/3.0;
        }
    }
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}

```

?? ?? ?? ?? commit?(?) ?????.

?? ?? 1

CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ???? ????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
 ? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

set interfaces fe-0/0/1 unit 0 family inet address 10.2.2.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.60.60.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.2/24

```

```

set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.2
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp neighbor 10.10.10.1
set routing-options static route 10.1.1.0/30 next-hop 10.2.2.2
set routing-options autonomous-system 65010
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 10.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface fe-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```





```

[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] set local-identity inet 172.16.1.100 [redacted] [redacted] [redacted] inet ip-address
[redacted] [redacted] [redacted] set remote-identity inet 192.168.1.100.

```

```
[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway spoke-to-hub-gw]
user@host# set ike-policy ike-policy1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/1.0
```

4. 2?? ???? ?????.

```
[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub]
user@host# set bind-interface st0.0
user@host# set ike gateway spoke-to-hub-gw
user@host# set ike ipsec-policy vpn-policy1
user@host# set establish-tunnels immediately
```



```

}
    fe-0/0/4 {
        unit 0 {
            family inet {
                address 10.60.60.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            multipoint;
            family inet {
                address 10.10.10.2/24;
            }
        }
    }
}
[edit]
user@host# show policy-options
policy-statement lan_nw {
    from interface fe-0/0/4.0;
    then accept;
}
[edit]
user@host# show protocols
bgp {
    group ibgp {
        type internal;
        local-address 10.10.10.2;
        export lan_nw;
        neighbor 10.10.10.1;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.1.1.0/30 next-hop 10.2.2.2;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
}

```

```

    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}

policy ike-policy1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}

gateway spoke-to-hub-gw {
    ike-policy ike-policy1;
    address 10.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface fe-0/0/1.0;
}

[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}

policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}

vpn spoke-to-hub {
    bind-interface st0.0;
    ike {
        gateway spoke-to-hub-gw;
        ipsec-policy vpn-policy1;
    }
    establish-tunnels immediately;
}

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {

```

```

        all;
    }
    protocols {
        all;
    }
}
interfaces {
    fe-0/0/1.0;
    st0.0;
}
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/4.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}
}

```

?? ?? ?? ?? ?? commit?(?) ?????.

?? 2 ??

CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ??? ????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```
set interfaces ge-0/0/1 unit 0 family inet address 10.3.3.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.70.70.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.3/24
set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.3
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp neighbor 10.10.10.1
set routing-options static route 10.1.1.0/30 next-hop 10.3.3.2
set routing-options autonomous-system 65010
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 10.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
```

```

set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 2? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.3.3.1/30
user@host# set fe-0/0/4 unit 0 family inet address 10.70.70.1/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.3/24

```

2. ??? ???? ????.

```

[edit policy-options]
user@host# set policy-statement lan_nw from interface fe-0/0/4.0
user@host# set policy-statement lan_nw then accept
[edit protocols bgp]
user@host# set group ibgp type internal
user@host# set group ibgp local-address 10.10.10.3
user@host# set group ibgp export lan_nw
user@host# set group ibgp neighbor 10.10.10.1
[edit routing-options]
user@host# set static route 10.1.1.0/30 next-hop 10.3.3.2
user@host# set autonomous-system 10

```

3. 1?? ??? ????.

??? ??? ?? ?? ?? ?? ???? ???? ???? ?? ????.

- `ike [edit security ike proposal ike-proposal] [?? [?? authentication-method rsa-signatures authentication-method pre-shared-keys.`
- `ike [edit security ike policy policy-name] [?? [?? certificate local-certificate Local1 pre-shared-key ascii-text key.`
- `ike(Internet Key Exchange) [edit security ike gateway hub-to-spoke-gw] [?? [??`
  - `[? ? local-identity hostname spoke2-hostname [?? [?? local-identity distinguished-name.`
    - `[?? [?? set local-identity hostname spoke2.juniper.net [??.`
  - `[? ? remote-identity hostname hub-hostname [?? [?? remote-identity distinguished-name.`
    - `[?? [?? set remote-identity hostname hub.juniper.net [??.`

```

[?? [?? [?? [?? [? [?? [?? [??, [? ? [? set local-identity inet 10.0.1.100 [?? [?? inet ip-address [?
[?? [?? set remote-identity inet 192.168.1.100.

```

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway spoke-to-hub-gw]
user@host# set ike-policy ike-policy1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface ge-0/0/1.0

```

#### 4. [?? [?? [?? [??.

```

[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14

```



```

user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub]
user@host# set bind-interface st0.0
user@host# set ike gateway spoke-to-hub-gw
user@host# set ike ipsec-policy vpn-policy1
user@host# set establish-tunnels immediately

```

5. `?? ????.`

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/4.0

```

6. `?? ?? ?? ????.`

```

[edit security policies]
user@host# set default-policy permit-all

```

7. CA `???? ????.` PSK `???? ? ? ? ? ????.`

```

[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable

```

??

?? ???? , show policy-options, , show routing-optionsshow protocols, show security ike, show security ipsec, show security zones, ? show security policiesshow security pki ??? ???? show interfaces??? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.3.3.1/30;
    }
  }
}
fe-0/0/4 {
  unit 0 {
    family inet {
      address 10.70.70.1/24;
    }
  }
}
st0 {
  unit 0 {
    multipoint;
    family inet {
      address 10.10.10.3/24;
    }
  }
}
[edit]
user@host# show policy-options
policy-statement lan_nw {
  from interface fe-0/0/4.0;
  then accept;
}
[edit]
user@host# show protocols
bgp {
  group ibgp {
    type internal;
    local-address 10.10.10.3;
```

```

        export lan_nw;
        neighbor 10.10.10.1;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.1.1.0/30 next-hop 10.3.3.2;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
gateway spoke-to-hub-gw {
    ike-policy ike-policy1;
    address 10.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface ge-0/0/1.0;
}
[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
}

```

```

        proposals ipsec-proposal;
    }
    vpn spoke-to-hub {
        bind-interface st0.0;
        ike {
            gateway spoke-to-hub-gw;
            ipsec-policy vpn-policy1;
        }
        establish-tunnels immediately;
    }
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/4.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;

```

??

- IKE(Internet Key Exchange) 1?? ?? ?? | 1099
- IPsec 2?? ?? ?? | 1100
- IPsec ?? ? ?? ?? | 1101
- BGP ?? | 1101
- ??? ?? ?? | 1102

??

IKE(Internet Key Exchange) 1?? ??? ?????.

??

?? **show security ike security-associations** ??? ?????.

```
user@host> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
5480163 UP    a558717f387074ab 6d0135c5ecaed61d Main 10.3.3.1
5480162 UP    7a63d16a5a723df1 c471f7ae166d3a34 Main 10.2.2.1
```

??

show security ike security-associations ??? ?? ?? IKE(Internet Key Exchange) 1?? SA? ??????. SA? ????? ?? ?? ??, 1?? ??? ??? ?? ?????, ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ??????. 1?? ?? ?? ?????? ?????? ?????? ???.

**IPsec 2?? ?? ??**

??

IPsec 2?? ??? ?????.

??

?? **security ipsec security-associations** ??? ?????.

```
user@host> security ipsec security-associations
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb Mon vsys Port Gateway
<268173400 ESP:des/ md5 9bf33bc7 3567/ unlim - root 500 10.2.2.1
>268173400 ESP:des/ md5 aae5196b 3567/ unlim - root 500 10.2.2.1
<268173401 ESP:des/ md5 69c24d81 622/ unlim - root 500 10.3.3.1
>268173401 ESP:des/ md5 e3fe0231 622/ unlim - root 500 10.3.3.1
```

??

show security ipsec security-associations ??? ?? ?? IKE 2?? SA? ??????. SA? ????? ?? ?? ??, 2?? ??? ??? ?? ?????, ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ??????. 2?? ?? ?? ??? ??? ?????? ?????? ??.

IPsec **?? ? ?? ??**

**??**

IPsec **?? ? ???? ?????**.

**??**

**?? ????? show security ipsec next-hop-tunnels ??? ?????**.

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface  IPSec VPN name      Flag    IKE-
ID                XAUTH username
10.10.10.2        st0.0      hub-to-spoke-vpn     Auto    C=IN, DC=example.net,
ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
10.10.10.3        st0.0      hub-to-spoke-vpn     Auto    C=IN, DC=example.net,
ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
```

**??**

**?? ? ??????? ???? ??????? IP ?? st0 ??? next hop? ??? IPSec VPN ??? ??????? ???**.

BGP **??**

**??**

BGP? **????? ??????? ?? st0 IP ??? ??????? ???????**.

**??**

**?? ????? show bgp summary ??? ?????**.

```
user@host> show bgp summary
Groups: 1 Peers: 2 Down peers: 0
Unconfigured peers: 2
Table      Tot Paths  Act Paths Suppressed  History  Damp State  Pending
inet.0      2           2           0           0         0         0
Peer      AS      InPkt    OutPkt    OutQ   Flaps Last Up/Dwn State|#Active/
Received/Accepted/Damped...
10.10.10.2    10      116      119       0       0       50:25
```

|            |         |     |     |   |   |       |
|------------|---------|-----|-----|---|---|-------|
| 1/1/1/0    | 0/0/0/0 |     |     |   |   |       |
| 10.10.10.3 | 10      | 114 | 114 | 0 | 0 | 50:04 |
| 1/1/1/0    | 0/0/0/0 |     |     |   |   |       |

???

??

□□□□ □□ □□□ □□□□□□ □□□□□.

??

?? ???? show route 10.60.60.0 ??? ??????.

```
user@host> show route 10.60.60.0
inet.0: 45 destinations, 45 routes (44 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.60.60.0/24          *[BGP/170] 00:50:57, localpref 100
                        AS path: I
                        > to 10.10.10.2 via st0.0
```

?? ???? show route 10.70.70.0 ??? ??????.

```
user@host> show route 10.70.70.0

inet.0: 45 destinations, 45 routes (44 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.70.70.0/24          *[BGP/170] 00:50:42, localpref 100
                        AS path: I
                        > to 10.10.10.3 via st0.0
```

## SEE ALSO

IPsec VPN | 452

???



?: IPv6 ???? ? iBGP? ???? ? AutoVPN ?

in this section

- **1103**
- **1103**
- **1107**
- **1136**

? ???? AutoVPN ??? ?? ? ???? ???? ? ? ? ???? ? ? ???? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?  
?? ???? VPN ??? ?? ???? iBGP? ???? IPv6? AutoVPN ??? ??????. ?? ?? ? ? ? ? ? ? ?."

iBGP" ??? 1067? ???? ?? AutoVPN ??.

?? ??

? ? ? ? ? ? ? ? ? ? ?

- 3?? SRX ??? AutoVPN ?? ? ????
- Junos OS ??? 18.1R1 ?? ???.

□□□□ □□:

- ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ (CA) ☐ ☐ ☐ ☐ ☐ (?: ☐ ☐ ☐ ☐) ☐ ☐ ☐ ☐.

[illegible]

??

in this section

- ???? | 1106

AutoVPN

? ???? ? ?? ??? SCEP(?? ??? ? ????)? ????? ? ?????? ??? ????? ?????, ????? ?????? ?? ??? OU(?? ?? ??) ? "SLT"? ????? ?????. ??? OU ??? ? "SLT"? ????? ?? IKE ID? ?????.

???? ???? ?? IPsec VPN ??? ????? ?? ??? ? ?? ?? ??? ??? ????? ? ?????. AutoVPN ??? ?? ????? ??? 1  
?? ? 2?? IKE ?? ??? ??? ?? ??? ???, ? 127 ??? 1104 ?(?) ? ??? ??? ??? ??????.

127: AutoVPN 1 111 111 11 111 1 211 11

*IKE(Internet Key Exchange) [??]:*

|                       |             |
|-----------------------|-------------|
| ?? ??                 | RSA ??? ??? |
| DH(Diffie-Hellman) ?? | 19          |
| ?? ?????              | SHA-384     |
| ??? ?????             | AES 256 CBC |

*IKE(Internet Key Exchange) [?]:*

|    |     |
|----|-----|
| ?? | ??? |
|----|-----|

*IPsec* **??**:

|                         |             |
|-------------------------|-------------|
| ???                     | ESP         |
| ???? (Lifetime Seconds) | 3000        |
| ?? ????                 | AES 256 GCM |

*IPsec* **??**:

|                                                                                                                                                                                                      |    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| PFS(Perfect Forward Secrecy)   | 19 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|

?? ???? ???? ?? ??(CA)? ?????.

Junos OS? ?? ??? ??? ??? ???.

128 1105 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927

## 128: 128 128 128 128 AutoVPN 128

|     |     |         |
|-----|-----|---------|
| 128 | 128 | 128 128 |
|-----|-----|---------|

*IKE(Internet Key Exchange) 128128:*

|                                   |                                                                  |                                                |
|-----------------------------------|------------------------------------------------------------------|------------------------------------------------|
| 128 IP 128                        | 128                                                              | 2001:db8:2000::1                               |
| 128 IKE(Internet Key Exchange) ID | OU(128 128 128) 128 128 SLT 1 128 128 128<br>128 128 DN(128 128) | 128 128 128 DNDN on the hub's certificate      |
| 128 IKE(Internet Key Exchange) ID | 128 128 128 DNDN on the hub's certificate                        | 128 128 128 DN                                 |
| 128 128 128                       | ge-0/0/0                                                         | 128 128 1: ge-0/0/0.0<br>128 128 2: ge-0/0/0.0 |

*VPN:*

|             |               |                              |
|-------------|---------------|------------------------------|
| 128 128 128 | st0.1         | st0.1                        |
| 128 128     | (128 128 128) | establish-tunnels on-traffic |

129 128 1105 1(1) 1 128 128 128 128 128 128.

## 129: 128 128 128

|                 |                                  |                                  |
|-----------------|----------------------------------|----------------------------------|
| 128             | 128 1                            | 128 2                            |
| st0.0 128 128   | 2001:db8:7000::2/64              | 2001:db8:7000::3/64              |
| 128 128 128 128 | (ge-0/0/1.0) 2001:db8:4000::1/64 | (ge-0/0/1.0) 2001:db8:6000::1/64 |
| 128 128 128     | (ge-0/0/0.0) 2001:db8:3000::2/64 | (ge-0/0/0.0) 2001:db8:5000::2/64 |

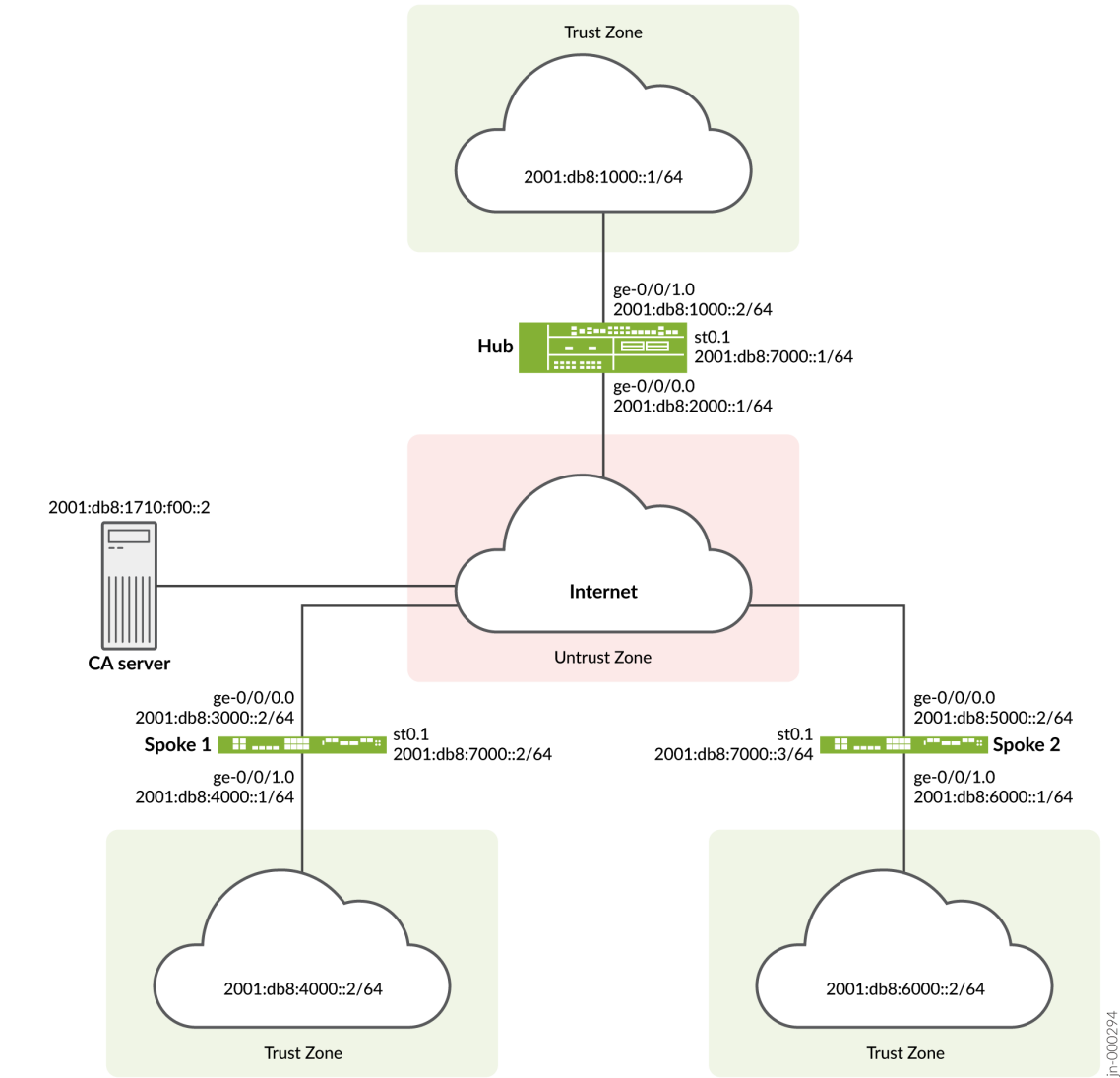
128 128 128 128 128 VPN 128 128 128 128.

?? 64 1106 ?? ? ??? AutoVPN? ?? ??? SRX ??? ????.

???

?? 64 1106 ?? ? ??? AutoVPN? ?? ??? SRX ??? ????.

?? 64: iBGP? ??? ?? AutoVPN ??



- SCEP? ???? ? ? ? ? ? ?Enroll Device Certificates with SCEP | 1107
- ? ? ? ? | 1112
- ? ? ? ? 1 | 1121
- ? ? ? ? 2 ? ? | 1129

?? ???? ?? ? ??? ????? SCEP(Simple Certificate Enrollment Protocol) ???? CA ? ? ????  
 ???? ????.

???

1. CA[?] [?][?][?][?][?].

**2.** CA       .

????? ???? yes CA ????? ?????.

3. `? ??? ????.`

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `?? ????? ????.`

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
```

5. `?? ????? ????.`

```
user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2012 09:39
  Not after: 11- 6-2013 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
  6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
```

```
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started
```

???

??? 1?? SCEP? ???? ???? ???? ?????:

### 1. CA? ?????.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

### 2. CA ???? ????.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

????? ???? yes CA ???? ????.

### 3. ? ???? ????.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

### 4. ?? ???? ????.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
```

**5.**           .

```

user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
Alternate subject: "spoke1@example.net", example.net, 10.2.2.1
Validity:
  Not before: 11- 6-2012 09:40
  Not after: 11- 6-2013 09:50
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d8:45:09:77:cd:36:9a:6f:58:44:18:91:db
  b0:c7:8a:ee:c8:d7:a6:d2:e2:e7:20:46:2b:26:1a:92:e2:4e:8a:ce
  c9:25:d9:74:a2:81:ad:ea:e0:38:a0:2f:2d:ab:a6:58:ac:88:35:f4
  90:01:08:33:33:75:2c:44:26:f8:25:18:97:96:e4:28:de:3b:35:f2
  4a:f5:92:b7:57:ae:73:4f:8e:56:71:ab:81:54:1d:75:88:77:13:64
  1b:6b:01:96:15:0a:1c:54:e3:db:f8:ec:ec:27:5b:86:39:c1:09:a1
  e4:24:1a:19:0d:14:2c:4b:94:a4:04:91:3f:cb:ef:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  b6:24:2a:0e:96:5d:8c:4a:11:f3:5a:24:89:7c:df:ea:d5:c0:80:56 (sha1)
  31:58:7f:15:bb:d4:66:b8:76:1a:42:4a:8a:16:b3:a9 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```



1. CA `?????`.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

2. CA `???? ?????`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
????? ???? yes CA ???? ????.
```

3. `? ??? ?????`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `?? ???? ?????`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke2@example.net ip-address 10.3.3.1 subject
DC=example.net,CN=spoke2,OU=SLT,O=example,L=Tumkur,ST=KA,C=IN challenge-password <password>
```

5. `?? ???? ?????`.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
Serial number: 40bb71d400000000258f
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Tumkur, Common name: spoke2, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
```

Alternate subject: "spoke2@example.net", example.net, 10.3.3.1

Validity:

Not before: 11- 6-2012 10:02

Not after: 11- 6-2013 10:12

Public key algorithm: rsaEncryption(1024 bits)

30:81:89:02:81:81:00:b6:2e:e2:da:e6:ac:57:e4:5d:ff:de:f6:89

27:d6:3e:1b:4a:3f:b2:2d:b3:d3:61:ed:ed:6a:07:d9:8a:d2:24:03

77:1a:fe:84:e1:12:8a:2d:63:6e:bf:02:6b:15:96:5a:4f:37:a0:46

44:09:96:c0:fd:bb:ab:79:2c:5d:92:bd:31:f0:3b:29:51:ce:89:8e

7c:2b:02:d0:14:5b:0a:a9:02:93:21:ea:f9:fc:4a:e7:08:bc:b1:6d

7c:f8:3e:53:58:8e:f1:86:13:fe:78:b5:df:0b:8e:53:00:4a:46:11

58:4a:38:e9:82:43:d8:25:47:7d:ef:18:f0:ef:a7:02:03:01:00:01

Signature algorithm: sha1WithRSAEncryption

Distribution CRL:

http://ca-server1/CertEnroll/CASERVER1.crl

file://\\ca-server1\CertEnroll\CASERVER1.crl

Fingerprint:

1a:6d:77:ac:fd:94:68:ce:cf:8a:85:f0:39:fc:e0:6b:fd:fe:b8:66 (sha1)

00:b1:32:5f:7b:24:9c:e5:02:e6:72:75:9e:a5:f4:77 (md5)

Auto-re-enrollment:

Status: Disabled

Next trigger time: Timer not started

?? ???? ???? OU(?? ?? ??) SLT???. ??? IKE(Internet Key Exchange) ????? ???? ???? ???? ???? ???? ???? ou=SLT .

?? ??

**CLI ?? ??**

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
```

```

set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate HUB
set security ike gateway IKE_GWA_1 ike-policy IKE_POL
set security ike gateway IKE_GWA_1 dynamic distinguished-name wildcard OU=SLT
set security ike gateway IKE_GWA_1 dead-peer-detection always-send
set security ike gateway IKE_GWA_1 dead-peer-detection interval 10
set security ike gateway IKE_GWA_1 dead-peer-detection threshold 3
set security ike gateway IKE_GWA_1 local-identity distinguished-name
set security ike gateway IKE_GWA_1 external-interface ge-0/0/0
set security ike gateway IKE_GWA_1 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPNA_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPNA_1 ike gateway IKE_GWA_1
set security ipsec vpn IPSEC_VPNA_1 ike ipsec-policy IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/0.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:2000::1/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1000::2/64
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::1/64
set routing-options rib inet6.0 static route 2001:db8:3000::/64 next-hop 2001:db8:2000::2
set routing-options rib inet6.0 static route 2001:db8:5000::/64 next-hop 2001:db8:2000::2
set routing-options autonomous-system 100
set routing-options forwarding-table export load_balance
set protocols bgp traceoptions file bgp
set protocols bgp traceoptions flag all
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 2001:db8:9000::1
set protocols bgp group ibgp export ibgp

```

```

set protocols bgp group ibgp cluster 10.1.3.4
set protocols bgp group ibgp peer-as 100
set protocols bgp group ibgp multipath
set protocols bgp group ibgp allow 2001:db8:9000::/64
set policy-options policy-statement ibgp from interface ge-0/0/1.0
set policy-options policy-statement ibgp then accept
set policy-options policy-statement load_balance then load-balance per-packet

```

???

?? ?? ?? ???? ???? ???? ???? ???? ???? ???? ???? CLI ???? ???? ???? ????.

??? ???? ???? ???? ????.

## 1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:2000::1/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:1000::2/64
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::1/64

```

## 2. ???? ???? ????.

```

[edit policy-options]
user@host# set policy-statement ibgp from interface ge-0/0/1.0
user@host# set policy-statement ibgp then accept
user@host# set policy-statement load_balance then load-balance per-packet
[edit protocols bgp]
user@host# set traceoptions file bgp
user@host# set traceoptions flag all
user@host# set group ibgp type internal
user@host# set group ibgp local-address 2001:db8:9000::1
user@host# set group ibgp export ibgp
user@host# set group ibgp cluster 10.1.3.4
user@host# set group ibgp peer-as 100
user@host# set group ibgp multipath
user@host# set group ibgp allow 2001:db8:9000::/64
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:3000::/64 next-hop 2001:db8:2000::2
user@host# set rib inet6.0 static route 2001:db8:5000::/64 next-hop 2001:db8:2000::2

```

```

user@host# set autonomous-system 100
user@host# set forwarding-table export load_balance

```

### 3. 1?? ??? ?????.

```

[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike proposal ike-proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate HUB
[edit security ike gateway IKE_GWA_1]
user@host# set ike-policy IKE_POL
user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/0
user@host# set version v1-only

```

### 4. 2?? ??? ?????.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPNA_1]
user@host# set bind-interface st0.1

```

```
user@host# set ike gateway IKE_GWA_1
user@host# set ike ipsec-policy IPSEC_POL
```

##### 5. `???` `??????`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0
```

##### 6. `??` `??` `???` `??????`.

```
[edit security policies]
user@host# set default-policy permit-all
```

##### 7. CA `????` `??????`.

```
[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable
```

`??`

`??` `????`, show policy-options, , show routing-optionsshow protocols, show security ike, show security ipsec, show security zones, ? show security policiesshow security pki `????` `????` show interfaces`???` `??????`. `???` `???` `???` `????` `????`, ? `??` `??` `????` `????` `??????`.

```
[edit]
user@host# show interfaces
```

```

ge-0/0/0 {
  unit 0 {
    family inet6 {
      address 2001:db8:2000::1/64;
    }
  }
}

ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:1000::2/64;
    }
  }
}

st0 {
  unit 1 {
    multipoint;
    family inet6 {
      address 2001:db8:7000::1/64;
    }
  }
}

[edit]
user@host# show policy-options
policy-statement ibgp {
  from interface ge-0/0/1.0;
  then accept;
}

policy-statement load_balance {
  then {
    load-balance per-packet;
  }
}

[edit]
user@host# show protocols
bgp {
  traceoptions {
    file bgp;
    flag all;
  }
  group ibgp {
    type internal;
    local-address 2001:db8:9000::1;
  }
}

```

```

        export ibgp;
        cluster 10.1.3.4;
        peer-as 100;
        multipath;
        allow 2001:db8:9000::/64;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route route 2001:db8:3000::/64 next-hop 2001:db8:2000::2;
        route 2001:db8:5000::/64 next-hop 2001:db8:2000::2;
    }
}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate HUB;
    }
}
gateway IKE_GWA_1 {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
    }
    dead-peer-detection {

```



```

        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPNA_1 {
    bind-interface st0.1;
    ike {
        gateway IKE_GWA_1;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.1;
    }
}

```

```

}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

```

?? ?? ?? ?? ?? commit?(?) ??.

```

?? ? 1

CLI    

```
? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? ? CLI? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? ?.
```

```
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE1
set security ike gateway IKE_GW_SPOKE_1 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_1 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_1 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_1 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_1 external-interface ge-0/0/0.0
set security ike gateway IKE_GW_SPOKE_1 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike gateway IKE_GW_SPOKE_1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_1 establish-tunnels on-traffic
set security policies default-policy permit-all
```

```

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::2/64
set routing-options rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:3000::1
set routing-options autonomous-system 100
set protocols bgp traceoptions file bgp
set protocols bgp traceoptions flag all
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 2001:db8:9000::2
set protocols bgp group ibgp export ibgp
set protocols bgp group ibgp peer-as 100
set protocols bgp group ibgp neighbor 2001:db8:9000::1
set policy-options policy-statement ibgp from interface ge-0/0/1.0
set policy-options policy-statement ibgp then accept

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 1? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::2/64

```

2. ??? ???? ????.

```

[edit policy-options]
user@host# set policy-statement ibgp from interface ge-0/0/1.0
user@host# set policy-statement ibgp then accept
[edit protocols bgp]

```

```

user@host# set traceoptions file bgp
user@host# set traceoptions flag all
user@host# set group ibgp type internal
user@host# set group ibgp local-address 2001:db8:9000::2
user@host# set group ibgp export ibgp
user@host# set group ibgp peer-as 100
user@host# set group ibgp neighbor 2001:db8:9000::1
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:3000::1
user@host# set autonomous-system 100

```

### 3. 1?? ???? ?????.

```

[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike proposal ike-proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE1
[edit security ike gateway IKE_GW_SPOKE_1]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0
user@host# set version v1-only

```

### 4. 2?? ???? ?????.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp

```

```

user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPNA_SPOKE_1]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GWA_SPOKE_1
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels on-traffic

```

5. `???` `??????`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0

```

6. `??` `??` `???` `??????`.

```

[edit security policies]
user@host# set default-policy permit-all

```

7. CA `????` `??????`.

```

[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable

```

??

?? ???? , show policy-options, , show routing-optionsshow protocols, show security ike, show security ipsec, show security zones, ? show security policiesshow security pki ??? ???? show interfaces??? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ???? ???? ????.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet6 {
      address 2001:db8:3000::2/64;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:4000::1/64;
    }
  }
}
st0 {
  unit 1{
    family inet6 {
      address 2001:db8:7000::2/64;
    }
  }
}
[edit]
user@host# show policy-options
policy-statement ibgp {
  from interface ge-0/0/1.0;
  then accept;
}
[edit]
user@host# show protocols
bgp {
  traceoptions {
    file bgp;
    flag all;
  }
}
```

```

group ibgp {
    type internal;
    local-address 2001:db8:9000::2;
    export ibgp;
    peer-as 100;
    neighbor 2001:db8:9000::1;
}
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route route 2001:db8:2000::/64 next-hop 2001:db8:3000::1;
    }
}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE1;
    }
}
gateway IKE_GWA_SPOKE1 {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
    }
    dead-peer-detection {

```



```

        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPNA_SPOKE_1 {
    bind-interface st0.1;
    ike {
        gateway IKE_GWA_SPOKE_1;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.1;
    }
}

```

```

}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

```

?? ?? ?? ?? ?? commit?(?) ??.

```

?? 2 ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE2
set security ike gateway IKE_GW_SPOKE_2 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_2 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_2 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_2 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_2 external-interface ge-0/0/0.0
set security ike gateway IKE_GW_SPOKE_2 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_2 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike gateway IKE_GW_SPOKE_2
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_2 establish-tunnels on-traffic
set security policies default-policy permit-all
```

```

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::3/64
set routing-options rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
set routing-options autonomous-system 100
set protocols bgp traceoptions file bgp
set protocols bgp traceoptions flag all
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 2001:db8:9000::3
set protocols bgp group ibgp export ibgp
set protocols bgp group ibgp peer-as 100
set protocols bgp group ibgp neighbor 2001:db8:9000::1
set policy-options policy-statement ibgp from interface ge-0/0/1.0
set policy-options policy-statement ibgp then accept

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 2? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::3/64

```

2. ??? ???? ????.

```

[edit policy-options]
user@host# set policy-statement ibgp from interface ge-0/0/1.0
user@host# set policy-statement ibgp then accept
[edit protocols bgp]

```

```

user@host# set traceoptions file bgp
user@host# set traceoptions flag all
user@host# set group ibgp type internal
user@host# set group ibgp local-address 2001:db8:9000::3
user@host# set group ibgp export ibgp
user@host# set group ibgp peer-as 100
user@host# set group ibgp neighbor 2001:db8:9000::1
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
user@host# set autonomous-system 100

```

### 3. 1?? 2?? 3????.

```

[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike proposal ike-proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE2
[edit security ike gateway IKE_GW_SPOKE_2]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0
user@host# set version v1-only

```

### 4. 2?? 3?? 4????.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp

```

```

user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPNA_SPOKE_2]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GWA_SPOKE_2
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels on-traffic

```

5. `???` `??????`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0

```

6. `??` `??` `???` `??????`.

```

[edit security policies]
user@host# set default-policy permit-all

```

7. CA `????` `??????`.

```

[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable

```



```

group ibgp {
    type internal;
    local-address 2001:db8:9000::3;
    export ibgp;
    peer-as 100;
    neighbor 2001:db8:9000::1;
}
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route route 2001:db8:2000::/64 next-hop 2001:db8:5000::1;
    }
}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE2;
    }
}
gateway IKE_GWA_SPOKE2 {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
    }
    dead-peer-detection {

```



```

        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPNA_SPOKE_2 {
    bind-interface st0.1;
    ike {
        gateway IKE_GWA_SPOKE_2;
        ipsec-policy IPSEC_POL;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.1;
    }
}

```

```

}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

?? ?? ?? ?? ?? commit?(?) ?????.

??

#### in this section

- [IKE\(Internet Key Exchange\) ?? ?? | 1137](#)
- [IPsec ?? ?? | 1137](#)

- IPsec 22 2 22 22 | 1138
- BGP 22 | 1139

222 2222 2222 222 222222.

**IKE(Internet Key Exchange) 22 22**

22

IKE 222 222222.

22

22 2222 show security ike sa 222 222222.

|                                 |       |                           |                           |      |                  |         |
|---------------------------------|-------|---------------------------|---------------------------|------|------------------|---------|
| user@host> show security ike sa |       |                           |                           |      |                  |         |
| Index                           | State | Initiator cookie          | Responder cookie          | Mode | Remote           | Address |
| 493333                          | UP    | 2001:db8:88b49d915e684c93 | 2001:db8:fe890b1cac8522b5 | Main | 2001:db8:3000::2 |         |
| 493334                          | UP    | 2001:db8:26e40244ad3d722d | 2001:db8:68b4d9f94097d32e | Main | 2001:db8:5000::2 |         |

22

show security ike sa 222 22 22 IKE(Internet Key Exchange) 122 SA2 222222. SA2 2222 22 22 22, 122 222 22 2 22 2222. 22222 IKE(Internet Key Exchange) 22 22 22 2 22 22222 222 222222. 122 22 22 222 222 222222 22 22 222.

**IPsec 22 22**

22

IPsec 222 222222.

??

?? ???? show security ipsec sa ??? ?????.

```
user@host> show security ipsec sa
Total active tunnels: 2
  ID          Algorithm      SPI  Life:sec/kb   Mon   lsys Port Gateway
>67108885 ESP:aes-gcm-256/None fdef4dab 2918/ unlim - root 500 2001:db8:3000::2
>67108885 ESP:aes-gcm-256/None e785dad3 2918/ unlim - root 500 2001:db8:3000::2
>67108887 ESP:aes-gcm-256/None 34a787af 2971/ unlim - root 500 2001:db8:5000::2
>67108887 ESP:aes-gcm-256/None cf57007f 2971/ unlim - root 500 2001:db8:5000::2
```

??

show security ipsec sa ??? ? ? IKE 2?? SA? ?????. SA? ????? ? ? ? ? , 2?? ??? ? ? ? ? ? . ??? ?  
IKE(Internet Key Exchange) ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? . 2?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? .

**IPsec ? ? ? ? ?**

??

IPsec ? ? ? ? ? ? ? ? ? ? .

??

?? ???? show security ipsec next-hop-tunnels ??? ?????.

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway          interface  IPsec VPN name  Flag  IKE-
ID                        XAUTH username
2001:db8:9000::2          st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available
2001:db8:9000::3          st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
2001:db8::5668:ad10:fcd8:163c st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available
```

```
2001:db8::5668:ad10:fcd8:18a1 st0.1      IPSEC_VPNA_1      Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
```

??

?? ? ???? ???? IP ?? st0 ??. next hop? ??? IPsec VPN ??? ???? ???.

BGP ??

??

BGP? ???? ???? ?? st0 IP ??? ???? ????.

??

?? ???? show bgp summary ??? ????.

```
user@host> show bgp summary
Groups: 1 Peers: 2 Down peers: 0
Unconfigured peers: 2
Table      Tot Paths  Act Paths  Suppressed History Damp State    Pending
inet6.0
          2         2         0         0         0         0
Peer      AS    InPkt    OutPkt  OutQ  Flaps Last Up/Dwn State
2001:db8:9000::2  100  4        4      0    0      32  Establ
  inet6.0: 1/1/1/0
2001:db8:9000::3  100  4        4      0    0      8  Establ
  inet6.0: 1/1/1/0
```

SEE ALSO

[? ? ? VPN ? | 453](#)

---

[??? ???? ??](#)

- ?? ?? | 1140
- ?? | 1140
- ?? | 1143
- ?? | 1167

?? ??

- AutoVPN ☐ ☐ ☐ ☐ ☐ ☐ SRX ☐ ☐ ☐ 2
- AutoVPN ☐ ☐ ☐ ☐ Junos OS ☐ ☐ 12.1X44-D10 ☐

[illegible]

??

● ???? | 1142

? ???? ? ?? ??? SCEP(?? ???? ?? ?????)? ???? ? ?????? ??? ????? ????? ?????, ????? ? IPsec VPN ??? ?? ? ?  
???? ??????, ????? ??? ? ????? ?? ??(DN)? OU(?? ?? ??) ? "SLT"? ????? ?????, ??? OU ??? ? "SLT"? ????? ??

IKE ID? ?????. ???? ? ? ???? DN? OU ? "SBU"? ???? ?????. ???? OU ??? ? "SBU"? ???? ? ? IKE ID? ?????.

???? ???? ? IPsec VPN ??? ???? ???? ???? ? ???? ?????. AutoVPN ?? ? ???? ???? 1?? ? 2?? IKE ?? ?? ? ???? ? ???? ?????.[? 130](#) [???? 1141](#) ?(?) ? ???? ???? ???? ?????.

