# Table of Contents

About the Documentation ............................................ xv
  Documentation and Release Notes ................................... xv
  Supported Platforms ................................................... xv
  Using the Examples in This Manual .................................. xv
    Merging a Full Example .............................................. xvi
    Merging a Snippet .................................................... xvi
  Documentation Conventions .......................................... xvii
  Documentation Feedback ............................................ xix
  Requesting Technical Support ...................................... xix
    Self-Help Online Tools and Resources ............................ xix
    Opening a Case with JTAC ......................................... xx

## Part 1 Overview

### Chapter 1 IPSecurity ................................................... 3
  VPN Overview .......................................................... 3
  IPsec VPN Topologies ............................................... 4
  Comparison of Policy-Based VPNs and Route-Based VPNs .......... 4
  Security Associations ............................................... 5
  IPsec Key Management ............................................... 6
    Manual Key ........................................................... 6
    AutoKey IKE ........................................................ 7
    Diffie-Hellman Exchange .......................................... 7
  IPsec Security Protocols ........................................... 8
    AH Protocol .......................................................... 8
    ESP Protocol ........................................................ 9
  IPsec Tunnel Negotiation .......................................... 9
  Understanding IKE and IPsec Packet Processing .................. 10
    Packet Processing in Tunnel Mode ................................. 11
    IKE Packet Processing ............................................. 13
    IPsec Packet Processing .......................................... 16
  Understanding Phase 1 of IKE Tunnel Negotiation ................. 18
    Main Mode .......................................................... 19
    Aggressive Mode .................................................... 20
  Understanding Phase 2 of IKE Tunnel Negotiation ................. 20
    Proxy IDs ............................................................ 21
    Perfect Forward Secrecy .......................................... 21
    Replay Protection .................................................. 21
  Understanding Internet Key Exchange Version 2 ................. 22
  Understanding NAT-T ................................................ 23
  Understanding Distributed VPNs in SRX Series Services Gateways 24
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Route-Based VPN</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Understanding Route-Based IPsec VPNs</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Understanding Virtual Router Limitations</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>Understanding Virtual Router Support for Route-Based VPNS</td>
<td>28</td>
</tr>
<tr>
<td>3</td>
<td>Policy-Based VPN</td>
<td>31</td>
</tr>
<tr>
<td></td>
<td>Understanding Policy-Based IPsec VPNs</td>
<td>31</td>
</tr>
<tr>
<td>4</td>
<td>Hub-and-Spoke VPN</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Understanding Hub-and-Spoke VPNs</td>
<td>33</td>
</tr>
<tr>
<td>5</td>
<td>Loopback Interface for High Availability VPN</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Understanding Loopback Interface for a High Availability VPN</td>
<td>35</td>
</tr>
<tr>
<td>6</td>
<td>IPv6 IPsec</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>Understanding VPN Tunnel Modes</td>
<td>37</td>
</tr>
<tr>
<td></td>
<td>VPN Feature Support for IPv6 Addresses</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Understanding Dual Stack Tunnels over an External Interface</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Understanding IPv6 IKE and IPsec Packet Processing</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>IPv6 IKE Packet Processing</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>IPv6 IPsec Packet Processing</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>AH Protocol in IPv6</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>ESP Protocol in IPv6</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>IPv4 Options and IPv6 Extension Headers with AH and ESP</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Integrity Check Value (ICV) Calculation in IPv6</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>Header Construction in Tunnel Modes</td>
<td>48</td>
</tr>
<tr>
<td>7</td>
<td>Traffic Selectors</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Understanding Traffic Selectors in Route-Based VPNS</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>Understanding Reverse Route Insertion</td>
<td>53</td>
</tr>
<tr>
<td></td>
<td>Understanding Traffic Selectors and Overlapping IP Addresses</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Overlapping IP Addresses in Different VPNS Bound to the Same st0 Interface</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Overlapping IP Addresses in the Same VPN Bound to the Same st0 Interface</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Overlapping IP Addresses in Different VPNS Bound to Different st0 Interfaces</td>
<td>55</td>
</tr>
<tr>
<td>8</td>
<td>VPN Alarms</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Understanding VPN Alarms and Auditing</td>
<td>59</td>
</tr>
<tr>
<td>9</td>
<td>VPN Peer Availability</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Understanding VPN Monitoring and DPD</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Understanding Dead Peer Detection</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Understanding Global SPI and VPN Monitoring Features</td>
<td>63</td>
</tr>
<tr>
<td>10</td>
<td>VPN Session Affinity</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>Understanding VPN Session Affinity</td>
<td>65</td>
</tr>
<tr>
<td>11</td>
<td>Suite B Cryptographic Suites</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>Understanding Suite B Cryptographic Suites</td>
<td>67</td>
</tr>
</tbody>
</table>
### Part 2  Configuration

#### Chapter 12  IP Security  .......................................................... 71
- IPsec VPN with Autokey IKE Configuration Overview  .............................. 71
- IPsec VPN with Manual Keys Configuration Overview  .............................. 72
- Recommended Configuration Options for Site-to-Site VPN with Static IP Addresses ................................................................. 73
- Recommended Configuration Options for Site-to-Site or Dialup VPNs with Dynamic IP Addresses ......................................................... 74
- Configuring Remote IKE IDs for Site-to-Site VPNs .................................. 75
- Configuring IPsec VPN Using the VPN Wizard ........................................ 76

#### Chapter 13  Route-Based VPN .................................................. 77
- Example: Configuring a Route-Based VPN ........................................... 77
- Example: Configuring a Route-Based VPN for IKEv2 .............................. 95
- Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device ................................................................. 111
- Example: Configuring an st0 Interface in a Virtual Router ....................... 138

#### Chapter 14  Policy-Based VPN .................................................. 143
- Example: Configuring a Policy-Based VPN ........................................... 143
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device ......................................................... 160

#### Chapter 15  Hub-and-Spoke VPN ............................................. 189
- Example: Configuring a Hub-and-Spoke VPN ....................................... 189

#### Chapter 16  Loopback Interface for High Availability VPN ................. 223
- Example: Configuring Redundancy Groups for Loopback Interfaces .......... 223

#### Chapter 17  IPv6 IPsec ............................................................ 231
- IPv6 IPsec Configuration Overview ...................................................... 231
- Example: Configuring Dual Stack Tunnels over an External Interface .......... 232
- Example: Configuring an IPv6 IPsec Manual VPN .................................. 242
- Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN ................ 244

#### Chapter 18  Traffic Selectors .................................................... 263
- Example: Configuring Traffic Selectors in a Route-Based VPN ............... 263

#### Chapter 19  VPN Alarms .......................................................... 279
- Example: Setting an Audible Alert as Notification of a Security Alarm ....... 279
- Example: Generating Security Alarms in Response to Potential Violations 280

#### Chapter 20  VPN Peer Availability ............................................ 283
- Example: Configuring Global SPI and VPN Monitoring Features .......... 283

#### Chapter 21  VPN Session Affinity ............................................. 285
- Enabling VPN Session Affinity .......................................................... 285
- Accelerating the IPsec VPN Traffic Performance ................................... 287
Chapter 22  IKE Configuration Statements .............................................. 289
  Security Configuration Statement Hierarchy ........................................ 290
  [edit security ike] Hierarchy Level .................................................. 291
  address (Security IKE Gateway) ....................................................... 293
  always-send ..................................................................................... 294
  authentication-algorithm (Security IKE) ............................................. 295
  authentication-method ....................................................................... 296
  certificate .......................................................................................... 297
  connections-limit ................................................................................ 298
  container ............................................................................................. 299
  dead-peer-detection ............................................................................. 300
  dh-group (Security IKE) ........................................................................ 301
  distinguished-name (Security) ............................................................. 302
  dynamic (Security) ................................................................................ 303
  encryption-algorithm (Security IKE) ................................................... 304
  external-interface (Security IKE Gateway) .......................................... 305
  gateway (Security IKE) ........................................................................ 306
  general-ikeid ....................................................................................... 307
  hostname ............................................................................................. 307
  ike (Security) ....................................................................................... 308
  ike (Security IPSec VPN) ..................................................................... 310
  ike-policy (Security Gateway) ............................................................ 311
  ike-user-type ....................................................................................... 312
  inet (Security Dynamic Peer) .............................................................. 313
  inet6 (Security IKE Gateway) ............................................................. 313
  interval (Security IKE) .......................................................................... 314
  lifetime-seconds (Security IKE) .......................................................... 314
  local-address ....................................................................................... 315
  local-certificate (Security) ................................................................. 316
  local-identity ....................................................................................... 317
  mode (Security IKE Policy) ................................................................. 318
  nat-keepalive ....................................................................................... 319
  no-nat-traversal .................................................................................. 319
  optimized (DPD) .................................................................................. 320
  peer-certificate-type .......................................................................... 320
  policy (Security IKE) ............................................................................ 321
  pre-shared-key (Security IKE Policy) ................................................. 322
  probe-idle-tunnel ............................................................................... 322
  proposal (Security IKE) ....................................................................... 323
  proposal-set (Security IKE) ................................................................. 324
  proposals (Security IKE) ..................................................................... 325
  remote-identity .................................................................................... 326
  respond-bad-spi .................................................................................. 327
  threshold (Security IKE Gateway) ....................................................... 328
  traceoptions (Security IKE) ................................................................. 329
  trusted-ca (Security IKE Policy) ......................................................... 331
  user-at-hostname ................................................................................ 332
  version (Security IKE Gateway) ........................................................ 332
  wildcard ............................................................................................... 333
Chapter 23 IPsec Configuration Statements ................................... 335

Security Configuration Statement Hierarchy ............................. 336
[edit security ipsec] Hierarchy Level ................................... 337
algorithm (Security) .................................................. 340
authentication (Security IPsec) ....................................... 341
authentication-algorithm (Security IPsec) ............................ 342
bind-interface ....................................................... 343
destination-ip (Security IPsec) ....................................... 343
df-bit ................................................................. 344
everypacket (Security) ............................................. 345
encryption-algorithm (Security IPsec) ................................ 346
establish-tunnels .................................................... 347
external-interface (Security Manual SA) ......................... 347
gateway (Security IPsec VPN) ..................................... 348
gateway (Security Manual SA) ..................................... 348
idle-time ............................................................ 349
ike (Security IPsec VPN) ........................................... 350
install-interval ..................................................... 351
ipsec (Security) ..................................................... 352
ipsec-performance-acceleration (Security Flow) ................... 354
ipsec-policy (Security) ............................................. 354
ipsec-vpn (Security Flow) ......................................... 355
lifetime-kilobytes ................................................... 355
lifetime-seconds (Security IPsec) .................................. 356
load-distribution .................................................... 356
local (Security IPsec) .............................................. 357
manual (Security IPsec) ........................................... 358
no-anti-replay (Security) ......................................... 359
optimized ............................................................ 359
peer-certificate-type ............................................... 360
perfect-forward-secrecy (Security IPsec) ............................ 361
policy (Security IPsec) ............................................. 362
proposal (Security IPsec) .......................................... 363
proposal-set (Security IPsec) ...................................... 364
proposals (Security IPsec) ........................................ 365
protocol (Security IPsec) .......................................... 366
protocol (Security IPsec Manual SA) ............................. 367
proxy-identity ....................................................... 368
refresh-interval .................................................... 369
remote (Security IPsec) ............................................ 369
service (Security IPsec) ........................................... 370
session-affinity .................................................... 370
source-interface (Security) ........................................ 371
spi (Security IPsec) ................................................. 371
traceoptions (Security IPsec) ...................................... 372
traffic-selector ..................................................... 373
vpn (Security) ..................................................... 374
Chapter 24 VPN Alarms Configuration Statements .................................................. 377

Security Configuration Statement Hierarchy .................................................... 377
[edit security alarms] Hierarchy Level .............................................................. 378
cryptographic-self-test .............................................................. 380
decryption-failures ................................................................. 381
efficiency-failures ................................................................. 382
key-generation-self-test .................................................. 383
ike-phase1-failures ....................................................... 384
ike-phase2-failures ....................................................... 385
non-cryptographic-self-test ........................................ 386
replay-attacks ......................................................... 387

Part 3 Administration

Chapter 25 Operational Commands ............................................................... 391

clear security ike respond-bad-spi-count ........................................ 392
clear security ike security-associations ........................................... 393
clear security ipsec security-associations ...................................... 395
clear security ipsec statistics .................................................. 397
request security ike debug-disable ............................................ 399
request security ike debug-enable ............................................ 400
show security ike active-peer ................................................ 401
show security ike debug-status ............................................. 402
show security ike pre-shared-key ........................................ 403
show security ike security-associations .................................. 404
show security ike tunnel-map ............................................... 411
show security ipsec inactive-tunnels ...................................... 412
show security ipsec next-hop-tunnels .................................. 415
show security ipsec security-associations ................................ 416
show security ipsec statistics ............................................. 424

Part 4 Index

Index ......................................................................................... 429
# List of Figures

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>IP Security</td>
</tr>
<tr>
<td>Figure 1: Tunnel Mode</td>
<td>11</td>
</tr>
<tr>
<td>Figure 2: Site-to-Site VPN in Tunnel Mode</td>
<td>12</td>
</tr>
<tr>
<td>Figure 3: Dial-Up VPN in Tunnel Mode</td>
<td>13</td>
</tr>
<tr>
<td>Figure 4: IKE Packet for Phases 1 and 2</td>
<td>14</td>
</tr>
<tr>
<td>Figure 5: Generic ISAKMP Payload Header</td>
<td>15</td>
</tr>
<tr>
<td>Figure 6: ISAKMP Header with Generic ISAKMP Payloads</td>
<td>16</td>
</tr>
<tr>
<td>Figure 7: IPsec Packet—ESP in Tunnel Mode</td>
<td>16</td>
</tr>
<tr>
<td>Figure 8: Outer IP Header (IP2) and ESP Header</td>
<td>17</td>
</tr>
<tr>
<td>Figure 9: Inner IP Header (IP1) and TCP Header</td>
<td>18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Hub-and-Spoke VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 10: Multiple Tunnels in a Hub-and-Spoke VPN Configuration</td>
<td>33</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 6</th>
<th>IPv6 IPsec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 11: IPv4-in-IPv4 Tunnel</td>
<td>37</td>
</tr>
<tr>
<td>Figure 12: IPv6-in-IPv6 Tunnel</td>
<td>38</td>
</tr>
<tr>
<td>Figure 13: IPv6-in-IPv4 Tunnel</td>
<td>38</td>
</tr>
<tr>
<td>Figure 14: IPv4-in-IPv6 Tunnel</td>
<td>38</td>
</tr>
<tr>
<td>Figure 15: Dual Stack Tunnels</td>
<td>43</td>
</tr>
<tr>
<td>Figure 16: IPv6 AH Tunnel Mode</td>
<td>46</td>
</tr>
<tr>
<td>Figure 17: IPv6 ESP Tunnel Mode</td>
<td>47</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Traffic Selectors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 18: Traffic Selector Example</td>
<td>51</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 13</td>
<td>Route-Based VPN</td>
</tr>
<tr>
<td>Figure 19: Route-Based VPN Topology</td>
<td>77</td>
</tr>
<tr>
<td>Figure 20: Route-Based VPN Topology with Only the Responder Behind a NAT Device</td>
<td>78</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 14</th>
<th>Policy-Based VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 21: Policy-Based VPN Topology</td>
<td>143</td>
</tr>
<tr>
<td>Figure 22: Policy-Based VPN Topology with Both an Initiator and a Responder Behind a NAT Device</td>
<td>144</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15</th>
<th>Hub-and-Spoke VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 23: Hub-and-Spoke VPN Topology</td>
<td>189</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 16</th>
<th>Loopback Interface for High Availability VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 12:</td>
<td>223</td>
</tr>
</tbody>
</table>
# List of Tables

**About the Documentation** .............................................. xv
Table 1: Notice Icons .................................................. xvii
Table 2: Text and Syntax Conventions .............................. xviii

<table>
<thead>
<tr>
<th>Part 1</th>
<th>Overview</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>IP Security ......................................................... 3</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>IPv6 IPsec .......................................................... 37</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 12</td>
<td>IP Security .......................................................... 71</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Route-Based VPN ................................................... 77</td>
</tr>
</tbody>
</table>

| Chapter 7 | Traffic Selectors .................................................. 51 |
| Table 9: Example Traffic Selector Pairs | 52 |

| Chapter 12 | IP Security .......................................................... 71 |
| Table 10: Recommended Configuration for Site-to-Site VPN with Static IP Addresses | 73 |
| Table 11: Recommended Configuration for Site-to-Site or Dialup VPNs with Dynamic IP Addresses | 74 |

| Chapter 13 | Route-Based VPN ................................................... 77 |
| Table 12: Interface, Static Route, Security Zone, and Address Book Information | 79 |
| Table 13: IKE Phase 1 Configuration Parameters | 79 |
| Table 14: IPsec Phase 2 Configuration Parameters | 80 |
| Table 15: Security Policy Configuration Parameters | 80 |
| Table 16: TCP-MSS Configuration Parameters | 80 |
| Table 17: Interface, Static Route, Security Zone, and Address Book Information | 95 |
| Table 18: IKE Phase 1 Configuration Parameters | 96 |
| Table 19: IPsec Phase 2 Configuration Parameters | 96 |
| Table 20: Security Policy Configuration Parameters | 97 |
| Table 21: TCP-MSS Configuration Parameters | 97 |
Table 22: Interface, Routing Options, Zones, and Security Policies for the Initiator ................................................. 114
Table 23: IKE Phase 1 Configuration Parameters for the Initiator ................................................................. 114
Table 24: IPsec Phase 2 Configuration Parameters for the Initiator ................................................................. 115
Table 25: Interface, Routing Options, Zones, and Security Policies for the Responder ............................................. 115
Table 26: IKE Phase 1 Configuration Parameters for the Responder ................................................................. 116
Table 27: IPsec Phase 2 Configuration Parameters for the Responder ................................................................. 116