**? 130: AutoVPN ?? ? ???? iBGP ECMP ??? ?? 1?? ? 2?? ??**

|    |    |
|----|----|
| ?? | ?? |
|----|----|

*IKE(Internet Key Exchange) ??:*

|                       |             |
|-----------------------|-------------|
| ?? ??                 | RSA ??? ??? |
| DH(Diffie-Hellman) ?? | 2           |
| ?? ?????              | SHA-1       |
| ??? ?????             | AES 128 CBC |

*IKE(Internet Key Exchange) ??:*

|    |     |
|----|-----|
| ?? | ??? |
|----|-----|

*IPsec ??:*

|           |             |
|-----------|-------------|
| ?????     | ESP         |
| ?? ?????  | HMAC MD5 96 |
| ??? ????? | DES CBC     |

*IPsec ??:*

|                                 |    |
|---------------------------------|----|
| PFS(Perfect Forward Secrecy) ?? | 14 |
|---------------------------------|----|

?? ???? ???? ? ?(CA)? ?????.







```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local2 domain-name example.net email hub_backup@example.net ip-address 10.1.2.1 subject
```

```
DC=example.net,CN=hub_backup,OU=SBU,O=example,L=Bengaluru,ST=KA,C=IN challenge-password
<password>
```

5. `?? ???? ?????.`

```
user@host> show security pki local-certificate certificate-id Local1 detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2012 09:39
  Not after: 11- 6-2013 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
  6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
```

Status: Disabled  
 Next trigger time: Timer not started

```
user@host> show security pki local-certificate certificate-id Local2 detail
```

```
Certificate identifier: Local2
Certificate version: 3
Serial number: 505efdf900000000259a
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SBU, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub_backup, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SBU, CN=hub_backup
Alternate subject: "hub_backup@example.net", example.net, 10.1.2.1
Validity:
  Not before: 11- 9-2012 10:55
  Not after: 11- 9-2013 11:05
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d5:44:08:96:f6:77:05:e6:91:50:8a:8a:2a
  4e:95:43:1e:88:ea:43:7c:c5:ac:88:d7:a0:8d:b5:d9:3f:41:db:db
  44:34:1f:56:a5:38:4b:b2:c5:85:f9:f1:bf:b2:7b:d4:b2:af:98:a0
  95:50:02:ad:f5:dd:4d:dc:67:85:dd:84:09:df:9c:68:a5:58:65:e7
  2c:72:cc:47:4b:d0:cc:4a:28:ca:09:db:ad:6e:5a:13:6c:e6:cc:f0
  29:ed:2b:2d:d1:38:38:bc:68:84:de:ae:86:39:c9:dd:06:d5:36:f0
  e6:2a:7b:46:4c:cd:a5:24:1c:e0:92:8d:ad:35:29:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  98:96:2f:ff:ca:af:33:ee:d7:4c:c8:4f:f7:71:53:c0:5d:5f:c5:59 (sha1)
  c9:87:e3:a4:5c:47:b5:aa:90:22:e3:06:b2:0b:e1:ea (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started
```

???

???

1. CA `?????`.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

2. CA `???? ?????`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
????? ???? yes CA ????
```

3. `? ???? ? ? ? ? ?`.

```
user@host> rrequest security pki generate-key-pair certificate-id Local1
user@host> request security pki generate-key-pair certificate-id Local2
```

4. `?? ???? ?????`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local2 domain-name example.net email spoke1_backup@example.net ip-address 10.3.3.1
subject DC=example.net,CN=spoke1_backup,OU=SBU,O=example,L=Mysore,ST=KA,C=IN challenge-
password <password>
```

5. `?? ???? ?????`.

```
user@host> show security pki local-certificate certificate-id Local1 detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
Common name: CASERVER1, Domain component: net, Domain component: internal
```

Subject:  
 Organization: example, Organizational unit: SLT, Country: IN, State: KA,  
 Locality: Mysore, Common name: spoke1, Domain component: example.net

Subject string:

C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1

Alternate subject: "spoke1@example.net", example.net, 10.2.2.1

Validity:

Not before: 11- 6-2012 09:40

Not after: 11- 6-2013 09:50

Public key algorithm: rsaEncryption(1024 bits)

30:81:89:02:81:81:00:d8:45:09:77:cd:36:9a:6f:58:44:18:91:db  
 b0:c7:8a:ee:c8:d7:a6:d2:e2:e7:20:46:2b:26:1a:92:e2:4e:8a:ce  
 c9:25:d9:74:a2:81:ad:ea:e0:38:a0:2f:2d:ab:a6:58:ac:88:35:f4  
 90:01:08:33:33:75:2c:44:26:f8:25:18:97:96:e4:28:de:3b:35:f2  
 4a:f5:92:b7:57:ae:73:4f:8e:56:71:ab:81:54:1d:75:88:77:13:64  
 1b:6b:01:96:15:0a:1c:54:e3:db:f8:ec:ec:27:5b:86:39:c1:09:a1  
 e4:24:1a:19:0d:14:2c:4b:94:a4:04:91:3f:cb:ef:02:03:01:00:01

Signature algorithm: sha1WithRSAEncryption

Distribution CRL:

http://ca-server1/CertEnroll/CASERVER1.crl

file://\ca-server1\CertEnroll\CASERVER1.crl

Fingerprint:

b6:24:2a:0e:96:5d:8c:4a:11:f3:5a:24:89:7c:df:ea:d5:c0:80:56 (sha1)

31:58:7f:15:bb:d4:66:b8:76:1a:42:4a:8a:16:b3:a9 (md5)

Auto-re-enrollment:

Status: Disabled

Next trigger time: Timer not started

user@host> **show security pki local-certificate certificate-id Local2 detail**

Certificate identifier: Local2

Certificate version: 3

Serial number: 506c3d0600000000259b

Issuer:

Common name: CASERVER1, Domain component: net, Domain component: internal

Subject:

Organization: example, Organizational unit: SBU, Country: IN, State: KA,

Locality: Mysore, Common name: spoke1\_backup, Domain component: example.net

Subject string:

C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SBU, CN=spoke1\_backup

Alternate subject: "spoke1\_backup@example.net", example.net, 10.3.3.1

Validity:

Not before: 11- 9-2012 11:09

?? ??

```
? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ???????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(? ??????).
```

```
set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/30
set interfaces ge-0/0/2 unit 0 family inet address 10.1.2.1/30
set interfaces ge-0/0/3 unit 0 family inet address 10.50.50.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.1/24
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet address 10.20.20.1/24
set policy-options policy-statement lan_nw from interface ge-0/0/3.0
set policy-options policy-statement lan_nw then accept
set policy-options policy-statement load_balance then load-balance per-packet
set protocols bgp group ibgp-1 type internal
set protocols bgp group ibgp-1 local-address 10.10.10.1
```

```

set protocols bgp group ibgp-1 export lan_nw
set protocols bgp group ibgp-1 cluster 10.2.3.4
set protocols bgp group ibgp-1 multipath
set protocols bgp group ibgp-1 allow 10.10.10.0/24
set protocols bgp group ibgp-2 type internal
set protocols bgp group ibgp-2 local-address 10.20.20.1
set protocols bgp group ibgp-2 export lan_nw
set protocols bgp group ibgp-2 cluster 10.2.3.5
set protocols bgp group ibgp-2 multipath
set protocols bgp group ibgp-2 allow 10.20.20.0/24
set routing-options static route 10.2.2.0/30 next-hop 10.1.1.2
set routing-options static route 10.3.3.0/30 next-hop 10.1.2.2
set routing-options autonomous-system 65010
set routing-options forwarding-table export load_balance
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy-1 mode main
set security ike policy ike-policy-1 proposals ike-proposal
set security ike policy ike-policy-1 certificate local-certificate Local1
set security ike policy ike-policy-2 mode main
set security ike policy ike-policy-2 proposals ike-proposal
set security ike policy ike-policy-2 certificate local-certificate Local2
set security ike gateway hub-to-spoke-gw-1 ike-policy ike-policy-1
set security ike gateway hub-to-spoke-gw-1 dynamic distinguished-name wildcard OU=SLT
set security ike gateway hub-to-spoke-gw-1 dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw-1 local-identity distinguished-name
set security ike gateway hub-to-spoke-gw-1 external-interface ge-0/0/1.0
set security ike gateway hub-to-spoke-gw-2 ike-policy ike-policy-2
set security ike gateway hub-to-spoke-gw-2 dynamic distinguished-name wildcard OU=SBU
set security ike gateway hub-to-spoke-gw-2 dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw-2 local-identity distinguished-name
set security ike gateway hub-to-spoke-gw-2 external-interface ge-0/0/2.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn-1 bind-interface st0.0
set security ipsec vpn hub-to-spoke-vpn-1 ike gateway hub-to-spoke-gw-1
set security ipsec vpn hub-to-spoke-vpn-1 ike ipsec-policy vpn-policy
set security ipsec vpn hub-to-spoke-vpn-2 bind-interface st0.1

```



```

set security ipsec vpn hub-to-spoke-vpn-2 ike gateway hub-to-spoke-gw-2
set security ipsec vpn hub-to-spoke-vpn-2 ike ipsec-policy vpn-policy
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? ????? ???? ?????.

## 1. ?????? ?????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.1.1.1/30
user@host# set ge-0/0/2 unit 0 family inet address 10.1.2.1/30
user@host# set ge-0/0/3 unit 0 family inet address 10.50.50.1/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.1/24
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 10.20.20.1/24

```

## 2. ??? ?????? ?????.

```

[edit policy-options]
user@host# set policy-statement lan_nw from interface ge-0/0/3.0
user@host# set policy-statement lan_nw then accept
user@host# set policy-statement load_balance then load-balance per-packet
[edit protocols bgp]
user@host# set group ibgp-1 type internal

```

```

user@host# set group ibgp-1 local-address 10.10.10.1
user@host# set group ibgp-1 export lan_nw
user@host# set group ibgp-1 cluster 10.2.3.4
user@host# set group ibgp-1 multipath
user@host# set group ibgp-1 allow 10.10.10.0/24
user@host# set group ibgp-2 type internal
user@host# set group ibgp-2 local-address 10.20.20.1
user@host# set group ibgp-2 export lan_nw
user@host# set group ibgp-2 cluster 10.2.3.5
user@host# set group ibgp-2 multipath
user@host# set group ibgp-2 allow 10.20.20.0/24
[edit routing-options]
user@host# set static route 10.2.2.0/30 next-hop 10.1.1.2
user@host# set static route 10.3.3.0/30 next-hop 10.1.2.2
user@host# set autonomous-system 65010
user@host# set forwarding-table export load_balance

```

### 3. 1?? ???? ?????.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy-1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike policy ike-policy-2]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local2
[edit security ike gateway hub-to-spoke-gw-1]
user@host# set ike-policy ike-policy-1
user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/1.0
[edit security ike gateway hub-to-spoke-gw-2]
user@host# set ike-policy ike-policy-2
user@host# set dynamic distinguished-name wildcard OU=SBU
user@host# set dynamic ike-user-type group-ike-id

```

```
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/2.0
```

#### 4. `set ipsec proposal`.

```
[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn hub-to-spoke-vpn-1]
user@host# set bind-interface st0.0
user@host# set ike gateway hub-to-spoke-gw-1
user@host# set ike ipsec-policy vpn-policy
[edit security ipsec vpn hub-to-spoke-vpn-2]
user@host# set bind-interface st0.1
user@host# set ike gateway hub-to-spoke-gw-2
user@host# set ike ipsec-policy vpn-policy
```

#### 5. `set security zone`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.0
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces ge-0/0/2.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/3.0
```

#### 6. `set security policy`.

```
[edit security policies]
user@host# set default-policy permit-all
```

## 7. CA `ca-profile1`.

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

??

?? `show policy-options`, `show routing-options`, `show protocols`, `show security ike`, `show security ipsec`, `show security zones`, `show security policies`, `show security pki` `ca-profile1` `show interfaces` `ge-0/0/1`, `ge-0/0/2`, `ge-0/0/3`, `st0`.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 10.1.1.1/30;
    }
  }
}
ge-0/0/2 {
  unit 0 {
    family inet {
      address 10.1.2.1/30;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.50.50.1/24;
    }
  }
}
st0 {
  unit 0 {
    multipoint;
    family inet {
```

```

        address 10.10.10.1/24;
    }
}
unit 1 {
    multipoint;
    family inet {
        address 10.20.20.1/24;
    }
}
}
[edit]
user@host# show policy-options
policy-statement lan_nw {
    from interface ge-0/0/3.0;
    then accept;
}
policy-statement load_balance {
    then {
        load-balance per-packet;
    }
}
[edit]
user@host# show protocols
bgp {
    group ibgp-1 {
        type internal;
        local-address 10.10.10.1;
        export lan_nw;
        cluster 10.2.3.4;
        multipath;
        allow 10.10.10.0/24;
    }
    group ibgp-2 {
        type internal;
        local-address 10.20.20.1;
        export lan_nw;
        cluster 10.2.3.5;
        multipath;
        allow 10.20.20.0/24;
    }
}
[edit]
user@host# show routing-options

```

```

static {
    route 10.2.2.0/30 next-hop 10.1.1.2;
    route 10.3.3.0/30 next-hop 10.1.2.2;
}
autonomous-system 65010;
    forwarding-table {
        export load_balance;
    }
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy-1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
policy ike-policy-2 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local2;
    }
}
gateway hub-to-spoke-gw-1 {
    ike-policy ike-policy-1;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/1.0;
}
gateway hub-to-spoke-gw-2 {
    ike-policy ike-policy-2;

```

```

        dynamic {
            distinguished-name {
                wildcard OU=SBU;
            }
            ike-user-type group-ike-id;
        }
        local-identity distinguished-name;
        external-interface ge-0/0/2.0;
    }
[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy vpn-policy {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn hub-to-spoke-vpn-1 {
    bind-interface st0.0;
    ike {
        gateway hub-to-spoke-gw-1;
        ipsec-policy vpn-policy;
    }
}
vpn hub-to-spoke-vpn-2 {
    bind-interface st0.1;
    ike {
        gateway hub-to-spoke-gw-2;
        ipsec-policy vpn-policy;
    }
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
}

```

```

        protocols {
            all;
        }
    }
    interfaces {
        st0.0;
        ge-0/0/1.0;
        ge-0/0/2.0;
        st0.1;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}
}

```

```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

```



?? 1

CLI ??

? ?? ???? ?????, ?? ???? ???? ???? ?? ?? ?? ?? ???? ???? ?????, ???? ???? ???? ? ???? ?? ???? ???? [edit] ?  
? ???? ???? CLI? ???? ?? ?? ??, ?? ???? commit?(?) ?????.

```
set interfaces fe-0/0/1 unit 0 family inet address 10.2.2.1/30
set interfaces fe-0/0/2 unit 0 family inet address 10.3.3.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.60.60.1/24
set interfaces st0 unit 0 family inet address 10.10.10.2/24
set interfaces st0 unit 1 family inet address 10.20.20.2/24
set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp-1 type internal
set protocols bgp group ibgp-1 local-address 10.10.10.2
set protocols bgp group ibgp-1 export lan_nw
set protocols bgp group ibgp-1 neighbor 10.10.10.1
set protocols bgp group ibgp-2 type internal
set protocols bgp group ibgp-2 local-address 10.20.20.2
set protocols bgp group ibgp-2 export lan_nw
set protocols bgp group ibgp-2 neighbor 10.20.20.1
set routing-options static route 10.1.1.0/30 next-hop 10.2.2.2
set routing-options static route 10.1.2.0/30 next-hop 10.3.3.2
set routing-options autonomous-system 65010
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy-1 mode main
set security ike policy ike-policy-1 proposals ike-proposal
set security ike policy ike-policy-1 certificate local-certificate Local1
set security ike policy ike-policy-2 mode main
set security ike policy ike-policy-2 proposals ike-proposal
set security ike policy ike-policy-2 certificate local-certificate Local2
set security ike gateway spoke-to-hub-gw-1 ike-policy ike-policy-1
set security ike gateway spoke-to-hub-gw-1 address 10.1.1.1
set security ike gateway spoke-to-hub-gw-1 local-identity distinguished-name
set security ike gateway spoke-to-hub-gw-1 remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw-1 external-interface fe-0/0/1.0
set security ike gateway spoke-to-hub-gw-2 ike-policy ike-policy-2
set security ike gateway spoke-to-hub-gw-2 address 10.1.2.1
```

```

set security ike gateway spoke-to-hub-gw-2 local-identity distinguished-name
set security ike gateway spoke-to-hub-gw-2 remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw-2 external-interface fe-0/0/2.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy proposals ipsec-proposal
set security ipsec vpn spoke-to-hub-1 bind-interface st0.0
set security ipsec vpn spoke-to-hub-1 ike gateway spoke-to-hub-gw-1
set security ipsec vpn spoke-to-hub-1 ike ipsec-policy vpn-policy
set security ipsec vpn spoke-to-hub-1 establish-tunnels immediately
set security ipsec vpn spoke-to-hub-2 bind-interface st0.1
set security ipsec vpn spoke-to-hub-2 ike gateway spoke-to-hub-gw-2
set security ipsec vpn spoke-to-hub-2 ike ipsec-policy vpn-policy
set security ipsec vpn spoke-to-hub-2 establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces fe-0/0/2.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 1? ?????:

1. ???? ????.

[edit interfaces]

```

user@host# set fe-0/0/1 unit 0 family inet address 10.2.2.1/30
user@host# set fe-0/0/2 unit 0 family inet address 10.3.3.1/30
user@host# set fe-0/0/4 unit 0 family inet address 10.60.60.1/24

```

```

user@host# set st0 unit 0 family inet address 10.10.10.2/24
user@host# set st0 unit 1 family inet address 10.20.20.2/24

```

## 2. `set policy-statement lan_nw`.

```

[edit policy-options]
user@host# set policy-statement lan_nw from interface fe-0/0/4.0
user@host# set policy-statement lan_nw then accept
[edit protocols bgp]
user@host# set group ibgp-1 type internal
user@host# set group ibgp-1 local-address 10.10.10.2
user@host# set group ibgp-1 export lan_nw
user@host# set group ibgp-1 neighbor 10.10.10.1
user@host# set group ibgp-2 type internal
user@host# set group ibgp-2 local-address 10.20.20.2
user@host# set group ibgp-2 export lan_nw
user@host# set group ibgp-2 neighbor 10.20.20.1
[edit routing-options]
user@host# set static route 10.1.1.0/30 next-hop 10.2.2.2
user@host# set static route 10.1.2.0/30 next-hop 10.3.3.2
user@host# set autonomous-system 65010

```

## 3. `set security ike proposal`.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy-1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike policy ike-policy-2]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local2
[edit security ike gateway spoke-to-hub-gw-1]
user@host# set ike-policy ike-policy-1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name

```

```

user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/1.0
[edit security ike gateway spoke-to-hub-gw-2]
user@host# set ike-policy ike-policy-2
user@host# set address 10.1.2.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/2.0

```

#### 4. `2?? ??? ?????.`

```

[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub-1]
user@host# set bind-interface st0.0
user@host# set ike gateway spoke-to-hub-gw-1
user@host# set ike ipsec-policy vpn-policy
user@host# set establish-tunnels immediately
[edit security ipsec vpn spoke-to-hub-2]
user@host# set bind-interface st0.1
user@host# set ike gateway spoke-to-hub-gw-2
user@host# set ike ipsec-policy vpn-policy
user@host# set establish-tunnels immediately

```

#### 5. `??? ?????.`

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/1.0
user@host# set interfaces st0.0
user@host# set interfaces fe-0/0/2.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all

```

```
[edit security policies]
user@host# set default-policy permit-all
```

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

```

[?] [?][?][?], show policy-options,, show routing-optionssh show protocols, show security ike, show security ipsec, show
security zones, [?] show security policiesshow security pki [?][?] [?][?] show interfaces[?][?] [?][?][?]. [?][?] [?][?] [?][?] [?][?][?]
[?][?], [?] [?][?] [?][?] [?][?] [?][?][?].

```

```
[edit]
user@host# show interfaces
fe-0/0/1 {
    unit 0 {
        family inet {
            address 10.2.2.1/30;
        }
    }
}

fe-0/0/2 {
    unit 0 {
        family inet {
            address 10.3.3.1/30;
        }
    }
}

fe-0/0/4 {
    unit 0 {
```

```

        family inet {
            address 10.60.60.1/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.10.10.2/24;
        }
    }
    unit 1 {
        family inet {
            address 10.20.20.2/24;
        }
    }
}
[edit]
user@host# show policy-options
policy-statement lan_nw {
    from interface fe-0/0/4.0;
    then accept;
}
[edit]
user@host# show protocols
bgp {
    group ibgp-1 {
        type internal;
        local-address 10.10.10.2;
        export lan_nw;
        neighbor 10.10.10.1;
    }
    group ibgp-2 {
        type internal;
        local-address 10.20.20.2;
        export lan_nw;
        neighbor 10.20.20.1;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.1.1.0/30 next-hop 10.2.2.2;

```

```

    route 10.1.2.0/30 next-hop 10.3.3.2;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy-1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
policy ike-policy-2 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local2;
    }
}
gateway spoke-to-hub-gw-1 {
    ike-policy ike-policy-1;
    address 10.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface fe-0/0/1.0;
}
gateway spoke-to-hub-gw-2 {
    ike-policy ike-policy-2;
    address 10.1.2.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface fe-0/0/2.0;
}
[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;

```

```

authentication-algorithm hmac-md5-96;
encryption-algorithm des-cbc;
}
policy vpn-policy {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn spoke-to-hub-1 {
    bind-interface st0.0;
    ike {
        gateway spoke-to-hub-gw-1;
        ipsec-policy vpn-policy;
    }
    establish-tunnels immediately;
}
vpn spoke-to-hub-2 {
    bind-interface st0.1;
    ike {
        gateway spoke-to-hub-gw-2;
        ipsec-policy vpn-policy;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/1.0;
        st0.0;
        fe-0/0/2.0;
        st0.1;
    }
}

```



```

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/4.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}

```

commit? commit?.

??

#### in this section

- [IKE\(Internet Key Exchange\) 1167 1168 | 1168](#)
- [IPsec 1167 1168 | 1168](#)
- [IPsec 1167 1168 | 1169](#)
- [BGP 1167 | 1170](#)



192.168.1.1 192.168.1.2 192.168.1.3.

**IKE(Internet Key Exchange) 192.168.1.1**

??

IKE(Internet Key Exchange) 192.168.1.1.

??

?? 192.168.1.1 show security ike security-associations 192.168.1.2.

```
user@host> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|---------|-------|------------------|------------------|------|----------------|
| 3733049 | UP    | bc9686796c2e52e9 | 1fbe46eee168f24e | Main | 10.2.2.1       |
| 3733048 | UP    | a88db7ed23ec5f6b | c88b81dff52617a5 | Main | 10.3.3.1       |

??

show security ike security-associations 192.168.1.1 IKE(Internet Key Exchange) 192.168.1.2 SA? 192.168.1.2. SA? 192.168.1.2. 192.168.1.2 192.168.1.2 192.168.1.2. 192.168.1.2 IKE(Internet Key Exchange) 192.168.1.2 192.168.1.2. 192.168.1.2 192.168.1.2. 192.168.1.2 192.168.1.2.

**IPsec 292.168.1.1**

??

IPsec 292.168.1.1.

??

?? ???? security ipsec security-associations ??? ?????.

```

user@host> security ipsec security-associations
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway
<268173315 ESP:des/ md5 93cfb417 1152/ unlim -   root 500    10.2.2.1
>268173315 ESP:des/ md5 101de6f7 1152/ unlim -   root 500    10.2.2.1
<268173313 ESP:des/ md5 272e29c0 1320/ unlim -   root 500    10.3.3.1
>268173313 ESP:des/ md5 a3bf8fad 1320/ unlim -   root 500    10.3.3.1

```

??

show security ipsec security-associations ??? ? IKE 2?? SA? ?????. SA? ????? ?? ?? ??, 2?? ??? ??? ?  
 ?????. ????? IKE(Internet Key Exchange) ?? ?? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?  
 ??.

**IPsec ?? ? ?? ??**

??

IPsec ?? ? ???? ?????.

??

?? ???? show security ipsec next-hop-tunnels ??? ?????.

```

user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface  IPSec VPN name      Flag    IKE-
ID                XAUTH username
10.10.10.2        st0.0      hub-to-spoke-vpn-1   Auto    C=IN, DC=example.net,
ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
10.20.20.2        st0.1      hub-to-spoke-vpn-2   Auto    C=IN, DC=example.net,
ST=KA, L=Mysore, O=example, OU=SBU, CN=spoke1_backup

```

??

?? ? ???? ??? ???? IP ?? st0 ??. next hop? ??? IPSec VPN ??? ????? ???.



```

Next hop type: Router
Next hop: 10.10.10.2 via st0.0
Next hop type: Router
Next hop: 10.20.20.2 via st0.1, selected
Protocol next hop: 10.10.10.2
Indirect next hop: 15c8000 262142
Protocol next hop: 10.20.20.2
Indirect next hop: 15c80e8 262143
State: <Act Int Ext>
Local AS: 65010 Peer AS: 65010
Age: 1d 12:16:25 Metric2: 0
Task: BGP_10.10.10.10.2+53120
Announcement bits (2): 0-KRT 3-Resolve tree 1
AS path: I
Accepted Multipath
Localpref: 100
Router ID: 10.207.36.182
BGP Preference: 170/-101
Next hop type: Indirect
Address: 0x15b8ac0
Next-hop reference count: 1
Source: 10.20.20.2
Next hop type: Router
Next hop: 10.20.20.2 via st0.1, selected
Protocol next hop: 10.20.20.2
Indirect next hop: 15c80e8 262143
State: <NotBest Int Ext>
Inactive reason: Not Best in its group - Update source
Local AS: 65010 Peer AS: 65010
Age: 1d 13:04:14 Metric2: 0
Task: BGP_10.20.20.20.2+50733
AS path: I
Accepted MultipathContrib
Localpref: 100
Router ID: 10.207.36.182

```

```

??? ?????? ?? ?? ??

```

```

??

```

```

???? ?? ??? ??? ?????? ??????? ???????.

```

??

```
?? ???? show route forwarding-table matching 10.60.60.0 ??? ?????.
```

```

user@host> show route forwarding-table matching 60.60.60.0
Routing table: default.inet
Internet:
Destination          Type RtRef Next hop          Type Index NhRef Netif
10.60.60.0/24        user    0                ulst 262144      1
                    ulst 262142      2
                    10.10.10.2    ucst   572      3 st0.0
                    indr 262143      2
                    10.20.20.2    ucst   573      3 st0.1

```

## SEE ALSO

?? ?? IPsec VPN | 452

**[?]: iBGP [?] Active-Backup [??] [??] AutoVPN [?]**

in this section

- ?? ?? | 1172
- ?? | 1173
- ?? | 1177
- ?? | 1201

? ???? AutoVPN ??? ???? ?? ?? ? ?? IPsec VPN ??? ?????? ? ???? ???? ???? ???? VPN ??? ?  
? ???? ????? iBGP? ??????, ?? ?? ?? ???? ???? ??: "iBGP" ??? 1067? ???? ?? AutoVPN ??.

?? ??

**[?] [??] [???] [???] [?] [????] ?? [???] ??? [???].**

- AutoVPN       SRX

- AutoVPN [?] [?] [?] [?] Junos OS [?] [?] 12.1X44-D10 [?]

□□□□ □□:

- `?? ???? ?? ???? ???? ? ?? ??(CA)? ???? ???? ??(?: ?? ?? ??)? ?????.`

[illegible]

??

in this section

● ???? | 1175

? ???? ? ?? IPsec VPN ??? ?? AutoVPN ??? ????? ??? ?? ???.

```
[?] [?][?][?] [?] [?] [?][?] SCEP([?] [?][?] [?] [?][?][?])? [?][?][?] [?] [?][?][?] [?][?] [?][?][?] [?][?][?], [?][?][?] [?] IPsec VPN [?][?] [?] [?] [?] [?][?] [?][?][?], [?][?][?] [?][?] [?] [?][?][?] [?] [?] [?](DN)? OU([?] [?] [?] [?]) [?] "SLT"? [?][?][?] [?][?][?], [?][?] OU [?][?] [?] "SLT"? [?][?][?] [?] IKE ID? [?][?][?][?], [?][?][?] [?] [?] [?][?][?][?] DN? OU [?] "SBU"? [?][?][?] [?][?][?], [?][?] OU [?][?] [?] "SBU"? [?][?][?] [?] IKE ID? [?][?][?][?].
```

???? ? IPsec VPN ??? ???? ???? ???? ? ???? ?????. AutoVPN ?? ? ???? ???? 1?? ? 2?? IKE ?? ??  
 ? ??? ? ???? ???? ? 132 ???? 1173 ?(?) ? ??? ???? ???? ??????.

### 132: AutoVPN iBGP Active-Backup 1 2

|                                       |             |
|---------------------------------------|-------------|
| ??                                    | ??          |
| <i>IKE(Internet Key Exchange) ??:</i> |             |
| ?? ??                                 | RSA ?? ??   |
| DH(Diffie-Hellman) ??                 | 2           |
| ?? ???? ?                             | SHA-1       |
| ??? ???? ?                            | AES 128 CBC |

**132: AutoVPN iBGP Active-Backup 1 2 (Continued)**

*IKE(Internet Key Exchange) [?]:*

|    |     |
|----|-----|
| ?? | ??? |
|----|-----|

*IPsec* ??:

|           |             |
|-----------|-------------|
| ???       | ESP         |
| ?? ?????  | HMAC MD5 96 |
| ??? ????? | DES CBC     |

*IPsec* **??**:

|                                                                                                                  |    |
|------------------------------------------------------------------------------------------------------------------|----|
| PFS(Perfect Forward Secrecy)  | 14 |
|------------------------------------------------------------------------------------------------------------------|----|

?? ???? ???? ?? ??(CA)? ?????.

Junos OS? ?? ??? ??? ??? ???.

133 1174 1111 1111 1111 1111 1111 1111.

### 133: 133.133.133.133 133.133 AutoVPN IBGP Active-Backup 133.133

|    |    |      |
|----|----|------|
| ?? | ?? | ?? 1 |
|----|----|------|

*IKE(Internet Key Exchange) ???????:*

|          |                                  |                                                     |
|----------|----------------------------------|-----------------------------------------------------|
| ?? IP ?? | ??-??-GW-1: ??<br>??-??-GW-2: ?? | ??? ? ??-GW-1: 1 0.1.1.1<br>??? ? ??-GW-2: 10.1.2.1 |
|----------|----------------------------------|-----------------------------------------------------|



### 133: 11.11.11 12.12 AutoVPN IBGP Active-Backup 11.11 (Continued)

|                                  |                                                                                                             |                                                                                                                             |
|----------------------------------|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| ??                               | ??                                                                                                          | ?? 1                                                                                                                        |
| ?? IKE(Internet Key Exchange) ID | <p>??-??-GW-1: OU ?? SLT ? ? ? ? ? ? ? ?<br/>? DN</p> <p>??-??-GW-2: OU ?? SBU ? ? ? ? ? ? ? ?<br/>? DN</p> | <p>?? ? ??-GW-1: ?? ? ? ? ? DNDN on the hub's certificate</p> <p>?? ? ??-GW-2: ?? ? ? ? ? DNDN on the hub's certificate</p> |
| ?? IKE(Internet Key Exchange) ID | ?? ? ? ? ? DNDN on the hub's certificate                                                                    | ?? ? ? ? ? DN                                                                                                               |
| ?? ? ? ? ? ? ?                   | <p>??-??-GW-1: ge-0/0/1.0</p> <p>??-??-GW-2: ge-0/0/2.0</p>                                                 | <p>?? ? ??-GW-1: ?-0/0/1.0</p> <p>?? ? ??-GW-2: ?-0/0/2.0</p>                                                               |

*VPN:*

|     |                                |                            |
|-----|--------------------------------|----------------------------|
| ??? | 1: st0.0<br>2: st0.1           | 1: st0.0<br>2: st0.1       |
| VPN | 1: ge-0/0/1.0<br>2: ge-0/0/2.0 | 1: 10.1.1.1<br>2: 10.1.2.1 |
|     |                                |                            |

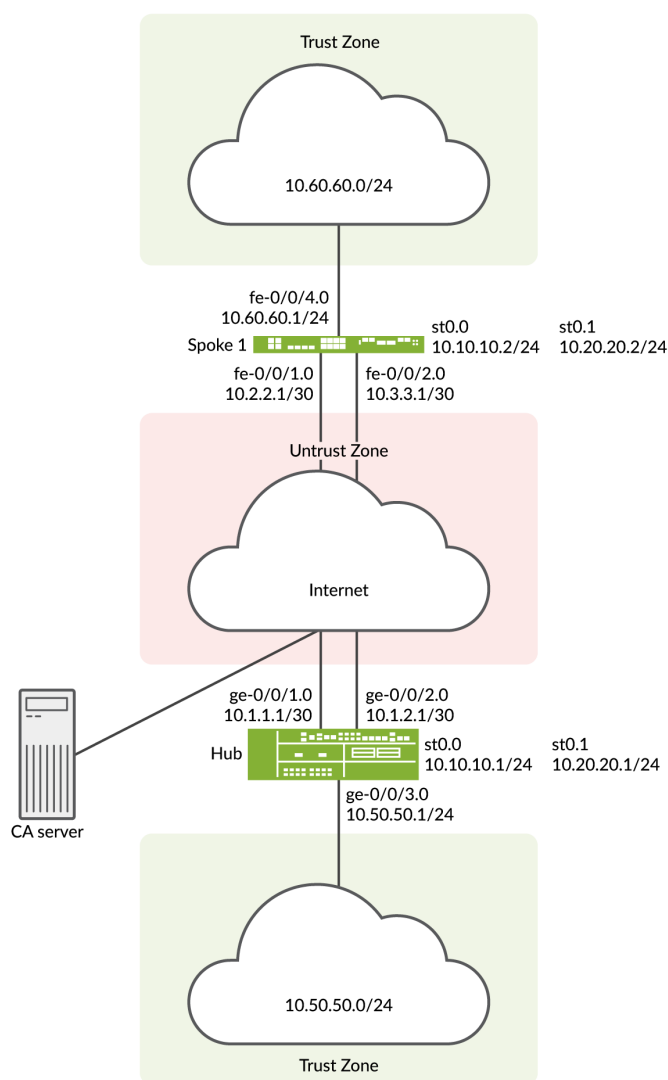
?? ???? ? ? ? ? VPN ? ? ? ? ?.

? ???? ?? ????? ???? ? ? ???? ? ? ?????. ?? ??? ? ? ? ? ???? ? ? ???? ???? ?????.

□□□□

66 1176 AutoVPN SRX

## 66: iBGP Active-Backup AutoVPN



1 IPsec VPN, iBGP, 10.60.60.0/24  
 st0.0, 1 st0.0, st0.1

VPN [redacted] [redacted] [redacted] [redacted]. [redacted] [redacted] [redacted] [redacted] [redacted](?: [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]) [redacted] [redacted] [redacted] [redacted]  
10.60.60.0/24[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

[SCEP? ???? ? ? ? ? ? ? ? ? Enroll Device Certificates with SCEP | 1177](#)  
[? ? ? ? | 1182](#)  
[? ? ? ? ? 1 | 1192](#)

?? ???? ?? ? ??? ????? SCEP(Simple Certificate Enrollment Protocol) ???? CA ? ? ????  
 ??? ????.

???

1. CA[?] [?][?][?][?][?].

[illegible]

????? ???? yes CA ???? ?????.

3. `? ???? ? ? ? ? ????.`

```
user@host> request security pki generate-key-pair certificate-id Local1
user@host> request security pki generate-key-pair certificate-id Local2
```

4. `?? ???? ????.`

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local2 domain-name example.net email hub_backup@example.net ip-address 10.1.2.1 subject
DC=example.net,CN=hub_backup,OU=SBU,O=example,L=Bengaluru,ST=KA,C=IN challenge-password
<password>
```

5. `?? ???? ????.`

```
user@host> show security pki local-certificate certificate-id Local1 detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2012 09:39
  Not after: 11- 6-2013 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
```

```

6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

```
user@host> show security pki local-certificate certificate-id Local2 detail
```

```

Certificate identifier: Local2
Certificate version: 3
Serial number: 505efdf900000000259a
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SBU, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub_backup, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SBU, CN=hub_backup
Alternate subject: "hub_backup@example.net", example.net, 10.1.2.1
Validity:
  Not before: 11- 9-2012 10:55
  Not after: 11- 9-2013 11:05
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d5:44:08:96:f6:77:05:e6:91:50:8a:8a:2a
  4e:95:43:1e:88:ea:43:7c:c5:ac:88:d7:a0:8d:b5:d9:3f:41:db:db
  44:34:1f:56:a5:38:4b:b2:c5:85:f9:f1:bf:b2:7b:d4:b2:af:98:a0
  95:50:02:ad:f5:dd:4d:dc:67:85:dd:84:09:df:9c:68:a5:58:65:e7
  2c:72:cc:47:4b:d0:cc:4a:28:ca:09:db:ad:6e:5a:13:6c:e6:cc:f0
  29:ed:2b:2d:d1:38:38:bc:68:84:de:ae:86:39:c9:dd:06:d5:36:f0
  e6:2a:7b:46:4c:cd:a5:24:1c:e0:92:8d:ad:35:29:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:

```

```

98:96:2f:ff:ca:af:33:ee:d7:4c:c8:4f:f7:71:53:c0:5d:5f:c5:59 (sha1)
c9:87:e3:a4:5c:47:b5:aa:90:22:e3:06:b2:0b:e1:ea (md5)
Auto-re-enrollment:
Status: Disabled
Next trigger time: Timer not started

```

???

??? 1?? SCEP? ???? ???? ???? ?????:

1. CA? ?????.

```

[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit

```

2. CA ???? ????.

```

user@host> request security pki ca-certificate enroll ca-profile ca-profile1

```

????? ???? yes CA ???? ????.

3. ? ???? ? ? ? ? ? ? ? ?.

```

user@host> rrequest security pki generate-key-pair certificate-id Local1
user@host> request security pki generate-key-pair certificate-id Local2

```

4. ?? ???? ????.

```

user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local2 domain-name example.net email spoke1_backup@example.net ip-address 10.3.3.1
subject DC=example.net,CN=spoke1_backup,OU=SBU,O=example,L=Mysore,ST=KA,C=IN challenge-
password <password>

```

5. `?? ???? ?????`.

```

user@host> show security pki local-certificate certificate-id Local1 detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
Alternate subject: "spoke1@example.net", example.net, 10.2.2.1
Validity:
  Not before: 11- 6-2012 09:40
  Not after: 11- 6-2013 09:50
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d8:45:09:77:cd:36:9a:6f:58:44:18:91:db
  b0:c7:8a:ee:c8:d7:a6:d2:e2:e7:20:46:2b:26:1a:92:e2:4e:8a:ce
  c9:25:d9:74:a2:81:ad:ea:e0:38:a0:2f:2d:ab:a6:58:ac:88:35:f4
  90:01:08:33:33:75:2c:44:26:f8:25:18:97:96:e4:28:de:3b:35:f2
  4a:f5:92:b7:57:ae:73:4f:8e:56:71:ab:81:54:1d:75:88:77:13:64
  1b:6b:01:96:15:0a:1c:54:e3:db:f8:ec:ec:27:5b:86:39:c1:09:a1
  e4:24:1a:19:0d:14:2c:4b:94:a4:04:91:3f:cb:ef:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  b6:24:2a:0e:96:5d:8c:4a:11:f3:5a:24:89:7c:df:ea:d5:c0:80:56 (sha1)
  31:58:7f:15:bb:d4:66:b8:76:1a:42:4a:8a:16:b3:a9 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

user@host> show security pki local-certificate certificate-id Local2 detail

Certificate identifier: Local2
Certificate version: 3
Serial number: 506c3d0600000000259b

```

```

Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SBU, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1_backup, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SBU, CN=spoke1_backup
Alternate subject: "spoke1_backup@example.net", example.net, 10.3.3.1
Validity:
  Not before: 11- 9-2012 11:09
  Not after: 11- 9-2013 11:19
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:a7:02:b5:e2:cd:79:24:f8:97:a3:8d:4d:27
  8c:2b:dd:f1:57:72:4d:2b:6d:d5:95:0d:9c:1b:5c:e2:a4:b0:84:2e
  31:82:3c:91:08:a2:58:b9:30:4c:5f:a3:6b:e6:2b:9c:b1:42:dd:1c
  cd:a2:7a:84:ea:7b:a6:b7:9a:13:33:c6:27:2b:79:2a:b1:0c:fe:08
  4c:a7:35:fc:da:4f:df:1f:cf:f4:ba:bc:5a:05:06:63:92:41:b4:f2
  54:00:3f:ef:ff:41:e6:ca:74:10:56:f7:2b:5f:d3:1a:33:7e:49:74
  1c:42:cf:c2:23:ea:4b:8f:50:2c:eb:1c:a6:37:89:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  d6:7f:52:a3:b6:f8:ae:cb:70:3f:a9:79:ea:8a:da:9e:ba:83:e4:5f (sha1)
  76:0b:72:73:cf:51:ee:58:81:2d:f7:b4:e2:5c:f4:5c (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

```

?? ??? ??? OU(?? ?? ??) ? SLT Local1 ? SBU Local2???. ??? IKE(Internet Key Exchange) ??? ???? ???
?? ? OU=SBU ? ??????OU=SLT.

```

```

?? ??

```

```

CLI ?? ??

```

```

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```

```

set interfaces ge-0/0/1 unit 0 family inet address 10.1.1.1/30
set interfaces ge-0/0/2 unit 0 family inet address 10.1.2.1/30

```



```

set interfaces ge-0/0/3 unit 0 family inet address 10.50.50.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.1/24
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet address 10.20.20.1/24
set policy-options policy-statement lan_nw from interface ge-0/0/3.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp-1 type internal
set protocols bgp group ibgp-1 local-address 10.10.10.1
set protocols bgp group ibgp-1 export lan_nw
set protocols bgp group ibgp-1 cluster 10.2.3.4
set protocols bgp group ibgp-1 allow 10.10.10.0/24
set protocols bgp group ibgp-2 type internal
set protocols bgp group ibgp-2 local-address 10.20.20.1
set protocols bgp group ibgp-2 export lan_nw
set protocols bgp group ibgp-2 cluster 10.2.3.5
set protocols bgp group ibgp-2 allow 10.20.20.0/24
set routing-options static route 10.2.2.0/30 next-hop 10.1.1.2
set routing-options static route 10.3.3.0/30 next-hop 10.1.2.2
set routing-options autonomous-system 65010
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy-1 mode main
set security ike policy ike-policy-1 proposals ike-proposal
set security ike policy ike-policy-1 certificate local-certificate Local1
set security ike policy ike-policy-2 mode main
set security ike policy ike-policy-2 proposals ike-proposal
set security ike policy ike-policy-2 certificate local-certificate Local2
set security ike gateway hub-to-spoke-gw-1 ike-policy ike-policy-1
set security ike gateway hub-to-spoke-gw-1 dynamic distinguished-name wildcard OU=SLT
set security ike gateway hub-to-spoke-gw-1 dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw-1 local-identity distinguished-name
set security ike gateway hub-to-spoke-gw-1 external-interface ge-0/0/1.0
set security ike gateway hub-to-spoke-gw-2 ike-policy ike-policy-2
set security ike gateway hub-to-spoke-gw-2 dynamic distinguished-name wildcard OU=SBU
set security ike gateway hub-to-spoke-gw-2 dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw-2 local-identity distinguished-name
set security ike gateway hub-to-spoke-gw-2 external-interface ge-0/0/2.0
set security ipsec vpn-monitor-options interval 5
set security ipsec vpn-monitor-options threshold 2
set security ipsec proposal ipsec-proposal protocol esp

```

```

set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn-1 bind-interface st0.0
set security ipsec vpn hub-to-spoke-vpn-1 vpn-monitor source-interface ge-0/0/1.0
set security ipsec vpn hub-to-spoke-vpn-1 ike gateway hub-to-spoke-gw-1
set security ipsec vpn hub-to-spoke-vpn-1 ike ipsec-policy vpn-policy
set security ipsec vpn hub-to-spoke-vpn-2 bind-interface st0.1
set security ipsec vpn hub-to-spoke-vpn-2 vpn-monitor source-interface ge-0/0/2.0
set security ipsec vpn hub-to-spoke-vpn-2 ike gateway hub-to-spoke-gw-2
set security ipsec vpn hub-to-spoke-vpn-2 ike ipsec-policy vpn-policy
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces ge-0/0/2.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? ???? ???? ????.

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.1.1.1/30
user@host# set ge-0/0/2 unit 0 family inet address 10.1.2.1/30
user@host# set ge-0/0/3 unit 0 family inet address 10.50.50.1/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.1/24

```

```

user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet address 10.20.20.1/24

```

## 2. `set policy-statement lan_nw`.

```

[edit policy-options]
user@host# set policy-statement lan_nw from interface ge-0/0/3.0
user@host# set policy-statement lan_nw then accept
[edit protocols bgp]
user@host# set group ibgp-1 type internal
user@host# set group ibgp-1 local-address 10.10.10.1
user@host# set group ibgp-1 export lan_nw
user@host# set group ibgp-1 cluster 10.2.3.4
user@host# set group ibgp-1 allow 10.10.10.0/24
user@host# set group ibgp-2 type internal
user@host# set group ibgp-2 local-address 10.20.20.1
user@host# set group ibgp-2 export lan_nw
user@host# set group ibgp-2 cluster 10.2.3.5
user@host# set group ibgp-2 allow 10.20.20.0/24
[edit routing-options]
user@host# set static route 10.2.2.0/30 next-hop 10.1.1.2
user@host# set static route 10.3.3.0/30 next-hop 10.1.2.2
user@host# set autonomous-system 65010

```

## 3. `set security ike proposal`.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy-1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike policy ike-policy-2]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local2
[edit security ike gateway hub-to-spoke-gw-1]
user@host# set ike-policy ike-policy-1

```

```

user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/1.0
[edit security ike gateway hub-to-spoke-gw-2]
user@host# set ike-policy ike-policy-2
user@host# set dynamic distinguished-name wildcard OU=SBU
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/2.0

```

#### 4. `vpn monitor`.

```

[edit security ipsec vpn-monitor]
user@host# set options interval 5
user@host# set options threshold 2
[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn hub-to-spoke-vpn-1]
user@host# set bind-interface st0.0
user@host# set vpn-monitor source-interface ge-0/0/1.0
user@host# set ike gateway hub-to-spoke-gw-1
user@host# set ike ipsec-policy vpn-policy
[edit security ipsec vpn hub-to-spoke-vpn-2]
user@host# set bind-interface st0.1
user@host# set vpn-monitor source-interface ge-0/0/2.0
user@host# set ike gateway hub-to-spoke-gw-2
user@host# set ike ipsec-policy vpn-policy

```

#### 5. `zones security-zone untrust`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.0
user@host# set interfaces ge-0/0/1.0

```

```
user@host# set interfaces ge-0/0/2.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/3.0
```

**6.**                     .

```
[edit security policies]
user@host# set default-policy permit-all
```

**7.** CA [ ][ ][ ][ ] [ ][ ][ ][ ].

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

??

```

[?] [?][?][?], show policy-options,, show routing-optionsshow protocols, show security ike, show security ipsec, show
security zones, [?] show security policiesshow security pki [?][?] [?][?][?] show interfaces[?][?] [?][?][?]. [?][?] [?][?] [?][?] [?][?][?]
[?][?], [?] [?] [?] [?][?] [?][?][?] [?][?][?].

```

```
[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet {
            address 10.1.1.1/30;
        }
    }
}

ge-0/0/2 {
    unit 0 {
        family inet {
            address 10.1.2.1/30;
        }
    }
}
```

```

    }
}
ge-0/0/3 {
    unit 0 {
        family inet {
            address 10.50.50.1/24;
        }
    }
}
st0 {
    unit 0 {
        multipoint;
        family inet {
            address 10.10.10.1/24;
        }
    }
    unit 1 {
        multipoint;
        family inet {
            address 10.20.20.1/24;
        }
    }
}
}
[edit]
user@host# show policy-options
policy-statement lan_nw {
    from interface ge-0/0/3.0;
    then accept;
}
[edit]
user@host# show protocols
bgp {
    group ibgp-1 {
        type internal;
        local-address 10.10.10.1;
        export lan_nw;
        cluster 10.2.3.4;
        allow 10.10.10.0/24;
    }
    group ibgp-2 {
        type internal;
        local-address 10.20.20.1;
        export lan_nw;
    }
}

```

```

        cluster 10.2.3.5;
        allow 10.20.20.0/24;
    }
}
[edit]
user@host# show routing-options
static {
    route 10.2.2.0/30 next-hop 10.1.1.2;
    route 10.3.3.0/30 next-hop 10.1.2.2;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy-1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
policy ike-policy-2 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local2;
    }
}
gateway hub-to-spoke-gw-1 {
    ike-policy ike-policy-1;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/1.0;
}

```

```

}
gateway hub-to-spoke-gw-2 {
    ike-policy ike-policy-2;
    dynamic {
        distinguished-name {
            wildcard OU=SBU;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/2.0;
}
[edit]
user@host# show security ipsec
vpn-monitor-options {
    interval 5;
    threshold 2;
}
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy vpn-policy {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn hub-to-spoke-vpn-1 {
    bind-interface st0.0;
    vpn-monitor {
        source-interface ge-0/0/1.0;
    }
    ike {
        gateway hub-to-spoke-gw-1;
        ipsec-policy vpn-policy;
    }
}
vpn hub-to-spoke-vpn-2 {
    bind-interface st0.1;
    vpn-monitor {
        source-interface ge-0/0/2.0;
    }
}

```



```

    }
    ike {
        gateway hub-to-spoke-gw-2;
        ipsec-policy vpn-policy;
    }
}

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.0;
        ge-0/0/1.0;
        ge-0/0/2.0;
        st0.1;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

[edit]

```

```

user@host# show security pki
ca-profile ca-profile1 {
  ca-identity ca-profile1;
  enrollment {
    url http://pc4/certsrv/mscep/mscep.dll;
  }
  revocation-check {
    disable;
  }
}

```

```

?? ?? ?? ?? commit?(?) ?????.

```

```

??? ?? 1

```

**CLI ?? ??**

```

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

```

set interfaces fe-0/0/1 unit 0 family inet address 10.2.2.1/30
set interfaces fe-0/0/2 unit 0 family inet address 10.3.3.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.60.60.1/24
set interfaces st0 unit 0 family inet address 10.10.10.2/24
set interfaces st0 unit 1 family inet address 10.20.20.2/24
set policy-options policy-statement default_route from protocol static
set policy-options policy-statement default_route from route-filter 0.0.0.0/0 exact
set policy-options policy-statement default_route then accept
set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp-1 type internal
set protocols bgp group ibgp-1 local-address 10.10.10.2
set protocols bgp group ibgp-1 export lan_nw
set protocols bgp group ibgp-1 neighbor 10.10.10.1
set protocols bgp group ibgp-2 type internal
set protocols bgp group ibgp-2 local-address 10.20.20.2
set protocols bgp group ibgp-2 export default_route
set protocols bgp group ibgp-2 neighbor 10.20.20.1
set routing-options static route 10.1.1.0/30 next-hop 10.2.2.2
set routing-options static route 10.1.2.0/30 next-hop 10.3.3.2
set routing-options static route 0.0.0.0/0 next-hop st0.1
set routing-options autonomous-system 65010

```

```

set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy-1 mode main
set security ike policy ike-policy-1 proposals ike-proposal
set security ike policy ike-policy-1 certificate local-certificate Local1
set security ike policy ike-policy-2 mode main
set security ike policy ike-policy-2 proposals ike-proposal
set security ike policy ike-policy-2 certificate local-certificate Local2
set security ike gateway spoke-to-hub-gw-1 ike-policy ike-policy-1
set security ike gateway spoke-to-hub-gw-1 address 10.1.1.1
set security ike gateway spoke-to-hub-gw-1 local-identity distinguished-name
set security ike gateway spoke-to-hub-gw-1 remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw-1 external-interface fe-0/0/1.0
set security ike gateway spoke-to-hub-gw-2 ike-policy ike-policy-2
set security ike gateway spoke-to-hub-gw-2 address 10.1.2.1
set security ike gateway spoke-to-hub-gw-2 local-identity distinguished-name
set security ike gateway spoke-to-hub-gw-2 remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw-2 external-interface fe-0/0/2.0
set security ipsec vpn-monitor-options interval 5
set security ipsec vpn-monitor-options threshold 2
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy proposals ipsec-proposal
set security ipsec vpn spoke-to-hub-1 bind-interface st0.0
set security ipsec vpn spoke-to-hub-1 vpn-monitor destination-ip 10.1.1.1
set security ipsec vpn spoke-to-hub-1 ike gateway spoke-to-hub-gw-1
set security ipsec vpn spoke-to-hub-1 ike ipsec-policy vpn-policy
set security ipsec vpn spoke-to-hub-1 establish-tunnels immediately
set security ipsec vpn spoke-to-hub-2 bind-interface st0.1
set security ipsec vpn spoke-to-hub-2 vpn-monitor destination-ip 10.1.2.1
set security ipsec vpn spoke-to-hub-2 ike gateway spoke-to-hub-gw-2
set security ipsec vpn spoke-to-hub-2 ike ipsec-policy vpn-policy
set security ipsec vpn spoke-to-hub-2 establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces fe-0/0/2.0
set security zones security-zone untrust interfaces st0.1

```

```

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 1? ?????:

1. ???? ????.

```

[edit interfaces]
user@host# set fe-0/0/1 unit 0 family inet address 10.2.2.1/30
user@host# set fe-0/0/2 unit 0 family inet address 10.3.3.1/30
user@host# set fe-0/0/4 unit 0 family inet address 10.60.60.1/24
user@host# set st0 unit 0 family inet address 10.10.10.2/24
user@host# set st0 unit 1 family inet address 10.20.20.2/24

```

2. ??? ???? ????.

```

[edit policy-options]
user@host# set policy-statement default_route from protocol static
user@host# set policy-statement default_route from route-filter 0.0.0.0/0 exact
user@host# set policy-statement default_route then accept
user@host# set policy-statement lan_nw from interface fe-0/0/4.0
user@host# set policy-statement lan_nw then accept
[edit protocols bgp]
user@host# set group ibgp-1 type internal
user@host# set group ibgp-1 local-address 10.10.10.2
user@host# set group ibgp-1 export lan_nw
user@host# set group ibgp-1 neighbor 10.10.10.1
user@host# set group ibgp-2 type internal
user@host# set group ibgp-2 local-address 10.20.20.2
user@host# set group ibgp-2 export default_route
user@host# set group ibgp-2 neighbor 10.20.20.1
[edit routing-options]

```

```

user@host# set static route 10.1.1.0/30 next-hop 10.2.2.2
user@host# set static route 10.1.2.0/30 next-hop 10.3.3.2
user@host# set static route 0.0.0.0/0 next-hop st0.1
user@host# set autonomous-system 65010

```

### 3. 1?? 2?? 3????.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy-1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike policy ike-policy-2]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local2
[edit security ike gateway spoke-to-hub-gw-1]
user@host# set ike-policy ike-policy-1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/1.0
[edit security ike gateway spoke-to-hub-gw-2]
user@host# set ike-policy ike-policy-2
user@host# set address 10.1.2.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/2.0

```

### 4. 2?? 3?? 4????.

```

[edit security ipsec vpn-monitor]
user@host# set options interval 5
user@host# set options threshold 2
[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96

```

```

user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub-1]
user@host# set bind-interface st0.0
user@host# set vpn-monitor destination-ip 10.1.1.1
user@host# set ike gateway spoke-to-hub-gw-1
user@host# set ike ipsec-policy vpn-policy
user@host# set establish-tunnels immediately
[edit security ipsec vpn spoke-to-hub-2]
user@host# set bind-interface st0.1
user@host# set vpn-monitor destination-ip 10.1.2.1
user@host# set ike gateway spoke-to-hub-gw-2
user@host# set ike ipsec-policy vpn-policy
user@host# set establish-tunnels immediately

```

#### 5. `set security ipsec`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/1.0
user@host# set interfaces st0.0
user@host# set interfaces fe-0/0/2.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/4.0

```

#### 6. `set security ipsec`.

```

[edit security policies]
user@host# set default-policy permit-all

```

#### 7. CA `set security pki`.

```

[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1

```

```
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

??

```

[?] [?][?][?], show policy-options, , show routing-optionsshow protocols, show security ike, show security ipsec, show
security zones, [?] show security policiesshow security pki [?][?] [?][?] show interfaces[?][?] [?][?][?]. [?][?] [?][?] [?][?] [?][?][?]
[?][?], [?] [?][?] [?][?] [?][?][?] [?][?][?].

```

```
[edit]
user@host# show interfaces
fe-0/0/1 {
    unit 0 {
        family inet {
            address 10.2.2.1/30;
        }
    }
}
fe-0/0/2 {
    unit 0 {
        family inet {
            address 10.3.3.1/30;
        }
    }
}
fe-0/0/4 {
    unit 0 {
        family inet {
            address 10.60.60.1/24;
        }
    }
}
st0 {
    unit 0 {
        family inet {
            address 10.10.10.2/24;
        }
    }
    unit 1 {
        family inet {
            address 10.20.20.2/24;
        }
    }
}
```

```

    }
  }
}
[edit]
user@host# show policy-options
policy-statement default_route {
  from {
    protocol static;
    route-filter 0.0.0.0/0 exact;
  }
  then accept;
}
policy-statement lan_nw {
  from interface fe-0/0/4.0;
  then accept;
}
[edit]
user@host# show protocols
bgp {
  group ibgp-1 {
    type internal;
    local-address 10.10.10.2;
    export lan_nw;
    neighbor 10.10.10.1;
  }
  group ibgp-2 {
    type internal;
    local-address 10.20.20.2;
    export default_route;
    neighbor 10.20.20.1;
  }
}
[edit]
user@host# show routing-options
static {
  route 10.1.1.0/30 next-hop 10.2.2.2;
  route 10.1.2.0/30 next-hop 10.3.3.2;
  route 0.0.0.0/0 next-hop st0.1;
}
autonomous-system 65010;
[edit]
user@host# show security ike
proposal ike-proposal {

```



```

authentication-method rsa-signatures;
dh-group group2;
authentication-algorithm sha1;
encryption-algorithm aes-128-cbc;
}

policy ike-policy-1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}

policy ike-policy-2 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local2;
    }
}

gateway spoke-to-hub-gw-1 {
    ike-policy ike-policy-1;
    address 10.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface fe-0/0/1.0;
}

gateway spoke-to-hub-gw-2 {
    ike-policy ike-policy-2;
    address 10.1.2.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface fe-0/0/2.0;
}

[edit]
user@host# show security ipsec
vpn-monitor-options {
    interval 5;
    threshold 2;
}

proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;

```

```

}
policy vpn-policy {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn spoke-to-hub-1 {
    bind-interface st0.0;
    vpn-monitor {
        destination-ip 10.1.1.1;
    }
    ike {
        gateway spoke-to-hub-gw-1;
        ipsec-policy vpn-policy;
    }
    establish-tunnels immediately;
}
vpn spoke-to-hub-2 {
    bind-interface st0.1;
    vpn-monitor {
        destination-ip 10.1.2.1;
    }
    ike {
        gateway spoke-to-hub-gw-2;
        ipsec-policy vpn-policy;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/1.0;
        st0.0;
    }
}

```

```

        fe-0/0/2.0;
        st0.1;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/4.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}

```

commit? (y) [enter].

??

#### in this section



IKE(Internet Key Exchange) 1?? ?? ??(?? ?? ?? ??) | 1202

| Index | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|-------|-------|------------------|------------------|------|----------------|
|-------|-------|------------------|------------------|------|----------------|





??

?? ???? show route 10.60.60.0 ??? ?????.

```
user@host> show route 10.60.60.0
inet.0: 48 destinations, 48 routes (47 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

60.60.60.0/24      *[BGP/170] 00:01:11, localpref 100
                   AS path: I
                   > to 10.10.10.2 via st0.0
```

?? ???? show route 0.0.0.0 ??? ?????.

```
user@host> show route 0.0.0.0
inet.0: 48 destinations, 48 routes (47 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 00:04:55, localpref 100
                   AS path: I
                   > to 10.20.20.2 via st0.1
```

**IKE(Internet Key Exchange) 1?? ?? ??(?? ??? ????)**

??

?? ??? ???? IKE(Internet Key Exchange) 1?? ??? ?????.

??

?? ???? show security ike security-associations ??? ?????.

```
user@host> show security ike security-associations

Index   State Initiator cookie Responder cookie Mode Remote Address
-----
3733075 UP    d4f51c28c0a82101 05b125993a864d3c Main 10.3.3.1
3733076 UP    d53c8a0b7d4c319b c23c5f7a26388247 Main 10.2.2.1
```

??

```
show security ike security-associations ??? ? ? IKE(Internet Key Exchange) 1? SA? ?????. SA? ???? ?
?? ??, 1?? ???? ???? ? ?????. ???? IKE(Internet Key Exchange) ?? ?? ? ? ? ???? ???? ?????. 1?? ?? ?
???? ? ? ???? ???? ????.
```

**IPsec 2?? ? ? ?(?? ? ? ?)**

??

```
?? ???? ???? IPsec 2?? ???? ?????.
```

??

```
?? ???? security ipsec security-associations ??? ?????.
```

```
user@host> security ipsec security-associations
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway
<268173313 ESP:des/ md5 7c6ffca3 3156/ unlim U   root 500    10.3.3.1
>268173313 ESP:des/ md5 33bf6f2f 3156/ unlim U   root 500    10.3.3.1
```

??

```
show security ipsec security-associations ??? ? ? IKE 2?? SA? ?????. SA? ???? ? ? ? ? ? , 2?? ???? ? ?
?????. ???? IKE(Internet Key Exchange) ?? ?? ? ? ? ???? ???? ?????. 2?? ? ? ? ? ? ? ? ? ? ? ? ? ?
??.
```

**IPsec ?? ? ? ? ?(?? ???? ????)**

??

```
IPsec ?? ? ???? ?????.
```

??

```
?? ???? show security ipsec next-hop-tunnels ??? ?????.
```

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface  IPSec VPN name  Flag  IKE-
```



|            |                |                    |      |                                                                               |
|------------|----------------|--------------------|------|-------------------------------------------------------------------------------|
| ID         | XAUTH username |                    |      |                                                                               |
| 10.20.20.2 | st0.1          | hub-to-spoke-vpn-2 | Auto | C=IN, DC=example.net,<br>ST=KA, L=Mysore, O=example, OU=SBU, CN=spoke1_backup |

??

?? ? ?????? ???? ???? st0 IP ?????, ?? ?? ???? IPSec VPN ??( ? ? ? ? VPN ?? ) ? ????? ???.

**BGP** ??(?? ?? ??)

??

?? ??? ?????? ? BGP? ??? ?????? IP ??? st0 ????? ????.

??

?? ????? **show bgp summary** ??? ?????.

```
user@host> show bgp summary
Groups: 2 Peers: 1 Down peers: 0
Unconfigured peers: 1
Table          Tot Paths  Act Paths Suppressed    History  Damp State   Pending
inet.0          1          1          0          0          0          0
Peer           AS        InPkt    OutPkt    OutQ   Flaps  Last Up/Dwn  State|#Active/
Received/Accepted/Damped...
10.20.20.2      10        20       24        0        0        7:24
1/1/1/0         0/0/0/0
```

??? ?? ??(?? ?? ???)

??

?? ??? ?????? ? ?????? ?? ??? ?????? ??????. 10.60.60.0/24? ?? ??? ? ???? st0.1 ?????? ? ????.

??

?? ???? show route 10.60.60.0 ??? ?????.

```
user@host> show route 60.60.60.0
inet.0: 46 destinations, 46 routes (45 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 00:07:41, localpref 100
                   AS path: I
                   > to 10.20.20.2 via st0.1
```

?? ???? show route 0.0.0.0 ??? ?????.

```
user@host> show route 0.0.0.0
inet.0: 46 destinations, 46 routes (45 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

0.0.0.0/0          *[BGP/170] 00:07:47, localpref 100
                   AS path: I
                   > to 10.20.20.2 via st0.1
```

SEE ALSO

| [?? ?? IPsec VPN](#) | [452](#)

**?: OSPF? ??? ?? AutoVPN ??**

in this section

[?? ??](#) | [1209](#)

[??](#) | [1209](#)

[??](#) | [1213](#)

[??](#) | [1238](#)

|                                       |             |
|---------------------------------------|-------------|
| ??                                    | ??          |
| <i>IKE(Internet Key Exchange)</i> ??: |             |
| ?? ??                                 | RSA ??? ??? |

134: AutoVPN
OSPF
1
2
(Continued)

|                    |             |
|--------------------|-------------|
|                    |             |
| DH(Diffie-Hellman) | 2           |
|                    | SHA-1       |
|                    | AES 128 CBC |

IKE(Internet Key Exchange):

|  |  |
|--|--|
|  |  |
|--|--|

IPsec:

|  |             |
|--|-------------|
|  | ESP         |
|  | HMAC MD5 96 |
|  | DES CBC     |

IPsec:

|                              |    |
|------------------------------|----|
| PFS(Perfect Forward Secrecy) | 14 |
|------------------------------|----|

(CA)

Junos OS

135
1210

135:
AutoVPN
OSPF

|  |  |  |
|--|--|--|
|  |  |  |
|--|--|--|

IKE(Internet Key Exchange):

**? 135: ?? ? ?? ???? ?? AutoVPN ?? OSPF ?? (Continued)**

|                                  |                                                      |                                       |
|----------------------------------|------------------------------------------------------|---------------------------------------|
| ??                               | ??                                                   | ?? ???                                |
| ?? IP ??                         | ??                                                   | 1 0.1.1.1                             |
| ?? IKE(Internet Key Exchange) ID | OU(?? ?? ??) ??? ??? SLT ? ?? ??? ???<br>? DN(?? ??) | ?? ??? DNDN on the hub's certificate  |
| ?? IKE(Internet Key Exchange) ID | ?? ??? DNDN on the hub's certificate                 | ??? ??? DN                            |
| ?? ???                           | ge-0/0/1.0                                           | ??? 1: ?-0/0/1.0<br>??? 2: ge-0/0/1.0 |

*VPN:*

|           |          |        |
|-----------|----------|--------|
| ?? ???? ? | st0.0    | st0.0  |
| ?? ?      | (???? ?) | ?? ? ? |

**136** **1211** **(?)** **?** **?????** **??** **??** **??? ?????.**

**136: OSPF**

| ??            | ??? 1                      | ??? 2                     |
|---------------|----------------------------|---------------------------|
| st0.0 ?????   | 10.10.10.2/24              | 10.10.10.3/24             |
| ?? ???? ????? | fe-0.0/4.0: 100.60.60.1/24 | fe-0.0/4.0: 10.70.70.1/24 |
| ??? ?????     | fe-0/0/1.0: 10.2.2.1/30    | ge-0/0/1.0: 10.3.3.1/30   |

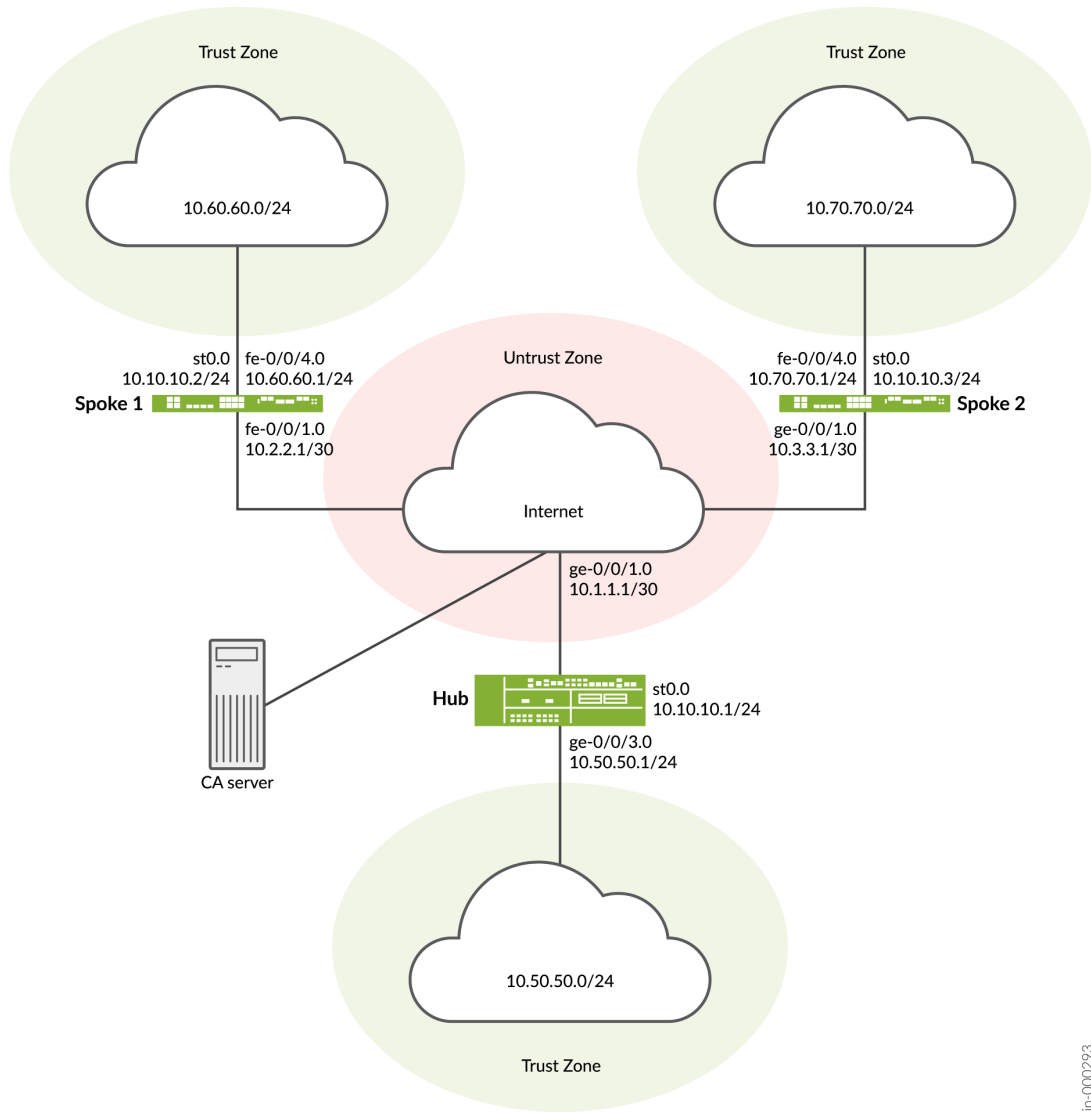
?? ???? ?? ??? ??? VPN ??? ?? ?????.

[illegible]

???

?? 67 ??? 1212 ?? ? ??? AutoVPN? ?? ??? SRX ??? ??? ? ? ???.

?? 67: OSPF? ??? ?? AutoVPN ??



jn-000293



3. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
```

5. `? ? ? ? ? ? ? ? ? ? ? ?`.

```
user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2012 09:39
  Not after: 11- 6-2013 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
  6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
```



```
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started
```

???

??? 1?? SCEP? ???? ???? ???? ?????:

### 1. CA? ?????.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

### 2. CA ???? ????.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

????? ???? yes CA ???? ????.

### 3. ? ???? ????.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

### 4. ?? ???? ????.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
```

**5.**           .

```

user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a7975f00000000258e
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Mysore, Common name: spoke1, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
Alternate subject: "spoke1@example.net", example.net, 10.2.2.1
Validity:
  Not before: 11- 6-2012 09:40
  Not after: 11- 6-2013 09:50
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:d8:45:09:77:cd:36:9a:6f:58:44:18:91:db
  b0:c7:8a:ee:c8:d7:a6:d2:e2:e7:20:46:2b:26:1a:92:e2:4e:8a:ce
  c9:25:d9:74:a2:81:ad:ea:e0:38:a0:2f:2d:ab:a6:58:ac:88:35:f4
  90:01:08:33:33:75:2c:44:26:f8:25:18:97:96:e4:28:de:3b:35:f2
  4a:f5:92:b7:57:ae:73:4f:8e:56:71:ab:81:54:1d:75:88:77:13:64
  1b:6b:01:96:15:0a:1c:54:e3:db:f8:ec:ec:27:5b:86:39:c1:09:a1
  e4:24:1a:19:0d:14:2c:4b:94:a4:04:91:3f:cb:ef:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  b6:24:2a:0e:96:5d:8c:4a:11:f3:5a:24:89:7c:df:ea:d5:c0:80:56 (sha1)
  31:58:7f:15:bb:d4:66:b8:76:1a:42:4a:8a:16:b3:a9 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

1. CA `?????`.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/
mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

2. CA `???? ?????`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
????? ???? yes CA ???? ????.
```

3. `? ??? ?????`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

4. `?? ???? ?????`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke2@example.net ip-address 10.3.3.1 subject
DC=example.net,CN=spoke2,OU=SLT,O=example,L=Tumkur,ST=KA,C=IN challenge-password <password>
```

5. `?? ???? ?????`.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
Serial number: 40bb71d400000000258f
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Tumkur, Common name: spoke2, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
```



```

set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway hub-to-spoke-gw ike-policy ike-policy1
set security ike gateway hub-to-spoke-gw dynamic distinguished-name wildcard OU=SLT
set security ike gateway hub-to-spoke-gw dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw local-identity distinguished-name
set security ike gateway hub-to-spoke-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn bind-interface st0.0
set security ipsec vpn hub-to-spoke-vpn ike gateway hub-to-spoke-gw
set security ipsec vpn hub-to-spoke-vpn ike ipsec-policy vpn-policy1
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ???? ???? ???? ???? ???? CLI ???? ???? ???? ????.

??? ???? ???? ????.

1. ???? ????.

[edit interfaces]

user@host# set ge-0/0/1 unit 0 family inet address 10.1.1.1/30

user@host# set ge-0/0/3 unit 0 family inet address 10.50.50.1/24

```

user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.1/24

```

## 2. `set area 0.0.0.0`.

```

[edit protocols ospf]
user@host# set area 0.0.0.0 interface st0.0 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.0 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/3.0
[edit routing-options]
user@host# set static route 2.2.2.0/30 next-hop 10.1.1.2
user@host# set static route 3.3.3.0/30 next-hop 10.1.1.2

```

## 3. `set authentication-method rsa-signatures`.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway hub-to-spoke-gw]
user@host# set ike-policy ike-policy1
user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/1.0

```

## 4. `set protocol esp`.

```

[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal

```

```
[edit security ipsec vpn hub-to-spoke-vpn]
user@host# set bind-interface st0.0
user@host# set ike gateway hub-to-spoke-gw
user@host# set ike ipsec-policy vpn-policy1
```

5.       .

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.0

[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/3.0
```

**6.**                     .

```
[edit security policies]
user@host# set default-policy permit-all
```

**7.** CA [?] [?] [?] [?] [?] [?] [?].

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

??

```

[?] [?] [?] [?], show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show
security policies[?] show security pki [?] [?] [?] [?] show interfaces[?] [?] [?] [?]. [?] [?] [?] [?] [?] [?], [?] [?] [?] [?] [?]
[?] [?] [?] [?] [?].

```

```
[edit]
user@host# show interfaces
ge-0/0/1 {
```

```

    unit 0 {
        family inet {
            address 10.1.1.1/30;
        }
    }
}

ge-0/0/3 {
    unit 0 {
        family inet {
            address 10.50.50.1/24;
        }
    }
}

st0 {
    unit 0 {
        multipoint;
        family inet {
            address 10.10.10.1/24;
        }
    }
}

[edit]
user@host# show protocols
ospf {
    area 0.0.0.0 {
        interface st0.0 {
            interface-type p2mp;
            dynamic-neighbors;
        }
        interface ge-0/0/3.0;
    }
}

[edit]
user@host# show routing-options
static {
    route 10.2.2.0/30 next-hop 10.1.1.2;
    route 10.3.3.0/30 next-hop 10.1.1.2;
}

[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
}

```



```

authentication-algorithm sha1;
encryption-algorithm aes-128-cbc;
}

policy ike-policy1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}

gateway hub-to-spoke-gw {
    ike-policy ike-policy1;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
        ike-user-type group-ike-id;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/1.0;
}

[edit]
user@host# show security ipsec
traceoptions {
    flag all;
}

proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}

policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}

vpn hub-to-spoke-vpn {
    bind-interface st0.0;
    ike {
        gateway hub-to-spoke-gw;
        ipsec-policy vpn-policy1;
    }
}

```

```

    }
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.0;
        ge-0/0/1.0;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/3.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {

```

**???** **??** **1**

```
? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? CLI ? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? ?.
```

```

set interfaces fe-0/0/1 unit 0 family inet address 10.2.2.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.60.60.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.2/24
set protocols ospf area 0.0.0.0 interface st0.0 interface-type p2mp
set protocols ospf area 0.0.0.0 interface st0.0 neighbor 10.10.10.1
set protocols ospf area 0.0.0.0 interface fe-0/0/4.0
set routing-options static route 10.1.1.0/30 next-hop 10.2.2.2
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 10.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface fe-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately

```

```

set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ??????.

??? 1? ??????:

1. ?????? ??????.

```

[edit interfaces]
user@host# set fe-0/0/1 unit 0 family inet address 10.2.2.1/30
user@host# set fe-0/0/4 unit 0 family inet address 10.60.60.1/24
user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.2/24

```

2. ??? ?????? ??????.

```

[edit protocols ospf]
user@host# set area 0.0.0.0 interface st0.0 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.0 neighbor 10.10.10.1
user@host# set area 0.0.0.0 interface fe-0/0/4.0
[edit routing-options]
user@host# set static route 10.1.1.0/30 next-hop 10.2.2.2

```

3. 1?? ??? ??????.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2

```

```

user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway spoke-to-hub-gw]
user@host# set ike-policy ike-policy1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface fe-0/0/1.0

```

#### 4. `set ipsec proposal`.

```

[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub]
user@host# set bind-interface st0.0
user@host# set ike gateway spoke-to-hub-gw
user@host# set ike ipsec-policy vpn-policy1
user@host# set establish-tunnels immediately

```

#### 5. `set host-inbound-traffic`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/1.0
user@host# set interfaces st0.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/4.0

```

6. `set default-policy permit-all`.