Chapter 14 Policy-Based VPN ........................................... 143
Table 28: Interface, Security Zone, and Address Book Information ................................................................. 145
Table 29: IKE Phase 1 Configuration Parameters ................................................................. 145
Table 30: IPsec Phase 2 Configuration Parameters ................................................................. 146
Table 31: Security Policy Configuration Parameters ................................................................. 146
Table 32: TCP-MSS Configuration Parameters ................................................................. 147
Table 33: Interface, Routing Options, and Security Zones for the Initiator ................................................................. 163
Table 34: IKE Phase 1 Configuration Parameters for the Initiator ................................................................. 163
Table 35: IPsec Phase 2 Configuration Parameters for the Initiator ................................................................. 164
Table 36: Security Policy Configuration Parameters for the Initiator ................................................................. 164
Table 37: Interface, Routing Options, and Security Zones for the Responder ................................................................. 164
Table 38: IKE Phase 1 Configuration Parameters for the Responder ................................................................. 165
Table 39: IPsec Phase 2 Configuration Parameters for the Responder ................................................................. 165
Table 40: Security Policy Configuration Parameters for the Responder ................................................................. 166

Chapter 15 Hub-and-Spoke VPN ........................................... 189
Table 41: Interface, Security Zone, and Address Book Information ................................................................. 190
Table 42: IKE Phase 1 Configuration Parameters ................................................................. 192
Table 43: IPsec Phase 2 Configuration Parameters ................................................................. 193
Table 44: Security Policy Configuration Parameters ................................................................. 194
Table 45: TCP-MSS Configuration Parameters ................................................................. 195

Chapter 17 IPv6 IPsec .................................................. 231
Table 46: Phase 1 Options for Dual Stack Tunnel Configuration ................................................................. 232
Table 47: Phase 2 Options for Dual Stack Tunnel Configuration ................................................................. 233
Table 48: Interface, Security Zone, and Address Book Information ................................................................. 247
Table 49: IPv6 IKE Phase 1 Configuration Parameters ................................................................. 247
Table 50: IPv6 IPsec Phase 2 Configuration Parameters ................................................................. 247
Table 51: Security Policy Configuration Parameters ................................................................. 248
Table 52: TCP-MSS Configuration Parameters ................................................................. 249

Chapter 18 Traffic Selectors .............................................. 263
Table 53: Traffic Selector Configurations ................................................................. 263
Table 54: Phase 1 Options for Traffic Selector Configurations ................................................................. 264
Table 55: Phase 2 Options for Traffic Selector Configurations ................................................................. 265

Part 3 Administration
Chapter 25 Operational Commands ........................................... 391
Table 56: show security ike security-associations Output Fields ................................................................. 405
Table 57: show security ipsec inactive-tunnels Output Fields ................................................................. 413
Table 58: show security ipsec next-hop-tunnels Output Fields ................................................................. 415
Table 59: show security ipsec security-associations ......................... 417
Table 60: show security ipsec statistics Output Fields ......................... 424
About the Documentation

- Documentation and Release Notes on page xv
- Supported Platforms on page xv
- Using the Examples in This Manual on page xv
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xix

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- J Series
- SRX Series
- LN Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the load merge or the load merge relative command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.
If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a full example. In this case, use the `load merge` command.

If the example configuration does not start at the top level of the hierarchy, the example is a snippet. In this case, use the `load merge relative` command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file `ex-script.conf`. Copy the `ex-script.conf` file to the `/var/tmp` directory on your routing platform.