```
[edit security policies]
user@host# set default-policy permit-all
```

7. CA `ca-profile1`.

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

`show`

`show protocols`, `show security ike`, `show security ipsec`, `show security zones`, `show security policies`, `show security pki ca-profile1`, `show interfaces fe-0/0/1`, `show interfaces fe-0/0/4`, `show interfaces st0`.

```
[edit]
user@host# show interfaces
fe-0/0/1 {
  unit 0 {
    family inet {
      address 10.2.2.1/30;
    }
  }
}
fe-0/0/4 {
  unit 0 {
    family inet {
      address 10.60.60.1/24;
    }
  }
}
st0 {
  unit 0 {
    multipoint;
    family inet {
      address 10.10.10.2/24;
```

```

    }
  }
}
[edit]
user@host# show protocols
ospf {
  area 0.0.0.0 {
    interface st0.0 {
      interface-type p2mp;
      neighbor 10.10.10.1;
    }
    interface fe-0/0/4.0;
  }
}
[edit]
user@host# show routing-options
static {
  route 10.1.1.0/30 next-hop 10.2.2.2;
}
[edit]
user@host# show security ike
proposal ike-proposal {
  authentication-method rsa-signatures;
  dh-group group2;
  authentication-algorithm sha1;
  encryption-algorithm aes-128-cbc;
}
policy ike-policy1 {
  mode main;
  proposals ike-proposal;
  certificate {
    local-certificate Local1;
  }
}
gateway spoke-to-hub-gw {
  ike-policy ike-policy1;
  address 10.1.1.1;
  local-identity distinguished-name;
  remote-identity distinguished-name;
  external-interface fe-0/0/1.0;
}
[edit]
user@host# show security ipsec

```

```

proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}

policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}

vpn spoke-to-hub {
    bind-interface st0.0;
    ike {
        gateway spoke-to-hub-gw;
        ipsec-policy vpn-policy1;
    }
    establish-tunnels immediately;
}

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/1.0;
        st0.0;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
}

```



```
default-policy {
    permit-all;
}
```

```
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}
```

???

```
? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ?????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.
```

```
set interfaces ge-0/0/1 unit 0 family inet address 10.3.3.1/30
set interfaces fe-0/0/4 unit 0 family inet address 10.70.70.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.3/24
set protocols ospf area 0.0.0.0 interface st0.0 interface-type p2mp
set protocols ospf area 0.0.0.0 interface st0.0 neighbor 10.10.10.1
set protocols ospf area 0.0.0.0 interface fe-0/0/4.0
set routing-options static route 10.1.1.1/32 next-hop 10.3.3.2
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
```

```

set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 10.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI/ ??? ??? ?????.

??? 2? ?????:

1. ???? ????.

[edit interfaces]

user@host# set ge-0/0/1 unit 0 family inet address 10.3.3.1/30

user@host# set fe-0/0/4 unit 0 family inet address 10.70.70.1/24

```

user@host# set st0 unit 0 multipoint
user@host# set st0 unit 0 family inet address 10.10.10.3/24

```

## 2. `???` `?????` `??????`.

```

[edit protocols ospf]
user@host# set area 0.0.0.0 interface st0.0 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.0 neighbor 10.10.10.1
user@host# set area 0.0.0.0 interface fe-0/0/4.0
[edit routing-options]
user@host# set static route 10.1.1.1/32 next-hop 10.3.3.2

```

## 3. `1??` `???` `??????`.

```

[edit security ike proposal ike-proposal]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group2
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-128-cbc
[edit security ike policy ike-policy1]
user@host# set mode main
user@host# set proposals ike-proposal
user@host# set certificate local-certificate Local1
[edit security ike gateway spoke-to-hub-gw]
user@host# set ike-policy ike-policy1
user@host# set address 10.1.1.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name
user@host# set external-interface ge-0/0/1.0

```

## 4. `???` `???` `??????`.

```

[edit security ipsec proposal ipsec-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-md5-96
user@host# set encryption-algorithm des-cbc
[edit security ipsec policy vpn-policy1]
user@host# set perfect-forward-secrecy keys group14
user@host# set proposals ipsec-proposal
[edit security ipsec vpn spoke-to-hub]

```

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
user@host# set interfaces st0.0

[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces fe-0/0/4.0
```

```
[edit security policies]
user@host# set default-policy permit-all
```

```
[edit security pki]
user@host# set ca-profile ca-profile1 ca-identity ca-profile1
user@host# set ca-profile ca-profile1 enrollment url http://pc4/certsrv/mscep/mscep.dll
user@host# set ca-profile ca-profile1 revocation-check disable
```

```

[?] [?] [?] [?], show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show
security policies[?] show security pki [?] [?] [?] [?] show interfaces[?] [?] [?] [?]. [?] [?] [?] [?] [?] [?], [?] [?] [?] [?] [?]
[?] [?] [?] [?] [?].

```

```
[edit]
user@host# show interfaces
ge-0/0/1 {
```

```

    unit 0 {
        family inet {
            address 10.3.3.1/30;
        }
    }
}

fe-0/0/4 {
    unit 0 {
        family inet {
            address 10.70.70.1/24;
        }
    }
}

st0 {
    unit 0 {
        multipoint;
        family inet {
            address 10.10.10.3/24;
        }
    }
}

[edit]
user@host# show protocols
ospf {
    area 0.0.0.0 {
        interface st0.0 {
            interface-type p2mp;
            neighbor 10.10.10.1;
        }
        interface fe-0/0/4.0;
    }
}

[edit]
user@host# show routing-options
static {
    route 10.1.1.1/32 next-hop 10.3.3.2;
}

[edit]
user@host# show security ike
proposal ike-proposal {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm sha1;
}

```

```

    encryption-algorithm aes-128-cbc;
}
policy ike-policy1 {
    mode main;
    proposals ike-proposal;
    certificate {
        local-certificate Local1;
    }
}
gateway spoke-to-hub-gw {
    ike-policy ike-policy1;
    address 10.1.1.1;
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface ge-0/0/1.0;
}
[edit]
user@host# show security ipsec
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm des-cbc;
}
policy vpn-policy1 {
    perfect-forward-secrecy {
        keys group14;
    }
    proposals ipsec-proposal;
}
vpn spoke-to-hub {
    bind-interface st0.0;
    ike {
        gateway spoke-to-hub-gw;
        ipsec-policy vpn-policy1;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;

```

```

    }
    protocols {
        all;
    }
}
interfaces {
    ge-0/0/1.0;
    st0.0;
}
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        fe-0/0/4.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ca-profile1 {
    ca-identity ca-profile1;
    enrollment {
        url http://pc4/certsrv/mscep/mscep.dll;
    }
    revocation-check {
        disable;
    }
}
}

```

```

?? ?? ?? ?? commit?(?) ??.

```

??

in this section

- [IKE\(Internet Key Exchange\) 1?? ?? ?? | 1238](#)
- [IPsec 2?? ?? ?? | 1239](#)
- [IPsec ?? ? ?? ?? | 1239](#)
- [OSPF ?? | 1240](#)
- [??? ?? ?? | 1240](#)

??? ????? ????? ??? ??????

**IKE(Internet Key Exchange) 1?? ?? ??**

??

IKE(Internet Key Exchange) 1?? ??? ??????

??

?? ????? **show security ike security-associations** ??? ??????

```
user@host> show security ike security-associations
```

| Index   | State | Initiator cookie | Responder cookie | Mode | Remote Address |
|---------|-------|------------------|------------------|------|----------------|
| 5480159 | UP    | 22432fb6f7fbc389 | 412b751f79b45099 | Main | 10.2.2.1       |
| 5480161 | UP    | d455050707bc3eaf | b3dde111232270d2 | Main | 10.3.3.1       |

??

show security ike security-associations ??? ?? ?? IKE(Internet Key Exchange) 1?? SA? ?????, SA? ????? ??  
?? ??, 1?? ??? ??? ?? ?????, ????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ??????, 1?? ?? ??  
???? ??? ?????? ????? ????



IPsec 2?? ?? ??

??

IPsec 2?? ??? ?????.

??

?? ????? security ipsec security-associations ??? ?????.

```
user@host> security ipsec security-associations
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway
<268173400 ESP:des/ md5 f38eea12 2954/ unlim -   root 500    10.2.2.1
>268173400 ESP:des/ md5 bb48d228 2954/ unlim -   root 500    10.2.2.1
<268173401 ESP:des/ md5 bcd1390b 3530/ unlim -   root 500    10.3.3.1
>268173401 ESP:des/ md5 77fcf6e2 3530/ unlim -   root 500    10.3.3.1
```

??

show security ipsec security-associations ??? ?? ?? IKE 2?? SA? ??????. SA? ?????? ?? ?? ??, 2?? ??? ???? ????  
?????. ?????? IKE(Internet Key Exchange) ?? ?? ?? ? ?? ?????? ??? ?????. 2?? ?? ?? ???? ???? ?????? ????? ?  
??.

IPsec ?? ? ?? ??

??

IPsec ?? ? ????? ?????.

??

?? ????? show security ipsec next-hop-tunnels ??? ?????.

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway  interface  IPSec VPN name      Flag    IKE-
ID                XAUTH username
10.10.10.2        st0.0      hub-to-spoke-vpn     Auto    C=IN, DC=example.net,
ST=KA, L=Mysore, O=example, OU=SLT, CN=spoke1
```

```
10.10.10.3      st0.0      hub-to-spoke-vpn      Auto      C=IN, DC=example.net,
ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
```

??

?? ? ???? ???? IP ?? st0 ??. next hop? ??? IPsec VPN ??? ???? ???.

OSPF ??

??

OSPF? ???? ???? st0 IP ??? ???? ????.

??

?? ???? show ospf neighbor ??? ????.

```
user@host> show ospf neighbor
Address      Interface      State      ID              Pri  Dead
10.10.10.3   st0.0          Full       10.255.226.179 128   32
10.10.10.2   st0.0          Full       10.207.36.182  128   38
```

??? ?? ??

??

???? ?? ??? ?????? ????.

??

?? ???? show route 60.60.60.0 ??? ????.

```
user@host> show route 10.60.60.0
inet.0: 48 destinations, 48 routes (47 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.60.60.0/24      *[OSPF/10] 00:51:13, metric 2
                   > to 10.10.10.2 via st0.0
```





### 137: AutoVPN **OSPFv3** **1** **2** (Continued)

|                              |             |
|------------------------------|-------------|
|                              |             |
| <i>IPsec</i> :               |             |
|                              | ESP         |
|                              | 3000        |
|                              | AES 256 GCM |
| <i>IPsec</i> :               |             |
| PFS(Perfect Forward Secrecy) | 19          |

(CA) .

138 1243 .

### 138: AutoVPN **OSPFv3**

|                                     |                               |                                |
|-------------------------------------|-------------------------------|--------------------------------|
|                                     |                               |                                |
| <i>IKE(Internet Key Exchange)</i> : |                               |                                |
| IP                                  |                               | 2001:db8:2000::1               |
| IKE(Internet Key Exchange) ID       | OU( ) SLT  DN( )              | DNDN on the hub's certificate  |
| IKE(Internet Key Exchange) ID       | DNDN on the hub's certificate | DN                             |
|                                     | ge-0/0/0                      | 1: ge-0/0/0.0<br>2: ge-0/0/0.0 |

**? 138: ?? ? ?? ???? ?? AutoVPN OSPFv3 ?? (Continued)**

|    |    |        |
|----|----|--------|
| ?? | ?? | ?? ??? |
|----|----|--------|

*VPN:*

|              |                 |             |
|--------------|-----------------|-------------|
| ?? ? ? ? ? ? | st0.1           | st0.1       |
| ?? ? ?       | (? ? ? ? ? ? ?) | ? ? ? ? ? ? |

139  1244 () ?     .

**139: OSPFv3**

| ??            | ??? 1                            | ??? 2                            |
|---------------|----------------------------------|----------------------------------|
| st0.1 ?????   | 2001:db8:7000::2/64              | 2001:db8:7000::3/64              |
| ?? ???? ????? | (ge-0/0/1.0) 2001:db8:4000::1/64 | (ge-0/0/1.0) 2001:db8:6000::1/64 |
| ??? ?????     | (ge-0/0/0.0) 2001:db8:3000::2/64 | (ge-0/0/0.0) 2001:db8:5000::2/64 |

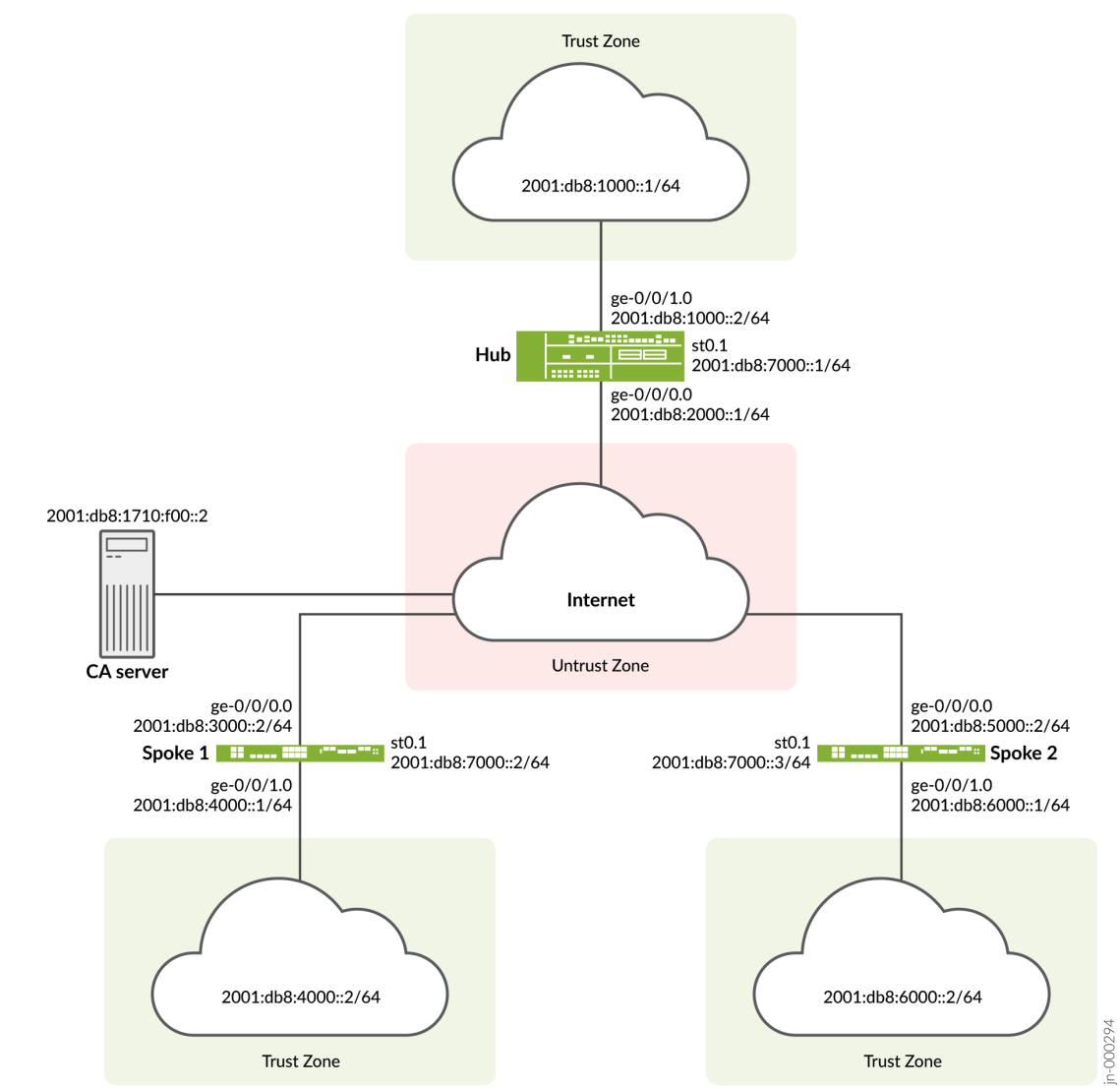
?? ???? ? ???? ???? VPN ??? ?? ?????.

? ???? ?? ????? ??? ? ? ? ? ? ? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? .

□□□□

[??](#) [68](#) [???](#) [1245](#) [??](#) [?](#) [????](#) AutoVPN? [??](#) [????](#) SRX [???](#) [????](#) [??](#) [????](#).

68: OSPFv3? ???? ?? AutoVPN ??



??

in this section

- SCEP? ???? ?? ???? ??Enroll Device Certificates with SCEP | 1246
- ?? ?? | 1251
- ??? ?? 1 | 1259

● [2 22](#) | 1266

AutoVPN? [22222 22 222 22222](#).

[2 22 22222 22 2 222 222222](#) SCEP(Simple Certificate Enrollment Protocol)? [22222 222222](#) CA [2 22 22222 22 2222 222222](#).

## SCEP? [22222 22 222 22](#)Enroll Device Certificates with SCEP

[222 22](#)

[22222](#) SCEP? [22222 222 22222 222222 222 222222](#).

### 1. CA? [222222](#).

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

### 2. CA [22222 222222](#).

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

[222222 22222](#) yes CA [22222 222222](#).

### 3. [2 2222 222222](#).

```
user@host> request security pki generate-key-pair certificate-id Local1
```



4. `?? ???? ?????.`

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email hub@example.net ip-address 10.1.1.1 subject
DC=example.net,CN=hub,OU=SLT,O=example,L=Bengaluru,ST=KA,C=IN challenge-password <password>
```

5. `?? ???? ?????.`

```
user@host> show security pki local-certificate detail

Certificate identifier: Local1
Certificate version: 3
Serial number: 40a6d5f300000000258d
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Bengaluru, Common name: hub, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Bengaluru, O=example, OU=SLT, CN=hub
Alternate subject: "hub@example.net", example.net, 10.1.1.1
Validity:
  Not before: 11- 6-2020 09:39
  Not after: 11- 6-2021 09:49
Public key algorithm: rsaEncryption(1024 bits)
  30:81:89:02:81:81:00:c9:c9:cc:30:b6:7a:86:12:89:b5:18:b3:76
  01:2d:cc:65:a8:a8:42:78:cd:d0:9a:a2:c0:aa:c4:bd:da:af:88:f3
  2a:78:1f:0a:58:e6:11:2c:81:8f:0e:7c:de:86:fc:48:4c:28:5b:8b
  34:91:ff:2e:91:e7:b5:bd:79:12:de:39:46:d9:fb:5c:91:41:d1:da
  90:f5:09:00:9b:90:07:9d:50:92:7d:ff:fb:3f:3c:bc:34:e7:e3:c8
  ea:cb:99:18:b4:b6:1d:a8:99:d3:36:b9:1b:36:ef:3e:a1:fd:48:82
  6a:da:22:07:da:e0:d2:55:ef:57:be:09:7a:0e:17:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  e1:f7:a1:a6:1e:c3:97:69:a5:07:9b:09:14:1a:c7:ae:09:f1:f6:35 (sha1)
  a0:02:fa:8d:5c:63:e5:6d:f7:f4:78:56:ac:4e:b2:c4 (md5)
Auto-re-enrollment:
```

```
Status: Disabled
Next trigger time: Timer not started
```

```
???
```

```
??? 1?? SCEP? ???? ???? ???? ?????:
```

### 1. CA? ?????.

```
[edit]
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

### 2. CA ???? ????.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
????? ???? yes CA ???? ????.
```

### 3. ? ???? ????.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

### 4. ?? ???? ????.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke1@example.net ip-address 10.2.2.1 subject
DC=example.net,CN=spoke1,OU=SLT,O=example,L=Mysore,ST=KA,C=IN challenge-password <password>
```

### 5. ?? ???? ????.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
```

?? ???? ???? OU(?? ?? ??)? SLT???? . ??? IKE(Internet Key Exchange) ????? ???? ???? ???? ???? ???? ???? ou=SLT .

???

2025 SCEP 2025 2025 2025 2025.

1. CA? ?????.

[edit]

```
user@host# set security pki ca-profile ca-profile1 ca-identity ca-profile1
user@host# set security pki ca-profile ca-profile1 enrollment url http://2001:db8:1710:f00::2/
```

```
certsrv/mscep/mscep.dll
user@host# set security pki ca-profile ca-profile1 revocation-check disable
user@host# commit
```

## 2. CA `ca-profile1`.

```
user@host> request security pki ca-certificate enroll ca-profile ca-profile1
```

```
yes CA ca-profile1.
```

## 3. `ca-profile1`.

```
user@host> request security pki generate-key-pair certificate-id Local1
```

## 4. `ca-profile1`.

```
user@host> request security pki local-certificate enroll ca-profile ca-profile1 certificate-
id Local1 domain-name example.net email spoke2@example.net ip-address 10.3.3.1 subject
DC=example.net,CN=spoke2,OU=SLT,O=example,L=Tumkur,ST=KA,C=IN challenge-password <password>
```

## 5. `ca-profile1`.

```
user@host> show security pki local-certificate detail
```

```
Certificate identifier: Local1
Certificate version: 3
Serial number: 40bb71d400000000258f
Issuer:
  Common name: CASERVER1, Domain component: net, Domain component: internal
Subject:
  Organization: example, Organizational unit: SLT, Country: IN, State: KA,
  Locality: Tumkur, Common name: spoke2, Domain component: example.net
Subject string:
  C=IN, DC=example.net, ST=KA, L=Tumkur, O=example, OU=SLT, CN=spoke2
Alternate subject: "spoke2@example.net", example.net, 10.3.3.1
Validity:
  Not before: 11- 6-2020 10:02
  Not after: 11- 6-2021 10:12
Public key algorithm: rsaEncryption(1024 bits)
```

```

30:81:89:02:81:81:00:b6:2e:e2:da:e6:ac:57:e4:5d:ff:de:f6:89
27:d6:3e:1b:4a:3f:b2:2d:b3:d3:61:ed:ed:6a:07:d9:8a:d2:24:03
77:1a:fe:84:e1:12:8a:2d:63:6e:bf:02:6b:15:96:5a:4f:37:a0:46
44:09:96:c0:fd:bb:ab:79:2c:5d:92:bd:31:f0:3b:29:51:ce:89:8e
7c:2b:02:d0:14:5b:0a:a9:02:93:21:ea:f9:fc:4a:e7:08:bc:b1:6d
7c:f8:3e:53:58:8e:f1:86:13:fe:78:b5:df:0b:8e:53:00:4a:46:11
58:4a:38:e9:82:43:d8:25:47:7d:ef:18:f0:ef:a7:02:03:01:00:01
Signature algorithm: sha1WithRSAEncryption
Distribution CRL:
  http://ca-server1/CertEnroll/CASERVER1.crl
  file://\ca-server1\CertEnroll\CASERVER1.crl
Fingerprint:
  1a:6d:77:ac:fd:94:68:ce:cf:8a:85:f0:39:fc:e0:6b:fd:fe:b8:66 (sha1)
  00:b1:32:5f:7b:24:9c:e5:02:e6:72:75:9e:a5:f4:77 (md5)
Auto-re-enrollment:
  Status: Disabled
  Next trigger time: Timer not started

```

?? ???? ???? OU(?? ?? ??) SLT???. ??? IKE(Internet Key Exchange) ???? ???? ???? ???? ???? ???? ???? ou=SLT .

?? ??

## CLI ?? ??

? ?? ???? ?????, ?? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? [edit] ?  
 ? ???? ???? CLI? ???? ???? ???? ???? ???? ???? ???? commit?(?) ?????.

```

set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP

```

```

set security ike policy IKE_POL certificate local-certificate HUB
set security ike gateway IKE_GWA_1 ike-policy IKE_POL
set security ike gateway IKE_GWA_1 dynamic distinguished-name wildcard OU=SLT
set security ike gateway IKE_GWA_1 dead-peer-detection always-send
set security ike gateway IKE_GWA_1 dead-peer-detection interval 10
set security ike gateway IKE_GWA_1 dead-peer-detection threshold 3
set security ike gateway IKE_GWA_1 local-identity distinguished-name
set security ike gateway IKE_GWA_1 external-interface ge-0/0/0
set security ike gateway IKE_GWA_1 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPNA_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPNA_1 ike gateway IKE_GWA_1
set security ipsec vpn IPSEC_VPNA_1 ike ipsec-policy IPSEC_POL
set security policies default-policy permit-all
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces ge-0/0/0.0
set security zones security-zone untrust interfaces st0.1
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/1..0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:2000::1/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:1000::2/64
set interfaces st0 unit 1 multipoint
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::1/64
set routing-options rib inet6.0 static route 2001:db8:3000::/64 next-hop 2001:db8:2000::1
set routing-options rib inet6.0 static route 2001:db8:5000::/64 next-hop 2001:db8:2000::1
set protocols ospf3 traceoptions file ospf
set protocols ospf3 traceoptions flag all
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 demand-circuit
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors
set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ??? ??? ?? ???? CLI/ ??? ??? ?????.

?? ???? ? ????.

1. ???? ????.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:2000::1/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:1000::2/64
user@host# set st0 unit 1 multipoint
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::1/64
```

2. ??? ???? ????.

```
[edit protocols ospf3]
user@host# set traceoptions file ospf
user@host# set traceoptions flag all
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/1.0
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:3000::/64 next-hop 2001:db8:2000::1
user@host# set rib inet6.0 static route 2001:db8:5000::/64 next-hop 2001:db8:2000::1
```

3. 1?? ? ????.

```
[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate HUB
[edit security ike gateway IKE_GWA_1]
user@host# set ike-policy IKE_POL
```

```

user@host# set dynamic distinguished-name wildcard OU=SLT
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/0
user@host# set version v1-only

```

#### 4. `set ipsec proposal`.

```

[edit security ipsec proposal IPSEC_PROP]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPNA_1]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GWA_1
user@host# set ike ipsec-policy IPSEC_POL

```

#### 5. `set security zone`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0
user@host# set interfaces st0.1
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/1.0

```

#### 6. `set security policy`.

```

[edit security policies]
user@host# set default-policy permit-all

```



## 7. CA `???` `?????`.

```
[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set pki ca-profile ROOT-CA revocation-check disable
```

`??`

`?? ???? , show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show security policies? show security pki ??? ???? show interfaces???? ?????. ??? ??? ???? ???? ???? , ? ?? ?? ???? ? ???? ?????.`

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet6 {
      address 2001:db8:2000::1/64;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:1000::2/64;
    }
  }
}
st0 {
  unit 1 {
    family inet6 {
      address 2001:db8:7000::1/64;
    }
  }
}
[edit]
```

```

user@host# show protocols
ospf3 {
    traceoptions {
        file ospf;
        flag all;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            demand-circuit;
            dynamic-neighbors;
        }
        interface ge-0/0/1.0;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 2001:db8:3000::/64 next-hop 2001:db8::1;
        route 2001:db8:5000::/64 next-hop 2001:db8::1;
    }
}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate HUB;
    }
}

```

```

gateway IKE_GWA_1 {
    ike-policy IKE_POL;
    dynamic {
        distinguished-name {
            wildcard OU=SLT;
        }
    }
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    external-interface ge-0/0/0.0;
    version v1-only;
}
[edit]
user@host# show security ipsec
    proposal IPSEC_PROP {
        protocol esp;
        authentication-algorithm aes-256-gcm;
        set lifetime-seconds 3000;
    }
    policy IPSEC_POL {
        perfect-forward-secrecy {
            keys group19;
        }
        proposals IPSEC_PROP;
    }
    vpn IPSEC_VPNA_1 {
        bind-interface st0.1;
        ike {
            gateway IKE_GWA_1;
            ipsec-policy IPSEC_POL;
        }
    }
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
}

```

```

        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
        st0.1;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}
}

```

```

?? ?? ?? ?? ?? commit?(?) ??.

```

?? ? 1

CLI    

```
? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit] ?  
? ? ? ? ? ? ? ? ? ? CLI? ? ? ? ? ? ? ? , ? ? ? ? ? ? commit?(?) ? ? ? ? ? ?.
```

```
set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE1
set security ike gateway IKE_GW_SPOKE_1 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_1 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_1 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_1 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_1 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_1 external-interface ge-0/0/0.0
set security ike gateway IKE_GW_SPOKE_1 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_1 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike gateway IKE_GW_SPOKE_1
set security ipsec vpn IPSEC_VPN_SPOKE_1 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_1 establish-tunnels immediately
set security policies default-policy permit-all
```

```

set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::2/64
set routing-options rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:3000::2
set protocols ospf3 traceoptions file ospf
set protocols ospf3 traceoptions flag all
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 demand-circuit
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors
set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0

```

???

?? ?? ?? ???? ???? ???? ?????. ??? ??? ?? ???? CLI ??? ??? ?????.

??? 1? ?????.

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:3000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:4000::1/64
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::2/64

```

2. ??? ???? ????.

```

[edit protocols ospf3]
user@host# set traceoptions file ospf
user@host# set traceoptions flag all
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/1.0

```

```
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:3000::2
```

### 3. 1?? ??? ?????.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE1
[edit security ike gateway IKE_GW_SPOKE_1]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0.0
user@host# set version v1-only
```

### 4. 2?? ??? ?????.

```
[edit security ipsec proposal IPSEC_PROPI]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPN_SPOKE_1]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GW_SPOKE_1
```

```
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels immediately
```

##### 5. `?? ?????`.

```
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/1.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0
```

##### 6. `?? ? ? ? ? ? ? ? ?`.

```
[edit security policies]
user@host# set default-policy permit-all
```

##### 7. CA `???? ???? ?`.

```
[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable
```

`??`

`?? ???? ?`, show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show security policies? show security pki `???? ???? ?` show interfaces`???? ???? ?`, `?? ? ? ? ? ? ? ? ?`, `? ? ? ? ? ? ? ? ? ?` `???? ???? ?`.

```
[edit]
user@host# show interfaces
```



```

ge-0/0/0 {
    unit 0 {
        family inet6 {
            address 2001:db8:3000::2/64;
        }
    }
}
ge-0/0/1 {
    unit 0 {
        family inet6 {
            address 2001:db8:4000::1/64;
        }
    }
}
st0 {
    unit 1 {
        family inet6 {
            address 2001:db8:7000::2/64;
        }
    }
}
[edit]
user@host# show protocols
ospf3 {
    traceoptions {
        file ospf;
        flag all;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            demand-circuit;
            dynamic-neighbors;
        }
        interface ge-0/0/1.0;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 2001:db8:2000::/64 next-hop [ 2001:db8:3000::1 2001:db8:5000::1 ];
    }
}

```

```

}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE1;
    }
}
gateway IKE_GW_SPOKE_1 {
    ike-policy IKE_POL;
    address 2001:db8:2000::1;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=SLT;
    external-interface ge-0/0/0.0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {

```

```

        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPN_SPOKE_1 {
    bind-interface st0.1;
    ike {
        gateway IKE_GW_SPOKE_1;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/1.0;
        st0.1;
    }
}
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
[edit]
user@host# show security policies

```

```

default-policy {
    permit-all;
}
[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}

```

```

?? ?? ?? ?? commit?(?) ?????.

```

```

??? 2 ??

```

## CLI ?? ??

```

? ?? ??? ?????, ?? ??? ????? ??? ?? ?? ?? ?? ?????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```

```

set security pki ca-profile ROOT-CA ca-identity ROOT-CA
set security pki ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
set security pki ca-profile ROOT-CA enrollment retry 5
set security pki ca-profile ROOT-CA enrollment retry-interval 0
set security pki ca-profile ROOT-CA revocation-check disable
set security ike traceoptions file ik
set security ike traceoptions flag all
set security ike proposal IKE_PROP authentication-method rsa-signatures
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-384
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 6000
set security ike policy IKE_POL mode main
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL certificate local-certificate SPOKE2

```

```

set security ike gateway IKE_GW_SPOKE_2 ike-policy IKE_POL
set security ike gateway IKE_GW_SPOKE_2 address 2001:db8:2000::1
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection always-send
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection interval 10
set security ike gateway IKE_GW_SPOKE_2 dead-peer-detection threshold 3
set security ike gateway IKE_GW_SPOKE_2 local-identity distinguished-name
set security ike gateway IKE_GW_SPOKE_2 remote-identity distinguished-name container OU=SLT
set security ike gateway IKE_GW_SPOKE_2 external-interface ge-0/0/0.0
set security ike gateway IKE_GW_SPOKE_2 version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3000
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn IPSEC_VPN_SPOKE_2 bind-interface st0.1
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike gateway IKE_GW_SPOKE_2
set security ipsec vpn IPSEC_VPN_SPOKE_2 ike ipsec-policy IPSEC_POL
set security ipsec vpn IPSEC_VPN_SPOKE_2 establish-tunnels on-traffic
set security policies default-policy permit-all
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols ospf3
set security zones security-zone trust interfaces ge-0/0/0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols ospf3
set security zones security-zone untrust interfaces st0.1
set security zones security-zone untrust interfaces ge-0/0/1.0
set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
set interfaces ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
set interfaces st0 unit 1 family inet6 address 2001:db8:7000::3/64
set routing-options rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
set protocols ospf3 traceoptions file ospf
set protocols ospf3 traceoptions flag all
set protocols ospf3 area 0.0.0.0 interface st0.1 interface-type p2mp
set protocols ospf3 area 0.0.0.0 interface st0.1 demand-circuit
set protocols ospf3 area 0.0.0.0 interface st0.1 dynamic-neighbors
set protocols ospf3 area 0.0.0.0 interface ge-0/0/1.0

```

???

?? ?? ?? ???? ???? ???? ???? ???? ???? ???? ???? CLI ???? ???? ???? ????.

??? 2? ?????:

1. `???` `???`.

```
[edit interfaces]
user@host# set ge-0/0/0 unit 0 family inet6 address 2001:db8:5000::2/64
user@host# set ge-0/0/1 unit 0 family inet6 address 2001:db8:6000::1/64
user@host# set st0 unit 1 family inet6 address 2001:db8:7000::3/64
```

2. `???` `???` `???`.

```
[edit protocols ospf3]
user@host# set traceoptions file ospf
user@host# set traceoptions flag all
user@host# set area 0.0.0.0 interface st0.1 interface-type p2mp
user@host# set area 0.0.0.0 interface st0.1 demand-circuit
user@host# set area 0.0.0.0 interface st0.1 dynamic-neighbors
user@host# set area 0.0.0.0 interface ge-0/0/1.0
[edit routing-options]
user@host# set rib inet6.0 static route 2001:db8:2000::/64 next-hop 2001:db8:5000::1
```

3. `1??` `???` `???`.

```
[edit security ike proposal IKE_PROP]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group19
user@host# set authentication-algorithm sha-384
user@host# set encryption-algorithm aes-256-cbc
user@host# set lifetime-seconds 6000
[edit security ike traceoptions]
user@host# set file ik
user@host# set flag all
[edit security ike policy IKE_POL]
user@host# set mode main
user@host# set proposals IKE_PROP
user@host# set certificate local-certificate SPOKE2
[edit security ike gateway IKE_GW_SPOKE_2]
user@host# set ike-policy IKE_POL
user@host# set address 2001:db8:2000::1
user@host# set dead-peer-detection always-send
user@host# set dead-peer-detection interval 10
user@host# set dead-peer-detection threshold 3
```

```

user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container OU=SLT
user@host# set external-interface ge-0/0/0.0
user@host# set version v1-only

```

#### 4. `set ipsec proposal`.

```

[edit security ipsec proposal IPSEC_PROPI]
user@host# set protocol esp
user@host# set encryption-algorithm aes-256-gcm
user@host# set lifetime-seconds 3000
[edit security ipsec policy IPSEC_POL]
user@host# set perfect-forward-secrecy keys group19
user@host# set proposals IPSEC_PROP
[edit security ipsec vpn IPSEC_VPN_SPOKE_2]
user@host# set bind-interface st0.1
user@host# set ike gateway IKE_GW_SPOKE_2
user@host# set ike ipsec-policy IPSEC_POL
user@host# set establish-tunnels on-traffic

```

#### 5. `set security zone`.

```

[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/1.0
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols ospf3
user@host# set interfaces ge-0/0/0.0

```

#### 6. `set security policy`.

```

[edit security policies]
user@host# set default-policy permit-all

```

## 7. CA `???` `????`.

```
[edit security pki]
user@host# set ca-profile ROOT-CA ca-identity ROOT-CA
user@host# set ca-profile ROOT-CA enrollment url http://2001:db8:1710:f00::2/certsrv/mscep/
mscep.dll
user@host# set ca-profile ROOT-CA enrollment retry 5
user@host# set ca-profile ROOT-CA enrollment retry-interval 0
user@host# set ca-profile ROOT-CA revocation-check disable
```

`??`

`??` `????`, show protocols, , show security ikeshow routing-options, show security ipsec, show security zones, show security policies? show security pki `???` `????` show interfaces`???` `????`. `???` `???` `???` `????` `???`, ? `??` `??` `????` ? `????` `????`.

```
[edit]
user@host# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet6 {
      address 2001:db8:5000::2/64;
    }
  }
}
ge-0/0/1 {
  unit 0 {
    family inet6 {
      address 2001:db8:6000::1/64;
    }
  }
}
st0 {
  unit 1 {
    family inet6 {
      address 2001:db8:7000::3/64;
    }
  }
}
[edit]
```



```

user@host# show protocols
ospf3 {
    traceoptions {
        file ospf;
        flag all;
    }
    area 0.0.0.0 {
        interface st0.1 {
            interface-type p2mp;
            demand-circuit;
            dynamic-neighbors;
        }
        interface ge-0/0/1.0;
    }
}
[edit]
user@host# show routing-options
rib inet6.0 {
    static {
        route 2001:db8:2000::/64 next-hop [ 2001:db8:3000::1 2001:db8:5000::1 ];
    }
}
[edit]
user@host# show security ike
traceoptions {
    file ik;
    flag all;
}
proposal IKE_PROP {
    authentication-method rsa-signatures;
    dh-group group19;
    authentication-algorithm sha-384;
    encryption-algorithm aes-256-cbc;
    lifetime-seconds 6000;
}
policy IKE_POL {
    mode main;
    proposals IKE_PROP;
    certificate {
        local-certificate SPOKE2;
    }
}
gateway IKE_GW_SPOKE_2 {

```

```

    ike-policy IKE_POL;
    address 2001:db8:2000::1;
    dead-peer-detection {
        always-send;
        interval 10;
        threshold 3;
    }
    local-identity distinguished-name;
    remote-identity distinguished-name container OU=SLT;
    external-interface ge-0/0/0.0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    encryption-algorithm aes-256-gcm;
    lifetime-seconds 3000;
}
policy IPSEC_POL {
    perfect-forward-secrecy {
        keys group19;
    }
    proposals IPSEC_PROP;
}
vpn IPSEC_VPN_SPOKE_2 {
    bind-interface st0.1;
    ike {
        gateway IKE_GW_SPOKE_2;
        ipsec-policy IPSEC_POL;
    }
    establish-tunnels on-traffic;
}
[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
}

```

```

    }
    interfaces {
        ge-0/0/1.0;
        st0.0;
    }
}

security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            ospf3;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

[edit]
user@host# show security pki
ca-profile ROOT-CA {
    ca-identity ROOT-CA;
    enrollment {
        url http://2001:db8:1710:f00::2/certsrv/mscep/mscep.dll;
        retry 5;
        retry-interval 0;
    }
    revocation-check {
        disable;
    }
}

```

```

?? ?? ?? ?? commit?(?) ??.