   ```
   system {
     scripts {
       commit {
         file ex-script.xsl;
       }
     }
   }
   interfaces {
     fxp0 {
       disable;
       unit 0 {
         family inet {
           address 10.0.0.1/24;
         }
       }
     }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the `load merge` configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file `ex-script-snippet.conf`. Copy the `ex-script-snippet.conf` file to the `/var/tmp` directory on your routing platform.

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```
2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the `load merge relative` configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the `load` command, see the CLI User Guide.

**Documentation Conventions**

Table 1 on page xvii defines notice icons used in this guide.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon.png" alt="i" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![!] (exclamation mark)</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![] (triangle with exclamation mark)</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="laser_icon.png" alt="" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td>![] (circle with exclamation mark)</td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td><img src="laser_icon.png" alt="" /></td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

Table 2 on page xviii defines the text and syntax conventions used in this guide.
### Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>user@host&gt;</code> <code>configure</code></td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td><code>user@host&gt;</code> <code>show chassis alarms</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No alarms currently active</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>• Introduces or emphasizes important new terms.</td>
<td>• A policy term is a named structure that defines match conditions and actions.</td>
</tr>
<tr>
<td></td>
<td>• Identifies guide names.</td>
<td>• Junos OS CLI User Guide</td>
</tr>
<tr>
<td></td>
<td>• Identifies RFC and Internet draft titles.</td>
<td>• RFC 1997, BGP Communities Attribute</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>[edit]</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>root@#</code> <code>set system domain-name</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>domain-name</code></td>
</tr>
<tr>
<td><strong>Text like this</strong></td>
<td>Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.</td>
<td>• To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The console port is labeled <code>CONSOLE</code>.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code> (angle brackets)</td>
<td>Encloses optional keywords or variables.</td>
<td><code>stub &lt;default-metric metric &gt;;</code></td>
</tr>
<tr>
<td><code>{ }</code> (square brackets)</td>
<td>Encloses a variable for which you can substitute one or more values.</td>
<td>community name members <code>{ community-ids }</code></td>
</tr>
<tr>
<td>Indention and braces ( <code>{ }</code> )</td>
<td>Identifies a level in the configuration hierarchy.</td>
<td>[edit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>routing-options</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>[static</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>route default</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>nexthop address;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>retain;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>}</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>}</code></td>
</tr>
</tbody>
</table>

---

**GUI Conventions**
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents graphical user interface (GUI) items you click or select.</td>
<td>• In the Logical Interfaces box, select <em>All Interfaces</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• To cancel the configuration, click <em>Cancel</em>.</td>
</tr>
<tr>
<td><strong>&gt; (bold right angle bracket)</strong></td>
<td>Separates levels in a hierarchy of menu selections.</td>
<td>In the configuration editor hierarchy, select <em>Protocols&gt;Osfp</em>.</td>
</tr>
</tbody>
</table>

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- **Online feedback rating system**—On any page at the Juniper Networks Technical Documentation site at [http://www.juniper.net/techpubs/index.html](http://www.juniper.net/techpubs/index.html), simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at [http://www.juniper.net/techpubs/feedback/](http://www.juniper.net/techpubs/feedback/).

- **E-mail**—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.


- **Product warranties**—For product warranty information, visit [http://www.juniper.net/support/warranty/](http://www.juniper.net/support/warranty/).

- **JTAC hours of operation**—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:
• Find CSC offerings: http://www.juniper.net/customers/support/
• Search for known bugs: http://www2.juniper.net/kb/
• Find product documentation: http://www.juniper.net/techpubs/
• Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
• Download the latest versions of software and review release notes:
  http://www.juniper.net/customers/csc/software/
• Search technical bulletins for relevant hardware and software notifications:
  http://kb.juniper.net/InfoCenter/
• Join and participate in the Juniper Networks Community Forum:
  http://www.juniper.net/company/communities/
• Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

• Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
• Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.
PART 1

Overview

• IP Security on page 3
• Route-Based VPN on page 27
• Policy-Based VPN on page 31
• Hub-and-Spoke VPN on page 33
• Loopback Interface for High Availability VPN on page 35
• IPv6 IPsec on page 37
• Traffic Selectors on page 51
• VPN Alarms on page 59
• VPN Peer Availability on page 61
• VPN Session Affinity on page 65
• Suite B Cryptographic Suites on page 67
A virtual private network (VPN) provides a means for securely communicating among remote computers across a public WAN such as the Internet.

A VPN connection can link two LANs (site-to-site VPN) or a remote dial-up user and a LAN. The traffic that flows between these two points passes through shared resources such as routers, switches, and other network equipment that make up the public WAN. To secure VPN communication while passing through the WAN, the two participants create an IP Security (IPsec) tunnel.

**NOTE:** The term *tunnel* does not denote tunnel mode (see “Packet Processing in Tunnel Mode” on page 11). Instead, it refers to the IPsec connection.

IPsec is a suite of related protocols for cryptographically securing communications at the IP Packet Layer. IPsec also provides methods for the manual and automatic negotiation of security associations (SAs) and key distribution, all the attributes for which are gathered in a domain of interpretation (DOI). The IPsec DOI is a document containing definitions for all the security parameters required for the successful negotiation of a VPN tunnel—essentially, all the attributes required for SA and IKE negotiations. See RFC 2407 and RFC 2408 for more information.
This topic includes the following sections:

- IPsec VPN Topologies on page 4
- Comparison of Policy-Based VPNs and Route-Based VPNs on page 4
- Security Associations on page 5
- IPsec Key Management on page 6
- IPsec Security Protocols on page 8
- IPsec Tunnel Negotiation on page 9

IPsec VPN Topologies

The following are some of the IPsec VPN topologies that Junos operating system (OS) supports:

- Site-to-site VPNs—Connects two sites in an organization together and allows secure communications between the sites.
- Hub-and-spoke VPNs—Connects branch offices to the corporate office in an enterprise network. You can also use this topology to connect spokes together by sending traffic through the hub.
- Remote access VPNs—Allows users working at home or traveling to connect to the corporate office and its resources. This topology is sometimes referred to as an end-to-site tunnel.

Comparison of Policy-Based VPNs and Route-Based VPNs

Table 3 on page 4 summarizes the differences between policy-based VPNs and route-based VPNs.

<table>
<thead>
<tr>
<th>Policy-Based VPNs</th>
<th>Route-Based VPNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>In policy-based VPNs, a tunnel is treated as an object that, together with source, destination, application, and action, constitutes a tunnel policy that permits VPN traffic.</td>
<td>In route-based VPNs, a policy does not specifically reference a VPN tunnel.</td>
</tr>
<tr>
<td>A tunnel policy specifically references a VPN tunnel by name.</td>
<td>A route determines which traffic is sent through the tunnel based on a destination IP address.</td>
</tr>
<tr>
<td>The number of policy-based VPN tunnels that you can create is limited by the number of tunnels that the device supports.</td>
<td>The number of route-based VPN tunnels that you create is limited by the number of st0 interfaces (for point-to-point VPNs) or the number of tunnels that the device supports, whichever is lower.</td>
</tr>
<tr>
<td>With a policy-based VPN, although you can create numerous tunnel policies referencing the same VPN tunnel, each tunnel policy pair creates an individual IPsec SA with the remote peer. Each SA counts as an individual VPN tunnel.</td>
<td>Because the route, not the policy, determines which traffic goes through the tunnel, multiple policies can be supported with a single SA or VPN.</td>
</tr>
<tr>
<td>In a policy-based VPN, the action must be permit and must include a tunnel.</td>
<td>In a route-based VPN, the regulation of traffic is not coupled to the means of its delivery.</td>
</tr>
</tbody>
</table>
Table 3: Comparison Between Policy-Based VPNs and Route-Based VPNs (continued)

<table>
<thead>
<tr>
<th>Policy-Based VPNs</th>
<th>Route-Based VPNs</th>
</tr>
</thead>
<tbody>
<tr>
<td>The exchange of dynamic routing information is not supported in policy-based VPNs.</td>
<td>Route-based VPNs support the exchange of dynamic routing information through VPN tunnels. You can enable an instance of a dynamic routing protocol, such as OSPF, on an st0 interface that is bound to a VPN tunnel.</td>
</tr>
<tr>
<td>If you need more granularity than a route can provide to specify the traffic sent to a tunnel, using a policy-based VPN with security policies is the best choice.</td>
<td>Route-based VPNs uses routes to specify the traffic sent to a tunnel; a policy does not specifically reference a VPN tunnel.</td>
</tr>
<tr>
<td>With a policy-based VPN tunnel, you can consider a tunnel as an element in the construction of a policy.</td>
<td>When the security device does a route lookup to find the interface through which it must send traffic to reach an address, it finds a route through a secure tunnel (st0) interface. With a route-based VPN tunnel, you can consider a tunnel as a means for delivering traffic, and can consider the policy as a method for either permitting or denying the delivery of that traffic.</td>
</tr>
</tbody>
</table>

Security Associations

A security association (SA) is a unidirectional agreement between the VPN participants regarding the methods and parameters to use in securing a communication channel. Full bidirectional communication requires at least two SAs, one for each direction. Through the SA, an IPsec tunnel can provide the following security functions:

- Privacy (through encryption)
- Content integrity (through data authentication)
- Sender authentication and—if using certificates—nonrepudiation (through data origin authentication)

The security functions you employ depend on your needs. If you need only to authenticate the IP packet source and content integrity, you can authenticate the packet without applying any encryption. On the other hand, if you are concerned only with preserving privacy, you can encrypt the packet without applying any authentication mechanisms. Optionally, you can both encrypt and authenticate the packet. Most network security designers choose to encrypt, authenticate, and replay-protect their VPN traffic.

An IPsec tunnel consists of a pair of unidirectional SAs—one SA for each direction of the tunnel—that specify the security parameter index (SPI), destination IP address, and security protocol (Authentication Header [AH] or Encapsulating Security Payload [ESP]) employed. An SA groups together the following components for securing communications:

- Security algorithms and keys.
- Protocol mode, either transport or tunnel. Junos OS devices always use tunnel mode. (See “Packet Processing in Tunnel Mode” on page 11.)
• Key-management method, either manual key or AutoKey IKE. (See “IPsec Key Management” on page 6.)

• SA lifetime.

For inbound traffic, Junos OS looks up the SA by using the following triplet:

• Destination IP address.

• Security protocol, either AH or ESP. (See “IPsec Security Protocols” on page 8.)

• Security parameter index (SPI) value.

For outbound VPN traffic, the policy invokes the SA associated with the VPN tunnel.

**IPsec Key Management**

The distribution and management of keys are critical to using VPNs successfully. Junos OS supports IPsec technology for creating VPN tunnels with three kinds of key creation mechanisms:

• Manual key

• AutoKey IKE with a preshared key or a certificate

You can choose your key creation mechanism—also called authentication method—during Phase 1 and Phase 2 proposal configuration. See “IPsec Tunnel Negotiation” on page 9.

---

**NOTE:** Manual key creation and AutoKey IKE with certificates are not supported with the dynamic VPN feature at this time.

---

This topic includes the following sections:

• Manual Key on page 6

• AutoKey IKE on page 7

• Diffie-Hellman Exchange on page 7

**Manual Key**

With manual keys, administrators at both ends of a tunnel configure all the security parameters. This is a viable technique for small, static networks where the distribution, maintenance, and tracking of keys are not difficult. However, safely distributing manual-key configurations across great distances poses security issues. Aside from passing the keys face-to-face, you cannot be completely sure that the keys have not been compromised while in transit. Also, whenever you want to change the key, you are faced with the same security issues as when you initially distributed it.
AutoKey IKE

When you need to create and manage numerous tunnels, you need a method that does not require you to configure every element manually. IPsec supports the automated generation and negotiation of keys and security associations using the Internet Key Exchange (IKE) protocol. Junos OS refers to such automated tunnel negotiation as AutoKey IKE and supports AutoKey IKE with preshared keys and AutoKey IKE with certificates.

- AutoKey IKE with preshared keys—Using AutoKey IKE with preshared keys to authenticate the participants in an IKE session, each side must configure and securely exchange the preshared key in advance. In this regard, the issue of secure key distribution is the same as that with manual keys. However, once distributed, an autokey, unlike a manual key, can automatically change its keys at predetermined intervals using the IKE protocol. Frequently changing keys greatly improves security, and automatically doing so greatly reduces key-management responsibilities. However, changing keys increases traffic overhead; therefore, changing keys too often can reduce data transmission efficiency.

NOTE: A preshared key is a key for both encryption and decryption, which both participants must have before initiating communication.

- AutoKey IKE with certificates—When using certificates to authenticate the participants during an AutoKey IKE negotiation, each side generates a public-private key pair and acquires a certificate. As long as the issuing certificate authority (CA) is trusted by both sides, the participants can retrieve the peer’s public key and verify the peer’s signature. There is no need to keep track of the keys and SAs; IKE does it automatically.

Diffie-Hellman Exchange

A Diffie-Hellman (DH) exchange allows participants to produce a shared secret value. The strength of the technique is that it allows participants to create the secret value over an unsecured medium without passing the secret value through the wire. There are five DH groups; Junos OS supports groups 1, 2, 5, and 14. The size of the prime modulus used in each group’s calculation differs as follows:

- DH Group 1—768-bit modulus
- DH Group 2—1024-bit modulus
- DH Group 5—1536-bit modulus
- DH Group 14—2048-bit modulus

NOTE: The strength of DH Group 1 security has depreciated; therefore, we do not recommend its use.
The larger the modulus, the more secure the generated key is considered to be; however, the larger the modulus, the longer the key-generation process takes. Because the modulus for each DH group is a different size, the participants must agree to use the same group.

**NOTE:** If you configure multiple (up to four) proposals for Phase 1 negotiations, use the same DH group in all proposals. The same guideline applies to multiple proposals for Phase 2 negotiations.

### IPsec Security Protocols

IPsec uses two protocols to secure communications at the IP layer:

- Authentication Header (AH)—A security protocol for authenticating the source of an IP packet and verifying the integrity of its content
- Encapsulating Security Payload (ESP)—A security protocol for encrypting the entire IP packet (and authenticating its content)

You can choose your security protocols—also called authentication and encryption algorithms—during Phase 2 proposal configuration. See “IPsec Tunnel Negotiation” on page 9.

This topic includes the following sections:

- AH Protocol on page 8
- ESP Protocol on page 9

### AH Protocol

The Authentication Header (AH) protocol provides a means to verify the authenticity and integrity of the content and origin of a packet. You can authenticate the packet by the checksum calculated through a Hash Message Authentication Code (HMAC) using a secret key and either MD5 or SHA-1 hash functions.

- Message Digest 5 (MD5)—An algorithm that produces a 128-bit hash (also called a digital signature or message digest) from a message of arbitrary length and a 16-byte key. The resulting hash is used, like a fingerprint of the input, to verify content and source authenticity and integrity.
- Secure Hash Algorithm (SHA-1)—An algorithm that produces a 160-bit hash from a message of arbitrary length and a 20-byte key. It is generally regarded as more secure than MD5 because of the larger hashes it produces. Because the computational processing is done in the ASIC, the performance cost is negligible.

**NOTE:** For more information on MD5 hashing algorithms, see RFC 1321 and RFC 2403. For more information on SHA hashing algorithms, see RFC 2404. For more information on HMAC, see RFC 2104.
ESP Protocol

The Encapsulating Security Payload (ESP) protocol provides a means to ensure privacy (encryption) and source authentication and content integrity (authentication). ESP in tunnel mode encapsulates the entire IP packet (header and payload) and then appends a new IP header to the now-encrypted packet. This new IP header contains the destination address needed to route the protected data through the network. (See “Packet Processing in Tunnel Mode” on page 11.)

With ESP, you can both encrypt and authenticate, encrypt only, or authenticate only. For encryption, you can choose one of the following encryption algorithms:

- Data Encryption Standard (DES)—A cryptographic block algorithm with a 56-bit key.
- Triple DES (3DES)—A more powerful version of DES in which the original DES algorithm is applied in three rounds, using a 168-bit key. DES provides significant performance savings but is considered unacceptable for many classified or sensitive material transfers.
- Advanced Encryption Standard (AES)—An encryption standard which offers greater interoperability with other devices. Junos OS supports AES with 128-bit, 192-bit, and 256-bit keys.

For authentication, you can use either the MD5 or the SHA-1 algorithm.

NOTE: Even though it is possible to select NULL for encryption, it has been demonstrated that IPsec might be vulnerable to attack under such circumstances. Therefore, we suggest that you choose an encryption algorithm for maximum security.

IPsec Tunnel Negotiation

To establish an AutoKey IKE IPsec tunnel, two phases of negotiation are required:

- In Phase 1, the participants establish a secure channel in which to negotiate the IPsec security associations (SAs).
- In Phase 2, the participants negotiate the IPsec SAs for encrypting and authenticating the ensuing exchanges of user data.

For a manual key IPsec tunnel, because all the SA parameters have been previously defined, there is no need to negotiate which SAs to use. In essence, the tunnel has already been established. When traffic matches a policy using that manual key tunnel or when a route involves the tunnel, the Juniper Networks device simply encrypts and authenticates the data, as you determined, and forwards it to the destination gateway.

The remote IKE gateway address can be in any virtual routing (VR) instance. VR is determined during IKE Phase 1 and Phase 2 negotiation. VR does not have to be configured in the IKE proposals. If the IKE gateway interface is moved from one VR to another, the
existing IKE Phase 1 and Phase 2 negotiations for the IKE gateway are cleared, and new Phase 1 and Phase 2 negotiations are performed.

NOTE:

- On SRX Series devices, when you enable VPN, overlapping of IP addresses across virtual routers is supported with the following limitations:
  - An IKE external interface address cannot overlap with any other virtual router.
  - An internal or trust interface address can overlap across virtual routers.
  - An St0 interface address cannot overlap in route-based VPN in point-to-multipoint tunnel such as NHTB.
  - An St0 interface address can overlap in route-based VPN in point-to-point tunnel.
  - The combinations of local IP addresses and remote gateway IP addresses of IP sec VPN tunnels configured across VRs have to be unique.
  - When the loopback interface is used as the IKE gateway external interface, the physical interface for IKE negotiation should be in the same VR.

Related Documentation
- IPsec VPN Feature Guide for Security Devices
- Example: Configuring a Policy-Based VPN on page 143
- Example: Configuring a Route-Based VPN on page 77
- Understanding IKE and IPsec Packet Processing on page 10
- Understanding Phase 1 of IKE Tunnel Negotiation on page 18
- Understanding Phase 2 of IKE Tunnel Negotiation on page 20
- Understanding Hub-and-Spoke VPNs on page 33

Understanding IKE and IPsec Packet Processing

Supported Platforms J Series, LN Series, SRX Series

An IPsec VPN tunnel consists of tunnel setup and applied security. During tunnel setup, the peers establish security associations (SAs), which define the parameters for securing traffic between themselves. (See “VPN Overview” on page 3.) After the tunnel is established, IPsec protects the traffic sent between the two tunnel endpoints by applying the security parameters defined by the SAs during tunnel setup. Within the Junos OS implementation, IPsec is applied in tunnel mode, which supports the Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols.
This topic includes the following sections:

- Packet Processing in Tunnel Mode on page 11
- IKE Packet Processing on page 13
- IPsec Packet Processing on page 16

Packet Processing in Tunnel Mode

IPsec operates in one of two modes—transport or tunnel. When both ends of the tunnel are hosts, you can use either mode. When at least one of the endpoints of a tunnel is a security gateway, such as a Junos OS router or firewall, you must use tunnel mode. Juniper Networks devices always operate in tunnel mode for IPsec tunnels.

In tunnel mode, the entire original IP packet—payload and header—is encapsulated within another IP payload, and a new header is appended to it, as shown in Figure 1 on page 11. The entire original packet can be encrypted, authenticated, or both. With the Authentication Header (AH) protocol, the AH and new headers are also authenticated. With the Encapsulating Security Payload (ESP) protocol, the ESP header can also be authenticated.

Figure 1: Tunnel Mode

In a site-to-site VPN, the source and destination addresses used in the new header are the IP addresses of the outgoing interface. See Figure 2 on page 12.
In a dial-up VPN, there is no tunnel gateway on the VPN dial-up client end of the tunnel; the tunnel extends directly to the client itself (see Figure 3 on page 13). In this case, on packets sent from the dial-up client, both the new header and the encapsulated original header have the same IP address: that of the client's computer.

**NOTE:** Some VPN clients, such as the dynamic VPN client and Netscreen-Remote, use a virtual inner IP address (also called a “sticky address”). Netscreen-Remote enables you to define the virtual IP address. The dynamic VPN client uses the virtual IP address assigned during the XAuth configuration exchange. In such cases, the virtual inner IP address is the source IP address in the original packet header of traffic originating from the client, and the IP address that the ISP dynamically assigns the dial-up client is the source IP address in the outer header.
IKE Packet Processing

When a cleartext packet arrives on a Juniper Networks device that requires tunneling, and no active Phase 2 SA exists for that tunnel, Junos OS begins IKE negotiations and drops the packet. The source and destination addresses in the IP packet header are those of the local and remote IKE gateways, respectively. In the IP packet payload, there is a UDP segment encapsulating an ISAKMP (IKE) packet. The format for IKE packets is the same for Phase 1 and Phase 2. See Figure 4 on page 14.

Meanwhile, the source host has sent the dropped packet again. Typically, by the time the second packet arrives, IKE negotiations are complete, and Junos OS protects the packet and all subsequent packets in the session—with IPsec before forwarding it.
Figure 4: IKE Packet for Phases 1 and 2

The Next Payload field contains a number indicating one of the following payload types:

- 0002—SA Negotiation Payload contains a definition for a Phase 1 or Phase 2 SA.
- 0004—Proposal Payload can be a Phase 1 or Phase 2 proposal.
- 0008—Transform Payload gets encapsulated in a proposal payload that gets encapsulated in an SA payload.
- 0010—Key Exchange (KE) Payload contains information necessary for performing a key exchange, such as a DH public value.
• 0020—Identification (IDx) Payload.
  - In Phase 1, IDii indicates the initiator ID, and IDir indicates the responder ID.
  - In Phase 2, IDui indicates the user initiator, and IDur indicates the user responder.
  The IDs are IKE ID types such as FQDN, U-FQDN, IP address, and ASN.1_DN.
• 0040—Certificate (CERT) Payload.
• 0080—Certificate Request (CERT_REQ) Payload.
• 0100—Hash (HASH) Payload contains the digest output of a particular hash function.
• 0200—Signature (SIG) Payload contains a digital signature.
• 0400—Nonce (Nx) Payload contains some pseudorandom information necessary for the exchange.
• 0800—Notify Payload.
• 1000—ISAKMP Delete Payload.
• 2000—Vendor ID (VID) Payload can be included anywhere in Phase 1 negotiations. Junos OS uses it to mark support for NAT-T.

Each ISAKMP payload begins with the same generic header, as shown in Figure 5 on page 15.

**Figure 5: Generic ISAKMP Payload Header**

<table>
<thead>
<tr>
<th>Next Header</th>
<th>Reserved</th>
<th>Transform Payload Length (in bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payload</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

There can be multiple ISAKMP payloads chained together, with each subsequent payload type indicated by the value in the Next Header field. A value of 0000 indicates the last ISAKMP payload. See Figure 6 on page 16 for an example.
After IKE negotiations complete and the two IKE gateways have established Phase 1 and Phase 2 security associations (SAs), all subsequent packets are forwarded using the tunnel. If the Phase 2 SA specifies the Encapsulating Security Protocol (ESP) in tunnel mode, the packet looks like the one shown in Figure 7 on page 16. The device adds two additional headers to the original packet that the initiating host sends.

NOTE: For information about ESP, see “ESP Protocol” on page 9. For information about tunnel mode, see “Packet Processing in Tunnel Mode” on page 11.

As shown in Figure 7 on page 16, the packet that the initiating host constructs includes the payload, the TCP header, and the inner IP header (IP1).

The router IP header (IP2), which Junos OS adds, contains the IP address of the remote gateway as the destination IP address and the IP address of the local router as the source IP address. Junos OS also adds an ESP header between the outer and inner IP headers.
The ESP header contains information that allows the remote peer to properly process the packet when it receives it. This is shown in Figure 8 on page 17.

Figure 8: Outer IP Header (IP2) and ESP Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version of the IP header</td>
</tr>
<tr>
<td>Header</td>
<td>Protocol number</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Type of service</td>
</tr>
<tr>
<td>Total Packet Length (in Bytes)</td>
<td>Total length of the packet excluding headers</td>
</tr>
<tr>
<td>Identification</td>
<td>Identification field of the IP header</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td>Fragment offset of the IP header</td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td>Time to live of the IP header</td>
</tr>
<tr>
<td>Protocol (SD for ESP)</td>
<td>Protocol number for ESP</td>
</tr>
<tr>
<td>Header Checksum</td>
<td>Header checksum</td>
</tr>
<tr>
<td>Source Address (Local Peer’s Gateway)</td>
<td>Source address of the local peer</td>
</tr>
<tr>
<td>Destination Address (Remote Peer’s Gateway)</td>
<td>Destination address of the remote peer</td>
</tr>
<tr>
<td>Options (if any)</td>
<td>Options</td>
</tr>
<tr>
<td>Padding</td>
<td>Padding</td>
</tr>
<tr>
<td>Payload</td>
<td>Payload</td>
</tr>
</tbody>
</table>

The Next Header field indicates the type of data in the payload field. In tunnel mode, this value is 4, indicating an IP packet is contained within the payload. See Figure 9 on page 18.
Figure 9: Inner IP Header (IP1) and TCP Header

### Inner IP Header (IP1)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Header</td>
</tr>
<tr>
<td>Type of Service</td>
<td>Total Packet Length (in Bytes)</td>
</tr>
<tr>
<td>Identification</td>
<td>O D M</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td></td>
</tr>
<tr>
<td>Time to Live (TTL)</td>
<td>Protocol (6 for TCP)</td>
</tr>
<tr>
<td>Header Checksum</td>
<td></td>
</tr>
<tr>
<td>Source Address (Installing Host)</td>
<td></td>
</tr>
<tr>
<td>Destination Address (Receiving Host)</td>
<td></td>
</tr>
<tr>
<td>IP Options (if any)</td>
<td>Padding</td>
</tr>
<tr>
<td>Payload</td>
<td></td>
</tr>
</tbody>
</table>

### TCP Header

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Port</td>
<td>Destination Port</td>
</tr>
<tr>
<td>Sequence Number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgement Number</td>
<td></td>
</tr>
<tr>
<td>Window Size</td>
<td></td>
</tr>
<tr>
<td>Header Length</td>
<td>Reserved</td>
</tr>
<tr>
<td>U R C A P S H T S Y I N</td>
<td></td>
</tr>
<tr>
<td>Checksum</td>
<td>Urgent Pointer</td>
</tr>
<tr>
<td>IP Options (if any)</td>
<td>Padding</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

**Related Documentation**
- VPN Overview on page 3
- Understanding Phase 1 of IKE Tunnel Negotiation on page 18
- Understanding Phase 2 of IKE Tunnel Negotiation on page 20
- Understanding Hub-and-Spoke VPNs on page 33
- Example: Configuring a Policy-Based VPN on page 143
- Example: Configuring a Route-Based VPN on page 77
- **IPsec VPN Feature Guide for Security Devices**

**Understanding Phase 1 of IKE Tunnel Negotiation**

**Supported Platforms**
- J Series, LN Series, SRX Series
Phase 1 of an AutoKey Internet Key Exchange (IKE) tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel. The participants exchange proposals for acceptable security services such as:

- Encryption algorithms—Data Encryption Standard (DES), triple Data Encryption Standard (3DES), and Advanced Encryption Standard (AES). (See “IPsec Security Protocols” on page 8.)
- Authentication algorithms—Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1). (See “IPsec Security Protocols” on page 8.)
- Diffie-Hellman (DH) group. (See “Diffie-Hellman Exchange” on page 7.)
- Preshared key or RSA/DSA certificates. (See “IPsec Key Management” on page 6.)

A successful Phase 1 negotiation concludes when both ends of the tunnel agree to accept at least one set of the Phase 1 security parameters proposed and then process them. Juniper Networks devices support up to four proposals for Phase 1 negotiations, allowing you to define how restrictive a range of security parameters for key negotiation you will accept.

Junos OS provides the following predefined Phase 1 proposals:

- Standard—pre-g2-aes128-sha and pre-g2-3des-sha
- Compatible—pre-g2-3des-sha, pre-g2-3des-md5, pre-g2-des-sha, and pre-g2-des-md5
- Basic—pre-g1-des-sha and pre-g1-des-md5

You can also define custom Phase 1 proposals.

Phase 1 exchanges can take place in either main mode or aggressive mode. You can choose your mode during IKE policy configuration.

This topic includes the following sections:

- Main Mode on page 19
- Aggressive Mode on page 20

## Main Mode

In main mode, the initiator and recipient send three two-way exchanges (six messages total) to accomplish the following services:

- First exchange (messages 1 and 2)—Proposes and accepts the encryption and authentication algorithms.
- Second exchange (messages 3 and 4)—Executes a DH exchange, and the initiator and recipient each provide a pseudorandom number.
- Third exchange (messages 5 and 6)—Sends and verifies the identities of the initiator and recipient.
The information transmitted in the third exchange of messages is protected by the encryption algorithm established in the first two exchanges. Thus, the participants’ identities are encrypted and therefore not transmitted “in the clear.”

**Aggressive Mode**

In aggressive mode, the initiator and recipient accomplish the same objectives as with main mode, but in only two exchanges, with a total of three messages:

- **First message**—The initiator proposes the security association (SA), initiates a DH exchange, and sends a pseudorandom number and its IKE identity.
- **Second message**—The recipient accepts the SA; authenticates the initiator; and sends a pseudorandom number, its IKE identity, and, if using certificates, the recipient’s certificate.
- **Third message**—The initiator authenticates the recipient, confirms the exchange, and, if using certificates, sends the initiator’s certificate.

Because the participants’ identities are exchanged in the clear (in the first two messages), aggressive mode does not provide identity protection.

---

**NOTE:** When a dial-up VPN user negotiates an AutoKey IKE tunnel with a preshared key, aggressive mode must be used. Therefore, you must always use aggressive mode with the dynamic VPN feature. Note also that a dial-up VPN user can use an e-mail address, a fully qualified domain name (FQDN), or an IP address as its IKE ID. A dynamic peer can use either an e-mail address or an FQDN, but not an IP address.

---

**Related Documentation**

- [VPN Overview on page 3](#)
- [Understanding Phase 2 of IKE Tunnel Negotiation on page 20](#)
- [Example: Configuring a Policy-Based VPN on page 143](#)
- [Example: Configuring a Route-Based VPN on page 77](#)
- [IPsec VPN Feature Guide for Security Devices](#)

---

**Understanding Phase 2 of IKE Tunnel Negotiation**

**Supported Platforms**

J Series, LN Series, SRX Series

After the participants have established a secure and authenticated channel, they proceed through Phase 2, in which they negotiate security associations (SAs) to secure the data to be transmitted through the IPsec tunnel.

Similar to the process for Phase 1, the participants exchange proposals to determine which security parameters to employ in the SA. A Phase 2 proposal also includes a security protocol—either Encapsulating Security Payload (ESP) or Authentication Header.
(AH)—and selected encryption and authentication algorithms. The proposal can also specify a Diffie-Hellman (DH) group, if Perfect Forward Secrecy (PFS) is desired.

Regardless of the mode used in Phase 1, Phase 2 always operates in quick mode and involves the exchange of three messages.

Juniper Networks devices support up to four proposals for Phase 2 negotiations, allowing you to define how restrictive a range of tunnel parameters you will accept. Junos OS provides the following predefined Phase 2 proposals:

- Standard—g2-esp-3des-sha and g2-esp-aes128-sha
- Basic—nopfs-esp-des-sha and nopfs-esp-des-md5

You can also define custom Phase 2 proposals.

This topic includes the following sections:

- Proxy IDs on page 21
- Perfect Forward Secrecy on page 21
- Replay Protection on page 21

Proxy IDs

In Phase 2, the peers exchange proxy IDs. A proxy ID consists of a local and remote IP address prefix. The proxy ID for both peers must match, which means that the local IP address specified for one peer must be the same as the remote IP address specified for the other peer.

Perfect Forward Secrecy

PFS is a method for deriving Phase 2 keys independent from and unrelated to the preceding keys. Alternatively, the Phase 1 proposal creates the key (the SKEYID_d key) from which all Phase 2 keys are derived. The SKEYID_d key can generate Phase 2 keys with a minimum of CPU processing. Unfortunately, if an unauthorized party gains access to the SKEYID_d key, all your encryption keys are compromised.

PFS addresses this security risk by forcing a new DH key exchange to occur for each Phase 2 tunnel. Using PFS is thus more secure, although the rekeying procedure in Phase 2 might take slightly longer with PFS enabled.

Replay Protection

A replay attack occurs when an unauthorized person intercepts a series of packets and uses them later either to flood the system, causing a denial of service (DoS), or to gain entry to the trusted network. Junos OS provides a replay protection feature that enables devices to check every IPsec packet to see if it has been received previously. If packets arrive outside a specified sequence range, Junos OS rejects them. Use of this feature does not require negotiation, because packets are always sent with sequence numbers. You simply have the option of checking or not checking the sequence numbers.
Understanding Internet Key Exchange Version 2

Supported Platforms  LN Series, SRX Series

Internet Key Exchange Version 2 (IKEv2) is the next generation standard for secure key exchange between peer devices, defined in RFC 4306. IKEv2 is available in this release for securing IPsec traffic.

The gateway configuration is used to distinguish between IKEv1 and IKEv2. A remote peer is configured as either IKEv1 or IKEv2. When a peer is configured as IKEv2, it cannot fall back to IKEv1 if the peer initiates IKEv1 negotiation. The default value for the version is "v1-only". The version "v2-only" is supported from Junos OS Release 11.3 onward.

Use the version configuration statement at the [edit security ike gateway gateway-name] hierarchy level to configure IKEv2. To view the version information in the CLI, enter the following commands:

• user@host>show security ike security-associations
• user@host>show security ipsec security-associations

The advantages of using version 2 over version 1 are as follows:

• Simplifies the existing IKEv1
  • Single RFC, including NAT-T, EAP and remote address acquisition
  • Replaces the 8 initial exchanges with a single 4 message exchange

• Reduces the latency for the IPSEC SA setup and increases connection establishment speed.

• Increases robustness against DOS attack.

• Improves reliability through the use of sequence numbers, acknowledgements, and error correction.

• Forward Compatibility

• Simple cryptographic mechanisms

• Reliability
  • All messages are request/response.
  • Initiator is responsible for retransmission if it doesn’t receive a response.

IKEv2 includes support for:
- Route-based VPN
- Site-to-site VPN
- Dead peer detection (liveness check)
- Chassis cluster
- Certificate-based authentication
- Hardware offloading of the ModExp operations in a Diffie Hellman (DH) exchange

An IKEv2 child SA is known as a Phase 2 SA in IKEv1. The child SA differs in behavior from the Phase 2 SA in the following ways:

- IKE and child SA rekeying—In IKEv2, a child security association (SA) cannot exist without the underlying IKE SA. If a child SA is required, it will be rekeyed; however, if the child SAs are currently active, the corresponding IKE SA will be rekeyed.

- Version 1 and version 2

### Related Documentation

- Example: Configuring a Route-Based VPN for IKEv2 on page 95
- *IPsec VPN Feature Guide for Security Devices*

## Understanding NAT-T

### Supported Platforms

J Series, LN Series, SRX Series

Network Address Translation-Traversal (NAT-T) is a method for getting around IP address translation issues encountered when data protected by IPsec passes through a NAT device for address translation. Any changes to the IP addressing, which is the function of NAT, causes IKE to discard packets. After detecting one or more NAT devices along the data path during Phase 1 exchanges, NAT-T adds a layer of User Datagram Protocol (UDP) encapsulation to IPsec packets so they are not discarded after address translation.

Junos OS implements NAT-T one-to-one IP addressing (static NAT) when a NAT device is located along a VPN data path, such as in route-based, policy-based, and hub-and-spoke topologies. The location of a NAT device can be such that:

- Only the initiator is behind a NAT device.
- Initiators connect through multiple NAT devices to the responder.
- Initiators are behind separate NAT devices.
- Only the responder is behind a NAT device.
- Both the initiator and the responder are behind a NAT device.

Configuration examples for NAT-T are provided for the topology in which only the responder is behind a NAT device and the topology in which both the initiator and responder are behind a NAT device. Site-to-site IKE gateway configuration for NAT-T is supported on both the initiator and responder. A remote IKE ID is used to validate a peer’s local IKE ID during Phase 1 of IKE tunnel negotiation. Both the initiator and responder require a `local-identity` and a `remote-identity` setting.
All the VPN topologies use the following hardware:

- SRX Series Services Gateways
- J Series Services Routers

**NOTE:** If SRX Series hardware is used as a responder, when you upgrade to the current Junos OS release, you must upgrade the responder first, then configure local-identity before upgrading the initiator. This approach is required in case of a Dynamic End Point (DEP) scenario, in which an ID type is used instead of an IP address. If the responder is not upgraded first, and a NAT device is added in front of an SRX Series responder, then the initiator hardware must be configured such that remote-identity is the responder’s private IP address.

**Related Documentation**
- VPN Overview on page 3
- Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device on page 3
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device on page 160
- IPsec VPN Feature Guide for Security Devices

### Understanding Distributed VPNs in SRX Series Services Gateways

**Supported Platforms**

SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

In the SRX3000 and SRX5000 lines, the IKE provides tunnel management for IPsec and authenticates end entities. The IKE performs a Diffie-Hellman (DH) key exchange to generate an IPsec tunnel between network devices. The IPsec tunnels generated by IKE are used to encrypt, decrypt, and authenticate user traffic between the network devices at the IP layer.

The VPN is created by distributing the IKE and IPsec workload among the multiple Services Processing Units (SPUs) of the platform. For site-to-site tunnels, least loaded SPC is chosen as the anchor SPC. If multiple SPCs have the same smallest load, any of them can be chosen as an anchor SPC. Here, load corresponds to the number of site-to-site gateways or manual VPN tunnels anchored on an SPC. For dynamic tunnels, the newly established dynamic tunnels will follow the round-robin algorithm.

In IPsec, the workload is distributed by the same algorithm that distributes the IKE. The Phase 2 SA for a given VPN tunnel termination points pair is exclusively owned by a particular SPU, and all IPsec packets belonging to this Phase 2 SA are forwarded to the anchoring SPU of that SA for IPsec processing.

**Related Documentation**
- IPsec VPN Feature Guide for Security Devices
Understanding VPN Support for Inserting Services Processing Cards

**Supported Platforms**

LN Series, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

The high-end SRX Series devices have a chassis-based distributed processor architecture. The flow processing power is shared and is based on the number of Services Processing Cards (SPCs). You can scale the processing power of the device by installing a new SPC. Previously, whenever you installed a new SPC on a device either in standalone mode or in chassis cluster mode, the distributed VPNs on the device were disrupted.

This feature enables you to insert an SPC on a device, in a chassis cluster, without disrupting the traffic on the existing VPN tunnels created by the IKE and IPsec workload. Now when you insert a new SPC in each chassis of the cluster, the existing tunnels are not affected and traffic continues to flow over them without any disruption.

However, existing tunnels cannot use the processing power of the new SPC and redistribute it to the new SPC. The newly inserted SPC can anchor the newly configured site-to-site tunnels and dynamic tunnels. The newly configured tunnels are not guaranteed to be anchored on the new SPC.

Site-to-site tunnels are anchored on different SPCs based on a load-balancing algorithm. For site-to-site tunnels, the least loaded SPC is chosen as the anchor SPC. If multiple SPCs have the same smallest load, then any of the SPCs can be chosen as the anchor SPC. The newly configured site-to-site tunnels are guaranteed to be anchored on the new SPC only if the load of the old SPCs are all greater than 0. The load corresponds to the number of site-to-site gateways or manual VPN tunnels anchored on an SPC.

Dynamic tunnels are anchored on different SPCs based on a round-robin algorithm. The newly configured dynamic tunnels are not guaranteed to be anchored on the new SPC.

**Related Documentation**

- VPN Overview on page 3
CHAPTER 2

Route-Based VPN

- Understanding Route-Based IPsec VPNs on page 27
- Understanding Virtual Router Limitations on page 28
- Understanding Virtual Router Support for Route-Based VPNs on page 28

Understanding Route-Based IPsec VPNs

**Supported Platforms**  
J Series, LN Series, SRX Series

With route-based VPNs, you can configure dozens of security policies to regulate traffic flowing through a single VPN tunnel between two sites, and there is just one set of IKE and IPsec SAs at work. Unlike policy-based VPNs, for route-based VPNs, a policy refers to a destination address, not a VPN tunnel. When Junos OS looks up a route to find the interface to use to send traffic to the packet’s destination address, it finds a route through a secure tunnel interface (st0.x). The tunnel interface is bound to a specific VPN tunnel, and the traffic is routed to the tunnel if the policy action is permit.

---

**NOTE:** A secure tunnel (st0) interface supports only one IPv4 address and one IPv6 address at the same time. This applies to all route-based VPNs.

---

Examples of where route-based VPNs can be used:

- There are overlapping subnets or IP addresses between the two LANs.
- A hub-and-spoke VPN topology is used in the network, and spoke-to-spoke traffic is required.
- Primary and backup VPNs are required.
- A dynamic routing protocol (for example, OSPF, RIP, or BGP) is running across the VPN.
NOTE: We recommend that you use route-based VPN when you want to configure VPN between multiple remote sites. Route-based VPN allows for routing between the spokes between multiple remote sites; it is easier to configure, monitor, and troubleshoot.

Use policy-based VPN when your topology has a third-party device and requires a separate SAs for each remote subnet.

Related Documentation
- VPN Overview on page 3
- Example: Configuring a Hub-and-Spoke VPN on page 189
- Example: Configuring a Policy-Based VPN on page 143
- IPsec VPN Feature Guide for Security Devices

Understanding Virtual Router Limitations

Supported Platforms J Series, LN Series, SRX Series

The following features are not supported in this release for virtual router (VR):
- Dynamic VPN or remote access VPN inside VR
- Public key infrastructure (PKI) inside VR
- Chassis cluster active/active with VPN inside VR

Related Documentation
- Understanding Virtual Router Support for Route-Based VPNs on page 28
- IPsec VPN Feature Guide for Security Devices

Understanding Virtual Router Support for Route-Based VPNs

Supported Platforms J Series, LN Series, SRX Series

For route-based VPNS, you configure a unit of the secure tunnel (st0) interface and bind it to the IPsec VPN tunnel. You can configure a unit of the st0 interface in different virtual router instances. The following functions are supported for nondefault virtual router instances:
- Manual key management
- Transit traffic
- Self-traffic
- VPN monitoring
- Hub-and-spoke VPNS
- Encapsulating Security Payload (ESP) protocol
• Authentication Header (AH) protocol
• Aggressive mode or main mode
• st0 anchored on the loopback (lo0) interface
• Maximum number of virtual routers (VRs) supported on an SRX Series device
• Applications such as Application Layer Gateway (ALG), Intrusion Detection and Prevention (IDP), and Unified Threat Management (UTM)
• Dead peer detection (DPD)
• Chassis cluster active/backup
• Open Shortest Path First (OSPF) over st0
• Routing Information Protocol (RIP) over st0
• Policy-based VPN inside VR

Related Documentation:
• Understanding Virtual Router Limitations on page 28
• *IPsec VPN Feature Guide for Security Devices*
Understanding Policy-Based IPsec VPNs

For policy-based IPsec VPNs, a security policy specifies as its action the VPN tunnel to be used for transit traffic that meets the policy’s match criteria. A VPN is configured independent of a policy statement. The policy statement refers to the VPN by name to specify the traffic that is allowed access to the tunnel. For policy-based VPNs, each policy creates an individual IPsec security association (SA) with the remote peer, each of which counts as an individual VPN tunnel. For example, if a policy contains a group source address and a group destination address, whenever one of the users belonging to the address set attempts to communicate with any one of the hosts specified as the destination address, a new tunnel is negotiated and established. Because each tunnel requires its own negotiation process and separate pair of SAs, the use of policy-based IPsec VPNs can be more resource-intensive than route-based VPNs.

Examples of where policy-based VPNs can be used:

- You are implementing a dial-up VPN.
- You require more granularity than a route can provide when determining which traffic is sent to a tunnel (for example, you need to specify that traffic to a certain destination goes through the tunnel only if the traffic originated from a particular source).
- The remote VPN device is a non-Juniper device that requires separate SAs for each remote subnet.

NOTE: We recommend that you use route-based VPN when you want to configure VPN between multiple remote sites. Route-based VPN allows for routing between the spokes between multiple remote sites; it is easier to configure, monitor, and troubleshoot.

Use policy-based VPN when your topology has a third-party device and requires a separate SAs for each remote subnet.
Related Documentation

- VPN Overview on page 3
- Example: Configuring a Route-Based VPN on page 77
- Example: Configuring a Hub-and-Spoke VPN on page 189
- Example: Configuring a Policy-Based VPN on page 143
- *IPsec VPN Feature Guide for Security Devices*
Hub-and-Spoke VPN

Understanding Hub-and-Spoke VPNs

Supported Platforms

J Series, LN Series, SRX Series

If you create two VPN tunnels that terminate at a device, you can set up a pair of routes so that the device directs traffic exiting one tunnel to the other tunnel. You also need to create a policy to permit the traffic to pass from one tunnel to the other. Such an arrangement is known as hub-and-spoke VPN. (See Figure 10 on page 33.)

You can also configure multiple VPNs and route traffic between any two tunnels.

NOTE: SRX Series devices support only the route-based hub-and-spoke feature.

Figure 10: Multiple Tunnels in a Hub-and-Spoke VPN Configuration

Related Documentation

- VPN Overview on page 3
- Example: Configuring a Hub-and-Spoke VPN on page 189
- IPsec VPN Feature Guide for Security Devices
CHAPTER 5

Loopback Interface for High Availability VPN

- Understanding Loopback Interface for a High Availability VPN on page 35

Understanding Loopback Interface for a High Availability VPN

**Supported Platforms**

LN Series, SRX Series

An Internet Key Exchange (IKE) gateway needs an external interface to communicate with a peer device. In a high availability (HA) setup, the node on which the external interface is active selects a Services Processing Unit (SPU) to support the VPN tunnel. IKE and IPsec packets are processed on that SPU. Therefore, the active external interface decides the anchor SPU.

In a HA setup, this external interface can be the reth interface or a standalone interface. These interfaces can go down when the physical interfaces are down. Therefore, loopback interfaces can be used to reach the peer gateway as they are alternate physical interfaces.

This feature allows the loopback interface to be configured for any redundancy group. This redundancy group configuration is only checked for VPN packets, because only VPN packets must find the anchor SPU through the active interface.

On branch SRX Series devices, the lo0 pseudointerface can be configured in any redundancy group; for example, RG0, RG1, RG2, and so on. However, on high-end SRX Series devices, the lo0 pseudointerface cannot be configured in RG0 when it is used as an IKE gateway external interface. Because a VPN is only supported in an active-passive HA environment on high-end SRX Series devices, the lo0 pseudointerface can be configured in such a setup for RG1. In an HA setup, the node on which the external interface is active selects an SPU to anchor the VPN tunnel. IKE and IPsec packets are processed on that SPU. Thus an active external interface decides the anchor SPU.

**Related Documentation**

- VPN Overview on page 3
Understanding VPN Tunnel Modes

Supported Platforms  SRX Series

In VPN tunnel mode, IPsec encapsulates the original IP datagram—including the original IP header—within a second IP datagram. The outer IP header contains the IP address of the gateway, while the inner header contains the ultimate source and destination IP addresses. The outer and inner IP headers can have a protocol field of IPv4 or IPv6. SRX Series devices support four tunnel modes for route-based site-to-site VPNs.

IPv4-in-IPv4 tunnels encapsulate IPv4 packets inside IPv4 packets, as shown in Figure 11 on page 37. The protocol fields for both the outer and inner headers are IPv4.

Figure 11: IPv4-in-IPv4 Tunnel

IPv6-in-IPv6 tunnels encapsulate IPv6 packets inside IPv6 packets, as shown in Figure 12 on page 38. The protocol fields for both the outer and inner headers are IPv6.
IPv6-in-IPv6 tunnels encapsulate IPv6 packets inside IPv4 packets, as shown in Figure 13 on page 38. The protocol field for the outer header is IPv4 and the protocol field for the inner header is IPv6.

IPv4-in-IPv6 tunnels encapsulate IPv4 packets inside IPv6 packets, as shown in Figure 14 on page 38. The protocol field for the outer header is IPv6 and the protocol field for the inner header is IPv4.

A single IPsec VPN tunnel can carry both IPv4 and IPv6 traffic. For example, an IPv4 tunnel can operate in both IPv4-in-IPv4 and IPv6-in-IPv4 tunnel modes at the same time. To allow both IPv4 and IPv6 traffic over a single IPsec VPN tunnel, the st0 interface bound to that tunnel must be configured with both family inet and family inet6.

A physical interface configured with both IPv4 and IPv6 addresses can be used as the external interface for parallel IPv4 and IPv6 tunnels to a peer in a route-based site-to-site VPN. This feature is known as dual stack tunnels and requires separate st0 interfaces for each tunnel.
NOTE: For policy-based VPNs, IPv6-in-IPv6 is the only tunnel mode supported and is only supported on branch SRX devices.

Related Documentation
- VPN Feature Support for IPv6 Addresses on page 39
- Understanding Dual Stack Tunnels over an External Interface on page 43
- Understanding IPv6 IKE and IPsec Packet Processing on page 44
- IPsec VPN Feature Guide for Security Devices

VPN Feature Support for IPv6 Addresses

Supported Platforms  SRX Series

A route-based site-to-site VPN tunnel with a point-to-point secure tunnel interface can operate in IPv4-in-IPv4, IPv6-in-IPv6, IPv6-in-IPv4, or IPv4-in-IPv6 tunnel modes. IPv6 addresses can be in the outer IP header, which represents the tunnel endpoint, or in the inner IP header, which represents the final source and destination addresses for a packet.

Table 4 on page 39 defines the support for IPv6 addresses in VPN features.

Table 4: IPv6 Address Support in VPN Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Not Supported</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE and IPsec Support:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKEv1 and IKEv2</td>
<td>X</td>
<td></td>
<td>Unless specified, all supported features are applicable for IKEv1 and IKEv2.</td>
</tr>
<tr>
<td>Route-based VPN</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy-based VPN</td>
<td>X</td>
<td>X</td>
<td>IPv6 policy-based VPNs are not supported on high-end SRX Series devices or on branch SRX Series devices in chassis cluster configurations. IPv6 policy-based VPNs are only supported with IPv6-in-IPv6 tunnels on standalone branch SRX Series devices.</td>
</tr>
<tr>
<td>Site-to-site VPN</td>
<td>X</td>
<td></td>
<td>Only one-to-one, site-to-site VPN is supported. Many-to-one, site-to-site VPN (NHTB) is not supported. NHTB configuration cannot be committed for tunnel modes other than IPv4-in-IPv4 tunnels.</td>
</tr>
<tr>
<td>Dynamic endpoint VPN</td>
<td>X</td>
<td></td>
<td>IPv6 dynamic endpoint VPNs are blocked during negotiation.</td>
</tr>
<tr>
<td>Dialup VPN</td>
<td>X</td>
<td></td>
<td>IPv6 dialup VPNs are blocked during negotiation.</td>
</tr>
<tr>
<td>Feature</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Exceptions</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-----------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoVPN</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Group VPN</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Dynamic VPN and local IP pool management</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Point-to-point tunnel interfaces</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Point-to-multipoint tunnel interfaces</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Hub-and-spoke scenario for site-to-site VPNs</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Numbered and unnumbered tunnel interfaces</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Unicast static and dynamic (RIP, OSPF, BGP) routing</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Multicast dynamic routing (PIM)</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Virtual router</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Logical system</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Automatic and manual SA and key management</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Multiple SPUs</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Chassis cluster</td>
<td>X</td>
<td>–</td>
<td>IPsec VPN with active-active mode is supported only on branch SRX Series devices for route-based IPv6 tunnels. IPsec VPN with active-active mode is not supported on high-end SRX Series devices.</td>
</tr>
<tr>
<td>Statistics, logs, per-tunnel debugging</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>SNMP MIB</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Local address selection</td>
<td>X</td>
<td>–</td>
<td>When multiple addresses in the same address family are configured on a physical external interface to a VPN peer, we recommend that you also configure local-address at the [edit security ike gateway gateway-name] hierarchy level.</td>
</tr>
<tr>
<td>Loopback address termination</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
<tr>
<td>Xauth or modecfg over IPv6</td>
<td>X</td>
<td>–</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4: IPv6 Address Support in VPN Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Not Supported</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPC insert</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISSU</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DNS name as IKE gateway address</td>
<td>X</td>
<td></td>
<td>As with IPv4 tunnels, peer gateway address changes in the DNS name are not supported with IPv6 tunnels.</td>
</tr>
<tr>
<td>Preshared key or certificate authentication</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NAT-Traversal (NAT-T) for IPv4 IKE peers</td>
<td>X</td>
<td></td>
<td>NAT-T is supported only for IPv6-in-IPv4 and IPv4-in-IPv6 tunnel modes with IKEv1. IPv6-in-IPv6 and IPv4-in-IPv6 tunnel modes are not supported. IKEv2 is not supported for NAT-T. NAT-T from IPv6 to IPv4 or from IPv4 to IPv6 is not supported.</td>
</tr>
<tr>
<td>Dead peer detection (DPD) and DPD gateway failover</td>
<td>X</td>
<td></td>
<td>DPD gateway failover is only supported for different gateway addresses within the same family. Failover from an IPv6 gateway address to an IPv4 gateway address, or vice versa, is not supported.</td>
</tr>
<tr>
<td>Encryption sets, authentication algorithms, and DH groups supported in Junos OS Release 12.1X45-D10 release for SRX Series devices.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Generic proposals and policies for IPv6 and IPv4</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General IKE ID</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ESP and AH transport modes</td>
<td>X</td>
<td></td>
<td>These modes are not supported for IPv4.</td>
</tr>
<tr>
<td>ESP and AH tunnel modes</td>
<td>X</td>
<td></td>
<td>AH tunnel mode with mutable extension headers and options is not supported.</td>
</tr>
<tr>
<td>Extended sequence number</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Single proxy ID pairs</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple traffic selector pairs</td>
<td>X</td>
<td></td>
<td>Supported with IKEv1 only.</td>
</tr>
<tr>
<td>Lifetime of IKE or IPsec SA, in seconds</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lifetime of IKE SA, in kilobytes</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN monitoring</td>
<td>X</td>
<td></td>
<td>Configuration with IPv6 tunnels cannot be committed.</td>
</tr>
</tbody>
</table>
Table 4: IPv6 Address Support in VPN Features (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Supported</th>
<th>Not Supported</th>
<th>Exceptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF bit</td>
<td>X</td>
<td></td>
<td>For IPv6-in-IPv6 tunnels, the DF bit is set only if configured at the [edit security ipsec vpn vpn-name] hierarchy level. df-bit clear is the default.</td>
</tr>
<tr>
<td>Dual stack over tunnel external interface</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 extension headers</td>
<td>X</td>
<td></td>
<td>IPv6 extension headers and IPv4 options for IKE and IPsec packets are accepted but are not processed. AH with mutable EHs and options is not supported.</td>
</tr>
<tr>
<td>Fragmentation and reassembly</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN session affinity</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multicast traffic</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tunnel IP services (Screen, NAT, ALG, IPS, AppSecure)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI Support:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PKI in virtual router</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA signature authentication (512-, 1024-, 2048-, or 4096-bit key size)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSA signature authentication (512-, 1024-, 2048-, or 4096-bit key size)</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECDSA signatures</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate chain authentication</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic or manual enrollment over IPv4</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic or manual revocation over IPv4</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic or manual enrollment over IPv6</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatic or manual revocation over IPv6</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 addresses within PKI certificate fields</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Related Documentation
- Understanding VPN Tunnel Modes on page 37
- IPsec VPN Feature Guide for Security Devices
Understanding Dual Stack Tunnels over an External Interface

**Supported Platforms**  
**SRX Series**

Dual stack tunnels—parallel IPv4 and IPv6 tunnels over a single physical interface to a peer—are supported for route-based site-to-site VPNs. A physical interface configured with both IPv4 and IPv6 addresses can be used as the external interface to IPv4 and IPv6 gateways on the same peer or on different peers at the same time. In Figure 15 on page 43, the physical interfaces reth0.0 and ge-0/0/0.1 support parallel IPv4 and IPv6 tunnels between two devices.

**Figure 15: Dual Stack Tunnels**

![Diagram of Dual Stack Tunnels]

**NOTE:** In Figure 15 on page 43, separate secure tunnel (st0) interfaces must be configured for each IPsec VPN tunnel. Parallel IPv4 and IPv6 tunnels that are bound to the same st0 interface are not supported.

A single IPsec VPN tunnel can carry both IPv4 and IPv6 traffic. For example, an IPv4 tunnel can operate in both IPv4-in-IPv4 and IPv6-in-IPv4 tunnel modes at the same time. To allow both IPv4 and IPv6 traffic over a single IPsec VPN tunnel, the st0 interface bound to that tunnel must be configured with both `family inet` and `family inet6`.

If multiple addresses in the same address family are configured on the same external interface to a VPN peer, we recommend that you configure `local-address` at the `[edit security ike gateway gateway-name]` hierarchy level.

If `local-address` is configured, the specified IPv4 or IPv6 address is used as the local gateway address. If only one IPv4 and one IPv6 address is configured on a physical external interface, `local-address` configuration is not required.

**NOTE:** `local-address` must be an IP address that is configured on an interface on the SRX Series device. We recommend that `local-address` belong to the external interface of the IKE gateway. If `local-address` does not belong to the external interface of the IKE gateway, the interface must be in the same zone as the external interface of the IKE gateway and an intra-zone security policy must be configured to permit traffic.

`local-address` and the remote IKE gateway address must be in the same address family, either IPv4 or IPv6.
If `local-address` is not configured, the local gateway address is based on the remote gateway address. If the remote gateway address is an IPv4 address, the local gateway address is the primary IPv4 address of the external physical interface. If the remote gateway address is an IPv6 address, the local gateway address is the primary IPv6 address of the external physical interface.

**Related Documentation**

- Example: Configuring Dual Stack Tunnels over an External Interface on page 232
- Understanding VPN Tunnel Modes on page 37
- VPN Feature Support for IPv6 Addresses on page 39
- *IPsec VPN Feature Guide for Security Devices*

---

**Understanding IPv6 IKE and IPsec Packet Processing**

**Supported Platforms**  
J Series, LN Series, SRX Series

This topic includes the following sections:

- IPv6 IKE Packet Processing on page 44
- IPv6 IPsec Packet Processing on page 46

**IPv6 IKE Packet Processing**

Internet Key Exchange (IKE) is part of the IPsec suite of protocols. It automatically enables two tunnel endpoints to set up security associations (SAs) and negotiate secret keys with each other. There is no need to manually configure the security parameters. IKE also provides authentication for communicating peers.

IKE packet processing in IPv6 networks involves the following elements:

- Internet Security Association and Key Management Protocol (ISAKMP) Identification Payload

  ISAKMP identification payload is used to identify and authenticate the communicating IPv6 peers. Two ID types (ID_IPV6_ADDR and ID_IPV6_ADDR_SUBNET) are enabled for IPv6. The ID type indicates the type of identification to be used. The ID_IPV6_ADDR type specifies a single 16-octet IPv6 address. This ID type represents an IPv6 address. The ID_IPV6_ADDR_SUBNET type specifies a range of IPv6 addresses represented by two 16-octet values. This ID type represents an IPv6 network mask. Table 5 on page 44 lists the ID types and their assigned values in the identification payload.

**Table 5: ISAKMP ID Types and Their Values**

<table>
<thead>
<tr>
<th>ID Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED</td>
<td>0</td>
</tr>
<tr>
<td>ID_IPV4_ADDR</td>
<td>1</td>
</tr>
<tr>
<td>ID_FQDN</td>
<td>2</td>
</tr>
</tbody>
</table>
Table 5: ISAKMP ID Types and Their Values (continued)

<table>
<thead>
<tr>
<th>ID Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_USER_FQDN</td>
<td>3</td>
</tr>
<tr>
<td>ID_IPV4_ADDR_SUBNET</td>
<td>4</td>
</tr>
<tr>
<td>ID_IPV6_ADDR</td>
<td>5</td>
</tr>
<tr>
<td>ID_IPV6_ADDR_SUBNET</td>
<td>6</td>
</tr>
<tr>
<td>ID_IPV4_ADDR_RANGE</td>
<td>7</td>
</tr>
<tr>
<td>ID_IPV6_ADDR_RANGE</td>
<td>8</td>
</tr>
<tr>
<td>ID_DER_ASN1_DN</td>
<td>9</td>
</tr>
<tr>
<td>ID_DER_ASN1_GN</td>
<td>10</td>
</tr>
<tr>
<td>ID_KEY_ID</td>
<td>11</td>
</tr>
<tr>
<td>ID_LIST</td>
<td>12</td>
</tr>
</tbody>
</table>

The ID_IPV6_ADDR_RANGE type specifies a range of IPv6 addresses represented by two 16-octet values. The first octet value represents the starting IPv6 address and the second octet value represents the ending IPv6 address in the range. All IPv6 addresses falling between the first and last IPv6 addresses are considered to be part of the list.

NOTE: Two ID types in ISAKMP identification payload (ID_IPV6_ADDR_RANGE and ID_IPV4_ADDR_RANGE) are not supported in this release.

• Proxy ID

A proxy ID is used during Phase 2 of IKE negotiation. It is generated before an IPsec tunnel is established. A proxy ID identifies the SA to be used for the VPN. Two proxy IDs are generated—local and remote. The local proxy ID refers to the local IPv4 or IPv6 address/network and subnet mask. The remote proxy ID refers to the remote IPv4 or IPv6 address/network and subnet mask.

• Security Association

An SA is an agreement between VPN participants to support secure communication. SAs are differentiated based on three parameters—security parameter index (SPI), destination IPv6 address, and security protocol (either AH or ESP). The SPI is a unique value assigned to an SA to help identify an SA among multiple SAs. In an IPv6 packet, the SA is identified from the destination address in the outer IPv6 header and the security protocol is identified from either the AH or the ESP header.
IPv6 IPsec Packet Processing

After IKE negotiations are completed and the two IKE gateways have established Phase 1 and Phase 2 SAs, IPv6 IPsec employs authentication and encryption technologies to secure the IPv6 packets.

This topic includes the following sections:

- AH Protocol in IPv6 on page 46
- ESP Protocol in IPv6 on page 46
- IPv4 Options and IPv6 Extension Headers with AH and ESP on page 47
- Integrity Check Value (ICV) Calculation in IPv6 on page 47
- Header Construction in Tunnel Modes on page 48

AH Protocol in IPv6

The AH protocol provides data integrity and data authentication for IPv6 packets. IPv6 IPsec uses extension headers (for example, hop-by-hop and routing options) that must be arranged in a particular way in the IPv6 datagram. In AH tunnel mode, the AH header immediately follows the new outer IPv6 header similar to that in IPv4 AH tunnel mode. The extension headers are placed after the original inner header. Therefore, in AH tunnel mode, the entire packet is encapsulated by adding a new outer IPv6 header, followed by an authentication header, an inner header, extension headers, and the rest of the original datagram as shown in Figure 16 on page 46.

Figure 16: IPv6 AH Tunnel Mode

<table>
<thead>
<tr>
<th>New IP Header</th>
<th>New Extension Headers or Options</th>
<th>AH Header</th>
<th>Original IP Header</th>
<th>Original Extension Headers or Options</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Unlike ESP, the AH authentication algorithm covers the outer header as well as any new extension headers and options.

NOTE: AH tunnel mode on SRX Series devices does not support IPv4 mutable options or IPv6 mutable extension headers. See Table 6 on page 47.

ESP Protocol in IPv6

ESP protocol provides both encryption and authentication for IPv6 packets. Because IPv6 IPsec uses extension headers (for example, hop-by-hop and routing options) in the IPv6 datagram, the most important difference between IPv6 ESP tunnel mode and IPv4 ESP tunnel mode is the placement of extension headers in the packet layout. In ESP tunnel mode, the ESP header immediately follows the new outer IPv6 header similar to that in IPv4 ESP tunnel mode. Therefore, in ESP tunnel mode, the entire packet is encapsulated by adding a new outer IPv6 header, followed by an ESP header, an inner
header, extension headers, and the rest of the original datagram as shown in Figure 17 on page 47.

Figure 17: IPv6 ESP Tunnel Mode

<table>
<thead>
<tr>
<th>New IP Header</th>
<th>New Extension Headers or Options</th>
<th>AH Header</th>
<th>Original IP Header</th>
<th>Original Extension Headers or Options</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

IPv4 Options and IPv6 Extension Headers with AH and ESP

IPsec packets with IPv4 options or IPv6 extension headers can be received for decapsulation on SRX Series devices. Table 6 on page 47 shows the IPv4 options or IPv6 extension headers that are supported with the ESP or AH protocol on SRX Series devices. If an unsupported IPsec packet is received, ICV calculation fails and the packet is dropped.

Table 6: Support for IPv4 Options or IPv6 Extension Headers

<table>
<thead>
<tr>
<th>Options or Extension Headers</th>
<th>Branch SRX Devices</th>
<th>High-End SRX Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESP with IPv4 options</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>ESP with IPv6 extension headers</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>AH with IPv4 immutable options</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>AH with IPv6 immutable extension headers</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>AH with IPv4 mutable options</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>AH with IPv6 mutable extension headers</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
</tbody>
</table>

Integrity Check Value (ICV) Calculation in IPv6

AH protocol verifies the integrity of the IPv6 packet by computing an ICV on the packet contents. ICV is usually built over an authentication algorithm such as MD5 or SHA-1. The IPv6 ICV calculations differ from that in IPv4 in terms of two header fields—mutable header and optional extension header.

You can calculate the AH ICV over the IPv6 header fields that are either immutable in transit or predictable in value upon arrival at the tunnel endpoints. You can also calculate the AH ICV over the AH header and the upper level protocol data (considered to be immutable in transit). You can calculate the ESP ICV over the entire IPv6 packet, excluding the new outer IPv6 header and the optional extension headers.
NOTE: Unlike IPv4, IPv6 has a method for tagging options as mutable in transit. IPv6 optional extension headers contain a flag that indicates mutability. This flag determines the appropriate processing.

IPv4 mutable options and IPv6 extension headers are not supported with the AH protocol.

Header Construction in Tunnel Modes

In tunnel mode, the source and destination addresses of the outer IPv4 or IPv6 header represent the tunnel endpoints, while the source and destination addresses of the inner IPv4 or IPv6 header represent the final source and destination addresses. Table 7 on page 48 summarizes how the outer IPv6 header relates to the inner IPv6 or IPv4 header for IPv6-in-IPv6 or IPv4-in-IPv6 tunnel modes. In outer header fields, “Constructed” means that the value of the outer header field is constructed independently of the value in the inner header field.

Table 7: IPv6 Header Construction for IPv6-in-IPv6 and IPv4-in-IPv6 Tunnel Modes

<table>
<thead>
<tr>
<th>Header Fields</th>
<th>Outer Header at Encapsulator</th>
<th>Inner Header at Decapsulator</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>6.</td>
<td>No change.</td>
</tr>
<tr>
<td>DS field</td>
<td>Copied from the inner header.</td>
<td>No change.</td>
</tr>
<tr>
<td>ECN field</td>
<td>Copied from the inner header.</td>
<td>Constructed.</td>
</tr>
<tr>
<td>flow label</td>
<td>0.</td>
<td>No change.</td>
</tr>
<tr>
<td>payload length</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>next header</td>
<td>AH, ESP, and routing header.</td>
<td>No change.</td>
</tr>
<tr>
<td>hop limit</td>
<td>64.</td>
<td>Decrement.</td>
</tr>
<tr>
<td>src address</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>dest address</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>Extension headers</td>
<td>Never copied.</td>
<td>No change.</td>
</tr>
</tbody>
</table>

Table 8 on page 49 summarizes how the outer IPv4 header relates to the inner IPv6 or IPv4 header for IPv6-in-IPv4 or IPv4-in-IPv4 tunnel modes. In outer header fields, “Constructed” means that the value of the outer header field is constructed independently of the value in the inner header field.
Table 8: IPv4 Header Construction for IPv6-in-IPv4 and IPv4-in-IPv4 Tunnel Modes

<table>
<thead>
<tr>
<th>Header Fields</th>
<th>Outer Header</th>
<th>Inner Header</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>4.</td>
<td>No change.</td>
</tr>
<tr>
<td>header length</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>DS field</td>
<td>Copied from the inner header.</td>
<td>No change.</td>
</tr>
<tr>
<td>ECN field</td>
<td>Copied from the inner header.</td>
<td>Constructed.</td>
</tr>
<tr>
<td>total length</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>ID</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>flags (DF, MF)</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>fragment offset</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>TTL</td>
<td>64.</td>
<td>Decrement.</td>
</tr>
<tr>
<td>protocol</td>
<td>AH, ESP</td>
<td>No change.</td>
</tr>
<tr>
<td>checksum</td>
<td>Constructed.</td>
<td>Constructed.</td>
</tr>
<tr>
<td>src address</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>dest address</td>
<td>Constructed.</td>
<td>No change.</td>
</tr>
<tr>
<td>options</td>
<td>Never copied.</td>
<td>No change.</td>
</tr>
</tbody>
</table>

For IPv6-in-IPv4 tunnel mode, the Don’t Fragment (DF) bit is cleared by default. If the `df-bit set` or `df-bit copy` options are configured at the `[edit security ipsec vpn vpn-name]` hierarchy level for the corresponding IPv4 VPN, the DF bit is set in the outer IPv4 header.

For IPv4-in-IPv4 tunnel mode, the DF bit in the outer IPv4 header is based on the `df-bit` option configured for the inner IPv4 header. If `df-bit` is not configured for the inner IPv4 header, the DF bit is cleared in the outer IPv4 header.

Related Documentation
- VPN Overview on page 3
- IPv6 IPsec Configuration Overview on page 231
- Example: Configuring an IPv6 IPsec Manual VPN on page 242
- Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN on page 244
- IPsec VPN Feature Guide for Security Devices
Understanding Traffic Selectors in Route-Based VPNs

A traffic selector (also known as a proxy ID in IKEv1) is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote addresses. With this feature, you can define multiple traffic selectors within a specific route-based VPN, resulting in a unique Phase 2 IPsec security association (SA) for each traffic selector configured. Only traffic that conforms to a traffic selector is permitted through the associated SA.

In Figure 18 on page 51, subnetworks 10.1.1.0/24 and 10.1.2.0/24 are behind device A while subnetworks 20.1.1.0/24 and 20.1.2.0/24 are behind device B.

Figure 18: Traffic Selector Example

For traffic to flow from a subnetwork behind device A to a subnetwork behind device B, four traffic selectors are configured on device A. For each traffic selector, different tunnels and Phase 2 SAs are allocated as shown in Table 9 on page 52.
Table 9: Example Traffic Selector Pairs

<table>
<thead>
<tr>
<th>Local Address</th>
<th>Remote Address</th>
<th>Tunnel</th>
<th>Phase 2 SA</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.0/24</td>
<td>20.1.1.0/24</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10.1.1.0/24</td>
<td>20.1.2.0/24</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>10.2.0.1/24</td>
<td>20.1.1.0/24</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>10.1.2.0/24</td>
<td>20.1.2.0/24</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

For a given traffic selector, only a single address or subnetwork can be specified for the local and remote addresses. Traffic selectors can be configured with IPv4 or IPv6 addresses. Address books cannot be used to specify local or remote addresses.

Multiple traffic selectors can be configured for the same VPN. A maximum of 200 traffic selectors can be configured for each VPN. Traffic selectors can be used with IPv4-in-IPv4, IPv4-in-IPv6, IPv6-in-IPv6, or IPv6-in-IPv4 tunnel modes. Traffic selectors are supported with IKEv1 only.

Traffic selectors configured in VPN peers must exactly match local and remote IP subnetworks. For example, the local and remote IP addresses specified for a traffic selector on device A must exactly match the remote and local IP addresses specified for a traffic selector on peer device B.

When traffic selectors are configured, static routes are automatically added during configuration processing or when traffic selectors are negotiated; this process is known as reverse route insertion (RRI). These routes might conflict with those that are populated through routing protocols. We recommend that you do not configure routing protocols on st0 interfaces that are bound to VPNs where traffic selectors are configured.

When a traffic selector is deleted, all corresponding IPsec SAs, routes, and tunnel sessions are cleared. This might affect traffic passing through these tunnels.

When a traffic selector is modified, deleted, or added, traffic selectors that follow it in the configuration are affected. The tunnels, SAs, and routes are cleared and reinstalled. Traffic selectors that precede the new or modified traffic selector in the configuration are unaffected.

For example, three traffic selectors are configured for the same VPN in the following order:

1. ts-red
2. ts-blue
3. ts-green

If you modify the local or remote IP address in ts-blue, the tunnels, SAs, and routes for ts-blue and ts-green are cleared; the tunnel, SA, and route associated with ts-red are not affected. If you delete ts-blue, the tunnel, SA, and route associated with ts-green are
cleared; the tunnel, SA, and route associated with ts-red are not affected. If ts-white is inserted after ts-blue, the tunnels, SAs, and routes associated with ts-white and ts-green are cleared; the tunnels, SAs, and routes associated with ts-red and ts-blue are not affected.

Traffic selectors cannot be configured with the following features:

- Policy-based VPNs
- Group or shared IKE IDs
- IKE version 2
- Point-to-multipoint secure tunnel (st0) interfaces
- VPNs on which VPN monitoring is configured
- Different address families configured for the local and remote IP addresses
- VPNs configured with proxy identity values used in negotiation
- Remote address value 0.0.0.0/0 (IPv4) or 0::0 (IPv6)

To configure a traffic selector, use the traffic-selector configuration statement at the edit security ipsec vpn vpn-name hierarchy level. The traffic selector is defined with the mandatory local-ip ip-address and remote-ip ip-address statements. The CLI operational command show security ipsec security-association detail displays traffic selector information for SAs. The show security ipsec security-association traffic-selector traffic-selector-name CLI command displays information for a specified traffic selector.

**Related Documentation**

- Understanding VPN Tunnel Modes on page 37
- Understanding Traffic Selectors and Overlapping IP Addresses on page 54
- Understanding Reverse Route Insertion on page 53
- IPsec VPN Feature Guide for Security Devices

## Understanding Reverse Route Insertion

**Supported Platforms**  
SRX Series

Reverse route insertion (RRI) automatically inserts a static route for the remote network and hosts protected by a remote tunnel endpoint. A route is created based on the remote IP address configured in the traffic-selector. In the case of traffic selectors, the configured remote address is inserted as a route in the routing instance associated with the st0 interface that is bound to the VPN.

**NOTE:** Routing protocols and traffic selector configuration are mutually exclusive ways of steering traffic to a tunnel. RRI routes might conflict with routes that are populated through routing protocols. Therefore, you should not configure routing protocols on an st0 interface that is bound to a VPN on which traffic selectors are configured.
RRI routes are inserted in the route table as follows:

- If the `establish-tunnels immediately` option is configured at the `[edit security ipsec vpn vpn-name]` hierarchy level, RRI routes are added after Phase 1 and Phase 2 negotiations are complete. Because a route is not added until SAs are established, a failed negotiation does not result in traffic being routed to a st0 interface that is down. An alternate or backup tunnel is used instead.

- If the `establish-tunnels immediately` option is not configured at the `[edit security ipsec vpn vpn-name]` hierarchy level, RRI routes are added at configuration commit.

- An RRI route is not added if the configured or negotiated remote address in a traffic selector is 0.0.0.0/0 or 0::0.

The route preference for the static RRI is 5. This value is necessary to avoid conflict with similar routes that might be added by a routing protocol process.

**Related Documentation**
- Understanding Traffic Selectors in Route-Based VPNs on page 51
- IPsec VPN Feature Guide for Security Devices

**Understanding Traffic Selectors and Overlapping IP Addresses**

**Supported Platforms**

SRX Series

This section discusses overlapping IP addresses in traffic selector configurations.

- Overlapping IP Addresses in Different VPNs Bound to the Same st0 Interface on page 54
- Overlapping IP Addresses in the Same VPN Bound to the Same st0 Interface on page 54
- Overlapping IP Addresses in Different VPNs Bound to Different st0 Interfaces on page 55

**Overlapping IP Addresses in Different VPNs Bound to the Same st0 Interface**

This scenario is not supported with traffic selectors. Traffic selectors cannot be configured on different VPNs that are bound to the same point-to-multipoint st0 interface, as shown in the following example:

```
[edit]
uuser@host# show security ipsec
vpn vpn-1 {
   bind-interface st0.1;
}
vpn vpn-2 {
   bind-interface st0.1;
}
```

**Overlapping IP Addresses in the Same VPN Bound to the Same st0 Interface**

When overlapping IP addresses are configured for multiple traffic selectors in the same VPN, the first configured traffic selector that matches the packet determines the tunnel used for packet encryption.
In the following example, four traffic selectors (ts-1, ts-2, ts-3, and ts-4) are configured for the VPN (vpn-1), which is bound to the point-to-point st0.1 interface:

```
[edit]
user@host# show security ipsec vpn vpn-1
vpn vpn-1 {
  bind-interface st0.1;
  traffic-selector ts-1 {
    local-ip 20.1.5.0/24;
    remote-ip 10.1.5.0/24;
  }
  traffic-selector ts-2 {
    local-ip 20.1.0.0/16;
    remote-ip 10.1.0.0/16;
  }
  traffic-selector ts-3 {
    local-ip 40.1.0.0/16;
    remote-ip 50.1.0.0/16;
  }
  traffic-selector ts-4 {
    local-ip 40.1.5.0/24;
    remote-ip 50.1.5.0/24;
  }
}
```

A packet with a source address 20.1.5.5 and a destination address 10.1.5.10 matches traffic selectors ts-1 and ts-2. However, traffic selector ts-1 is the first configured match and the tunnel associated with ts-1 is used for packet encryption.

A packet with a source address 40.1.5.5 and a destination address 50.1.5.10 matches the traffic selectors ts-3 and ts-4. However, traffic selector ts-3 is the first configured match and the tunnel associated with traffic selector ts-3 is used for packet encryption.

**Overlapping IP Addresses in Different VPNs Bound to Different st0 Interfaces**

When overlapping IP addresses are configured for multiple traffic selectors in different VPNs that are bound to different point-to-point st0 interfaces, an st0 interface is first selected by the longest prefix match for a given packet. Within the VPN that is bound to the selected st0 interface, the traffic selector is then selected based on the first configured match for the packet.

In the following example, a traffic selector is configured in each of two VPNs. The traffic selectors are configured with the same local subnetwork but different remote subnetworks.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
  bind-interface st0.1;
  traffic-selector ts-1 {
    local-ip 20.1.1.0/24;
    remote-ip 10.1.1.0/24;
  }
}
vpn vpn-2 {
```
Different remote subnetworks are configured in each traffic selector, therefore two different routes are added to the routing table. Route lookup uses the st0 interface bound to the appropriate VPN.