```

??? ???? ???? ??? ?????.

??

IKE      .

??

?? ???? show security ike sa ??? ?????.

```
user@host> show security ike sa
```

| Index  | State | Initiator cookie          | Responder cookie          | Mode | Remote Address   |
|--------|-------|---------------------------|---------------------------|------|------------------|
| 493333 | UP    | 2001:db8:88b49d915e684c93 | 2001:db8:fe890b1cac8522b5 | Main | 2001:db8:3000::2 |
| 493334 | UP    | 2001:db8:26e40244ad3d722d | 2001:db8:68b4d9f94097d32e | Main | 2001:db8:5000::2 |

??

```
show security ike sa [redacted] IKE(Internet Key Exchange) 1[redacted] SA? [redacted]. SA? [redacted] [redacted] [redacted], 1[redacted] [redacted] [redacted] [redacted] [redacted] IKE(Internet Key Exchange) [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]. 1[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].
```

IPsec **?? ??**

**??**

IPsec **??? ??????**.

**??**

**?? ????? show security ipsec sa** **??? ??????**.

```
user@host> show security ipsec sa
Total active tunnels: 2
ID      Algorithm      SPI  Life:sec/kb    Mon    lsys Port Gateway
>67108885 ESP:aes-gcm-256/None fdef4dab 2918/ unlim - root 500  2001:db8:3000::2
>67108885 ESP:aes-gcm-256/None e785dad3 2918/ unlim - root 500  2001:db8:3000::2
>67108887 ESP:aes-gcm-256/None 34a787af 2971/ unlim - root 500  2001:db8:5000::2
>67108887 ESP:aes-gcm-256/None cf57007f 2971/ unlim - root 500  2001:db8:5000::2
```

**??**

show security ipsec sa **??? ?? ?? IKE 2?? SA? ??????**. **SA? ????? ?? ?? ??, 2?? ??? ??? ?? ?????, ?????**  
IKE(Internet Key Exchange) **?? ?? ?? ? ?? ?????? ??? ??????, 2?? ?? ?? ??? ??? ?????? ????? ????**.

IPsec **?? ? ?? ??**

**??**

IPsec **?? ? ??? ??????**.

**??**

**?? ????? show security ipsec next-hop-tunnels** **??? ??????**.

```
user@host> show security ipsec next-hop-tunnels
Next-hop gateway      interface  IPSec VPN name  Flag  IKE-
ID                    XAUTH username
2001:db8:9000::2      st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available
```

```
2001:db8:9000::3          st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
```

```
2001:db8::5668:ad10:fcd8:163c st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE1 Not-Available
```

```
2001:db8::5668:ad10:fcd8:18a1 st0.1      IPSEC_VPNA_1    Auto  C=US, DC=example.net, ST=CA,
L=Sunnyvale, O=example, OU=SLT, CN=SPOKE2 Not-Available
```

??

?? ? ???? ???? ???? IP ?? st0 ??? next hop? ??? IPsec VPN ??? ???? ????.

### OSPFv3 ??

??

OSPFv3? ??? ???? IP ??? st0 ???? ????.

??

?? ???? show ospf3 neighbor detail ??? ????.

??:

```
user@host> show ospf3 neighbor detail
ID                               Interface  State Pri  Dead
2001:db8:7000:2  st0.1      Full  128  -
  Neighbor-address 2001:db8::5668:ad10:fcd8:18a1
  Area 0.0.0.0, opt 0x33, OSPF3-Intf-Index 2
  DR-ID 0.0.0.0, BDR-ID 0.0.0.0
  Up 00:01:35, adjacent 00:01:31 Hello suppressed 00:01:31 ago
2001:db8:7000:3  st0.1      Full  128  -
  Neighbor-address 2001:db8::5668:ad10:fcd8:163c
  Area 0.0.0.0, opt 0x33, OSPF3-Intf-Index 2
  DR-ID 0.0.0.0, BDR-ID 0.0.0.0
  Up 00:01:41, adjacent 00:01:37 Hello suppressed 00:01:37 ago
```

**???** 1:

```

user@host> show ospf3 neighbor detail
ID                               Interface      State      Pri    Dead
2001:db8:7000:1    st0.1        Full      128    -
  Neighbor-address 2001:db8::5668:ad10:fcd8:1946
  Area 0.0.0.0, opt 0x33, OSPF3-Intf-Index 2
  DR-ID 0.0.0.0, BDR-ID 0.0.0.0
  Up 00:05:38, adjacent 00:05:38 Hello suppressed 00:05:34 ago

```

???:

```
user@host> show ospf3 neighbor detail
```

| ID                    | Interface | State | Pri | Dead |
|-----------------------|-----------|-------|-----|------|
| 2001:db8:7000:1 st0.1 | Full      | 128   | -   |      |

Neighbor-address 2001:db8::5668:ad10:fcd8:1946  
Area 0.0.0.0, opt 0x33, OSPF3-Intf-Index 2  
DR-ID 0.0.0.0, BDR-ID 0.0.0.0  
Up 00:04:44, adjacent 00:04:44 Hello suppressed 00:04:40 ago

## SEE ALSO

🔗: 📄 📄 VPN 📄 | 453

?: ? ? ? ? ? ? ? ? AutoVPN ? ? ? ? ? ? ? ?

in this section

- ?? ?? | 1278
- ?? | 1278
- ?? | 1281
- ?? | 1294

```

? ???? AutoVPN ???? VPN ??? ?? ??? ?????? ?? ??? ?????? ?? ??? ?????? ??? ??????. ??? ????? ????
?? ??(st0) ?????? ??? ? ??? ????? ????. ??? ????? ?? ? ??? ????? ????? ??????, ? ??? ???? ?? ??? ????? ???
?. ?? ?? ?? ??? ??? ?? ?:" iBGP" ??? 1067? ????? ?? AutoVPN ??.

```

?? ??

? ? ? ? ? ? ? ? ? ? ?

- [illegible]

□□□□ □□:

- ?? ???? ?? ???? ???? ? ?? ??(CA) ? ??? ??? ??(?: ?? ?? ??) ? ????.
- ? ??? ??? ????? ??????. ??? ??? ???????.

??

in this section

● ???? | 1280

? ???? ???? ???? AutoVPN ?? ? ?????? ??????. ??? ???? ????? ?????? ????? ???? ?? ??????, ????? ???? ????? ?? IP ?  
 ? 192.0.0.0/8 ? ?? IP ?? 172.0.0.0/8? ??????, ?????? ??? ????? ?? IP ?? 172.0.0.0/8 ? ?? IP ??  
 192.0.0.0/8? ??????.

???? ???? ???? ???? IP ???? ???? ???? ???? ???? IP ???? ?? ???? ? ?????. ?? /??? /??? /??? /??? /???.

AutoVPN ?? ? ???? ?? ? 1?? ? 2?? IKE ?? ??? ??? ?? ??? ???. ? 140 ??? 1278 ?(?) ? ?? ??? ?? ????  
?.

**? 140: ??? ???? ?? AutoVPN ?? ? ????? ?? 1?? ? 2?? ??**

*IKE(Internet Key Exchange) ??:*



**140: AutoVPN 1 (Continued)**

| ??                    | ??          |
|-----------------------|-------------|
| ?? ??                 | RSA ??      |
| DH(Diffie-Hellman) ?? | group5      |
| ?? ?????              | ?-1         |
| ???? ?????            | AES-256-CBC |

*IKE(Internet Key Exchange) ??:*

|     |        |
|-----|--------|
| ??  | main   |
| ??? | ?? ??? |

*IKE(Internet Key Exchange) ?????:*

|            |                                  |
|------------|----------------------------------|
| ??         | ?? ?? ???? DC=Common_component   |
| IKE ??? ?? | ?? IKE(Internet Key Exchange) ID |
| ?? ID      | ?? ??                            |
| ??         | v1 ??                            |

*IPsec ??:*

|          |              |
|----------|--------------|
| ????     | esp          |
| ?? ????? | hmac-sha1-96 |

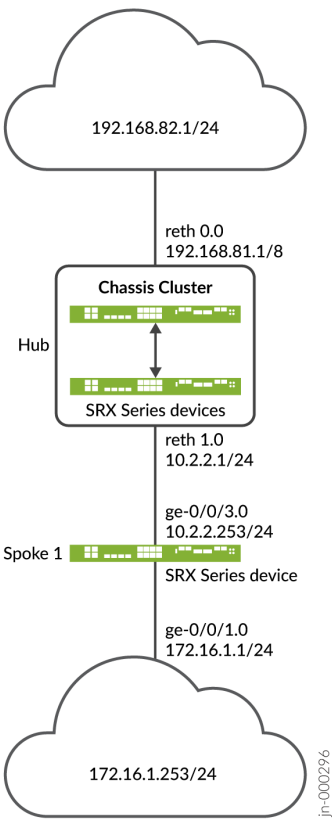
140: AutoVPN 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 (Continued)

|                                                |                         |
|------------------------------------------------|-------------------------|
| 1                                              | 2                       |
| 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 | AES-192-CBC             |
| 1                                              | 3600 2<br>150,000345678 |
| IPsec 12:                                      |                         |
| PFS(Perfect Forward Secrecy) 12                | group5                  |

3456

69 1281 1(1) 2 3456 789 SRX 1011 121314151617181920.

69: AutoVPN



??

in this section

- ?? ?? | 1282
- ?? ?? | 1289

?? ??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ??????.

```
set interfaces ge-0/0/2 gigether-options redundant-parent reth1
set interfaces ge-0/0/3 gigether-options redundant-parent reth0
set interfaces ge-8/0/2 gigether-options redundant-parent reth1
set interfaces ge-8/0/3 gigether-options redundant-parent reth0
set interfaces lo0 unit 0 family inet address 10.100.1.100/24
set interfaces lo0 redundant-pseudo-interface-options redundancy-group 1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 192.168.81.1/8
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.2.2.1/24
set interfaces st0 unit 1 family inet
set security ike proposal prop_ike authentication-method rsa-signatures
set security ike proposal prop_ike dh-group group5
set security ike proposal prop_ike authentication-algorithm sha1
set security ike proposal prop_ike encryption-algorithm aes-256-cbc
set security ike policy ikepol1 mode main
set security ike policy ikepol1 proposals prop_ike
set security ike policy ikepol1 certificate local-certificate Hub_ID
set security ike gateway HUB_GW ike-policy ikepol1
set security ike gateway HUB_GW dynamic distinguished-name wildcard DC=Domain_component
set security ike gateway HUB_GW dynamic ike-user-type group-ike-id
set security ike gateway HUB_GW local-identity distinguished-name
set security ike gateway HUB_GW external-interface reth1
set security ike gateway HUB_GW version v1-only
set security ipsec proposal prop_ipsec protocol esp
set security ipsec proposal prop_ipsec authentication-algorithm hmac-sha1-96
set security ipsec proposal prop_ipsec encryption-algorithm aes-192-cbc
set security ipsec proposal prop_ipsec lifetime-seconds 3600
set security ipsec proposal prop_ipsec lifetime-kilobytes 150000
set security ipsec policy ipsecpol1 perfect-forward-secrecy keys group5
set security ipsec policy ipsecpol1 proposals prop_ipsec
set security ipsec vpn HUB_VPN bind-interface st0.1
set security ipsec vpn HUB_VPN ike gateway HUB_GW
set security ipsec vpn HUB_VPN ike ipsec-policy ipsecpol1
set security ipsec vpn HUB_VPN traffic-selector ts1 local-ip 192.0.0.0/8
```

```

set security ipsec vpn HUB_VPN traffic-selector ts1 remote-ip 172.0.0.0/8
set security pki ca-profile rsa ca-identity rsa
set security pki ca-profile rsa revocation-check disable
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces st0.1
set security zones security-zone trust interfaces reth0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces reth1.0
set security policies default-policy permit-all

```

[edit security ike gateway *gateway-name* dynamic] **??** **????** CLI **???** reject-duplicate-connection**????** **??** **??** **????** **??**  
**??** IKE(Internet Key Exchange) ID**?** **???** **?** **????** **??** **???** **????** **??** **????**. **????** **???** IKE(Internet Key  
Exchange) ID**?** **??** **?** **????** **????** **??** **????** **??????**. **?** reject-duplicate-connection **???** IKE(Internet Key Exchange) **?**  
**??????** **??** **??** ike-user-type shared-ike-id **?(?)** **????** **?????** ike-user-type group-ike-id **?????**, aaa access-profile  
*profile-name* **?** **??????** **????** **?????** **?????**.

**???** IKE(Internet Key Exchange) ID**?** **??** **?** **????** **?????** **??????** **????** **?????** **?????** CLI **???** reject-duplicate-  
connection **??????**.

**????** **??**

**??** **??** **??** **?????** **????** **????** **??????**. **??** **?????** **????** **??** **???** CLI **????** **?????** **??** **?????** CLI **????** **???** **??????**.

**????** **??????** **????** **??????**.

# 1. **??????** **??????**.

```

[edit interfaces]
user@host# set ge-0/0/2 gigether-options redundant-parent reth1
user@host# set ge-0/0/3 gigether-options redundant-parent reth0
user@host# set ge-8/0/2 gigether-options redundant-parent reth1
user@host# set ge-8/0/3 gigether-options redundant-parent reth0
user@host# set lo0 unit 0 family inet address 10.100.1.100/24
user@host# set lo0 redundant-pseudo-interface-options redundancy-group 1
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 192.168.81.1/8
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 10.2.2.1/24
user@host# set st0 unit 1 family inet

```

## 2. 1?? ??? ?????.

```
[edit security ike proposal prop_ike]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy ikepol1]
user@host# set mode main
user@host# set proposals prop_ike
user@host# set certificate local-certificate Hub_ID
[edit security ike gateway HUB_GW]
user@host# set ike-policy ikepol1
user@host# set dynamic distinguished-name wildcard DC=Domain_component
user@host# set dynamic ike-user-type group-ike-id
user@host# set local-identity distinguished-name
user@host# set external-interface reth1
user@host# set version v1-only
```

## 3. 2?? ??? ?????.

```
[edit security ipsec proposal prop_ipsec]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-192-cbc
user@host# set lifetime-seconds 3600
user@host# set lifetime-kilobytes 150000
[edit security ipsec policy ipsecpol1]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals prop_ipsec
[edit security ipsec HUB_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway HUB_GW
user@host# set ike ipsec-policy ipsecpol1
user@host# set traffic-selector ts1 local-ip 192.0.0.0/8
user@host# set traffic-selector ts1 remote-ip 172.0.0.0/8
```

4. `set ca-profile rsa ca-identity rsa`.

```
[edit security pki]
user@host# set ca-profile rsa ca-identity rsa
user@host# set ca-profile rsa revocation-check disable
```

5. `set host-inbound-traffic system-services all`.

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.1
user@host# set interfaces reth0.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces lo0.0
user@host# set interfaces reth1.0
[edit security policies]
user@host# set default-policy permit-all
```

??

?? `show interfaces`, `show security ike`, `show security ipsec`, `show security pki`, `show security zones` ? `show security policies` `set default-policy permit-all`. ?? `show security ike`, `show security ipsec`, `show security pki`, `show security zones` ? `show security policies` `set default-policy permit-all`.

```
[edit]
user@host# show interfaces
ge-0/0/2 {
  gigether-options {
    redundant-parent reth1;
  }
}
ge-0/0/3 {
  gigether-options {
    redundant-parent reth0;
  }
}
lo0 {
```

```

    unit 0 {
        family inet {
            address 10.100.1.100/24;
        }
    }
    redundant-pseudo-interface-options {
        redundancy-group 1;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 192.168.81.1/8;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 10.2.2.1/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
[edit]
user@host# show security ike
proposal prop_ike {
    authentication-method rsa-signatures;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-256-cbc;
}
policy ikepol1 {

```



```

    mode main;
    proposals prop_ike;
    certificate {
        local-certificate Hub_ID;
    }
}
gateway HUB_GW {
    ike-policy ikepol1;
    dynamic distinguished-name wildcard DC=Domain_component;
    dynamic ike-user-type group-ike-id;
    local-identity distinguished-name;
    external-interface reth1;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal prop_ipsec {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-seconds 3600;
    lifetime-kilobytes 150000;
}
policy ipsecpol1 {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals prop_ipsec;
}
vpn HUB_VPN {
    bind-interface st0.1;
    ike {
        gateway HUB_GW;
        ipsec-policy ipsecpol1;
    }
    traffic-selector ts1 {
        local-ip 192.0.0.0/8;
        remote-ip 172.0.0.0/8;
    }
}
[edit]
user@host# show security pki
ca-profile rsa {

```

```

    ca-identity rsa;
    revocation-check {
        disable;
    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        reth0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        lo0.0;
        reth1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

```

?? ?? ?? ?? ?? commit?(?) ?????.

```



```

set security zones security-zone trust interfaces ge-0/0/3.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

??? ????? ???? ?????.

## 1. ?????? ?????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 172.16.1.1/24
user@host# set ge-0/0/3 unit 0 family inet address 10.2.2.253/24
user@host# set st0 unit 1 family inet

```

## 2. 1?? ??? ?????.

```

[edit security ike proposal prop_ike]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy ikepol1]
user@host# set mode main
user@host# set proposals prop_ike
user@host# set certificate local-certificate Spoke1_ID
[edit security ike gateway SPOKE_GW]
user@host# set ike-policy ikepol1
user@host# set address 10.2.2.1
user@host# set local-identity distinguished-name
user@host# set remote-identity distinguished-name container DC=Domain_component
user@host# set external-interface ge-0/0/3.0
user@host# set version v1-only

```

3. `2?? ??? ?????.`

```
[edit security ipsec proposal prop_ipsec]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-192-cbc
user@host# set lifetime-seconds 3600
user@host# set lifetime-kilobytes 150000
[edit security ipsec policy ipsecpol1]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals prop_ipsec
[edit security ipsec SPOKE_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway SPOKE_GW
user@host# set ike ipsec-policy ipsecpol1
user@host# set traffic-selector ts1 local-ip 172.0.0.0/8
user@host# set traffic-selector ts1 remote-ip 192.0.0.0/8
user@host# set establish-tunnels immediately
```

4. `??? ??? ?????.`

```
[edit security pki]
user@host# set ca-profile rsa ca-identity rsa
user@host# set ca-profile rsa revocation-check disable
```

5. `?? ??? ?????.`

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/3.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces ge-0/0/1.0
[edit security policies]
user@host# set default-policy permit-all
```

??

?? ???? show interfaces, show security ike, show security ipsec, show security pki, show security zones ? show security policies ??? ???? ???? ?????. ?? ???? ???? ???? ???? ???? ? ? ? ???? ???? ???? ?????.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 172.16.1.1/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.2.2.253/24;
    }
  }
}
st0 {
  unit 1 {
    family inet;
  }
}
[edit]
user@host# show security ike
proposal prop_ike {
  authentication-method rsa-signatures;
  dh-group group5;
  authentication-algorithm sha1;
  encryption-algorithm aes-256-cbc;
}
policy ikepol1 {
  mode main;
  proposals prop_ike;
  certificate {
    local-certificate Spoke1_ID;
  }
}
gateway SPOKE_GW {
```

```

    ike-policy ikepol1;
    address 10.2.2.1;
    local-identity distinguished-name;
    remote-identity distinguished-name container DC=Domain_component;
    external-interface ge-0/0/3.0;
    version v1-only;
}
[edit]
user@host# show security ipsec
proposal prop_ipsec {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-192-cbc;
    lifetime-seconds 3600;
    lifetime-kilobytes 150000;
}
policy ipsecpol1 {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals prop_ipsec;
}
vpn SPOKE_VPN {
    bind-interface st0.1;
    ike {
        gateway SPOKE_GW;
        ipsec-policy ipsecpol1;
    }
    traffic-selector ts1 {
        local-ip 172.0.0.0/8;
        remote-ip 192.0.0.0/8;
    }
    establish-tunnels immediately;
}
[edit]
user@host# show security pki
ca-profile rsa {
    ca-identity rsa;
    revocation-check {
        disable;
    }
}
[edit]

```

```

user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/3.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

```

commit? (1) ?

??

#### in this section



?? ?? | 1295



ASA 9.7(3) VPN 9.7(3) VPN 9.7(3) VPN.

ASA 9.7

ASA

AutoVPN ASA 9.7(3) VPN 9.7(3) VPN 9.7(3) VPN 9.7(3) VPN.

ASA

ASA 9.7(3) VPN show security ike security-associations show security ipsec security-associations ASA 9.7(3) VPN.

```
user@host> show security ike security-associations
node0:
-----
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
1350248074 UP    d195bce6ccfcf9af  8f1569c6592c8408  Main           10.2.2.253

user@host> show security ipsec security-associations
node0:
-----
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<77594650 ESP:aes-cbc-192/sha1 ac97cb1 2799/ 150000 - root 500 10.2.2.253
>77594650 ESP:aes-cbc-192/sha1 828dc013 2798/ 150000 - root 500 10.2.2.253

user@host> show security ipsec security-associations detail
node0:
-----
ID: 77594650 Virtual-system: root, VPN Name: HUB_VPN
Local Gateway: 10.2.2.1, Remote Gateway: 10.2.2.253
Traffic Selector Name: ts1
Local Identity: ipv4(192.0.0.0-192.255.255.255)
Remote Identity: ipv4(172.0.0.0-172.255.255.255)
Version: IKEv1
```

```

DF-bit: clear, Bind-interface: st0.1
Port: 500, Nego#: 2, Fail#: 0, Def-Del#: 0 Flag: 0x24608b29
Tunnel events:
  Tue Dec 30 2014 11:30:21 -0800: IPSec SA negotiation successfully completed (1 times)
  Tue Dec 30 2014 11:30:20 -0800: Tunnel is ready. Waiting for trigger event or peer to
trigger negotiation (1 times)
  Tue Dec 30 2014 11:30:20 -0800: IKE SA negotiation successfully completed (3 times)
Location: FPC 5, PIC 0, KMD-Instance 1
Direction: inbound, SPI: ac97cb1, AUX-SPI: 0
  Hard lifetime: Expires in 2796 seconds
  Lifesize Remaining: 150000 kilobytes
  Soft lifetime: Expires in 2211 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (192 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64
Location: FPC 5, PIC 0, KMD-Instance 1
Direction: outbound, SPI: 828dc013, AUX-SPI: 0
  Hard lifetime: Expires in 2796 seconds
  Lifesize Remaining: 150000 kilobytes
  Soft lifetime: Expires in 2211 seconds
  Mode: Tunnel(0 0), Type: dynamic, State: installed
  Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (192 bits)
  Anti-replay service: counter-based enabled, Replay window size: 64

```

?? ???? ???? show security ike security-associations ? show security ipsec security-associations ??? ?????.

```

user@host> show security ike security-associations
Index   State Initiator cookie Responder cookie Mode Remote Address
276505646 UP d195bce6ccfcf9af 8f1569c6592c8408 Main 10.2.2.1

user@host> show security ipsec security-associations
Total active tunnels: 1
ID      Algorithm SPI Life:sec/kb Mon lsys Port Gateway
<69206018 ESP:aes-cbc-192/sha1 828dc013 2993/ 150000 - root 500 10.2.2.1
>69206018 ESP:aes-cbc-192/sha1 ac97cb1 2993/ 150000 - root 500 10.2.2.1

user@host> show security ipsec security-associations detail
ID: 69206018 Virtual-system: root, VPN Name: SPOKE_VPN
Local Gateway: 10.2.2.253, Remote Gateway: 10.2.2.1
Traffic Selector Name: ts1
Local Identity: ipv4(172.0.0.0-172.255.255.255)
Remote Identity: ipv4(192.0.0.0-192.255.255.255)

```



??

?? ???? ???? show security ipsec traffic-selector interface-name st0.1 ??? ?????.

```
user@host> show security ipsec traffic-selector interface-name st0.1
node0:
-----
Source IP                Destination IP                Interface  Tunnel-id  IKE-
ID
192.0.0.0-192.255.255.255  172.0.0.0-172.255.255.255  st0.1     77594650
DC=Domain_component, CN=Spoke1_ID, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
```

?? ???? ???? ???? ?????? show security ipsec traffic-selector interface-name st0.1 .

```
user@host> show security ipsec traffic-selector interface-name st0.1
Source IP                Destination IP                Interface  Tunnel-id  IKE-
ID
172.0.0.0-172.255.255.255  192.0.0.0-192.255.255.255  st0.1     69206018
DC=Domain_component, CN=Hub_ID, OU=Sales, O=XYZ, L=Sunnyvale, ST=CA, C=US
```

??

??? ???? ???? ?? ? ?? ???? ?? ? ?? ???? ?? ???? ???? ???? ???? IKE(Internet Key Exchange) ?? ?? ?????.  
??? ???? ???? ???? SA? ?? ?????. ??? ???? ???? ???? (SRX ??? ?) ?? ?????.

SEE ALSO

| [?? ?? VPN? ??? ??? ?????](#) | 578

**?: AutoVPN ? ??? ???? ?? VPN ?? ??? ??**

in this section

- [?? ??](#) | 1299
- [??](#) | 1299

? ???? SRX ??? ?????? ?? ???? ????? AutoVPN ??? ????? eNodeB ?????? ?? ?? ?? IPsec VPN ??????? ???? ?  
 ?????, ?? ?? ??(ARI)? ??? ???? ?????? eNodeB ?????? ??? ????? ????? ? ??????, ?? ?? ARI ??? BGP? ?? ?????  
 ?? ?? ?????? ??????, ? ????? ??? ?? ??? ????? ?????, ?? ?? ?? ??? ??? ?? ?:" iBGP" ??? 1067? ????? ??  
 AutoVPN ??.

☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐

- □□:

- ?? BGP ?? ???? ???? ???? ???? ???? eNodeB ???? ???? ???? ????.

in this section

- [????](#) | 1301

● [?] [?] [?] [?] | 1301

|            |                                  |
|------------|----------------------------------|
| ??         | ?? ?? ???? DC=Common_component   |
| IKE ??? ?? | ?? IKE(Internet Key Exchange) ID |
| ?? ?? ??   | probe-idle-tunnel                |
| ?? ID      | ?? ??                            |
| ??         | v2 ??                            |

**? 141: Georedundant AutoVPN ??? ? 1?? ? 2?? ?? (Continued)**

*IPsec* **??**:

|           |              |
|-----------|--------------|
| ???       | esp          |
| ?? ?????  | hmac-sha1-96 |
| ??? ????? | AES-256-CBC  |

*IPsec* :

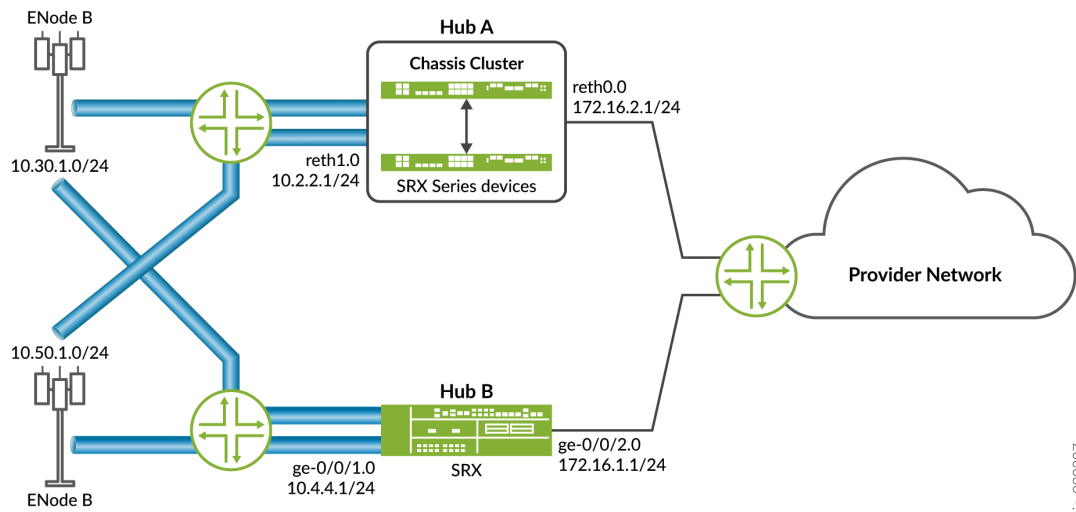
|                                 |        |
|---------------------------------|--------|
| PFS(Perfect Forward Secrecy) ?? | group5 |
|---------------------------------|--------|

? ???? ?? ???? ???? ?? ?? ???? ?? ?????? ??????, ?? ??? ? ? ? ???? ?? ??? ???? ???, ?? ?? ??? ????????.  
???? ?? SRX ??? ???? ??? ?? ???? ????? ????? ??????, ? ??? ???? ??? ???? ????.

□ □ □ □

?? 70 ??? 1302 ?(?) ? ??? ??? SRX ??? ????.

70: eNodeB IPsec VPN



??

in this section

- ?? A ?? | 1302
- ?? B ?? | 1312
- eNodeB ??(?? ??) | 1321

?? A ??

CLI ?? ??

?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??, ?? ?? ?? ?? ?? ?? ?? ?? ?? [edit] ?  
? ?? ?? ?? CLI? ?? ?? ?? ??, ?? ?? ?? commit?(?) ????

```
set interfaces ge-0/0/2 gigether-options redundant-parent reth1
set interfaces ge-0/0/3 gigether-options redundant-parent reth0
set interfaces ge-8/0/2 gigether-options redundant-parent reth1
set interfaces ge-8/0/3 gigether-options redundant-parent reth0
```



```

set interfaces lo0 unit 0 family inet address 10.100.1.100/24
set interfaces lo0 redundant-pseudo-interface-options redundancy-group 1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 172.16.2.1/24
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 10.2.2.1/24
set interfaces st0 unit 1 family inet
set security ike proposal prop_ike authentication-method rsa-signatures
set security ike proposal prop_ike dh-group group5
set security ike proposal prop_ike authentication-algorithm sha1
set security ike proposal prop_ike encryption-algorithm aes-256-cbc
set security ike policy ph1_ike_policy proposals prop_ike
set security ike policy ph1_ike_policy certificate local-certificate HubA_certificate
set security ike gateway HUB_GW ike-policy ph1_ike_policy
set security ike gateway HUB_GW dynamic distinguished-name wildcard DC=Common_component
set security ike gateway HUB_GW dynamic ike-user-type group-ike-id
set security ike gateway HUB_GW dead-peer-detection probe-idle-tunnel
set security ike gateway HUB_GW local-identity distinguished-name
set security ike gateway HUB_GW external-interface reth1
set security ike gateway HUB_GW version v2-only
set security ipsec proposal prop_ipsec protocol esp
set security ipsec proposal prop_ipsec authentication-algorithm hmac-sha1-96
set security ipsec proposal prop_ipsec encryption-algorithm aes-256-cbc
set security ipsec policy ph2_ipsec_policy perfect-forward-secrecy keys group5
set security ipsec policy ph2_ipsec_policy proposals prop_ipsec
set security ipsec vpn HUB_VPN bind-interface st0.1
set security ipsec vpn HUB_VPN ike gateway HUB_GW
set security ipsec vpn HUB_VPN ike ipsec-policy ph2_ipsec_policy
set security ipsec vpn HUB_VPN traffic-selector ts1 local-ip 172.16.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts1 remote-ip 10.50.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts2 local-ip 172.16.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts2 remote-ip 10.30.0.0/16
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 172.16.2.1
set protocols bgp group internal-peers export inject_ts1_routes
set protocols bgp group internal-peers export inject_ts2_routes
set protocols bgp group internal-peers export inject_up_routes
set protocols bgp group internal-peers neighbor 172.16.2.4
set policy-options policy-statement inject_ts1_routes term cp_allow from protocol static
set policy-options policy-statement inject_ts1_routes term cp_allow from route-filter
10.30.1.0/24 orlonger
set policy-options policy-statement inject_ts1_routes term cp_allow from route-filter
10.30.1.0/24 orlonger

```

```

set policy-options policy-statement inject_ts1_routes term cp_allow then next-hop self
set policy-options policy-statement inject_ts1_routes term cp_allow then accept
set policy-options policy-statement inject_ts2_routes term mp_allow from protocol static
set policy-options policy-statement inject_ts2_routes term mp_allow from route-filter
10.50.1.0/24 orlonger
set policy-options policy-statement inject_ts2_routes term mp_net_allow from route-filter
10.50.2.0/24 orlonger
set policy-options policy-statement inject_ts2_routes term mp_net_allow then next-hop self
set policy-options policy-statement inject_ts2_routes term mp_net_allow then accept
set policy-options policy-statement inject_up_routes term up_allow from protocol static
set policy-options policy-statement inject_up_routes term up_allow from route-filter
172.16.1.0/24 orlonger
set policy-options policy-statement inject_up_routes term up_allow from route-filter
172.16.2.0/24 orlonger
set policy-options policy-statement inject_up_routes term up_allow then next-hop self
set policy-options policy-statement inject_up_routes term up_allow then accept
set security pki ca-profile csa ca-identity csa
set security pki ca-profile csa revocation-check disable
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces st0.1
set security zones security-zone trust interfaces reth0.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces reth1.0
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ??? ?????.

?? A? ???? ???? ????.

1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/2 gigether-options redundant-parent reth1
user@host# set ge-0/0/3 gigether-options redundant-parent reth0
user@host# set ge-8/0/2 gigether-options redundant-parent reth1
user@host# set ge-8/0/3 gigether-options redundant-parent reth0
user@host# set lo0 unit 0 family inet address 10.100.1.100/24

```

```

user@host# set lo0 redundant-pseudo-interface-options redundancy-group 1
user@host# set reth0 redundant-ether-options redundancy-group 1
user@host# set reth0 unit 0 family inet address 172.16.2.1/24
user@host# set reth1 redundant-ether-options redundancy-group 1
user@host# set reth1 unit 0 family inet address 10.2.2.1/24
user@host# set st0 unit 1 family inet

```

## 2. 1?? ???? ?????.

```

[edit security ike proposal prop_ike]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy ph1_ike_policy]
user@host# set proposals prop_ike
user@host# set certificate local-certificate HubA_certificate
[edit security ike gateway HUB_GW]
user@host# set ike-policy ph1_ike_policy
user@host# set dynamic distinguished-name wildcard DC=Common_component
user@host# set dynamic ike-user-type group-ike-id
user@host# set dead-peer-detection probe-idle-tunnel
user@host# set local-identity distinguished-name
user@host# set external-interface reth1
user@host# set version v2-only

```

## 3. 2?? ???? ?????.

```

[edit security ipsec proposal prop_ipsec]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy ph2_ipsec_policy]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals prop_ipsec
[edit security ipsec vpn HUB_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway HUB_GW
user@host# set ike ipsec-policy ph2_ipsec_policy
user@host# set traffic-selector ts1 local-ip 172.16.0.0/16
user@host# set traffic-selector ts1 remote-ip 10.50.0.0/16

```

```

user@host# set traffic-selector ts2 local-ip 172.16.0.0/16
user@host# set traffic-selector ts2 remote-ip 10.30.0.0/16

```

#### 4. BGP `???` `?????` `??????`.

```

[edit protocols bgp group internal-peers]
user@host# set type internal
user@host# set local-address 172.16.2.1
user@host# set export inject_ts1_routes
user@host# set export inject_ts2_routes
user@host# set export inject_up_routes
user@host# set neighbor 172.16.2.4

```

#### 5. `???` `???` `??????`.

```

[edit policy-options policy-statement inject_ts1_routes]
user@host# set term cp_allow from protocol static
user@host# set term cp_allow from route-filter 10.30.2.0/24 orlonger
user@host# set term cp_allow from route-filter 10.30.1.0/24 orlonger
user@host# set term cp_allow then next-hop self
user@host# set term cp_allow then accept
[edit policy-options policy-statement inject_ts2_routes]
user@host# set term mp_allow from protocol static
user@host# set term mp_allow from route-filter 10.50.1.0/24 orlonger
user@host# set term mp_allow from route-filter 10.50.2.0/24 orlonger
user@host# set term mp_allow then next-hop self
user@host# set term mp_allow then accept
[edit policy-options policy-statement inject_up_routes]
user@host# set term up_allow from protocol static
user@host# set term up_allow from route-filter 172.16.1.0/24 orlonger
user@host# set term up_allow from route-filter 172.16.2.0/24 orlonger
user@host# set term up_allow then next-hop self
user@host# set term up_allow then accept

```

#### 6. `???` `???` `??????`.

```

[edit security pki]
user@host# set ca-profile csa ca-identity csa
user@host# set ca-profile csa revocation-check disable

```



```

        redundant-parent reth0;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.100.1.100/24;
        }
    }
    redundant-pseudo-interface-options {
        redundancy-group 1;
    }
}
reth0 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 172.16.2.1/16;
        }
    }
}
reth1 {
    redundant-ether-options {
        redundancy-group 1;
    }
    unit 0 {
        family inet {
            address 10.2.2.1/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
[edit]
user@host# show security ike
proposal prop_ike {
    authentication-method rsa-signatures;
    dh-group group5;

```

```

        authentication-algorithm sha1;
        encryption-algorithm aes-256-cbc;
    }
    policy ph1_ike_policy {
        proposals prop_ike;
        certificate {
            local-certificate HubA_certificate;
        }
    }
    gateway HUB_GW {
        ike-policy ph1_ike_policy;
        dynamic {
            distinguished-name {
                wildcard DC=Common_component;
            }
            ike-user-type group-ike-id;
        }
        dead-peer-detection {
            probe-idle-tunnel;
        }
        local-identity distinguished-name;
        external-interface reth1;
        version v2-only;
    }
[edit]
user@host# show security ipsec
    proposal prop_ipsec {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-256-cbc;
    }
    policy ph2_ipsec_policy {
        perfect-forward-secrecy {
            keys group5;
        }
        proposals prop_ipsec;
    }
    vpn HUB_VPN {
        bind-interface st0.1;
        ike {
            gateway HUB_GW;
            ipsec-policy ph2_ipsec_policy;
        }
    }

```

```

        traffic-selector ts1 {
            local-ip 172.16.0.0/16;
            remote-ip 10.50.0.0/16;
        }
        traffic-selector ts2 {
            local-ip 172.16.0.0/16;
            remote-ip 10.30.0.0/16;
        }
    }
[edit]
user@host# show protocols bgp
    group internal-peers {
        type internal;
        local-address 172.16.2.1;
        export [ inject_ts1_routes inject_ts2_routes inject_up_routes ];
        neighbor 172.16.2.4;
    }
[edit]
user@host# show policy-options
policy-statement inject_ts1_routes {
    term cp_allow {
        from {
            protocol static;
            route-filter 10.30.2.0/24 orlonger;
            route-filter 10.30.1.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}
policy-statement inject_ts2_routes {
    term mp_allow {
        from {
            protocol static;
            route-filter 10.50.1.0/24 orlonger;
            route-filter 10.50.2.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}

```



```

    }
}
policy-statement inject_up_routes {
    term up_allow {
        from {
            protocol static;
            route-filter 172.16.1.0/24 orlonger;
            route-filter 172.16.2.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}
[edit]
user@host# show security pki
ca-profile csa {
    ca-identity csa;
    revocation-check {
        disable;
    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        reth0.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;

```

```

    }
    protocols {
        all;
    }
}
interfaces {
    lo0.0;
    reth1.0;
}
}
[edit]
user@host# show security policies
    default-policy {
        permit-all;
    }

```

```

?? ?? ???? ? ???? commit?(?) ??????.