In the following example, a traffic selector is configured in each of two VPNs. The traffic selectors are configured with different remote subnetworks. The same local subnetwork is configured for each traffic selector, but different netmask values are specified.

[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 20.0.0.0/8;
        remote-ip 10.1.1.0/24;
    }
}
vpn vpn-2 {
    bind-interface st0.2;
    traffic-selector ts-2 {
        local-ip 21.1.0.0/16;
        remote-ip 11.1.1.0/24;
    }
}
A different remote subnetwork is configured in each traffic selector, therefore two different routes are added to the routing table. Route lookup uses the st0 interface bound to the appropriate VPN.

In the following example, traffic selectors are configured in each of two VPNs. The traffic selectors are configured with different local and remote subnetworks.

[edit]
user@host# show security ipsec
vpn vpn-1 {
    bind-interface st0.1;
    traffic-selector ts-1 {
        local-ip 20.1.1.0/24;
        remote-ip 10.1.1.0/24;
    }
}
vpn vpn-2 {
    bind-interface st0.2;
    traffic-selector ts-2 {
        local-ip 21.1.1.0/24;
        remote-ip 11.1.1.0/24;
    }
}
In this case, the traffic selectors do not overlap. The remote subnetworks configured in the traffic selectors are different, therefore two different routes are added to the routing table. Route lookup uses the st0 interface bound to the appropriate VPN.