```

**?? B ??**

**CLI ?? ??**

```

? ?? ???? ?????, ?? ??? ????? ???? ???? ? ? ? ? ? ? ???? ???? ???? ???? ???? ???? [edit] ?
? ????? ???? CLI? ???? ? ? ? ? ? ? ???? commit?(?) ??????.

```

```

set interfaces ge-0/0/1 unit 0 family inet address 10.4.4.1/24
set interfaces ge-0/0/2 unit 0 family inet address 172.16.1.1/16
set interfaces lo0 unit 0 family inet address 10.100.1.101/24
set interfaces st0 unit 1 family inet
set security ike proposal prop_ike authentication-method rsa-signatures
set security ike proposal prop_ike dh-group group5
set security ike proposal prop_ike authentication-algorithm sha1
set security ike proposal prop_ike encryption-algorithm aes-256-cbc
set security ike policy ph1_ike_policy proposals prop_ike
set security ike policy ph1_ike_policy certificate local-certificate HubB_certificate
set security ike gateway HUB_GW ike-policy ph1_ike_policy
set security ike gateway HUB_GW dynamic distinguished-name wildcard DC=Common_component
set security ike gateway HUB_GW dynamic ike-user-type group-ike-id
set security ike gateway HUB_GW dead-peer-detection probe-idle-tunnel
set security ike gateway HUB_GW local-identity distinguished-name
set security ike gateway HUB_GW external-interface ge-0/0/1
set security ike gateway HUB_GW version v2-only

```

```

set security ipsec proposal prop_ipsec protocol esp
set security ipsec proposal prop_ipsec authentication-algorithm hmac-sha1-96
set security ipsec proposal prop_ipsec encryption-algorithm aes-256-cbc
set security ipsec policy ph2_ipsec_policy perfect-forward-secrecy keys group5
set security ipsec policy ph2_ipsec_policy proposals prop_ipsec
set security ipsec vpn HUB_VPN bind-interface st0.1
set security ipsec vpn HUB_VPN ike gateway HUB_GW
set security ipsec vpn HUB_VPN ike ipsec-policy ph2_ipsec_policy
set security ipsec vpn HUB_VPN traffic-selector ts1 local-ip 172.16.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts1 remote-ip 10.50.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts2 local-ip 172.16.0.0/16
set security ipsec vpn HUB_VPN traffic-selector ts2 remote-ip 10.30.0.0/8
set protocols bgp group internal-peers type internal
set protocols bgp group internal-peers local-address 172.16.1.1
set protocols bgp group internal-peers export inject_ts1_routes
set protocols bgp group internal-peers export inject_ts2_routes
set protocols bgp group internal-peers export inject_up_routes
set policy-options policy-statement inject_ts1_routes term cp_allow from protocol static
set policy-options policy-statement inject_ts1_routes term cp_allow from route-filter
10.30.2.0/24 orlonger
set policy-options policy-statement inject_ts1_routes term cp_allow from route-filter
10.30.1.0/24 orlonger
set policy-options policy-statement inject_ts1_routes term cp_allow then next-hop self
set policy-options policy-statement inject_ts1_routes term cp_allow then accept
set policy-options policy-statement inject_ts2_routes term mp_allow from protocol static
set policy-options policy-statement inject_ts2_routes term mp_allow from route-filter
10.50.1.0/24 orlonger
set policy-options policy-statement inject_ts2_routes term mp_net_allow from route-filter
10.50.2.0/24 orlonger
set policy-options policy-statement inject_ts2_routes term mp_net_allow then next-hop self
set policy-options policy-statement inject_ts2_routes term mp_net_allow then accept
set policy-options policy-statement inject_up_routes term up_allow from protocol static
set policy-options policy-statement inject_up_routes term up_allow from route-filter
172.16.1.0/24 orlonger
set policy-options policy-statement inject_up_routes term up_allow from route-filter
172.16.2.0/24 orlonger
set policy-options policy-statement inject_up_routes term up_allow then next-hop self
set policy-options policy-statement inject_up_routes term up_allow then accept
set security pki ca-profile csa ca-identity csa
set security pki ca-profile csa revocation-check disable
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces st0.1

```

```

set security zones security-zone trust interfaces ge-0/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces lo0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security policies default-policy permit-all

```

???

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ???? CLI ??? ???? ?? ???? CLI ??? ???? ?????.

?? B? ???? ???? ????.

## 1. ???? ????.

```

[edit interfaces]
user@host# set ge-0/0/1 unit 0 family inet address 10.4.4.1/24
user@host# set ge-0/0/2 unit 0 family inet address 172.16.1.1/16
user@host# set lo0 unit 0 family inet address 10.100.1.101/24
user@host# set st0 unit 1 family inet

```

## 2. 1?? ???? ????.

```

[edit security ike proposal prop_ike]
user@host# set authentication-method rsa-signatures
user@host# set dh-group group5
user@host# set authentication-algorithm sha1
user@host# set encryption-algorithm aes-256-cbc
[edit security ike policy ph1_ike_policy]
user@host# set proposals prop_ike
user@host# set certificate local-certificate HubB_certificate
[edit security ike gateway HUB_GW]
user@host# set ike-policy ph1_ike_policy
user@host# set dynamic distinguished-name wildcard DC=Common_component
user@host# set dynamic ike-user-type group-ike-id
user@host# set dead-peer-detection probe-idle-tunnel
user@host# set local-identity distinguished-name
user@host# set external-interface ge-0/0/1
user@host# set version v2-only

```

3. `set ipsec`.

```
[edit security ipsec proposal prop_ipsec]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm aes-256-cbc
[edit security ipsec policy ph2_ipsec_policy]
user@host# set perfect-forward-secrecy keys group5
user@host# set proposals prop_ipsec
[edit security ipsec vpn HUB_VPN]
user@host# set bind-interface st0.1
user@host# set ike gateway HUB_GW
user@host# set ike ipsec-policy ph2_ipsec_policy
user@host# set traffic-selector ts1 local-ip 172.16.0.0/16
user@host# set traffic-selector ts1 remote-ip 10.50.0.0/16
user@host# set traffic-selector ts2 local-ip 172.16.0.0/16
user@host# set traffic-selector ts2 remote-ip 10.30.0.0/16
```

4. BGP `set internal`.

```
[edit protocols bgp group internal-peers]
user@host# set type internal
user@host# set local-address 172.16.1.1
user@host# set export inject_ts1_routes
user@host# set export inject_ts2_routes
user@host# set export inject_up_routes
user@host# set neighbor 172.16.1.2
```

5. `set policy`.

```
[edit policy-options policy-statement inject_ts1_routes]
user@host# set term cp_allow from protocol static
user@host# set term cp_allow from route-filter 10.30.2.0/24 orlonger
user@host# set term cp_allow from route-filter 10.30.1.0/24 orlonger
user@host# set term cp_allow then next-hop self
user@host# set term cp_allow then accept
[edit policy-options policy-statement inject_ts2_routes]
user@host# set term mp_allow from protocol static
user@host# set term mp_allow from route-filter 10.50.1.0/24 orlonger
user@host# set term mp_allow from route-filter 10.50.2.0/24 orlonger
```

```
[edit security pki]
user@host# set ca-profile csa ca-identity csa
user@host# set ca-profile csa revocation-check disable
```

```
[edit security zones security-zone trust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces st0.1
user@host# set interfaces ge-0/0/2.0
[edit security zones security-zone untrust]
user@host# set host-inbound-traffic system-services all
user@host# set host-inbound-traffic protocols all
user@host# set interfaces lo0.0
user@host# set interfaces ge-0/0/1.0
[edit security policies]
user@host# set default-policy permit-all
```

```

?? ???? , show security ipsec, show protocols bgp, show security pki, show security zones? show security policies ?
?? ???? show interfaces show security ike???? ??????. ?? ??? ??? ????? ?????? ?? ? ?? ??? ????? ??? ??????.

```

```
[edit]
user@host# show interfaces
    ge-0/0/1 {
        unit 0 {
```

```

        family inet {
            address 10.4.4.1/24;
        }
    }
}
ge-0/0/2 {
    unit 0 {
        family inet {
            address 172.16.1.1/16;
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.100.1.101/24;
        }
    }
}
st0 {
    unit 1 {
        family inet;
    }
}
[edit]
user@host# show security ike
    proposal prop_ike {
        authentication-method rsa-signatures;
        dh-group group5;
        authentication-algorithm sha1;
        encryption-algorithm aes-256-cbc;
    }
    policy ph1_ike_policy {
        proposals prop_ike;
        certificate {
            local-certificate HubB_certificate;
        }
    }
    gateway HUB_GW {
        ike-policy ph1_ike_policy;
        dynamic {
            distinguished-name {
                wildcard DC=Common_component;
            }
        }
    }
}

```

```

    }
    ike-user-type group-ike-id;
}
dead-peer-detection {
    probe-idle-tunnel;
}
local-identity distinguished-name;
external-interface reth1;
version v2-only;
}
[edit]
user@host# show security ipsec
proposal prop_ipsec {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-256-cbc;
}
policy ph2_ipsec_policy {
    perfect-forward-secrecy {
        keys group5;
    }
    proposals prop_ipsec;
}
vpn HUB_VPN {
    bind-interface st0.1;
    ike {
        gateway HUB_GW;
        ipsec-policy ph2_ipsec_policy;
    }
    traffic-selector ts1 {
        local-ip 172.16.0.0/16;
        remote-ip 10.50.0.0/16;
    }
    traffic-selector ts2 {
        local-ip 172.16.0.0/16;
        remote-ip 10.30.0.0/16;
    }
}
[edit]
user@host# show protocols bgp
group internal-peers {
    type internal;
    local-address 172.16.1.1;

```



```

        export [ inject_ts1_routes inject_ts2_routes inject_up_routes ];
        neighbor 172.16.1.2;
    }
user@host# show policy-options
policy-statement inject_ts1_routes {
    term cp_allow {
        from {
            protocol static;
            route-filter 10.30.2.0/24 orlonger;
            route-filter 10.30.1.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}
policy-statement inject_ts2_routes {
    term mp_allow {
        from {
            protocol static;
            route-filter 10.50.1.0/24 orlonger;
            route-filter 10.50.2.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}
policy-statement inject_up_routes {
    term up_allow {
        from {
            protocol static;
            route-filter 172.16.1.0/24 orlonger;
            route-filter 172.16.2.0/24 orlonger;
        }
        then {
            next-hop self;
            accept;
        }
    }
}

```

```
[edit]
user@host# show security pki
ca-profile csa {
    ca-identity csa;
    revocation-check {
        disable;
    }
}
[edit]
user@host# show security zones
security-zone trust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/2.0;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        ge-0/0/1.0;
        lo0.0;
    }
}
[edit]
user@host# show security policies
default-policy {
```

```
    permit-all;
}
```

?? ?? ?? ?? ?? ?? commit?(?) ?????.

## eNodeB ??(?? ??)

??? ??

1. ? ?? eNodeB ??? ?????? ??????. ??? eNodeB ?? ??? ? ??? ??? ??????. eNodeB ????? ?? ??? ?????? ?? ?.

- ?? ??(X.509v3) ? IKE ID ??
- SRX ??? IKE ID ?? ? ?? IP ??
- SRX ??? ??? ??? ????? 1?? ? 2?? ??

??

? ??? eNodeB ????? IPsec ?? VPN ??? ?? strongSwan ?? ?? ?????? ??????.

```
config setup
    plutostart=yes
    plutodebug=all
    charondebug="ike 4, cfg 4, chd 4, enc 1"
    charonstart=yes #ikev2 daemon"
    nat_traversal=yes #<===== need to enable even no nat_t

conn %default
    ikelifetime=60m
    keylife=45m
    rekeymargin=2m
    keyingtries=4
    mobike=no

conn Hub_A
    keyexchange=ikev2
    authby=pubkey
    ike=aes256-sha-modp1536
    esp=aes256-sha1-modp1536
    leftcert=/usr/local/etc/ipsec.d/certs/fight02Req.pem.Email.crt
    left=10.5.5.1 # self if
```

```

    leftsubnet=10.1.1.0/24 # left subnet
    leftid="CN=fight02, DC=Common_component, OU=Dept, O=Company, L=City, ST=CA, C=US " #
self id
    right=10.2.2.1 # peer if
    rightsubnet=10.1.1.0/24 # peer net for proxy id
    rightid="DC=Domain_component, CN=HubA_certificate, OU=Dept, O=Company, L=City, ST=CA,
C=US " # peer id
    auto=add
    leftfirewall=yes
    dpdaction=restart
    dpddelay=10
    dpdtimeout=120
    rekeyfuzz=10%
    reauth=no

conn Hub_B
    keyexchange=ikev2
    authby=pubkey
    ike=aes256-sha-modp1536
    esp=aes192-sha1-modp1536
    leftcert=/usr/local/etc/ipsec.d/certs/fight02Req.pem.Email.crt
    left=10.5.5.1 # self if
    leftsubnet=10.1.1.0/24 # self net for proxy id
    leftid="CN=fight02, DC=Common_component, OU=Dept, O=Company, L=City, ST=CA, C=US " #
self id
    right=10.4.4.1 # peer if
    rightsubnet=10.1.1.0/24 # peer net for proxy id
    rightid="DC=Domain_component, CN=HubB_certificate, OU=Dept, O=Company, L=City, ST=CA,
C=US " # peer id
    auto=add
    leftfirewall=yes
    dpdaction=restart
    dpddelay=10
    dpdtimeout=120
    rekeyfuzz=10%
    reauth=no

```

??

in this section

- AutoVPN [???? ? ?](#) | 1323
- [?? ? ? ?](#) | 1324
- ARI [? ?](#) | 1324

?? ???? ???? ???? ????.

AutoVPN [???? ? ?](#)

??

AutoVPN [???](#) eNodeB [???? ? ?](#) [?????? ?????](#).

??

[? ???? ??](#) show security ike security-associations [?](#) show security ipsec security-associations [??? ?????](#).

```
user@host> show security ike security-associations
node0:
-----
Index   State Initiator cookie Responder cookie Mode Remote Address
276505706 UP 16d6e53f0866b5cc ccd8ca944da7b63e IKEv2 10.5.5.1
1350247532 UP d5f0cb3a3b18cb92 91269f05527217a0 IKEv2 10.1.1.1

user@host> show security ipsec security-associations
node0:
-----
Total active tunnels: 2
ID      Algorithm      SPI      Life:sec/kb Mon lsys Port Gateway
<77594626 ESP:aes-cbc-192/sha1 a82bbc3 3600/ 64 - root 500 10.1.1.1
>77594626 ESP:aes-cbc-192/sha1 c930a858 3600/ 64 - root 500 10.1.1.1
<69206018 ESP:aes-cbc-192/sha1 2b437fc 3600/ 64 - root 500 10.5.5.1
>69206018 ESP:aes-cbc-192/sha1 c6e02755 3600/ 64 - root 500 10.5.5.1
```

??

show security ike security-associations **???** **??** **??** IKE(Internet Key Exchange) **1??** SA? **??????**. show security ipsec security-associations **???** **??** **??** IKE **2??** SA? **??????**, **?????** **?** eNodeB **??????** **????** **?** **??** **??** **????** **??????**.

IKE(Internet Key Exchange) **1????** **??** SA? **?????** **????** **1??** **????** **????** **??** **?????**, **?????** IKE(Internet Key Exchange) **??** **??** **??** **?** **??** **??????** **????** **??????**, **1??** **??** **??** **????** **??** **?** eNodeB **???????** **?????** **?????**.

IKE(Internet Key Exchange) **2????** **??** SA? **?????** **????** **2??** **????** **????** **??** **?????**, **?????** IKE(Internet Key Exchange) **??** **??** **??** **?** **??** **??????** **????** **??????**, **2??** **??** **??** **????** **??** **?** eNodeB **???????** **?????** **?????**.

**????** **????** **??**

??

**????** **?????** **???????**.

??

**??** **?????** show security ipsec traffic-selector interface-name st0.1 **????** **???????**.

```
user@host> show security ipsec traffic-selector interface-name st0.1
node0:
-----
Source IP                Destination IP                Interface  Tunnel-id  IKE-
ID
10.1.1.0-10.1.1.255      10.1.1.0-10.1.1.255        st0.1     69206018
DC=Common_component, CN=enodebA, OU=Dept, O=Company, L=City, ST=CA, C=US
10.1.1.0-10.1.1.255      10.1.1.0-10.1.1.255        st0.1     77594626
DC=Common_component, CN=enodebB, OU=Dept, O=Company, L=City, ST=CA, C=US
```

??

**????** **?????** **?????** **??** **?** **??** **????** **??** **?** **??** **?????** **??** **????** **?????** **?????** **?????** IKE(Internet Key Exchange) **??** **??** **???????**.  
**????** **?????** **?????** **?????** SA? **??** **???????**, **????** **?????** **?????** **?????**(SRX **????** **??**) **??** **???????**.

**ARI** **??** **??**

??

**ARI** **????** **????** **?????** **???????** **???????**.

??

?? ???? show route ??? ????.

```

user@host> show route
inet.0: 23 destinations, 23 routes (22 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.1.0.0/16      *[Static/5] 02:57:57
                 > to 2.2.2.253 via reth1.0
10.2.2.0/24      *[Direct/0] 02:58:43
                 > via reth1.0
10.2.2.1/32      *[Local/0] 02:59:25
                 Local via reth1.0
10.5.0.0/16      *[Static/5] 02:57:57
                 > to 2.2.2.253 via reth1.0
10.157.64.0/19   *[Direct/0] 21:54:52
                 > via fxp0.0
10.157.75.117/32 *[Local/0] 21:54:52
                 Local via fxp0.0
10.254.75.117/32 *[Direct/0] 21:54:52
                 > via lo0.0
10.30.1.0/24     *[ARI-TS/5] 02:28:10      [ARI route added based on TSi]
                 > via st0.1
10.50.1.0/24     *[ARI-TS/5] 02:28:26
                 > via st0.1
10.80.0.0/16     *[Direct/0] 02:57:57
                 > via reth0.0
10.80.1.1/32     *[Local/0] 02:57:57
                 Local via reth0.0
10.100.1.0/24    *[Direct/0] 02:57:57
                 > via lo0.0
10.100.1.100/32  *[Local/0] 02:57:57
                 Local via lo0.0
10.102.1.0/24    *[Static/5] 02:57:57
                 > to 10.2.2.253 via reth1.0
10.104.1.0/24    *[Static/5] 02:57:57
                 > to 10.2.2.253 via reth1.0
172.16.0.0/12    *[Static/5] 21:54:52

```

??

?? ?? ??(ARI)? ?? ?? ?????? ????? ?? ?????? ????? ?? ?? ??? ????? ??????, ??? ??? ????? ??? ?? IP ??? ???  
? ??????, ??? ????? ??, ??? ?? ??? VPN? ????? st0 ?????? ??? ?????? ????? ??????.

eNodeB ?? ? ?? ?? ?? 10.30.1.0/24 ? 10.50.1.0/24? SRX ??? ??? ???? ??????, ??? ??? st0.1 ??????  
? ?? ??? ? ?????.

SEE ALSO

| [?? ?? VPN? ??? ??? ????? | 578](#)

**?: ?? ?? ?? ????? AutoVPN ??**

in this section

- [?? ?? | 1326](#)
- [?? IKE ?? ?? ? ?? | 1327](#)
- [??? IKE ?? ?? ? ?? | 1329](#)

? ?????? ?? ??? ?????? ?? VPN ?????????? ?????? ?? IKE ?? ?? ?? ?????? ??? ?? ???, ?????? VPN ?????????? ?? ??  
? ????? ? ?????? ?? ??? IKE ?? ?? ?? ??????.

AutoVPN? ?? ? ?? ??? ????? ? ??? ?? ?? ????????

**?? ??**

? ??? ?????? ????? ? ?????? ?? ??? ??? ?????.

- AutoVPN? ????? MX-SPC3 ? Junos OS ??? 21.1R1? ??? MX240, MX480 ? MX960
- ?? AutoVPN? ????? SPC3 ? Junos OS ??? 21.2R1? SRX5000 ??
- ?? AutoVPN? junos-ike ????? iked ?????(???? ??) ? Junos OS ??? 21.2R1? ????? vSRX ?? ???







VPN [redacted] IKE [redacted]

- ```
[edit]
user@host# set security ike policy IKE_POL pre-shared-key ascii-text ascii text
```

```
user@host# # set security ike policy IKE_POL pre-shared-key ascii-text
ThisIsMySecretPreSharedkey
```

- ```
[edit]
user@peer# set security ike policy IKE_POL pre-shared-key ascii-text ascii text
```

```
user@peer# set security ike policy IKE_POL pre-shared-key ascii-text
ThisIsMySecretPreSharedkey
```

- ```
[edit]
user@host# set security ike gateway HUB_GW dynamic general-ikeid
```

??

?? ???? show security ??? ???? ???? ?????. ?? ??? ???? ???? ???? ? ? ? ???? ???? ???? ?????.

```
[edit]
user@host> show security
  ike {
    proposal IKE_PROP {
      authentication-method pre-shared-keys;
      dh-group group14;
      authentication-algorithm sha-256;
      encryption-algorithm aes-256-cbc;
      lifetime-seconds 750;
    }
    policy IKE_POL {
      proposals IKE_PROP;
      pre-shared-key ascii-text "$9$wo2oGk.569pDi9p0BSys24"; ## SECRET-DATA
    }
    gateway HUB_GW {
      ike-policy IKE_POL;
      dynamic {
        general-ikeid;
        ike-user-type group-ike-id;
      }
      local-identity user-at-hostname user1@juniper.net;
      external-interface lo0;
      local-address 11.0.0.1;
      version v2-only;
    }
  }
```

## P2MP ???? ???? ? ?

? ???? P2MP ???? ???? ???? ???? ???? ????.

???? ? ? ???? ???? ? "PIM? ? ? ??" ??? 1058 ? ? ? ? ? ? ? ?.

? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?.

????? ?????? ??

- st0.0 ?????? PIM? ?????? ??? ??????.set protocols pim interface *interface-name* command

```
[edit]
user@host# set protocols pim interface st0.0
```

st0.0 ?????? ?? ?? ?????? ?????.

- P2MP ??? ?? st0.0 ?????? ?????? ?????? ??? ?????? set interfaces *interface-name* unit *unit-number* multipoint .

```
[edit]
user@host# set interfaces st0.0 unit 0 multipoint
```

- st0.0 ?????? ?? IPv4 ??? ?????? ??? ??????.set interfaces *interface-name* unit *unit-number* family inet address *IPv4 address*

```
[edit]
user@host# set interfaces st0.0 unit 0 family inet address 192.168.1.3/24
```

??? 192.168.1.3/24? ?????? IP ?????.

- st0.0 ?????? PIM? ?????? ?? ??? disable????.

```
[edit]
user@host# set protocols pim interface st0.0 disable
```

????? ??? ?????? ?? CLI ??

?? ??? ?????? ?????? ??? ??? ? ?????.

- PIM ?????? ?????? ??? ?????? show pim interfaces .
- ?????? ??? ??? ??? ?????? ??? ?????? show pim join extensive .
- IP ?????? ??? ?????? ??? ??? ?????? show multicast route .
- ?????? ?? ? ?? ??? ??? ??? ?????? show multicast next-hops detail .
- IP ?????? ??? ??? ??? ?????? show multicast statistics .

- `show route forwarding-table extensive`.

SEE ALSO

|                           |
|---------------------------|
| <a href="#">PIM</a>       |
| <a href="#">PIM (PIM)</a> |
| <a href="#">pim</a>       |
| <a href="#">pim</a>       |
| <a href="#">PIM</a>       |
| <a href="#">PIM</a>       |
| <a href="#">PIM</a>       |
| <a href="#">PIM</a>       |

AutoVPN

in this section

• [PIM](#) | 1332

• [PIM](#) | 1333

142:

| SRX | <ul style="list-style-type: none"><li>• PSK SPC3 vSRX SRX5000 PSK AutoVPN iked IPsec VPN junos-ike PSK AutoVPN.</li></ul> |
|-----|---------------------------------------------------------------------------------------------------------------------------|



# 11

CHAPTER LABEL COVER PAGE

## ?? ???? VPN

---

### in this chapter

- [Juniper Secure Connect | 1335](#)
-



Juniper Secure Connect [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted].

in this section

- Juniper Secure Connect [?] | 1336
- [?] [?] | 1336

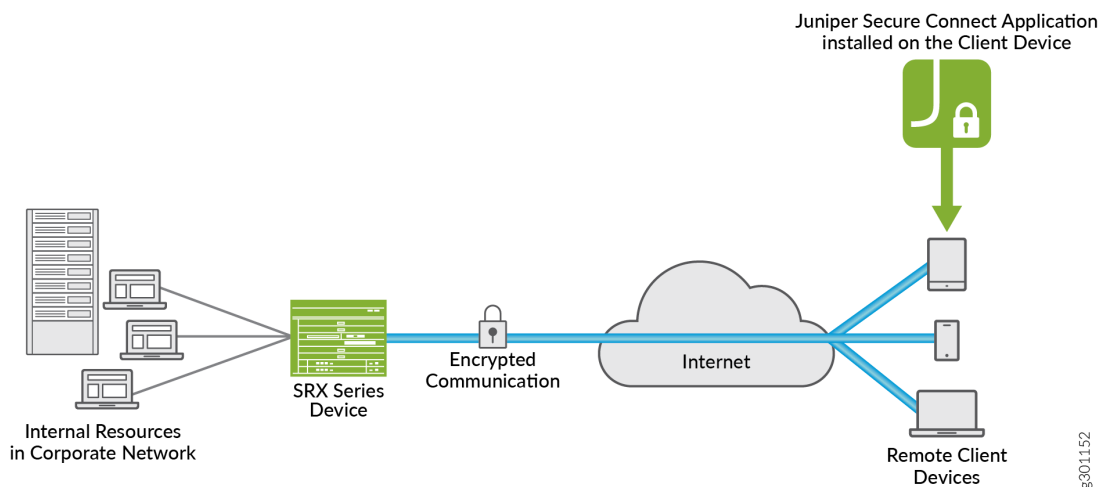
Juniper Secure Connect? ?? ??? ????? ????? ????? ?? ? ????? ? ??? ??? ?????? ?? SSL-VPN ??????????. ? ?  
 ?????? SRX ??? ????? ????? ????? ??? ? ?? ????? ?????? ????? ????? ??? ??? ??? ??? ? ?????, Juniper  
 Secure Connect? ?? VPN ??? ????? ????? ????? ????????? ?????? ??????

Juniper Secure Connect [REDACTED] [REDACTED] [REDACTED].

- SRX **???** **???** - Juniper Secure Connect **????** **??** **????** **??** **??????** **???** **??** **??** **???** **??** **??** **??** **????** **??????**.
- Juniper Secure Connect **??????** - Microsoft Windows, Apple macOS, Google Android **?** iOS **??** **??** **?** **?** **??** **????** **????** **???** **??????** **??** **????** **??????**. Juniper Secure Connect **????????** VPN **???** **??** SRX **???** **????** **????** **??????** **????** **???** **??** **????** **????**.

? ? 71 ? ? ? 1335?(?) ? ? ? ? ? ? ? ? ? ? VPN ? ? ? ? ? ? ? Juniper Secure Connect ? ? ? ? ? ? ? ? ? ?  
?.

**71: Juniper Secure Connect**



## 144: Juniper Secure Connect



?: Junos-FIPS [edit system services] web-management , FIPS SRX Junos-FIPS Juniper Junos-FIPS SRX . SRX > FIPS ?

?? ??

??

Junos OS VPN Juniper Secure Connect

Juniper Secure Connect

# 12

CHAPTER LABEL COVER PAGE

## VPN [?][?][?][?]

---

### in this chapter

- VPN [?][?][?][?] | 1339
  - VPN [?][?][?][?] | 1340
  - VPN [?][?], [?][?] [?][?][?] | 1349
-

# VPN 配置 指南

## summary

在 Junos OS 中配置 VPN 的步骤如下：

## in this section

● [VPN 配置 指南 | 1339](#)

VPN 配置包括以下步骤：配置 VPN 隧道、配置 VPN 用户、配置 VPN 策略。VPN 配置完成后，用户可以通过 VPN 隧道访问网络资源。

SRX 设备支持 SRX1 和 SRX2 两种 VPN 配置模式。SRX1 模式适用于单用户配置，SRX2 模式适用于多用户配置。SRX2 模式配置步骤如下：

- 配置 SRX2 模式 VPN 隧道。
- 配置 SRX2 模式 VPN 用户。
- 配置 SRX2 模式 VPN 策略。
- 配置 SRX2 模式 VPN 隧道。
- 配置 SRX2 模式 VPN 用户。
- 配置 SRX2 模式 VPN 策略。

在 SRX2 模式下配置 VPN 的步骤如下：

## VPN 配置 指南

Junos OS 中配置 VPN 的步骤如下：

- 配置 VPN 隧道。
- 配置 IKE(Internet Key Exchange) 隧道。
- 配置 VPN 用户。
- 配置 SPI(Security Parameter Index) 策略。
- 配置 VPN 策略。

?? ??

VPN [???? ??](#) | 1340

VPN [??, ?? ? ???](#) | 1349

# VPN [????](#) [??](#)

## summary

SRX [????](#) [??????](#) VPN [????](#) [??????](#) ? [??](#) [??](#) [??](#) [????](#) [??????](#) ? [????](#) [??????](#).

## in this section

- [IPsec \[???\]\(#\) \[??\]\(#\) \[??\]\(#\)](#) | 1341
- [Dead Peer Detection\(\[??\]\(#\) \[??\]\(#\) \[??\]\(#\)\)](#) | 1342
- [VPN \[??\]\(#\) \[????\]\(#\)](#) | 1345
- [Dead Peer Detection \[??\]\(#\)](#) | 1346
- [VPN \[??\]\(#\) \[????\]\(#\) \[??\]\(#\)](#) | 1347
- [???? VPN \[????\]\(#\) \[??\]\(#\)](#) | 1348

VPN [????](#) [??](#) [????](#) [????](#) [????](#) [??????](#), [????](#) [??](#) [????????](#) [??](#) [????](#) [????](#), [??](#) [??](#) [????](#) VPN [????](#) [????](#) ? [????](#) [??](#) [??](#) [??](#) [??](#) [??](#).

Junos OS? VPN? [??????](#) [??](#) [????](#) [??](#) [????](#) [??????](#).

- ICMP(Internet Control Message Protocol)? [????](#) IPsec datapath v?[??](#) [??](#) [????](#) [????](#) [??????](#).
- IKE(Internet Key Exchange) [????](#) [??](#) [????](#) [????](#) [??](#) DPD(Dead Peer Detection) [????](#) [??](#).
- IPsec [??](#) [??](#)(SA)? [????](#) [????](#) [??](#) VPN [??](#) [????](#) [??](#).

[??](#) [??????](#) [??](#) [????](#) [??](#) [????](#) VPN [????](#) [????](#) ? [????](#).

- [??](#) ? [????](#) [????](#) [????](#) SA? VPN [????](#) [??????](#) [??](#) ? [????](#), [??](#) [??](#) [??](#) ? [????](#) [??????](#) [????](#) SPI(Security Parameter Index)? [??](#) ? [????](#), [??????](#) [????](#) [????](#) [????](#) [????](#) SPI [??](#) [????](#) [????](#) [????](#) [????????](#) ? ? [????](#), [????](#) respond-bad-spi max-responses [??](#) [??](#) [????](#) [????](#) [ike\(??\)](#)? [????????](#).
- [????](#) [??????](#) ICMP [????](#) [????](#) [????](#) [????](#) ? [????](#) [????](#) [????](#) ? [????](#), [????](#) vpn-monitor-options [??](#) [????](#) [????](#) [ipsec\(??\)](#)? [????????](#).

? [????](#) [????](#) [??](#) ? [????](#) [????](#) VPN? [??????](#) [??????](#).

[illegible]

???? ???? ???? "???? VPN ???? ??" ??? 1348 ???? ?????.

## IPsec ☐ ☐ ☐ ☐ ☐

in this section

- IPsec [?] [?] [?] [?] [?] [?] [?] | 1341
- IPsec [?] [?] [?] [?] [?] [?] [?] | 1342

IPsec [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?] [?]

**IPsec** ??? ?? ???? ???? ???? ?????

?? ? VPN? ?? ???-?-??? ???? ? ??(st0) ?????? ??? ?????? VPN ??? ??? ???? ??. ????? SA(IPsec Security Association)? ??? ? Junos OS? st0 ?????? ??? ??? ??? ???? ?????, ????? VPN ?? ?????? ??? ? ? ????? ? ? ???? st0 ???????? ? ???? ???? IPsec ??? ????? ? ? ???? , ? ? ???? ??? ? ? ????.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 104

- [illegible]

IPsec datapath verification? ??? ?? ?? ??? ??????.

- VPN `set vpn vpn-name ipsec vpn-name ipsec vpn-name icmp vpn-name`
- IPsec datapath `set junos os st0 vpn-name vpn vpn-name ipsec datapath vpn-name vpn-monitor optimized vpn-name` [edit security ipsec vpn *vpn-name* *vpn-name*]

- IPsec [redacted] Junos OS [redacted] st0 [redacted]  
[redacted].
- IPsec SA [redacted], st0 [redacted] [redacted] Junos OS [redacted] IPsec datapath [redacted].
- Junos OS [redacted] AutoVPN, ADVPN(Auto Discovery VPN) [redacted] point-to-multipoint [redacted]  
st0 [redacted] IPsec datapath [redacted].
- VPN [redacted] IPsec datapath verification [redacted] IPv6 [redacted]. [redacted] IPv6 [redacted] IPsec datapath [redacted]  
[redacted].

# IPsec ??? ?? ??? ??? ????

IPsec ??? ?? ???? ?? ???? ??????.

1. `? ? ? ? ? VPN ? ? ? ? ? ? ? ? ? ? ICMP ? ? ? ? ? IPsec ? ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? VPN ? ? ?`  
`ICMP ? ? ? ? ? ? ? ? ? ? ICMP ? ? ? ? ? ? ? ? , ? ? ? ? ? ? ? ? ? ? ? ? show security ipsec  
security-association detail ? ? ? ? VPN Monitoring? V? ? ? ? ? ?.`
2. Junos OS? `? ? ? ? ? ? ? st0 ? ? ? ? ? ? ? ? . ? ? ? ? ? ? show interface st0.x ? ? ? ? ? ? ? ? ? ? ?  
? ? ? ? ? ? ? ? Link-Layer-Down ? ? ? Up ? ? ? st0 ? ? ? ? ? ? ? ? ? ? ?.`
3. `? ? ? ICMP ? ? ? ? ? ? ? ? ? ? VPN ? ? ? ? ? ? ? ? ? ? VPN ? ? ? ? ? ? ? ? ICMP ? ? ? ? ? ? . ? ?  
VPN ? ? ? ? ? ? 10? ? ? ? ? VPN ? ? ? ? ? ? 10? ? ? ? . ? ? ? ? ? KMD_VPN_DOWN_ALARM_USER ? ? ? ? ? ?  
? ? ? ? ? VPN ? ? ? ? verify-path ? ? ? ? ? ? ? ? . ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? show security  
ipsec security-association detail .show security ipsec tunnel-events-statistics ? ? ? ? ? ? ? ? ? ? ? ? ? ? [edit  
security ipsec] ? ? ? ? ? ? ? ? ? ? ? vpn-monitor-optionsVPN ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?.`
4. `? ? ? VPN ? ? ? ? ? ? ? ? ? ? ICMP ? ? ? ? ? ? ? ? Junos OS? VPN ? ? ? ? ? ? ? ? VPN ? ? ? ? ? ? ? ? ? ? ?.`

## SEE ALSO

?? ??

## Dead Peer Detection(?? ?? ??)

in this section

DPD? ??? ????? | 1343



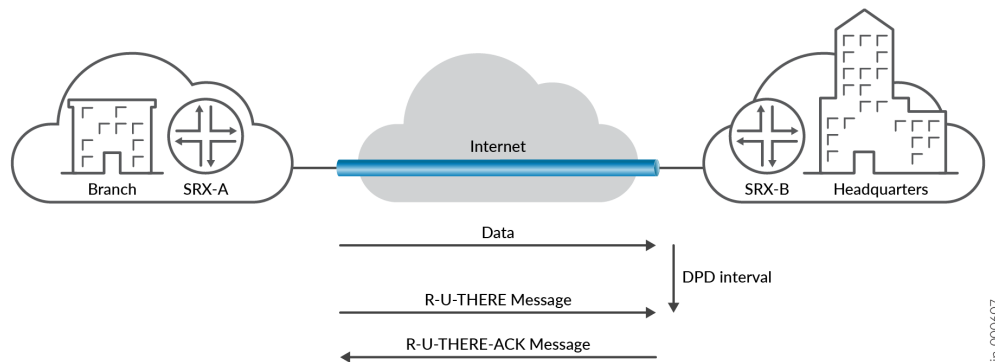
DPD(Dead Peer Detection) IPsec IKE(Internet Key Exchange) 。

## DPD 配置

IPsec VPN DPD(Dead Peer Detection) 配置。 DPD 配置 1. SA(Security Association) 。

SRX 配置 DPD IPsec VPN 。

### 72: DPD 配置



72 1343 IPsec VPN IKE(Internet Key Exchange) DPD 配置。

1. SRX-A 配置 DPD SRX-B 。
2. SRX-A 配置 DPD SRX-B 。
3. SRX-A 配置 DPD (R-U-THERE-ACK) 。



- `set ipsec sa 1 dpd enable` IKE (Internet Key Exchange) 1 SA `set ipsec sa 2 dpd enable`. [dead-peer-detection](#) `set ipsec sa 1 dpd enable`.
- `set ipsec sa 1 dpd enable` IKE 1 SA `set ipsec sa 2 dpd enable`, IKE 1 SA 2 SA `set ipsec sa 1 dpd enable`. [dead-peer-detection\(IKE\)](#) `set ipsec sa 1 dpd enable`.
- `set ipsec sa 1 dpd enable` IKE 1 SA `set ipsec sa 2 dpd enable` SA R-U-THERE `set ipsec sa 1 dpd enable`. `set ipsec sa 1 dpd enable` SA(IKEv2) `set ipsec sa 1 dpd enable`.



**i**: DPD (Dead Peer Detection) RFC 3706, IKE(Dead Internet Key Exchange) `set ipsec sa 1 dpd enable` `set ipsec sa 2 dpd enable`.

IKE (Internet Key Exchange) VPN (Virtual Private Network) `set ipsec sa 1 dpd enable`



**💡**: DPD (IPsec SA) `set ipsec sa 1 dpd enable`. "VPN (Virtual Private Network)" `set ipsec sa 1 dpd enable`.

## SEE ALSO

[dead-peer-detection](#)

[dead-peer-detection\(IKE\)](#)

## VPN (Virtual Private Network)

### in this section

- [VPN \(Virtual Private Network\) \(1346\)](#)

VPN (Virtual Private Network) Junos OS `set ipsec sa 1 dpd enable`.

DPD(Dead Peer Detection) (Internet Key Exchange) (IKE) VPN (Virtual Private Network) `set ipsec sa 1 dpd enable`. VPN (Virtual Private Network) IPsec SA `set ipsec sa 1 dpd enable` Junos OS `set ipsec sa 1 dpd enable`.

## VPN [??](#) [??????](#) [???](#) [???????](#)

VPN [?????](#) ICMP(Internet Control Message Protocol) [??](#) [??](#)([??](#) ping)[?](#) ICMP [???](#) [??](#) ID? [??](#) [??](#) [?????](#) [?????](#)  
VPN [????](#) [??](#) [????](#) [????](#) [???????](#).

VPN [??????](#) [??????](#) [??????](#) VPN [????](#) [??](#) [??](#) [??????](#) [??](#) [????](#) [??](#) [??](#) [??](#) [????](#) [?????](#) ICMP [??](#) [????](#) [?????](#). [??????](#) [??](#) [????](#) [??](#) 10? [??](#) 10? [?????](#) [????](#) [?????](#). [??????](#) 10? [??](#) ping [????](#) [????](#) [??](#) [????](#) VPN? [????](#) [????](#) [?????](#) IPsec [??](#) [????](#) [??](#) [????](#).

[??](#) [??](#) [????](#) [?????](#) VPN [????](#) [???????????](#).

- Always-send [??](#) - [?](#) [??????](#) [???????](#) [????](#) [?????](#) [?????](#) [????](#) [?????](#) [??](#) [??](#) VPN [?????](#) [????](#) [?????](#). VPN [???????](#) [?????](#) [??](#), [?????](#) [????](#) Junos OS? always-send [????](#) [??](#) [????](#) [???????](#).
- [????](#) [??](#) - [?](#) [???????](#) [????](#) [?????](#) [??](#) [??](#) [??](#) [????](#) [??](#) [?????](#) [??????](#) [??](#) [?????](#) [???????](#) [????](#) [?????](#) [??](#) [??](#) VPN [?????](#) [????](#) [??](#) [??](#). VPN [????](#) [??](#) [?????](#) [?????](#) [??](#) [??](#) [???????](#) [????](#) [??](#) [????](#) [?????](#) [?????](#) ping [????](#) [???????](#). [????](#) [????](#) [?????](#) [???????](#) [??](#) [????](#) [????](#) [??](#) [???](#), [?](#) [???????](#) [???????](#) [??](#) [????](#) [?????](#) [??](#) [??](#) ping? [?????](#) [???????](#). [??](#) [????](#) [??](#) [???????](#) [?????](#) [??](#) [????](#) [??](#) [??](#) [?????](#) [??](#) [?????](#).

[????](#) [????](#) [???????](#) [?????](#) [????](#) [???????](#) [??](#) [??](#) [??](#) [????](#) [???????](#).

## SEE ALSO

[vpn-\[????\]\(#\)](#)

[vpn](#) ([??](#))

## Dead Peer Detection [??](#)

[????](#) [??](#) IKE(Internet Key Exchange) [???????](#) [?????](#) [????](#) [???????](#) . [????](#) [????](#) [???????](#)([??](#) IKE) [?](#) [???????](#).

[?](#) [???????](#) [????](#) [??](#)@[??](#) SRX [????](#) [???????](#) DPD(Dead Peer Detection) [???????](#) [??](#) [??](#) [????](#) [?????](#) [????](#) [?????](#). DPD? [?](#) [???????](#) [???????](#):

1. [??](#) [?????](#) [edit security ike gateway *gateway-name*] DPD [????](#) probe-idle-tunnel [???????](#). [????](#) [????](#) "[??](#) [????](#) DPD [??](#) [??](#) " [????](#) 1342 [?](#) [??](#) [??](#) [??](#) [?](#) [???????](#).

[edit]

```
set security ike gateway vpngw1 dead-peer-detection probe-idle-tunnel
```

[?????](#) vpngw1? *gateway-name*.

2. `?? ???? [edit security ike gateway gateway-name] ??? ??????. ??? ??? "?? ??? DPD ?? ??" ??? 1342 ? ??  
?? ?? ? ????????`.

```
[edit]
set security ike gateway vpngw1 dead-peer-detection interval 40
```

???? ???? 40?? ???????.

3. `?? ???? ??? ? [edit security ike gateway gateway-name] ??????. ??? ??? "?? ??? DPD ?? ??" ??? 1342 ? ?  
? ?? ? ? ????????`.

```
[edit]
set security ike gateway vpngw1 dead-peer-detection threshold 3
```

???? ????? 3?? ??????, ?? ?????? ??? ???? ???? ???? ???? 3? ping???? ? ? ??????.



?:

?????iked IPsec VPN ????? ? ? ?????? ?????? ???? ???? ???? ???? DPD? ??? ? ??????. ??? ??  
? ??????(? IKE) ? ???????.

## VPN ?? ????? ??

???? ? ? VPN ??? ??? ????.

? ?????? VPN ?? ?????? ?????? ??? ??????® SRX ??? ?????? VPN ?????? ?????? ping ??? ? ? ??? ? ???? ????  
? ??? ? ? ??????.

1. `?? ???? ??? ????? vpn-monitor ?? VPN ??? ? [edit security ipsec vpn vpn-name] VPN ?????? ????????. vpn-monitor? ????????`.

```
[edit]
set security ipsec vpn vpn1 vpn-monitor
```

???? vpn1 *vpn-name*? .



Junos OS [?](#) [????](#) [?????](#), [????](#) [?????](#), [????????](#) [?????](#) [????](#) [????](#) [????](#) [????????](#). VPN [?????](#) [????](#) VPN [?](#) [??](#) [??](#) [?????](#) [????](#) [?????](#) [??](#), [??](#), [????](#) [?](#) [????](#) [??](#) [????](#) [?????](#) [??](#) [????](#) [??????](#), [??](#) [??](#) [????](#) [????](#) [????](#) [????](#) [?](#) [?????](#).

## VPN [?][?] [?] [?][?]

[illegible]

VPN ??? VPN? ?? ???? ???? ???? ? ? ? ???? ???? ??????. ??? ?????? ???? ???? ???? ? ???? ?  
?????. ????? ? ???? ????? ????? ??, ??? ? ???? ?????.

?? ? ???? ???? ? ?? ???? ?????.

- [illegible]

[illegible]

- *22 22 - 22 22 22 222 222 2222 222 2 222 222 22222 22222 222 2 2222.*
- *222 2 222 22 - 222 22 22222 222 222 2222 222 2 222 222 22222 22222 222 2 2222.*
- *IKE(Internet Key Exchange) 122 2 IKE(Internet Key Exchange) 222 22 - Junos OS IKE(Internet Key Exchange) SA(Internet Key Exchange) 22 22(SA)2 22222. 22 222 IKE(Internet Key Exchange) 222 2222 2 2222. IKE(Internet Key Exchange) 122 22 IKE 222 22 22 222 222 222 2 222 222 22222 22222 222 2 22 22.*
- *Self-test failures—22222 222 2222 2222 2 Junos OS 2222222 2 22 2222 2222 22 222222 222 222222. 22 2222 22 222 22222 2222 222222. Junos-FIPS 2222 2222 222 22 2 2222 22 2222 2222 2 22 222 22 22 22 22222 22222. 22 22 FIPS 22222 222 222 22, 22 2 22 2 22 222 22222 22 2222 222 2 22222. 22 22222 22 2 222 222 22222 22222 222 22 22222.*
- *22 22 2 22(IDP) 222 22 22 - 22 22 2 22(IDP) 222 2222 2222 2222 222 22 22 2 22 222 222222. 22 22 2 22 (IDP) 222 22 222 222 2 222 222 222222 22222 2222 2 22222.*
- *22 22 - 22 222 2222 222 222 22 2222 22222 22 2222 22222 22222 2222 222222. 22 222 222 2 222 222 2 2222 222222 222 2 2222.*

Junos OS? ???? ???? ???? ?? ??? ?( syslog ????? ?) ?????. ??? ?? syslog ???? ?  
?

- |    |   |    |    |
|----|---|----|----|
| ?? | ? | ?? | ?? |
|----|---|----|----|
- |     |   |    |    |
|-----|---|----|----|
| ??? | ? | ?? | ?? |
|-----|---|----|----|
- |    |   |    |    |
|----|---|----|----|
| ?? | ? | ?? | ?? |
|----|---|----|----|
- |    |   |    |    |
|----|---|----|----|
| ?? | ? | ?? | ?? |
|----|---|----|----|
- |   |    |    |
|---|----|----|
| ? | ?? | ?? |
|---|----|----|



- [illegible]

```
Junos OS? syslog ???? ???? ??? ??????. Junos OS? ?? ??? ?????? ????? ???? ???? ???? ?????, ?? ??? ??? ?
?? ????? show security alarms .?? ?? ? ??? ??? ??? ????? ?????, ??? ? ?? ??? O?? ?????? ??? ?? ?????
?????, ??? ?????? ?????? ??? ??? ? ???? ?? ??? ????? ? ???? ,??? ????? ??? ?????? clear security
alarms .
```

## SEE ALSO

```
cache(?? ??)
```

?? ?? ??

?? ?? ??

## VPN ?? ???

VPN **???** **???** **?** Junos OS? **??** **??** **??** **?** **??** **???** **???** **??** **???** **???** **???**. Junos OS? **??** **???** **???** IPsec **??** **??** **??**, IPsec **?** **???** **?** IKE **??** **??** **?** **???** **??** **???** **???** **???** **???**. ***??** **???** **???** **???** **??** **?** **??** **???** **???** **??** **???** **???***.

1??? 2???? Junos OS? ?? ?? pkid? ?? ?? ?????? ????? ???? iked ?? kmd ?????? ??? ??? ? ? ???? ?  
 ?????, ?? ????? ? ? ???? ?????? ?????? ?? ? ???? ???? ???? ? ? ????.

???? Junos OS? 1??? 8? ???, 2??? 8? ??? ? ? 16?? ????? ?????.

?? ???? ? ???? ???? ???? ? ???? ???? ???? ? ?????. ???? ???? ? ???? ???? ???? ? ? ???? ???? ?  
???, ??? ??? ? ??? ??? ???.

- IPsec `set security ipsec policy policy-name proposal-name`.
- IPsec `set security ipsec proposal proposal-name proposal-options`.
- IPsec `set security ipsec proposal proposal-name proposal-options proposal-name`.
- `set security ipsec proposal proposal-name proposal-options`.
- `set IKE ike-name ike-options IPsec proposal-name proposal-name`.

Junos OS<sup>2</sup> AutoVPN `set security ipsec policy policy-name proposal-name`, `set security ipsec proposal proposal-name proposal-options`, `set security ipsec proposal proposal-name proposal-options proposal-name`, `set security ipsec proposal proposal-name proposal-options`, `set security ipsec proposal proposal-name proposal-options`.

## VPN `set` `set`

`set security ipsec policy policy-name proposal-name`, `set security ipsec proposal proposal-name proposal-options`, `set security ipsec proposal proposal-name proposal-options proposal-name`, `set security ipsec proposal proposal-name proposal-options`, `set security ipsec proposal proposal-name proposal-options`.

```
[edit]
set security log cache
```

`set security ipsec policy policy-name proposal-name`.

`set security ipsec proposal proposal-name proposal-options`.

1. `set security ipsec proposal proposal-name proposal-options proposal-name`.

```
show security alarms
```

`show security ipsec policy policy-name proposal-name`.

2. `set security ipsec proposal proposal-name proposal-options`.

```
clear security alarms
```

`clear security ipsec policy policy-name proposal-name`.

in this section

- ?? ?? | 1353
- ?? | 1353
- ?? | 1353
- ?? | 1354

SRX300, SRX320, SRX340, SRX345, SRX550HM SRX1500 vSRX

?? ??

? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? .

??

.

??

in this section

- ?? | 1353

??

???

?? ?? ?????:

1. `?? ??? ???????`.

```
[edit]
user@host# edit security alarms
```

2. `???? ?? ?? ??? ?? ??? ??? ??????`.

```
[edit security alarms]
user@host# set audible
```

3. `???? ??? ????? ?? ??? ??????`.

```
[edit security alarms]
user@host# commit
```

`??`

`??? ??? ?????? ?????? ??? ??????` show security alarms detail.

SEE ALSO

| [IPsec ??](#) | [11](#)

**?: ?? ?? ?? ??**

in this section

●

[?? ??](#) | [1355](#)

●

[??](#) | [1355](#)

●

[??](#) | [1355](#)

●

[??](#) | [1358](#)

SRX300, SRX320, SRX340, SRX345, SRX550HM SRX1500 vSRX

- 6
- 
- 
- 
- 10
- 1
- IKE(Internet Key Exchange) 10
- IKE(Internet Key Exchange) 2
- 

in this section

| 1356

??

## CLI ?? ??

? ?? ??? ?????, ?? ??? ????? ??? ??? ?? ?? ?? ????????? ?????, ????? ??? ????? ? ??? ?? ??? ??? [edit] ?  
? ????? ??? CLI? ??? ?? ?? ??, ?? ????? commit?(?) ?????.

```
set security alarms potential-violation authentication 6
set security alarms potential-violation cryptographic-self-test
set security alarms potential-violation non-cryptographic-self-test
set security alarms potential-violation key-generation-self-test
set security alarms potential-violation encryption-failures threshold 10
set security alarms potential-violation decryption-failures threshold 1
set security alarms potential-violation ike-phase1-failures threshold 10
set security alarms potential-violation ike-phase2-failures threshold 1
set security alarms potential-violation replay-attacks
```

??? ??

?? ?? ?? ????? ??? ??? ?????, ?? ????? ??? ?? ??? [Junos OS CLI ??? ???](#) ?? ????? CLI ??? ??? ???  
??.

??? ??? ????? ??? ?????? ??? ??????

### 1. ?? ??? ????????

```
[edit]
user@host# edit security alarms
```

### 2. ?? ??? ??? ? ??? ?????? ??????

```
[edit security alarms potential-violation]
user@host# set authentication 6
```

### 3. ??? ?? ??? ??? ??? ? ??? ?????? ??????

```
[edit security alarms potential-violation]
user@host# set cryptographic-self-test
```

- [illegible]

```
[edit security alarms potential-violation]
user@host# set non-cryptographic-self-test
```

- 5.**    ? ?? ?? ??? ??? ??? ? ??? ?????????? .

```
[edit security alarms potential-violation]
user@host# set key-generation-self-test
```

- 6.**                                .

```
[edit security alarms potential-violation]
user@host# set encryption-failures threshold 10
```

- [illegible]

```
[edit security alarms potential-violation]
user@host# set decryption-failures threshold 1
```

8. IKE(Internet Key Exchange) 1?? ???? ???? ? ???? ????? ?????.

```
[edit security alarms potential-violation]
user@host# set ike-phase1-failures threshold 10
```

9. IKE(Internet Key Exchange) 2?? ???? ? ???? ?????????.

```
[edit security alarms potential-violation]
user@host# set ike-phase2-failures threshold 1
```

- [illegible]

```
[edit security alarms potential-violation]
user@host# set replay-attacks
```

??

?? ???? show security alarms ??? ???? ???? ?????. ??? ???? ???? ???? ???? , ? ?? ?? ???? ???? ?????.

```
potential-violation {
  authentication 6;
  cryptographic-self-test;
  decryption-failures {
    threshold 1;
  }
  encryption-failures {
    threshold 10;
  }
  ike-phase1-failures {
    threshold 10;
  }
  ike-phase2-failures {
    threshold 1;
  }
  key-generation-self-test;
  non-cryptographic-self-test;
  replay-attacks;
}
```

???? ?? ???? ? ? ???? commit?(?) ?????.

??

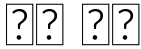
??? ??? ?????? ?????? ?? ????? ??? ?????? show security alarms .

SEE ALSO



# 13

CHAPTER LABEL COVER PAGE



---

## in this chapter

- VPN [??](#) [????](#) | 1360
  - PowerMode IPsec | 1368
-

# VPN **??** **???**

## summary

VPN **??** **???** **???** IPsec VPN **???** **???** **???** **??** **??** **???**.

## in this section

- [VPN \*\*??\*\* \*\*???\*\* \*\*??\*\* | 1360](#)
- [VPN \*\*??\*\* \*\*???\*\* \*\*???\*\* | 1361](#)
- [IPsec VPN \*\*???\*\* \*\*??\*\* \*\*???\*\* | 1364](#)
- [IPsec \*\*??\*\* \*\*???\*\* | 1365](#)
- [???](#) VPN **??** **???** **???** **???** **???** | 1366
- [???](#) **???** VPN **???** **???** **???** **??** | 1367

**??** **???** **???** **???** **???** **??** IPsec VPN **???** **???** VPN **??** **???** **?** **??** **???** **???** **???** **?** **???**.

[??](#) [???](#) [???](#) **??** **???** **??** **???** **?** **???** **???** **???** **???**.

**???** **???** **???** "[???](#) [???](#) VPN **???** **???** **???** **???**" **???** **1367** **???** **???**.

## VPN **??** **???** **??**

VPN **??** **???** IPsec **??** **???** **???** SPU **??** SPU(Services Processing Unit) **??** **???** **???** **??** **?** **???**. VPN **??** **???** **???** **???** SPU **??** **???** **?** IPsec **??** **???** **??** **???**.

VPN **??** **???** **???** **???** **??** **???** **??** **???** **???** **???** SPU **???** **?** **??** IPsec **??** **???** **??** **???** **??** SPU **???** **?** **???**. **??** **???** **???** IPsec **???** **???** **???** SPU **??** SPU **???** **???** **??** **??** **???**.

**???** VPN **??** **???** SRX **???** **???** **???** **???**. VPN **??** **???** **???** IPsec **??** **???** **???** SPU **???** **??** **??** **?** **???** **???**. **??** **??** **???** **???** **???** **??** **???**.

**???** **?** **???** **???** **??** **?** **??** **???** **??** VPN **??** **???** **???**. IOC **??** **???** **???** **??** **??** SPU **???** **???** **??** **???** **??** IPsec **??** **??** **???** **??** **???** **???** **???** **??** **??** **???** **???** IOC **???** **???** SPU **???** **???** **???** **??** **???** **???** **???** **?** **???** **???**. Express Path(**???** **???** **???**) **???** NP **??** **???** IOC **???** **???** **??** **??** **???** **???**.

SPU? ?? ?? ??? ?????? ??? ????? show security ipsec security-association SPU? ????? FPC(Flexible PIC Concentrator) ? PIC( *Physical Interface Card*) ??? ?????, ? ?? ?? ?? ??? ?????.

```
user@host> show security ipsec security-association fpc 3 pic 0
Total active tunnels: 1
ID      Algorithm      SPI      Life:sec/kb  Mon vsys Port  Gateway
<131073 ESP:aes-128/sha1 18c4fd00 491/      128000 - root 500    203.0.113.11
>131073 ESP:aes-128/sha1 188c0750 491/      128000 - root 500    203.0.113.11
```

???? ?? ? ??? ??? VPN ?? ??? ??? ???? ???? ???? ????.

????? VPN ?? ???? ???? ? ? ? ???? ? ? ? ? ?(SPU)? ? ? ? ? ? ? ???? ? ? ?????. ??? ? ? ? ?  
? ???? ? IPsec ?? ???? ? ? ? SPU?? ? ? ???? ?????.

VPN ?? ??? ??? ??? ?????.

- [illegible]

## SEE ALSO

SRX5000    ??    ?????    ???    ??    ??

?? ?? ??

Express Path 

?: ?? ??? Express Path ???

## Express Path

## VPN ?? ??? ???

???? VPN ?? ???? SRX ??? ?????? ?????? ?????. VPN ?? ???? ???? ???? ? ? ???? VPN ???? ???? ? ?  
 ???, ? ?????? CLI? ???? VPN ?? ???? ?????? ??? ?? ?????.

```

?? ???? ???? ?? SPU? IPsec ?? ???? ???? ???? ?????. ??? ???? ?? ???? ???? show security flow session ?? ??
???? ?????.

```

```

user@host> show security flow session

```

```

Flow Sessions on FPC3 PIC0:

```

```

Session ID: 60000001, Policy name: N/A, Timeout: N/A, Valid

```

```

  In: 203.0.113.11/6204 --> 203.0.113.6/41264;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

```

```

Session ID: 60000002, Policy name: N/A, Timeout: N/A, Valid

```

```

  In: 203.0.113.11/0 --> 203.0.113.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

```

```

Session ID: 60000003, Policy name: self-traffic-policy/1, Timeout: 58, Valid

```

```

  In: 203.0.113.6/500 --> 203.0.113.11/500;udp, If: .local..0, Pkts: 105386, Bytes: 12026528

```

```

  Out: 203.0.113.11/500 --> 203.0.113.6/500;udp, If: ge-0/0/2.0, Pkts: 106462, Bytes: 12105912

```

```

Session ID: 60017354, Policy name: N/A, Timeout: 1784, Valid

```

```

  In: 0.0.0.0/0 --> 0.0.0.0/0;0, If: N/A, Pkts: 0, Bytes: 0

```

```

  Out: 198.51.100.156/23 --> 192.0.2.155/53051;tcp, If: N/A, Pkts: 0, Bytes: 0

```

```

Total sessions: 4

```

```

Flow Sessions on FPC6 PIC0:

```

```

Session ID: 120000001, Policy name: N/A, Timeout: N/A, Valid

```

```

  In: 203.0.113.11/0 --> 203.0.113.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

```

```

Session ID: 120000002, Policy name: N/A, Timeout: N/A, Valid

```

```

  In: 203.0.113.11/0 --> 203.0.113.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

```

```

Session ID: 120031730, Policy name: default-policy-00/2, Timeout: 1764, Valid

```

```

  In: 192.0.2.155/53051 --> 198.51.100.156/23;tcp, If: ge-0/0/1.0, Pkts: 44, Bytes: 2399

```

```

  Out: 198.51.100.156/23 --> 192.0.2.155/53051;tcp, If: st0.0, Pkts: 35, Bytes: 2449

```

```

Total sessions: 3

```

```

? ???? FPC 3, PIC 0? ?? ???? ?? FPC 6, PIC 0? ?? ???? ???? ?????. ??? ??(?? ID 60017354)? FPC 3, PIC 0?
?????.

```

```

IOC FPC?? IPsec ?? ???? ?? ?? ???? ???? ? ?????. IPsec VPN ???? ???? ???? ???? IOC?? ?? ??? set
chassis fpc fpc-slot np-cache ???? ??.

```

```

VPN ?? ???? ??:

```



```
Session ID: 120000002, Policy name: N/A, Timeout: N/A, Valid
  In: 203.0.113.11/0 --> 203.0.113.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0
Total sessions: 2
```



- default-spc3-profile —IPsec **???** **??** **???** **??** **SPC3** **???** **?????** **?** **??** **???** **??** **?????** **?????**.

?? ? VPN ??? ???? ? ? ??, ??? ? ???? ? ???? ???? ?????. VPN ??? ???? ? ? ? SRX ??? ????  
 ??? ??? ? ???? ???? ???? ?????.

VPN [??] [??] [?] [??] [?] [?] [??](?) [??] [??] [?] [??].

?? ??? ??? ABC? ??? ?? ??? FPC 0, PIC 0? ?? ???.

```
userhost# show security {
    distribution-profile ABC {
        fpc 0 {
            pic 0;
        }
    }
}
```

???? VPN? ?? ???? ?????? ?????

IPsec VPN 22 22222 22 IKE(Internet Key Exchange) 222222 22222 22 22 2222222 22222 2222. 22 2222222 2222 22 2222 2222222 222 22 222 222 VPN2 22 2222222 222 2222 22222222 222222 22 22222. 2222 2222222 VPN 2222 22222 22222 22 2222 22222222 22 22222 2222222.

**VPN** ??? ???? ???? ?? SRX ??? ???? ? ???? SRX ??? ?????? ??????. ?? ????? ??-?? ????  
 ??? ?? ???? ???? ?? ? ???? ???? ? VPN ??? ???? ? ???? , ??? ?????? ?? ?? ???? ? ? ?  
 ? IKE(Internet Key Exchange) ????? ? ? ???? ?????. VPN ??? ? ???? ? ???? ???? .

?? ???? ???? ?? ??????? ???? ??? VPN ??? ??? SPU? ??????. IKE(Internet Key Exchange) ? IPsec ??? ?? SPU?? ??????. ??? ?? ?? ??????? ?? SPU? ??????.

```
[[[?]]] show chassis cluster interfaces [[?]] [[?]] [[?]] [[?]] [[?]] [[?]].
```

## SEE ALSO

?? ???? ???? ??



VPN

VPN

VPN

146: VPN

| VPN     | VPN                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------|
| SRX VPN | <ul style="list-style-type: none"><li>VPN SRX5400, SRX5600 SRX5800:</li><li>kmd SPC2 IKE RG0</li><li>iked SPC3 SPC3+SPC2</li></ul> |

VPN

VPN Feature Explorer

|                                    |                                                                                               |
|------------------------------------|-----------------------------------------------------------------------------------------------|
| release heading in release-history | desc heading in release-history                                                               |
| 20.2R2                             | Junos OS 20.2R2 ID commit-check IPsec                                                         |
| 19.2R1                             |                                                                                               |
| 17.4R1                             | Junos OS 17.4R1 VPN IPsec VPN                                                                 |
| 12.3X48-D50                        | Junos OS 12.3X48-D50, Junos OS 15.1X49-D90 Junos OS 17.3R1 SRX5400, SRX5600 SRX5800 VPN (SPU) |

VPN

- PowerMode IPsec ? ? ? IPsec ? ? ? ? | 1368
- ? : PMI ? ? Behavior Aggregate ? ? ? ? ? ? | 1373
- ? : vSRX ? ? ? ? ? ? ? ? ? ? PMI ? ? ? ? ?  
(Behavioral Aggregate) ? ? ? ? ? ? | 1379
- ? : PMI ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?  
| 1385
- ? : PMI ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? | 1392
- PMI ? ? IPsec ESP ? ? ? ? ? ? ? ? | 1397
- ? ? ? ? ? PMI ? ? ? | 1398
- ? ? ? ? ? ? ? ? | 1399

??? ???? "?? ??" ??? 1399 ?????.

## PowerMode IPsec?? IPsec ?? ??

in this section

- PMI 1369
- PMI 1369
- AES-NI(Advanced Encryption Standard New Instructions) FPGA(Field-Programmable Gate Array) | 1369
- PMI 1369
- PMI 1372
- PMI 1372

```
PMI(PowerMode IPsec)? ? ? ? ? Intel AES-NI(Advanced Encryption Standard New Instructions)? ???  
? IPsec ? ? ? ? ? ? ? ? ? ? . PMI? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ? PMI? ? ? ? ? ? ? ? ? ? ?  
IPsec ? ? ? ? ? ? ? ? ? ? AES-NI ? ? ? ? ? ? ? ? ? ?.
```

## PMI [?] [?] [?] [?] [?] [?] [?] [?].

- PMI ??

?? ?? ??? ????? PMI ??? show security flow pmi statistics ??? ? ?????.

?? ?? ??? ????? show security flow status PMI ? fat ?? ??? ??? ? ?????.

## AES-NI(Advanced Encryption Standard New Instructions) ? ? ? ? FPGA(Field-Programmable Gate Array)

. PMI ??? AES-NI ? SPU? ?? ???? ?? SPC3 ??? ?? ?? ??? ?????, ? ?? ??? ?? ??? ????? IPsec VPN? ???  
? ?????, PMI? ????? AES-NI ? ????? ??? ?? ?? FPGA? ?????.

AES-NI[?] PMI[?] [?] [?] [?] [?] [?] [?] power-mode-ipsec[?] [?][edit security flow].

```
?? FPGA? [edit security forwarding-process application-services] ??? ?? ??????? ? ???? ? ????inline-  
fpga-crypto (disabled | enabled).
```

## PMI[?] [??] [????] [??] [?] [????] [??] [??]

PMI 147 1370 ( ) PMI

150 1398

[illegible]

147: PMI

| PMI                                                        | PMI               |
|------------------------------------------------------------|-------------------|
| IKE(Internet Key Exchange)                                 | 4 - 7 : AppSecure |
| AutoVPN                                                    |                   |
| (HA)                                                       |                   |
| IPv6                                                       |                   |
|                                                            | (ALG)             |
| st0                                                        | HMAC-SHA-384      |
|                                                            | HMAC-SHA-512      |
| NAT (PMI NAT64 . NAT64 PMI )                               |                   |
| AES-GCM-128 AES-GCM-256 . AES-GCM                          |                   |
| HMAC-SHA1-96 SHA1 AES-CBC-128, AES-CBC-192 AES-CBC-256     |                   |
| HMAC-SHA-256-128 SHA2 AES-CBC-128, AES-CBC-192 AES-CBC-256 |                   |
| NULL                                                       |                   |
|                                                            |                   |
|                                                            |                   |
|                                                            |                   |
|                                                            |                   |

147: PMI (Continued)

| PMI | PMI |
|-----|-----|
|     |     |
|     |     |

PMI .

- **Antireplay window size**
  - Antireplay 64. fat-tunnel Antireplay 512 .
- **Class of Service (CoS)**
  - CoS(Class of Service) PMI BA(Behavior Aggregate), MF(Multifield) .
  - PMI CoS . , . CoS . . CoS .
- **Encryption algorithm**
  - PMI IPsec aes-128-cbc, aes-192-cbc aes-256-cbc .
- **GTP-U**
  - PMI TEID GTP-U .
  - PMI .
- **LAG and redundant (reth) interfaces**
  - PMI (LAG) (RETH) .
- **PMI fragmentation check**
  - PMI . PMI PMI . PMI .
  - . PMI .
- **PMI for NAT-T**
  - NAT-T PMI SRX5K-SPC3 SPC(Services Processing Card) vSRX .
- **PMI support (vSRX)**
  - vSRX .
  - PMI GTP-U Per-flow CoS .

- PMI `???` CoS `??`. PMI `????` `????` CoS `???` `???` `????`.
  - `???`
  - `??` `????` `??`
  - `?`
  - `???`(Shaping)
  - `????`

## PMI`?` `??`

- IPsec`?` `???` `???????`.

## `??` `????` PMI `??`

`??` `??????` `??` `???` PMI`?` `?????` `???` `??` `??????`.

`??` `???` PMI`?` `???????` IOC `?` `??` `??????` `??` `???` `??????` `???`.

### 1. IOC(IOC2 `?` IOC3)`??` `??` `??` `???`

```
user@host# set chassis fpc <fpc-slot> np-cache
```

### 2. VPN `??` `???` `??`

```
user@host# set security flow load-distribution session-affinity ipsec
```

### 3. PMI`??` `??` `?????` `???????`.

```
user@host#set security flow power-mode-ipsec
```

### 4. show security `???` `?????` `???` `???????`.

```
user@host# show security
flow {
    power-mode-ipsec;
}
```



?? ??

- SRX ??? ???.

- Junos OS  19.1R1  .

- **?? ?? ???? ?? ????? ? ??? ? DSCP? ????? ???? ???? ???? ? PLP? ?????.**

2 4

| mf-classifier $2 \times 2$ | CoS $2 \times 2 \times 2$              | ba-classifier $2 \times 2$                               |
|----------------------------|----------------------------------------|----------------------------------------------------------|
| be-class                   | Best-effort $2 \times 2$               | $2 \times 2 \times 2$ $2 \times 2$ $2 \times 2$ : 000001 |
| ef-class                   | $2 \times 2$ $2 \times 2$ $2 \times 2$ | $2 \times 2 \times 2$ $2 \times 2$ $2 \times 2$ : 101111 |
| af-class                   | $2 \times 2$ $2 \times 2$ $2 \times 2$ | $2 \times 2 \times 2$ $2 \times 2$ $2 \times 2$ : 001100 |



148: ba-classifier (Continued)

| mf-classifier | CoS | ba-classifier |
|---------------|-----|---------------|
| nc-class      |     | : 110001      |

in this section

CLI | 1375

| 1375

| 1377

CLI

,
,
[edit]
CLI,
commit()
.

```
set class-of-service classifiers dscp ba-classifier import default
set class-of-service classifiers dscp ba-classifier forwarding-class be-class loss-priority high
code-points 000001
set class-of-service classifiers dscp ba-classifier forwarding-class ef-class loss-priority high
code-points 101111
set class-of-service classifiers dscp ba-classifier forwarding-class af-class loss-priority high
code-points 001100
set class-of-service classifiers dscp ba-classifier forwarding-class nc-class loss-priority high
code-points 110001
set class-of-service interfaces ge-0/0/0 unit 0 classifiers dscp ba-classifier
```

Junos OS CLI
CLI
.

PMI?? ????? ?? Behavior Aggregate ??? ?????:

1. ??? ??? ?????.

```
[edit]
user@host# edit class-of-service
```

2. ????(DiffServ) CoS? ?? ?? ?? ????? ?????.

```
[edit class-of-service]
user@host# edit classifiers dscp ba-classifier
user@host# set import default
```

3. best-effort ??? ??? ?????.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class be-class loss-priority high code-points 000001
```

4. ??? ??? ??? ?????.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class ef-class loss-priority high code-points 101111
```

5. ??? ??? ??? ?????.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class af-class loss-priority high code-points 001100
```

6. ????? ?? ??? ??? ?????.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class nc-class loss-priority high code-points 110001
```



??

in this section

1378

**???? ???? ?????? ???? ???? ???? ?????:**

□□□□ □□□□□□ □□□□□□ □□

??

□□□□ □□□ □□□□□□ □□□□□□ □□□□□.

??

```
?? ???? show class-of-service interface ge-0/0/0 ??? ?????.
```

```
user@host> show class-of-service interface ge-0/0/0
Physical interface: ge-0/0/0, Index: 144
  Queues supported: 8, Queues in use: 4
  Scheduled map: <default>, Index:2
  Congestion-notification: Disabled
```

```
Logical interface: ge-1/0/3, Index: 333
Object      Name                Type      Index
Classifier  v4-ba-classifier    dscp      10755
```

??

□□□□□□ □□□□ □□□□□.

**?: vSRX ?? ??? ?????? ?? PMI?? ?? ??(Behavioral Aggregate) ??? ??**

in this section

- ?? ?? | 1379
- ?? | 1379
- ?? | 1380
- ?? | 1384

? ???? vSRX ?? ??? ?????? ?? BA(Behavior Aggregate) ????? ???? PMI?? ??? ??? ???? ???? ???? ???? ????.

?? ??

? ? ? ? ? ? ? ? ? ? ? ? ? ? ? ?

- vSRX `?? ??? ????`.
- Junos OS `??? 19.4R1 ?? ????`.

□□□□ □□:

- BA [?] [?] [?] [?] [?] [?] DSCP[?] [?] [?] [?] [?] [?] PLP[?] [?] [?] [?]

??

BA [REDACTED] DSCP[REDACTED], [REDACTED] BA [REDACTED]  
[REDACTED] IP [REDACTED]. [REDACTED] [edit class-of-service]  
[REDACTED] classifiers.

2 2222 DSCP BA 2222 22 DSCP 222 222222 ba-classifier . BE(best-effort) 222 22222 ( be-class2)2,  
 EF(Expedited Forwarding) 22222 ( ef-class2)2, AF(Assured Forwarding) 22222 ( af-class2)2, 22222 22 222 2222  
 2 (2)2 nc-class222222. 222222 BA 22222 222222 ge-0/0/0? 222222.

**[?] 2 BA [????] 4?? [???] [?????] ?? [??] ?? [?????] [????] [??] [?????].**

149: ba-classifier

| Multifield-Classifer | CoS | BA       |
|----------------------|-----|----------|
| be-class             | BE  | : 000001 |
| ef-class             | EF  | : 101111 |
| af-class             | AF  | : 001100 |
| nc-class             |     | : 110001 |

in this section

CLI | 1380

| 1381

| 1383

CLI

CLI [edit]
,
commit .

```
set class-of-service classifiers dscp ba-classifier forwarding-class be loss-priority low code-points be
set class-of-service classifiers dscp ba-classifier forwarding-class ef loss-priority low code-points ef
set class-of-service classifiers dscp ba-classifier forwarding-class ef loss-priority high code-points af41
set class-of-service classifiers dscp ba-classifier forwarding-class ef loss-priority high code-points af11
set class-of-service classifiers dscp ba-classifier forwarding-class ef loss-priority high code-points af31
```

```

set class-of-service classifiers dscp ba-classifier forwarding-class low_delay loss-priority low
code-points af21
set class-of-service classifiers dscp ba-classifier forwarding-class low_loss loss-priority low
code-points cs6
set class-of-service drop-profiles drop_profile fill-level 20 drop-probability 50
set class-of-service drop-profiles drop_profile fill-level 50 drop-probability 100
set class-of-service forwarding-classes queue 0 be
set class-of-service forwarding-classes queue 1 ef
set class-of-service forwarding-classes queue 2 low_delay
set class-of-service forwarding-classes queue 3 low_loss
set class-of-service interfaces ge-0/0/1 unit 0 classifiers dscp ba-classifier
set class-of-service interfaces ge-0/0/3 unit 0 scheduler-map SCHEDULER-MAP
set class-of-service interfaces ge-0/0/3 unit 0 shaping-rate 2k
set class-of-service scheduler-maps SCHEDULER-MAP forwarding-class ef scheduler voice
set class-of-service schedulers voice buffer-size temporal 5k
set class-of-service schedulers voice drop-profile-map loss-priority any protocol any drop-
profile drop_profile

```

??

??? ??

?? ?? ?? ???? ???? ???? ?????. ?? ???? ???? ?? ??? Junos OS CLI ??? ??? ? ??? ???? CLI ??? ???? ????  
??.

PMI?? ???? ?? BA ???? ?????:

## 1. CoS? ?????.

```

[edit]
user@host# edit class-of-service

```

## 2. ???? ???? (DiffServ) CoS? ?? BA ???? ????.

```

[edit class-of-service]
user@host# edit classifiers dscp ba-classifier

```

3. BE `???` `???` `????` `??????`.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class be loss-priority low code-points be
```

4. EF `???` `????` `??????`.

```
[edit class-of-service classifiers dscp ba-classifier]
user@host# set forwarding-class ef-class loss-priority low code-points ef
user@host# set forwarding-class ef-class loss-priority high code-points af41
user@host# set forwarding-class ef-class loss-priority high code-points af11
user@host# set forwarding-class ef-class loss-priority high code-points af31
user@host# set forwarding-class low_delay loss-priority low code-points af21
user@host# set forwarding-class low_loss loss-priority low code-points cs6
```

5. `??` `??????` `??????`.

```
[edit class-of-service drop-profiles]
user@host# set drop_profile fill-level 20 drop-probability 50
user@host# set drop_profile fill-level 50 drop-probability 100
```

6. `???` `???` `????` `??????`.

```
[edit class-of-service forwarding-classes ]
user@host# set queue 0 be
user@host# set queue 1 ef
user@host# set queue 2 low_delay
user@host# set 3 low_loss
```

7. `???????` `????` `??????`.

```
[edit class-of-service]
user@host# set interfaces ge-0/0/1 unit 0 classifiers dscp ba-classifier
user@host# set interfaces ge-0/0/3 unit 0 scheduler-map SCHEDULER-MAP
user@host# set interfaces ge-0/0/3 unit 0 shaping-rate 2k
```





```
queue 3 low_loss;
}
interfaces {
  ge-0/0/1 {
    unit 0 {
      classifiers {
        dscp ba-classifier;
      }
    }
  }
  ge-0/0/3 {
    unit 0 {
      scheduler-map SCHEDULER-MAP;
      shaping-rate 2k;
    }
  }
}
scheduler-maps {
  SCHEDULER-MAP {
    forwarding-class ef scheduler voice;
  }
}
schedulers {
  voice {
    buffer-size temporal 5k;
    drop-profile-map loss-priority any protocol any drop-profile drop_profile;
  }
}
```

?? ?? ?? ?? commit?(?) ??.

??

**in this section**

[?? ?? ??](#) | **1385**

?? ?? ???? ???? ?? ?? ?????:

##### ? ? ? ? ? ? ? ?

??

#### ???? ???? ???? ???? ???? ???? ???? ????.

??

?? ???? show class-of-service forwarding-class ?? ????.

```
user@host> show class-of-service forwarding-class
Forwarding class          ID      Queue  Restricted queue  Fabric priority
Policing priority  SPU priority
    be                      0       0         0                low
normal              low
    ef                      1       1         1                low
normal              low
    low_delay              2       2         2                low
normal              low
    low_loss               3       3         3                low
normal              low
```

??

#### ???? ???? ? ? ???? ???? ????.

**?: PMI?? ? ? ? ? ? ? ? ? ? ? ? ? ?**

in this section

- [?? ? ?](#) | 1386
- [??](#) | 1386
- [??](#) | 1386
- [??](#) | 1391





- 3.**                             .

```
[edit firewall filter mf-classifier term assured-forwarding]
user@host# set from destination-address 192.168.44.55
```

- 4.**

|  |  |  |
|--|--|--|
|  |  |  |
|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |
|--|--|--|
|  |  |  |
|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

|  |  |  |  |  |
|--|--|--|--|--|
|  |  |  |  |  |
|--|--|--|--|--|

.

```
[edit firewall filter mf-classifier term assured-forwarding]
user@host# set then forwarding-class af-class
user@host# set then loss-priority low
```

- [illegible]

```
[edit]
user@host# edit firewall filter mf-classifier
user@host# edit term expedited-forwarding
```

6.                             .

```
[edit firewall filter mf-classifier term expedited-forwarding]
user@host# set from destination-address 192.168.66.77
```

- 7.**    ??? ???? ???? ??? ??? ??? ???? ???? ?????.

```
[edit firewall filter mf-classifier term expedited-forwarding]
user@host# set then forwarding-class ef-class
user@host# set then policer ef-policer
```

- 8.**                                   .

```
[edit]
user@host# edit firewall filter mf-classifier
user@host# edit term network-control
```

9. `iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit firewall filter mf-classifier term network-control]
user@host# set from precedence net-control
```

10. `iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit firewall filter mf-classifier term network-control]
user@host# set then forwarding-class nc-class
```

11. `best-effort iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit]
user@host# edit firewall filter mf-classifier
user@host# edit term best-effort
```

12. `best-effort iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit firewall filter mf-classifier term best-effort]
user@host# set then forwarding-class be-class
```

13. `iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet filter input mf-classifier
```

14. `iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -j MASQUERADE`.

```
[edit]
user@host# set interfaces ge-0/0/4 unit 0 family inet filter output mf-classifier
```

??

?? ????? show firewall filter mf-classifier ??? ????? ???? ??????. ??? ??? ???? ????? ???, ? ?? ?? ??? ????? ??  
 ???.

```
[edit]
user@host# show firewall filter mf-classifier
interface-specific;
  term assured-forwarding {
    from {
      destination-address {
        192.168.44.55/32;
      }
    }
    then {
      loss-priority low;
      forwarding-class af-class;
    }
  }
  term expedited-forwarding {
    from {
      destination-address {
        192.168.66.77/32;
      }
    }
    then {
      policer ef-policer;
      forwarding-class ef-class;
    }
  }
  term network-control {
    from {
      precedence net-control;
    }
    then forwarding-class nc-class;
  }
  term best-effort {
    then forwarding-class be-class;
  }
}
```



?? ???? show interfaces ??? ???? ???? ?????. ??? ??? ???? ???? ???? , ? ?? ? ???? ???? ????.

```
[edit]
user@host# show show interfaces
ge-0/0/2 {
  unit 0 {
    family inet {
      filter {
        input mf-classifier;
      }
    }
  }
}
ge-0/0/4 {
  unit 0 {
    family inet {
      filter {
        output mf-classifier;
      }
    }
  }
}
```

???? ???? ???? ? ? ???? commit?(?) ????.

??

**in this section**

[?? ? ???? ???? ? ? ???? ? ? ? ?](#) | 1391

??? ??? ???? ???? ???? ???? ???? ????:

?? ?? ???? ???? ? ? ???? ? ?

??

?? ? ???? ? ? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ???? ????.

??

?? ???? show class-of-service forwarding-class ??? ?????.

```
user@host> show class-of-service forwarding-class
Forwarding class          ID      Queue  Restricted queue  Fabric priority
Policing priority  SPU priority
  BE-data              0        0          0              low
normal                low
  Premium-data         1        1          1              low
normal                low
  Voice                2        2          2              low
normal                low
  NC                   3        3          3              low
normal                low
```

??

???? ???? ???? ? ? ???? ???? ?????.

**?: PMI? ?? ?????? ?? ???? ? ? ? ? ?**

in this section

- [?? ?? | 1392](#)
- [?? | 1393](#)
- [?? | 1393](#)
- [?? | 1396](#)

? ?? PMI?? ?????? ?? ???? ???? ???? ???? ???? ????.

?? ??

? ??? ????? ???? ? ?????? ?? ??? ??? ????.

- SRX ??? ???.

```
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class be-class loss-priority
low code-point 000000
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class be-class loss-priority
high code-point 000001
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class ef-class loss-priority
low code-point 101110
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class ef-class loss-priority
high code-point 101111
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class af-class loss-priority
low code-point 001010
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class af-class loss-priority
```

```

high code-point 001100
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class nc-class loss-priority
low code-point 110000
set class-of-service rewrite-rules dscp rewrite-dscps forwarding-class nc-class loss-priority
high code-point 110001
set class-of-service interfaces ge-0/0/0 unit 0 rewrite-rules dscp rewrite-dscps

```

??

??? ??

?? ?? ?? ????? ??? ??? ??? ?????, ?? ????? ??? ?? ??? Junos OS CLI ??? ??? *? ?? ????? CLI/ ??? ?????????*  
??.

PMI?? ?????? ?? ?? ?? ??? ?????? ??????;

1. DiffServ CoS? ?? ??? ??? ??????

```

[edit]
user@host# edit class-of-service
user@host# edit rewrite-rules dscp rewrite-dscps

```

2. best-effort ??? ??? ??? ??? ??????

```

[edit class-of-service rewrite-rules dscp rewrite-dscps]
user@host# set forwarding-class be-class loss-priority low code-point 000000
user@host# set forwarding-class be-class loss-priority high code-point 000001

```

3. ??? ??? ??? ??? ??? ??????

```

[edit class-of-service rewrite-rules dscp rewrite-dscps]
user@host# set forwarding-class ef-class loss-priority low code-point 101110
user@host# set forwarding-class ef-class loss-priority high code-point 101111

```

```
[edit]
user@host# show class-of-service
interfaces {
  ge-0/0/0 {
    unit 0 {
      rewrite-rules {
        dscp rewrite-dscps;
      }
    }
  }
}

rewrite-rules {
  dscp rewrite-dscps {
    forwarding-class be-class {
      loss-priority low code-point 000000;
      loss-priority high code-point 000001;
    }
    forwarding-class ef-class {
```

```

        loss-priority low code-point 101110;
        loss-priority high code-point 101111;
    }
    forwarding-class af-class {
        loss-priority low code-point 001010;
        loss-priority high code-point 001100;
    }
    forwarding-class nc-class {
        loss-priority low code-point 110000;
        loss-priority high code-point 110001;
    }
}
}

```

?? ?? ?? ?? ?? commit?(?) ????.

??

#### in this section

● [?? ?? ?? ??](#) | 1396

?? ?? ?? ?? ?? ?? ?? ?? ???:

?? ? ? ? ?

??

?? ?? ?? ? ? ? ? ? ? ? ?.

??

?? ???? show class-of-service ??? ????.

```

user@host> show class-of-service
Physical interface: ge-0/0/0, Index: 130
Maximum usable queues: 8, Queues in use: 4
Scheduled map: <default>, Index:2
Congestion-notification: Disabled

```

```

Logical interface: ge0/0/0, Index: 71
Object      Name                      Type      Index
Classifier  ipprec-compatibility ip         13

```

??

??? ??? ??? ge-0/0/0 ?????? ????

## PMI?? IPsec ESP ?? ?? ?? ??

PMI?? ?? IPsec ??? ??? ??? ?? ??? ??? ??? ????. PMI ??? ESP(Encapsulating Security Payload) ?? ?  
 ? ??? ??? ? ???, ?? ??? ??? ??? ?? ??, ??? ?? ? ?? ??? ????

???? ??:

- ??? PMI? ?????? ????. "VPN ?? ???" ??? 1360? ??????.

ESP ?? ?? ??? ????:

1. IPsec ?? ? ??? ????

```

user@host# set security ipsec proposal IPSEC_PROP protocol esp
user@host# set security ipsec proposal IPSEC_PROP authentication-algorithm hmac-sha-256-128
user@host# set security ipsec policy IPSEC_POL proposals IPSEC_PROP

```

2. show security ipsec ??? ??? ???? ????.

```

user@host# show security ipsec
proposal IPSEC_PROP {
    protocol esp;
    authentication-algorithm hmac-sha-256-128;
}
policy IPSEC_POL {
    proposals IPSEC_PROP;
}

```

???? ??? ??? ???? commit?(?) ?????.

SEE ALSO

[??](#)

???? PMI ??

[??](#) [????](#) [????](#) ?? [???](#) ?? [???](#) ? [???](#) [???](#) [???????](#).

[???](#) [???](#) [???](#) "[??](#) [???](#) [??](#)" [???](#) [1399](#) [???????](#).

[??](#) [??](#) [????](#) [????](#) ?? [????](#) [???](#) [???](#) ? [????](#).

[?](#) **150:** [????](#) [??](#)

| ???                                                 | ???                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MX-SPC3? <a href="#">???</a> MX <a href="#">???</a> | <ul style="list-style-type: none"><li>PMI? <a href="#">???</a> MX <a href="#">???????</a> "<a href="#">PMI</a><a href="#">?</a> <a href="#">??</a> <a href="#">????</a> <a href="#">??</a> ? <a href="#">????</a> <a href="#">??</a> <a href="#">??</a> " <a href="#">???</a> <a href="#">1368</a> ? <a href="#">??</a> <a href="#">???</a> <a href="#">????</a> ? <a href="#">??</a> <a href="#">????</a> ?? <a href="#">???</a> <a href="#">???</a> <a href="#">???</a> <a href="#">????</a>.</li><li><a href="#">????</a> <a href="#">??</a> <a href="#">??</a>:<ul style="list-style-type: none"><li><a href="#">??</a> <a href="#">??</a> <a href="#">????</a></li><li>(?)<a href="#">????</a></li><li><a href="#">???????</a> <a href="#">??</a></li><li><a href="#">??</a>/<a href="#">??</a> <a href="#">???</a></li><li><a href="#">??</a> <a href="#">??</a> <a href="#">????</a> <a href="#">??</a> ? ESP <a href="#">??</a></li></ul></li><li><a href="#">????</a> <a href="#">??</a> <a href="#">??</a> <a href="#">??</a>:<ul style="list-style-type: none"><li>np-cache ? IPsec <a href="#">??</a> <a href="#">???</a></li></ul></li></ul> |



**150: (Continued)**

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ???    | ???                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| SRX ?? | <ul style="list-style-type: none"> <li>PMI? ???? SRX ?????? "PMI? ?? ???? ???? ???? ?? ??" ??? 1368? ?? ?? ????? ??? ???? ?? ???? ???? ????.</li> <li>???? ?? ??:             <ul style="list-style-type: none"> <li>NAT-T(SRX5K-SPC3 ? vSRX ?? ???)</li> <li>TEID ?? ? ???? ?? ?? ???? ??? GTP-U ?????</li> <li>QoS(Quality of Service)</li> <li>?? ?? ? ?? ???? ?? ? ?? ?? ? ?? ?? ??.</li> </ul> </li> <li>???? ?? ?? ??:             <ul style="list-style-type: none"> <li>IPsec ? IPsec ??</li> <li>GPRS ??? ?????(GTP) ? ??? ?? ?? ?????(SCTP) ???</li> <li>??? ???</li> <li>DES-CBC ??? ????</li> <li>3DES-CBC ??? ????</li> </ul> </li> </ul> |

?? ?? ??

[\[?\] \[???\] \[????\] \[?\] \[???\] \[?\] \[???\] \[?\] \[???\] \[???\] \[???????\]. \[?\] \[????\] \[???\] \[?\] \[????\]. \[????\] \[???\] \[???\] "\[????\] PMI \[?\]" \[??\]](#)  
 1398 [???] [?????].

151: 100 1000 100

|                                 |                                          |                           |                                                                       |
|---------------------------------|------------------------------------------|---------------------------|-----------------------------------------------------------------------|
| 100                             | SRX4100<br>SRX4200<br>SRX4600<br>SRX4700 | SPC30 1000<br>SRX5000 100 | vSRX 100 1000                                                         |
| PMI 1000 100 10000 1000<br>1000 | 100                                      | 1000                      | Junos OS 1000 19.2R1 100000 1000<br><br>Junos OS 1000 18.3R10 100 100 |

100 100 100

100 1000 100 100 10000 10000 100 1000000. [Feature Explorer](#) 100 10000 1000000 1000 1000000 10000000.

|                                    |                                                                                                        |
|------------------------------------|--------------------------------------------------------------------------------------------------------|
| release heading in release-history | desc heading in release-history                                                                        |
| 22.1R3                             | 10000 ESP 10000 100 PMI Express Path 100 1000 SRX 1000 10000 100000000.                                |
| 21.1R1                             | MX-SPC3 1000 1000 1000 FAT IPsec 1000 100 100.                                                         |
| 20.4R1                             | AES-NI0 100 1000 PMI0 100000000.                                                                       |
| 20.4R1                             | PMI0 100 1000 SRX46000 100000000.                                                                      |
| 19.4R1                             | SRX5K-SPC3 0 vSRX 00 10000 1000 FAT IPsec 1000 00 00.                                                  |
| 19.4R1                             | vSRX 00 10000 PMI 10000 GTP-U0 00 10000 CoS 1000 00 1000 100000000.                                    |
| 19.4R1                             | PMI00 ESP(Encapsulating Security Payload) 00 00 1000 00 1000 SRX5K-SPC30 100000000.                    |
| 19.3R1                             | SRX4100, SRX4200 0 vSRX 00 10000 PMI 10000 aes-128-cbc, aes-192-cbc 0 aes-256-cbc0 00 1000 0 10000000. |
| 19.3R1                             | 10000 00 00(NAT)0 00 PMI 1000 100000000.                                                               |
| 19.2R1                             | SRX5K-SPC30 PMI 10000 GTP-U0 00 10000 CoS 1000 00 1000 100000000.                                      |
| 19.2R1                             | SRX5K-SPC3 0 vSRX 00 100000 NAT-T0 00 PMI0 00 1000 100000000.                                          |

|        |                                                          |
|--------|----------------------------------------------------------|
| 19.1R1 | SRX5K-SPC3? ???? PMI?? CoS(class ifier) ? ??? ??? ?????. |
| 19.1R1 | PMI? ?? ??? SRX5K-SPC3? ???????.                         |
| 18.4R1 | PMI? ?? ??? SRX4100 ? SRX4200? ???????.                  |
| 18.3R1 | vSRX ?? ????? PMI ???? ???????.                          |

# 14

CHAPTER LABEL COVER PAGE

?? ??

---

## in this chapter

- ??? VPN ?? ?? ?? | **1403**
  - ?? ????? ????? ????? ?? VPN ?? ?? | **1405**
  - ??? VPN ?? ?? ?? | **1410**
  - IKE(Internet Key Exchange) 2?? VPN ?? ????? ?? ?? | **1412**
-

## VPN

in this section

- | 1403
- | 1403

Site-to-Site VPN IPsec VPN(, )

### 1. VPN

- : show log messages .

```
user@host # set system syslog file messages any info
```

```
VPN
```

**VPN up/down events:**

```
Jul 9 21:07:58 kmd[1496]: KMD_VPN_DOWN_ALARM_USER: VPN to_hub from 3.3.3.2 is down. Local-
ip: 4.4.4.4, gateway name: to_hub, vpn name: to_hub, tunnel-id: 131073, local tunnel-if:
st0.0, remote tunnel-ip: 70.70.70.1, Local IKE-ID: 4.4.4.4, Remote IKE-ID: 3.3.3.2, XAUTH
username: Not-Applicable, VR id: 4
Jul 9 21:08:10 kmd[1496]: KMD_VPN_UP_ALARM_USER: VPN to_hub from 3.3.3.2 is up. Local-ip:
4.4.4.4, gateway name: to_hub, vpn name: to_hub, tunnel-id: 131073, local tunnel-if:
st0.0, remote tunnel-ip: 70.70.70.1, Local IKE-ID: 4.4.4.4, Remote IKE-ID: 3.3.3.2, XAUTH
username: Not-Applicable, VR id: 4
Jul 9 21:09:58 kmd[1496]: KMD_VPN_DOWN_ALARM_USER: VPN to_hub from 3.3.3.2 is down. Local-
```

```
ip: 4.4.4.4, gateway name: to_hub, vpn name: to_hub, tunnel-id: 131073, local tunnel-if:
st0.0, remote tunnel-ip: 70.70.70.1, Local IKE-ID: 4.4.4.4, Remote IKE-ID: 3.3.3.2, XAUTH
username: Not-Applicable, VR id: 4
Jul 9 21:10:10 kmd[1496]: KMD_VPN_UP_ALARM_USER: VPN to_hub from 3.3.3.2 is up. Local-ip:
4.4.4.4, gateway name: to_hub, vpn name: to_hub, tunnel-id: 131073, local tunnel-if:
st0.0, remote tunnel-ip: 70.70.70.1, Local IKE-ID: 4.4.4.4, Remote IKE-ID: 3.3.3.2, XAUTH
username: Not-Applicable, VR id: 4
```

### Unstable VPN behavior (VPN constantly rebuilding):

```
Jul 9 20:43:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: inbound, SPI: 0xfd91b643, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
Jul 9 20:43:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: outbound, SPI: 0xbdec9669, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
Jul 9 20:44:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: inbound, SPI: 0x69b34ae4, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
Jul 9 20:44:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: outbound, SPI: 0x6f55d8ea, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
Jul 9 20:45:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: inbound, SPI: 0x6fa6b0b3, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
Jul 9 20:45:10 kmd[1496]: KMD_PM_SA_ESTABLISHED: Local gateway: 4.4.4.4, Remote gateway:
3.3.3.2, Local ID: ipv4_subnet(any:0,[0..7]=0.0.0.0/0), Remote ID: ipv4_subnet(any:0,
[0..7]=0.0.0.0/0), Direction: outbound, SPI: 0xa66ac906, AUX-SPI: 0, Mode: Tunnel, Type:
dynamic
```

- `[[[ ]: [[[ ] [[[ ] VPN [[[ ] [[[ ] [[[ ] [[[ ] SRX [[[ ] [[[ ] [[[ ] [[[ ] SRX [[[ ] [[[ ] [[[ ]`  
`[[[ ] [[[ ] [[[ ] [[[ ] [[[ ] [[[ ] show interfaces extensive .`

### 2. `[[[ ] [[[ ] show configuration security ipsec vpn vpn-name [[[ ] VPN [[[ ] VPN [[[ ] [[[ ] [[[ ] [[[ ] [[[ ] [[[ ]`

VPN [[[ ] [[[ ] [[[ ]

- `[[[ ]: 3[[[ ] [[[ ]`.

- `vpn: 5000 000000.`

3. VPN `0000 0000000` VPN `0000000.`

```
user@host# deactivate security ipsec vpn vpn-name vpn-monitor
user@host# commit
```

VPN `00000000?`

- `0: 000000 VPN 000 000 000 00000. 4000 000000.`
- `vpn: 5000 000000.`

4. `00` VPN `000` ICMP `00 000 00000 0000 0000?`

- `0: VPN Monitor 00 000000 0000 000000 00 000000 0 00 IP 000 000000. KB10119 0000000.`
- `vpn: 5000 000000.`

5. SRX `000 0000 000 00 00000 000 000 00 00000000?`

- `0: proxy-id SRX 000 000 0 00 VPN 0000000 00 000000.`
- `vpn: 6000 000000.`

6. VPN `00 00 00 0000000 0 0 0000 0000 0000000?`

- `0: 00000 00 00000 00 00 00 0 00000 000 000 0000000 000 000000.`
- `vpn: 00 00 VPN 0000000 0000 0 0000 00000 00 00 000000 00000 000000. 00 0000 00 0000 0000 00000000.`

`00 00000 00000 00000 00` **VPN** `00 00`

in this section

- `00` | [1406](#)
- `000` | [1406](#)

VPN? ?? ???? ? ?? ?? ???? ???? ???? ????.

? ???? ???? ?? VPN ??? ?????? ? ? ?? ???? ????? ? ???? ????.

VPN

???

```
user@CORPORATE> show security ipsec security-associations
total configured sa: 1
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<32785  2.2.2.2        1398  ESP:3des/sha1  29e26eba 28735/unlim  -   0
>32785  2.2.2.2        1398  ESP:3des/sha1  6d4e790b 28735/unlim  -   0
```

VPN [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] VPN [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] SPI [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED]

? MON ??? VPN ?????? ??? ??? ? ???? ?? ? ? ???? ?????.

- (???): VPN ??? ?? ????? VPN ??? ?? ??? ????? ??????.
- U (??): VPN ??? ?? ????? ??(VPN ????? ?? ???)? ?? ?????.
- D (???): VPN ??? ?? ????? ??(VPN ????? ?? ???)? ?????????.
- Yes: IPsec SA ??? ?? ?? ?? ??????, ??? "2" ??? 1406???????
- No: IPsec SA ??? ??????. ?????? ?????? ?? VPN ?? ??? ????? ??? ??????.

```
root> show configuration security ike
policy ike_pol {
    proposal-set compatible;
```



```

pre-shared-key ascii-text "$9$tMwDuIESreWX7yr4aGDkqIEhcvWbs2";
}
gateway gate1 {
    ike-policy ike_pol;
    address 10.10.10.2;
    external-interface lo0.0;
}

```

- **Yes:** VPN? ??? ?????? lo0 ?? ?????? ????? ?????, ??? "3" ??? 1407?????.
  - **No:** VPN? ??? ?????? lo0 ?? ?????? ????? ?? ?????, ??? "4" ??? 1407?????.
3. ?? ?????(??? ??????)? VPN ?? ?????? ????? lo0? ??? ?? ??? ??? ?????.
- **Yes:** ??? "4" ??? 1407?????.
  - **No:** VPN ?? ?????? ??? ?? ?????? ?? ??? ?? ??? ??? ?? ??? ??????, ??? ?????? IPsec VPN? ??? ? ??? ??? ??????.
4. VPN? ?? ?? VPN? ?? ??? "5" ??? 1407?????. ?? ?? VPN? ?? ??? "8" ??? 1409 ??????. ?? ?? VPN? ?? ?? VPN? ?????? ?????? ??????.
5. ??? st0 ?????? ?? ?? ?????? ?????? ??????. **show route remote network**

```

root@siteA > show route 192.168.20.10
inet.0: 8 destinations, 8 routes (8 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.2.0/24    *[ARI-TS/5] 00:00:53
                  > via st0.0 <-----

```

- **Yes:** ??? "6" ??? 1407?????.
- **No:** st0 ?????? ?? ?? ?????? ????? ??????. ?? ?? VPN? ?? ????? ????? ????? ?????, ??? ?????? ??



?: BGP ?? OSPF? ?? ?? ??? ?????? ?????? ?? ??? ?????? ??????.

6. ?? "5" ??? 1407?? ?? ?????? ??? ?????? VPN? ??? st0 ?????? ?????? ??? ??????. **show security ike**  
**show security ipsec**

- a. `?? ???? ???? show security ike IKE ?????? ??????`.

```
root@siteA # show security ike
...
gateway gw-siteB {          <-----
    ike-policy ike-phase1-policy;
    address 2.2.2.2;
    external-interface ge-0/0/3.0;
}
```

- b. `??? ????? ?? IKE ?????? ?? IPsec VPN? show security ipsec ????? ?(?) ?????? ?????? bind-interface st0 ??????`.

`? ??? VPN ike-vpn-siteB ? ?????? ?????? st0.0 .`

```
root@siteA # show security ipsec
...
vpn ike-vpn-siteB {
    bind-interface st0.0;
    ike {
        gateway gw-siteB;          <-----
        proxy-identity {
            local 192.168.2.0/24;
            remote 192.168.1.0/24;
            service any;
        }
        ipsec-policy ipsec-phase2-policy;
    }
    establish-tunnels immediately;
}
```

- **Yes:** `??? "7" ??? 1408??????`.
- **No:** VPN? ??? st0 ?????? ?????? ?? ?????, ?? ??? ?????? ??? st0 ?????? ??? ??????, ?? ?? VPN? ?? ?????? ?????? ?????? ?????? . ??? ????????

7. `?? ????? st0 ?? ????? ?????? ?????? ?? ??? ?????? ?????? show security policies`

- **Yes:** `??? "8" ??? 1409??????`.
- **No:** `??? ?? ????? ????? VPN? ?? ???????, ?? ?? VPN? ?? ??? ?????? ????? ??????`.

8. `vpn ipsec siteA show security policies`

```

root@siteA# show security policies
...
from-zone trust to-zone untrust {
  policy vpn_egress {
    match {
      source-address local-net;
      destination-address remote-net;
      application any;
    }
    then {
      permit {
        tunnel {
          ipsec-vpn ike-vpn-siteC;
        }
      }
    }
  }
}

from-zone untrust to-zone trust {
  policy vpn_ingress {
    match {
      source-address remote-net;
      destination-address local-net;
      application any;
    }
    then {
      permit {
        tunnel {
          ipsec-vpn ike-vpn-siteC;
        }
      }
    }
  }
}

```

- Yes: `vpn ipsec siteA` `show security policies`.
- No: `vpn ipsec siteA` `show security policies`.

9. `show security flow session`  
**source prefix** *source address* **destination prefix** *destination address*

```
root@siteA> show security flow session source-prefix 192.168.2.0/24 destination-prefix 192.168.1.0/24

Session ID: 5801, Policy name: AtoB/2, Timeout: 1790, Valid
In: 192.168.2.222/1 --> 192.168.1.13/23053;icmp, If: fe-0/0/2.0, Pkts: 59878, Bytes: 4602292
Out: 192.168.1.13/23053 --> 192.168.2.222/1;icmp, If: st0.0, Pkts: 52505, Bytes: 4189289
```

- **Yes:** `show security match policies`.
- **No:** `show security match policies`.

`show security match policies`



`show security match policies` displays the security match policies for the specified VPN. The output shows the policy name, the source and destination addresses, and the number of packets and bytes transferred.

10. `show security match policies`

- `show security match policies` - `show security match policies` IPsec VPN
- `show security match policies` 'traceoptions' 'security datapath-debug'
- `show security match policies` JTAC JTAC

## VPN

`show security match policies`

1. `show security match policies`

- `show security match policies` (LAN-to-LAN) VPN:

`show security match policies`

- `show security match policies` IPsec VPN

`show security match policies` SRX

SRX 2222 2222.

## 2. VPN 222 22 SA(22 22) 22222 22222

show security ipsec security-associations 222 22222 VPN 2 22222 222 22222. 22 2222222 22222 222 VPN SA 222222 22 22222. SA 22 222 222 KB10090 2222222.

```
user@host> show security ipsec security-associations
total configured sa: 2
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<32785  2.2.2.2        1398  ESP:3des/sha1  29e26eba 28735/unlim  -  0
>32785  2.2.2.2        1398  ESP:3des/sha1  6d4e790b 28735/unlim  -  0
total configured sa: 2
ID      Gateway      Port  Algorithm      SPI      Life:sec/kb  Mon vsys
<32786  3.3.3.3        500   ESP:3des/sha1  5c13215d 28782/unlim  U  0
>32786  3.3.3.3        500   ESP:3des/sha1  18f67b48 28782/unlim  U  0
```

- SA 2 222 2222 222 3222 222222.
- SA 2 2222(2222 22 22) 22222 22222 22 22 2 2222222 "22 22222 22222 22222 22 VPN 22 22" 2222 1405.
- SA 2 22 2222 2222 22 22222 22222 22 2 2222222 "2222 VPN 22 22 22" 2222 1403.

## 3. IKE(Internet Key Exchange) 1222 22222222

show security ike security-associations 22222 222222. VPN 2 22 2222 22222 22 22 22 State UP 22 222222.

```
user@host> show security ike security-associations
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
1      2.2.2.2         UP     744a594d957dd513 1e1307db82f58387  Main
2      3.3.3.3         UP     744a594d957dd513 1e1307db82f58387  Main
```

- 22 2222 22222 2222 22 DOWN 222 State 2 22, 22222 22 22222 IKE(Internet Key Exchange) 122 22222 222222. KB10101 2222222.
- 2222 UP 22, 22222 22 22222 IKE(Internet Key Exchange) 222 22222 222222. KB10101 2222222.

2222 2222 22222 2222 22 VPN 2222222 VPN 2222 22 122 22 222 2222 2222222. 22 22 22222 22222 22 2 22 22 422 2 222222.

## 4. 22, 222 22 22 2 IKE 22 2222 222 22 22 22 222222 22222 22222222. 222 2222 2222 22222222.

- 22 2222 22 2222 22 2222 2222 22222222.
- 2222 22 2222 22 2222 2222 KB16233 22222222.

- IKE(Internet Key Exchange) 2?? VPN ?? ???. [KB19943](#) ???.

## IKE(Internet Key Exchange) 2?? VPN ?? ??.

in this section

- ?? | 1412
- ??? | 1412

??

??

?? IKE(Internet Key Exchange) 2??? ?? ??? VPN ?? ???.

??

- IKE(Internet Key Exchange) 2??? ???.
- ?? show security ipsec security-associations VPN? ?? ???.

???

IKE(Internet Key Exchange) 2?? ??? ?? ?? ?? VPN ?? ???.

?? ??? ?? ?? ??? VPN? /???, ??? ?? ?? ?? VPN? /???

1. CLI? ??? VPN ?? ?? syslog ?? kmd-logs?(?) ???.

[KB10097-VPN](#) ?? ??? syslog? ???, VPN ??? ?? ? ? ? Idm-logs???

2. CLI? ??? 2?? ?? ???, show log kmd-logs

?? ?? ??:

- Message:  
Jul 10 16:14:30 210-2 kmd[52472]: IKE Phase-2: Failed to match the peer proxy IDs  
[p2\_remote\_proxy\_id=ipv4\_subnet(any:0,[0..7]=192.168.10.0/24),  
p2\_local\_proxy\_id=ipv4\_subnet(any:0,[0..7]=10.10.10.0/24)] for local ip: 2.2.2.1, remote  
peer ip:2.2.2.2

- `?? - ?? ????? ID? ?? ID? ?????`.
- `?? - ID? ??? ID? ??? KB10124 ?? - 2?? ??? ??, ?? ID? ?`  
`????`.

- Message:  
Jul 16 21:14:20 kmd[1456]: IKE Phase-2 Failure: Quick mode - no proposal chosen  
[spi=cf0f6152, src\_ip=4.4.4.4, dst\_ip=3.3.3.2]  
Jul 16 21:14:20 kmd[1456]: KMD\_VPN\_PV\_PHASE2: IKE Phase-2 Failure: Quick mode - no  
proposal chosen [spi=cf0f6152, src\_ip=4.4.4.4, dst\_ip=3.3.3.2]  
Jul 16 21:14:20 kmd[1456]: IKE Phase-2: Negotiations failed. Local gateway: 4.4.4.4,  
Remote gateway: 3.3.3.2

- `?? - Junos OS? ???? ???? IKE ??? IKE 2?? ???? ???? ?`.

- Action(??) - ?? 2?? VPN ?? ???? ?????. 2?? ?? ???? ???? ????.

- `?? ???? ?`
- `??? ???? ?`
- `?? ???? ?`
- `????? ?(?)`
- `???? ?`

- PFS(Perfect Forward Secrecy)

`?? ??? 2?? ?? ? ? ???? ???? ? ? ???? ???? ? ? ???? ???? ? ? ???? 2?? ??? ? ? ?`  
`? ???? IKE ??? ? ? ?`.

`?? ?? ?`:

- IPsec proposal mismatch

- Message:  
Sep 7 09:26:57 kmd[1393]: IKE negotiation failed with error: No proposal chosen. IKE  
Version: 1, VPN: vpn1 Gateway: ike-gw, Local: 10.10.10.1/500, Remote: 10.10.10.2/500,

Local IKE-ID: 10.10.10.1,  
Remote IKE-ID: 10.10.10.2, VR-ID: 0



?: Local IKE-ID ? Remote IKE-ID ?(?) ? Not-Available???? 1?? ?? ??????. [KB30548 - 12.1X44 ?? ???? IKE\(Internet Key Exchange\) 1?? VPN ?? ???? ?????.](#)

Action(?) - ?? 2?? VPN ?? ??? ?????, 2?? ?? ???? ???? ????.

- ?? ???? ?
  - ??? ???? ?
  - ?? ???? ?
  - ???? ?(?)
  - ??? ?
  - PFS(Perfect Forward Secrecy)
- **Proxy-ID mismatch**

?? ?? ??:

- Sep 7 09:23:05 kmd[1334]: IKE Phase-2: Failed to match the peer proxy IDs  
[p2\_remote\_proxy\_id=ipv4\_subnet(any:0,[0..7]=192.168.1.0/24),  
p2\_local\_proxy\_id=ipv4\_subnet(any:0,[0..7]=192.168.3.0/24)] for local ip: 10.10.10.2,  
remote peer ip:10.10.10.1
- Sep 7 09:23:05 kmd[1334]: IKE Phase-2: Failed to match the peer proxy IDs  
[p2\_remote\_proxy\_id=ipv4\_subnet(any:0,[0..7]=192.168.1.0/24),  
p2\_local\_proxy\_id=ipv4\_subnet(any:0,[0..7]=192.168.3.0/24)] for local ip: 10.10.10.2,  
remote peer ip:10.10.10.1

?? - ??? ID? ??? ??? ID? ??? ???? ???? ?????. [KB10124 ?? - 2?? ??? ???? ??: ?? ??? ID? ?? ???? ????.](#)

VPN ??? ?????? syslog?? ?? ???? ? ? ????.

- Sep 10 08:35:03 kmd[1334]: KMD\_PM\_SA\_ESTABLISHED: Local gateway: 10.10.10.2, Remote gateway: 10.10.10.1, Local ID: ipv4\_subnet(any:0,[0..7]=192.168.3.0/24), Remote ID: ipv4\_subnet(any:0,[0..7]=192.168.1.0/24), Direction: inbound, SPI: 0x4b23e914, AUX-SPI: 0, Mode: Tunnel, Type: dynamic



- ```

• Sep 9 06:57:34 kmd[1393]: KMD_PM_SA_ESTABLISHED: Local gateway: 10.10.10.1, Remote
gateway: 10.10.10.2, Local ID: ipv4_subnet(any:0,[0..7]=192.168.1.0/24), Remote ID:
ipv4_subnet(any:0,[0..7]=192.168.3.0/24), Direction: inbound, SPI: 0xa90982b3, AUX-SPI: 0,
Mode: Tunnel, Type: dynamic, Traffic-selector:
Sep 9 06:57:34 kmd[1393]: KMD_PM_SA_ESTABLISHED: Local gateway: 10.10.10.1, Remote
gateway: 10.10.10.2, Local ID: ipv4_subnet(any:0,[0..7]=192.168.1.0/24), Remote ID:
ipv4_subnet(any:0,[0..7]=192.168.3.0/24), Direction: outbound, SPI: 0x4b23e914, AUX-SPI:
0, Mode: Tunnel, Type: dynamic, Traffic-selector:
Sep 9 06:57:34 kmd[1393]: KMD_VPN_UP_ALARM_USER: VPN test_vpn from 10.10.10.2 is up. Local-
ip: 10.10.10.1, gateway name: ike-gw, vpn name: vpn1, tunnel-id: 131073, local tunnel-if:
st0.0, remote tunnel-ip: Not-Available, Local IKE-ID: 10.10.10.1, Remote IKE-ID:
10.10.10.2, XAUTH username: Not-Applicable, VR id: 0, Traffic-selector: , Traffic-selector
local ID: ipv4_subnet(any:0,[0..7]=192.168.1.0/24), Traffic-selector remote ID:
ipv4_subnet(any:0,[0..7]=192.168.3.0/24)ze: 12px;">IPsec Proposal mismatch

```

4. CLI? ???? 2?? ??? ????? ??? ??? ??? 2?? ??? ?????? ??????. show security ipsec

```
show security ipsec
proposal ipsec-phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
}
policy ipsec-phase2-policy {
    perfect-forward-secrecy {
        keys group2;
    }
    proposals ipsec-phase2-proposal;
}
vpn ike-vpn-srx1 {
```

- □□ □ □□□□□□□.

# 15

CHAPTER LABEL COVER PAGE

?? ? ? ? ? ? ? ?

---

## in this chapter

- Junos CLI ?? ?? | **1418**
-

# Junos CLI ?? ??

?? Junos CLI ??? ?? ???? ? ?? ????????, ? ???? ?? ?? ??? ???? ???? ?? ??????, ?? ???? ?? ? ???? ??? CLI ??? ???? ??? ??????.

- [Junos CLI](#) ??

??? ???? Junos OS ? Junos OS Evolved ?? ???? ?? ?? ??? ????????.

- [??](#) ?
- [??](#) ??