In the following example, a traffic selector is configured in each of two VPNs. The traffic selectors are configured with the same local subnetwork. The same remote subnetwork is configured for each traffic selector, but different netmask values are specified.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
  bind-interface st0.1;
  traffic-selector ts-1 {
    local-ip 20.1.1.0/24;
    remote-ip 10.1.1.0/24;
  }
}
vpn vpn-2 {
  bind-interface st0.2;
  traffic-selector ts-2 {
    local-ip 20.1.1.0/24;
    remote-ip 10.1.0.0/16;
  }
}
```

Note that the `remote-ip` configured for ts-1 is 10.1.1.0/24 while the `remote-ip` configured for ts-2 is 10.1.0.0/16. For a packet destined to 10.1.1.1, route lookup selects the st0.1 interface as it has the longer prefix match. The packet is encrypted based on the tunnel corresponding to the st0.1 interface.

In some cases, valid packets can be dropped due to traffic selector traffic enforcement. In the following example, traffic selectors are configured in each of two VPNs. The traffic selectors are configured with different local subnetworks. The same remote subnetwork is configured for each traffic selector, but different netmask values are specified.

```
[edit]
user@host# show security ipsec
vpn vpn-1 {
  bind-interface st0.1;
  traffic-selector ts-1 {
    local-ip 20.1.1.0/24;
    remote-ip 10.1.1.0/24;
  }
}
vpn vpn-2 {
  bind-interface st0.2;
  traffic-selector ts-2 {
    local-ip 21.1.1.0/16;
    remote-ip 10.1.0.0/16;
  }
}
```

Two routes to 10.1.1.0 (10.1.1.0/24 via interface st0.1 and 10.1.0.0/16 via interface st0.2) are added to the routing table. A packet sent from source 21.1.1.1 to destination 10.1.1.1...
matches the routing table entry for 10.1.1.0/24 via interface st0.1. However, the packet does not match the traffic specified by traffic selector ts-1 and is dropped.

NOTE: If multiple traffic selectors are configured with the same remote subnetwork and netmask, equal cost routes are added to the routing table. This case is not supported with traffic selectors as the route chosen cannot be predicted.

Related Documentation
- Understanding Traffic Selectors in Route-Based VPNs on page 51
- IPsec VPN Feature Guide for Security Devices
CHAPTER 8

VPN Alarms

- Understanding VPN Alarms and Auditing on page 59

Understanding VPN Alarms and Auditing

Supported Platforms

LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX650

Configure the following command to enable security event logging during the initial set up of the device.

```
set security log cache
```

The administrators (audit, cryptographic, IDS and security) cannot modify the security event logging configuration if the above command is configured and each administrator role is configured to have a distinct, unique set of privileges apart from all other administrative roles.

Alarms are triggered by a VPN failure. A VPN alarm is generated when the system monitors any of the following audited events:

- **Authentication failures**—You can configure the device to generate a system alarm when the packet authentication failures reaches a specified number.

- **Encryption and decryption failures**—You can configure the device to generate a system alarm when encryption or decryption failures exceed a specified number.

- **IKE Phase 1 and IKE Phase 2 failures**—Internet Key Exchange (IKE) Phase 1 negotiations are used to establish IKE security associations (SAs). These SAs protect the IKE Phase 2 negotiations. You can configure the device to generate a system alarm when IKE Phase 1 or IKE Phase 2 failures exceed a specified number.

- **Self-test failures**—Self tests are tests that a device runs upon power on or reboot to verify whether security software is implemented correctly on your device.

  Self-tests ensure the correctness of cryptographic algorithms. The JUNOS-FIPS image performs self-tests automatically upon power-on, and continuously for key-pair generation. In either domestic or FIPS images, self-tests may be configured to be performed according to a defined schedule, upon demand or immediately after key generation.

  You can configure the device to generate a system alarm when a self-test failure occurs.
• **IDP flow policy attacks**—An intrusion detection and prevention (IDP) policy allows you to enforce various attack detection and prevention techniques on network traffic. You can configure the device to generate a system alarm when IDP flow policy violations occur.

• **Replay attacks**—A replay attack is a network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. You can configure the device to generate a system alarm when a replay attack occurs.

The syslog messages are included in the following cases:

- Failed symmetric key generation
- Failed asymmetric key generation
- Failed manual key distribution
- Failed automated key distribution
- Failed key destruction
- Failed key handling and storage
- Failed data encryption or decryption
- Failed signature
- Failed key agreement
- Failed cryptographic hashing
- IKE failure
- Failed authentication of the received packets
- Decryption error due to invalid padding content
- Mismatch in the length specified in the alternative subject field of the certificate received from a remote VPN peer device.

Alarms are raised based on syslog messages. Every failure is logged, but an alarm is generated only when a threshold is reached.

To view the alarm information, run the `show security alarms` command. The violation count and the alarm do not persist across system reboots. After a reboot, the violation count resets to zero, and the alarm is cleared from the alarm queue.

After appropriate actions have been taken, you can clear the alarm. The alarm remains in the queue until you clear it (or until you reboot the device). To clear the alarm, run the `clear security alarms` command.

---

**Related Documentation**

- Example: Setting an Audible Alert as Notification of a Security Alarm on page 279
- Example: Generating Security Alarms in Response to Potential Violations on page 280
- *IPsec VPN Feature Guide for Security Devices*
CHAPTER 9

VPN Peer Availability

- Understanding VPN Monitoring and DPD on page 61
- Understanding Dead Peer Detection on page 62
- Understanding Global SPI and VPN Monitoring Features on page 63

Understanding VPN Monitoring and DPD

**Supported Platforms**  
SRX Series

VPN monitoring and dead peer detection (DPD) are features available on SRX Series devices to verify the availability of VPN peer devices. This section compares the operation and configuration of these features.

**NOTE:** You cannot use VPN monitoring and DPD simultaneously on the same SRX Series device.

VPN monitoring is a Junos OS mechanism that monitors only Phase 2 security associations (SAs). VPN monitoring is enabled on a per-VPN basis with the `vpn-monitor` statement at the `[edit security ipsec vpn vpn-name]` hierarchy level. The destination IP and source interface must be specified. The `optimized` option enables the device to use traffic patterns as evidence of peer liveliness; ICMP requests are suppressed.

VPN monitoring options are configured with the `vpn-monitor-options` statement at the `[edit security ipsec]` hierarchy level. These options apply to all VPNs for which VPN monitoring is enabled. Options you can configure include the interval at which ICMP requests are sent to the peer (the default is 10 seconds) and the number of consecutive ICMP requests sent without receiving a response before the peer is considered unreachable (the default is 10 consecutive requests).

DPD is an implementation of RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*. It operates at the IKE level and monitors the peer based on both IKE and IPsec traffic activity.

DPD is configured on an individual IKE gateway with the `dead-peer-detection` statement at the `[edit security ike gateway gateway-name]` hierarchy level. You can configure DPD modes of operation. The default (optimized) mode sends DPD messages to the peer if there is no incoming IKE or IPsec traffic within a configured interval after the local device...
sends outgoing packets to the peer. Other configurable options include the interval at which DPD messages are sent to the peer (the default is 10 seconds) and the number of consecutive DPD messages sent without receiving a response before the peer is considered unavailable (the default is five consecutive requests).

**Related Documentation**
- Understanding Dead Peer Detection on page 62
- IPsec VPN Feature Guide for Security Devices

---

**Understanding Dead Peer Detection**

**Supported Platforms**

SRX Series

Dead peer detection (DPD) is a method that network devices use to verify the current existence and availability of other peer devices.

You can use DPD as an alternative to VPN monitoring. However, you cannot use both features simultaneously. VPN monitoring applies to an individual IPsec VPN, while DPD is configured only in an individual IKE gateway context.

A device performs DPD verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE messages) to a peer and waiting for DPD acknowledgements (R-U-THERE-ACK messages) from the peer. The device sends an R-U-THERE message only if it has not received any traffic from the peer during a specified DPD interval. If the device receives an R-U-THERE-ACK message from the peer during this interval, it considers the peer alive. If the device receives traffic on the tunnel from the peer, it resets its R-U-THERE message counter for that tunnel, thus starting a new interval. If the device does not receive an R-U-THERE-ACK message during the interval, it considers the peer dead. When the device changes the status of a peer device to be dead, the device removes the Phase 1 security association (SA) and all Phase 2 SAs for that peer.

The following DPD modes are supported on the SRX Series devices:

- **Optimized**—R-U-THERE messages are triggered if there is no incoming IKE or IPsec traffic within a configured interval after the device sends outgoing packets to the peer. This is the default mode.
- **Probe idle tunnel**—R-U-THERE messages are triggered if there is no incoming or outgoing IKE or IPsec traffic within a configured interval. R-U-THERE messages are sent periodically to the peer until there is traffic activity. This mode helps in early detection of a downed peer and makes the tunnel available for data traffic.
- **Always send**—R-U-THERE messages are sent at configured intervals regardless of traffic activity between the peers.

**NOTE:** We recommend that the probe idle tunnel mode be used instead of the always-send mode.

DPD timers are active as soon as the Phase 1 SA is established. The DPD behavior is the same for both IKEv1 and IKEv2 protocols.
You can configure the following DPD parameters:

- The interval parameter specifies the amount of time (expressed in seconds) the device waits for traffic from its peer before sending an R-U-THERE message. The default interval is 10 seconds, with a permissible range of 10 to 60 seconds.

- The threshold parameter specifies the maximum number of times to send the R-U-THERE message without a response from the peer before considering the peer dead. The default number of transmissions is five times, with a permissible range of 1 to 5 retries.

Note the following considerations before configuring DPD:

- When a DPD configuration is added to an existing gateway with active tunnels, R-U-THERE messages are started without clearing Phase 1 or Phase 2 SAs.

- When a DPD configuration is deleted from an existing gateway with active tunnels, R-U-THERE messages are stopped for the tunnels. IKE and IPsec SAs are not affected.

- Modifying any DPD configuration option such as the mode, interval, or threshold values updates the DPD operation without clearing Phase 1 or Phase 2 SAs.

- If the IKE gateway is configured with DPD and VPN but the option to establish tunnels immediately is not configured, DPD does not initiate Phase 1 negotiation.

- If the IKE gateway is configured with multiple peer IP addresses and DPD but Phase 1 SA fails to be established to the first peer IP address, a Phase 1 SA is attempted with the next peer IP address. DPD is active only after a Phase 1 SA is established.

- If the IKE gateway is configured with multiple peer IP addresses and DPD but DPD fails with the current peer’s IP address, the Phase 1 and Phase 2 SAs are cleared and a failover to the next peer IP address is triggered.

- More than one Phase 1 or Phase 2 SA may exist with the same peer because of simultaneous negotiations. In this case, R-U-THERE messages are sent on all Phase 1 SAs. Failure to receive DPD responses for the configured number of consecutive times clears the Phase 1 SA and the associated Phase 2 SA (for IKEv2 only).

Related Documentation
- Understanding VPN Monitoring and DPD on page 61
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device on page 160
- IPsec VPN Feature Guide for Security Devices

Understanding Global SPI and VPN Monitoring Features

Supported Platforms 
J Series, LN Series, SRX Series

You can monitor and maintain the efficient operation of your VPN using the following global VPN features:

- SPI—Peers in a security association (SA) can become unsynchronized when one of the peers fails. For example, if one of the peers reboots, it might send an incorrect
security parameter index (SPI). You can enable the device to detect such an event and resynchronize the peers by configuring the bad SPI response feature.

- VPN monitoring—You can use the global VPN monitoring feature to periodically send Internet Control Message Protocol (ICMP) requests to the peer to determine if the peer is reachable.

Related Documentation

- VPN Overview on page 3
- Example: Configuring Global SPI and VPN Monitoring Features on page 283
- IPsec VPN Feature Guide for Security Devices
CHAPTER 10

VPN Session Affinity

- Understanding VPN Session Affinity on page 65

Understanding VPN Session Affinity

**Supported Platforms**

LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

VPN session affinity occurs when a clear-text session is located in a Services Processing Unit (SPU) that is different from the SPU where the IPsec tunnel session is located. The goal of VPN session affinity is to locate the clear-text and IPsec tunnel session in the same SPU.

Without VPN session affinity, a clear-text session created by a flow might be located in one SPU and the tunnel session created by IPsec might be located in another SPU. An SPU to SPU forward or hop is needed to route clear-text packets to the IPsec tunnel.

By default, VPN session affinity is disabled on SRX Series devices. When VPN session affinity is enabled, a new clear-text session is placed on the same SPU as the IPsec tunnel session. Existing clear-text sessions are not affected.

Enabling VPN session affinity can improve VPN throughput under the following traffic conditions:

- A number of IPsec tunnels are needed and they are distributed evenly among SPUs. If IPsec tunnels are already concentrated on several SPUs, then enabling VPN session affinity allows all clear-text SPUs to also use those SPUs. This can cause those SPUs to be overutilized while other SPUs might be underutilized.

To display active tunnel sessions on SPUs, use the `show security ipsec security-association` command and specify the Flexible PIC Concentrator (FPC) and Physical Interface Card (PIC) slots that contain the SPU. For example:

```
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 23.0.21.11
>131073 ESP:aes-128/sha1 188c0750 491/128000 root 500 23.0.21.11
```

- Clear-text sessions passing through the tunnels should be at the highest volume for the longest periods of time as possible. Applying VPN session affinity to clear-text sessions of small volumes and short periods (for example, DNS sessions) will decrease
the effect of session affinity and might even have a negative impact on VPN throughput under certain conditions.

NOTE: You need to evaluate the tunnel distribution and traffic patterns in your network to determine if VPN session affinity should be enabled.

The VPN session affinity limitations are as follows:

• Multicast traffic is not supported.
• Traffic across logical systems is not supported.
• If there is a route change, established clear-text sessions remain on an SPU and traffic is rerouted if possible. Sessions created after the route change may be set up on a different SPU.
• VPN session affinity only affects self traffic that terminates on the device (also known as host-inbound traffic); self traffic that originates from the device (also known as host-outbound traffic) is not affected.
• VPN session affinity can be enabled on an SRX1400 device; however, because the device only has one SPU there is no affect on VPN throughput.

Related Documentation

• Enabling VPN Session Affinity on page 285
• SRX1400, SRX3400, and SRX3600 Services Gateways Processing Overview
• SRX5600 and SRX5800 Services Gateways Processing Overview
• IPsec VPN Feature Guide for Security Devices
CHAPTER 11

Suite B Cryptographic Suites

- Understanding Suite B Cryptographic Suites on page 67

**Understanding Suite B Cryptographic Suites**

**Supported Platforms**  
LN Series, SRX110, SRX210, SRX220, SRX5400, SRX550, SRX5600, SRX5800, SRX650

Suite B is a set of cryptographic algorithms designated by the U.S. National Security Agency to allow commercial products to protect traffic that is classified at secret or top secret levels. Suite B protocols are defined in RFC 6379, *Suite B Cryptographic Suites for IPsec*. The Suite B cryptographic suites provide Encapsulating Security Payload (ESP) integrity and confidentiality and should be used when ESP integrity protection and encryption are both required.

The following Suite B cryptographic suites are supported:

- **Suite-B-GCM-128**
  - ESP: Advanced Encryption Standard (AES) encryption with 128-bit keys and 16-octet integrity check value (ICV) in Galois Counter Mode (GCM).
  - IKE: AES encryption with 128-bit keys in cipher block chaining (CBC) mode, integrity using SHA-256 authentication, and key establishment using Diffie-Hellman (DH) group 19 and authentication using Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit elliptic curve signatures.

- **Suite-B-GCM-256**
  - ESP: AES encryption with 256-bit keys and 16-octet ICV in GCM for ESP.
  - IKE: AES encryption with 256-bit keys in CBC mode, integrity using SHA-384 authentication, and key establishment using DH group 20 and authentication using ECDSA 384-bit elliptic curve signatures.

IKEv1 and IKEv2 configuration is supported.
NOTE: Suite B is not fully supported on SRX1400, SRX3400, and SRX3600 devices, and on SRX5600 and SRX5800 devices that do not have the NG-SPC installed. You can configure IKE with Suite B options on these devices, but AES-GCM options are not supported. If you configure IKE with Suite B options on these devices, VPN establishment is slower because the devices do not have the hardware processors that can accelerate Suite B algorithm processing.

NOTE: Suite B is not supported with the group VPN feature.

CLI options support Suite B compliance in IKE and IPsec proposal configuration:

- For IKE proposals configured at the `[edit security ike proposal proposal-name]` hierarchy level:
  - `authentication-algorithm` options include `sha-256` and `sha-384`.
  - `authentication-method` options include `ecdsa-signatures-256` and `ecdsa-signatures-384`.
  - `dh-group` options include `group19` and `group20`.

- For IPsec proposals configured at the `[edit security ipsec proposal proposal-name]` hierarchy level, `encryption-algorithm` options include `aes-128-gcm`, `aes-192-gcm`, and `aes-256-gcm`.

- For IPsec policies configured at the `[edit security ipsec policy policy-name]` hierarchy level, the `perfect-forward-secrecy keys` options include `group19` and `group20`.

- For convenience, predefined proposals that provide Suite B compliance—`suiteb-gcm-128` and `suiteb-gcm-256`—are available at the `[edit security ike policy policy-name]` and `[edit security ipsec policy policy-name]` hierarchy levels.

Related Documentation

- VPN Overview on page 3
- `[edit security ike]` Hierarchy Level on page 291
- `[edit security ipsec]` Hierarchy Level on page 337
PART 2

Configuration

- IP Security on page 71
- Route-Based VPN on page 77
- Policy-Based VPN on page 143
- Hub-and-Spoke VPN on page 189
- Loopback Interface for High Availability VPN on page 223
- IPv6 IPsec on page 231
- Traffic Selectors on page 263
- VPN Alarms on page 279
- VPN Peer Availability on page 283
- VPN Session Affinity on page 285
- IKE Configuration Statements on page 289
- IPsec Configuration Statements on page 335
- VPN Alarms Configuration Statements on page 377
Chapter 12
IP Security

- IPsec VPN with Autokey IKE Configuration Overview on page 71
- IPsec VPN with Manual Keys Configuration Overview on page 72
- Recommended Configuration Options for Site-to-Site VPN with Static IP Addresses on page 73
- Recommended Configuration Options for Site-to-Site or Dialup VPNs with Dynamic IP Addresses on page 74
- Configuring Remote IKE IDs for Site-to-Site VPNs on page 75
- Configuring IPsec VPN Using the VPN Wizard on page 76

IPsec VPN with Autokey IKE Configuration Overview

**Supported Platforms**
J Series, LN Series, SRX Series

IPsec VPN negotiation occurs in two phases. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA). In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel.

This overview describes the basic steps to configure a route-based or policy-based IPsec VPN using autokey IKE (preshared keys or certificates).

To configure a route-based or policy-based IPsec VPN using autokey IKE:

   (For route-based VPNs) Configure a secure tunnel st0.x interface. Configure routing on the device.

2. Configure Phase 1 of the IPsec VPN tunnel.
   a. (Optional) Configure a custom IKE Phase 1 proposal. This step is optional, as you can use a predefined IKE Phase 1 proposal set (Standard, Compatible, or Basic).

   b. Configure an IKE policy that references either your custom IKE Phase 1 proposal or a predefined IKE Phase 1 proposal set. Specify autokey IKE preshared key or certificate information. Specify the mode (main or aggressive) for the Phase 1 exchanges.
c. Configure an IKE gateway that references the IKE policy. Specify the IKE IDs for the local and remote devices. If the IP address of the remote gateway is not known, specify how the remote gateway is to be identified.

3. Configure Phase 2 of the IPsec VPN tunnel.
   a. (Optional) Configure a custom IPsec Phase 2 proposal. This step is optional, as you can use a predefined IPsec Phase 2 proposal set (Standard, Compatible, or Basic).
   b. Configure an IPsec policy that references either your custom IPsec Phase 2 proposal or a predefined IPsec Phase 2 proposal set. Specify perfect forward secrecy (PFS) keys.
   c. Configure an IPsec VPN tunnel that references both the IKE gateway and the IPsec policy. Specify the proxy IDs to be used in Phase 2 negotiations.
      (For route-based VPNs) Bind the secure tunnel interface st0.x to the IPsec VPN tunnel.

4. Configure a security policy to permit traffic from the source zone to the destination zone.
   (For policy-based VPNs) Specify the security policy action tunnel ipsec-vpn with the name of the IPsec VPN tunnel that you configured.


Related Documentation
- Understanding Route-Based IPsec VPNs on page 27
- Understanding Policy-Based IPsec VPNs on page 31
- Configuring IPsec VPN Using the VPN Wizard on page 76
- IPsec VPN Feature Guide for Security Devices

IPsec VPN with Manual Keys Configuration Overview

Supported Platforms: J Series, LN Series, SRX Series

This overview describes the basic steps to configure a route-based or policy-based IPsec VPN using manual keys.

To configure a route-based or policy-based IPsec VPN using manual keys:

   (For route-based VPNs) Configure routing. Configure a secure tunnel st0.x interface.

2. Configure an IPsec VPN tunnel by specifying the following parameters:
   - Authentication algorithm and key
   - Encryption algorithm and key
• Outgoing interface
• IP address of the peer
• IPsec protocol for the security association
• Security parameter index

(For route-based VPNs) Bind the secure tunnel interface st0.x to the IPsec VPN tunnel.

3. Configure security policy to permit traffic from the source zone to the destination zone.

(For policy-based VPNs) Specify the security policy action `tunnel ipsec-vpn` with the name of the IPsec VPN tunnel that you configured.

**Recommended Configuration Options for Site-to-Site VPN with Static IP Addresses**

**Supported Platforms**

J Series, LN Series, SRX Series

Table 10 on page 73 lists the configuration options for a generic site-to-site VPN between two security devices with static IP addresses. The VPN can be either route-based or policy-based.

**Table 10: Recommended Configuration for Site-to-Site VPN with Static IP Addresses**

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IKE configuration:</strong></td>
<td></td>
</tr>
<tr>
<td>Autokey IKE with certificates</td>
<td>Manual key is not recommended.</td>
</tr>
<tr>
<td>Main mode</td>
<td>Used when peers have static IP addresses.</td>
</tr>
<tr>
<td>RSA or DSA certificates</td>
<td>RSA or DSA certificates can be used on the local device. Specify the type of certificate (PKCS7 or X.509) on the peer.</td>
</tr>
<tr>
<td>Diffie–Hellman (DH) group 2</td>
<td>DH group 2 provides more security than DH group 1 and incurs less processing overhead than DH groups 5 and 14.</td>
</tr>
<tr>
<td>Advanced Encryption Standard (AES) encryption</td>
<td>AES is cryptographically stronger than Data Encryption Standard (DES) and Triple DES (3DES) when key lengths are equal. Approved encryption algorithm for Federal Information Processing Standards (FIPS) and Common Criteria EAL4 standards.</td>
</tr>
<tr>
<td>Secure Hash Algorithm (SHA-1)</td>
<td>SHA-1 provides more cryptographic security than Message Digest 5 (MD5) and incurs less processing overhead than SHA-256.</td>
</tr>
</tbody>
</table>

Copyright © 2016, Juniper Networks, Inc.
Table 10: Recommended Configuration for Site-to-Site VPN with Static IP Addresses (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local and remote IKE identifiers</td>
<td>IP addresses are used by default if local and remote peers have static IP addresses. Specify the peer’s address. IP addresses can be used with a certificate if the IP address appears in the SubjectAltName field.</td>
</tr>
</tbody>
</table>

**IPsec configuration:**

<table>
<thead>
<tr>
<th>IKE configuration:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect Forward Secrecy (PFS) DH group 2</td>
</tr>
<tr>
<td>Encapsulating Security Payload (ESP) protocol</td>
</tr>
<tr>
<td>AES encryption</td>
</tr>
<tr>
<td>SHA-1 authentication</td>
</tr>
<tr>
<td>Anti-replay protection</td>
</tr>
</tbody>
</table>

Related Documentation
- [VPN Overview on page 3](#)
- [IPsec VPN Feature Guide for Security Devices](#)

Recommended Configuration Options for Site-to-Site or Dialup VPNs with Dynamic IP Addresses

**Supported Platforms** J Series, LN Series, SRX Series

Table 11 on page 74 lists the configuration options for a generic site-to-site or dialup VPN, where the peer devices have dynamic IP addresses.

Table 11: Recommended Configuration for Site-to-Site or Dialup VPNs with Dynamic IP Addresses

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE configuration:</td>
<td></td>
</tr>
<tr>
<td>Autokey IKE with certificates</td>
<td>Manual key is not recommended.</td>
</tr>
<tr>
<td>Aggressive mode</td>
<td>Required when the IP address of one or both of the IPsec peers is dynamically assigned.</td>
</tr>
<tr>
<td>1024-bit certificates</td>
<td>RSA or DSA certificates can be used. Specify the certificate to be used on the local device. Specify the type of certificate (PKCS7 or X.509) on the peer.</td>
</tr>
<tr>
<td>Diffie-Hellman (DH) group 2</td>
<td>DH group 2 provides more security than DH group 1 and incurs less processing overhead than DH groups 5 and 14.</td>
</tr>
</tbody>
</table>
Table 11: Recommended Configuration for Site-to-Site or Dialup VPNs with Dynamic IP Addresses (continued)

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Encryption Standard (AES) encryption</td>
<td>AES is cryptographically stronger than Data Encryption Standard (DES) and Triple DES (3DES) when key lengths are equal. Approved encryption algorithm for Federal Information Processing Standards (FIPS) and Common Criteria EAL4 standards.</td>
</tr>
<tr>
<td>Secure Hash Algorithm (SHA-1) authentication</td>
<td>SHA-1 provides more cryptographic security than Message Digest 5 (MD5) and incurs less processing overhead than SHA-256.</td>
</tr>
<tr>
<td>Local and remote IKE IDs</td>
<td>User-Fully Qualified Domain Name (U-FQDN) is an e-mail address that can be used with a certificate if the U-FQDN appears in the SubjectAltName field.</td>
</tr>
</tbody>
</table>

**IPsec configuration:**

<table>
<thead>
<tr>
<th>Configuration Option</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perfect Forward Secrecy (PFS) DH group 2</td>
<td>PFS DH group 2 provides increased security because the peers perform a second DH exchange to produce the key used for IPsec encryption and decryption.</td>
</tr>
<tr>
<td>Encapsulating Security Payload (ESP) protocol</td>
<td>ESP provides both confidentiality through encryption and encapsulation of the original IP packet and integrity through authentication.</td>
</tr>
<tr>
<td>AES encryption</td>
<td>AES is cryptographically stronger than DES and 3DES when key lengths are equal. Approved encryption algorithm for FIPS and Common Criteria EAL4 standards.</td>
</tr>
<tr>
<td>SHA-1 authentication</td>
<td>SHA-1 provides more cryptographic security than MD5.</td>
</tr>
<tr>
<td>Anti-replay protection</td>
<td>Enabled by default. Disabling this might resolve compatibility issues with third-party peers.</td>
</tr>
</tbody>
</table>

**Related Documentation**

- [VPN Overview on page 3](#)
- [IPsec VPN Feature Guide for Security Devices](#)

**Configuring Remote IKE IDs for Site-to-Site VPNs**

As of Junos OS Release 11.4, checks are performed to validate the IKE ID received from the VPN peer device. By default, SRX Series and J Series devices validate the IKE ID received from the peer with the IP address configured for the IKE gateway. In certain network setups, the IKE ID received from the peer (which can be an IPv4 or IPv6 address, fully qualified domain name [FQDN], distinguished name, or e-mail address) does not match the IKE gateway configured on the SRX Series or J Series device. This can lead to a Phase 1 validation failure.

To modify the configuration of the SRX Series or J Series device or the peer device for the IKE ID that is used:

- On the SRX Series or J Series device, configure the `remote-identity` statement at the `[edit security ike gateway gateway-name]` hierarchy level to match the IKE ID that is used.
received from the peer. Values can be an IPv4 or IPv6 address, FQDN, distinguished name, or e-mail address.

NOTE: If you do not configure remote-identity, the device uses the IPv4 or IPv6 address that corresponds to the remote peer by default.

- On the peer device, ensure that the IKE ID is the same as the remote-identity configured on the SRX Series or J Series device. If the peer device is an SRX Series or J Series device, configure the local-identity statement at the [edit security ike gateway gateway-name] hierarchy level. Values can be an IPv4 or IPv6 address, FQDN, distinguished name, or e-mail address.

Related Documentation
- Understanding NAT-T on page 23
- Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device on page 111
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device on page 160
- IPsec VPN Feature Guide for Security Devices

Configuring IPsec VPN Using the VPN Wizard

Supported PlatformsLN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX650

The VPN Wizard enables you to perform basic IPsec VPN configuration, including both Phase 1 and Phase 2. For more advanced configuration, use the J-Web interface or the CLI.

To configure IPsec VPN using the VPN Wizard:

1. Select Configure>Tasks>Configure VPN in the J-Web interface.
2. Click the Launch VPN Wizard button.
3. Follow the wizard prompts.

The upper left area of the wizard page shows where you are in the configuration process. The lower left area of the page shows field-sensitive help. When you click a link under the Resources heading, the document opens in your browser. If the document opens in a new tab, be sure to close only the tab (not the browser window) when you close the document.

Related Documentation
- VPN Overview on page 3
- Understanding Phase 1 of IKE Tunnel Negotiation on page 18
- Understanding Phase 2 of IKE Tunnel Negotiation on page 20
CHAPTER 13

Route-Based VPN

- Example: Configuring a Route-Based VPN on page 77
- Example: Configuring a Route-Based VPN for IKEv2 on page 95
- Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device on page 111
- Example: Configuring an st0 Interface in a Virtual Router on page 138

**Example: Configuring a Route-Based VPN**

**Supported Platforms**

J Series, LN Series, SRX Series

This example shows how to configure a route-based IPsec VPN to allow data to be securely transferred between a branch office and the corporate office.

- Requirements on page 77
- Overview on page 77
- Configuration on page 81
- Verification on page 90

**Requirements**

This example uses the following hardware:

- SRX240 device
- SSG140 device

Before you begin, read “VPN Overview” on page 3.

**Overview**

In this example, you configure a route-based VPN for a branch office in Chicago, Illinois, because you want to conserve tunnel resources but still get granular restrictions on VPN traffic. Users in the Chicago office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

Figure 19 on page 78 shows an example of a route-based VPN topology. In this topology, the SRX Series device is located in Sunnyvale, and an SSG Series device (or a third-party device) is located in Chicago.
In this example, you configure interfaces, an IPv4 default route, security zones, and address books. Then you configure IKE Phase 1, IPsec Phase 2, security policy, and TCP-MSS parameters. See Table 12 on page 79 through Table 16 on page 80 for specific configuration parameters used in this example.
### Table 12: Interface, Static Route, Security Zone, and Address Book Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/0.0</td>
<td>10.10.10.1/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3.0</td>
<td>1.1.1.2/30</td>
</tr>
<tr>
<td></td>
<td>st0.0 (tunnel interface)</td>
<td>10.11.11.10/24</td>
</tr>
<tr>
<td>Static routes</td>
<td>0.0.0.0/0 (default route)</td>
<td>The next hop is 1.1.1.1.0.0 (default route)</td>
</tr>
<tr>
<td></td>
<td>192.168.168.0/24</td>
<td>The next hop is st0.0.0.0</td>
</tr>
<tr>
<td>Security zones</td>
<td>trust</td>
<td>• All system services are allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/0.0 interface is bound to this zone.</td>
</tr>
<tr>
<td></td>
<td>untrust</td>
<td>• IKE is the only allowed system service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/3.0 interface is bound to this zone.</td>
</tr>
<tr>
<td></td>
<td>vpn-chicago</td>
<td>The st0.0 interface is bound to this zone.</td>
</tr>
<tr>
<td>Address book entries</td>
<td>sunnyvale</td>
<td>• This address is an entry in the address book book1, which is attached to a zone called trust.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The address for this address book entry is 10.10.10.0/24.</td>
</tr>
<tr>
<td></td>
<td>chicago</td>
<td>• This address is an entry in the address book book2, which is attached to a zone called vpn-chicago.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The address for this address book entry is 192.168.168.0/24.</td>
</tr>
</tbody>
</table>

### Table 13: IKE Phase 1 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ike-phase1-proposal</td>
<td>• Authentication method: pre-shared-keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Diffie-Hellman group: group2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: sha1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: aes-128-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ike-phase1-policy</td>
<td>• Mode: main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proposal reference: ike-phase1-proposal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IKE Phase 1 policy authentication method: pre-shared-key ascii-text</td>
</tr>
<tr>
<td>Gateway</td>
<td>gw-chicago</td>
<td>• IKE policy reference: ike-phase1-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External interface: ge-0/0/3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gateway address: 2.2.2.2</td>
</tr>
</tbody>
</table>
Table 14: IPsec Phase 2 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal| ipsec-phase2-proposal | • Protocol: esp  
• Authentication algorithm: hmac-sha1-96  
• Encryption algorithm: aes-128-cbc |
| Policy  | ipsec-phase2-policy | • Proposal reference: ipsec-phase2-proposal  
• PFS: Diffie-Hellman group2 |
| VPN     | ike-vpn-chicago  | • IKE gateway reference: gw-chicago  
• IPsec policy reference: ipsec-phase2-policy  
• Bind to interface: st0.0 |

Table 15: Security Policy Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| The security policy permits traffic from the trust zone to the vpn-chicago zone. | vpn-tr-chi | • Match criteria:  
  • source-address sunnyvale  
  • destination-address chicago  
  • application any  
  • Action: permit |
| The security policy permits traffic from the vpn-chicago zone to the trust zone. | vpn-chi-tr | • Match criteria:  
  • source-address chicago  
  • destination-address sunnyvale  
  • application any  
  • Action: permit |

Table 16: TCP-MSS Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-MSS is negotiated as part of the TCP three-way handshake and limits the maximum size of a TCP segment to better fit the MTU limits on a network. For VPN traffic, the IPsec encapsulation overhead, along with the IP and frame overhead, can cause the resulting ESP packet to exceed the MTU of the physical interface, which causes fragmentation. Fragmentation increases bandwidth and device resources. <strong>NOTE:</strong> We recommend a value of 1350 as the starting point for most Ethernet-based networks with an MTU of 1500 or greater. You might need to experiment with different TCP-MSS values to obtain optimal performance. For example, you might need to change the value if any device in the path has a lower MTU, or if there is any additional overhead such as PPP or Frame Relay.</td>
<td>MSS value: 1350</td>
</tr>
</tbody>
</table>
Configuration

- Configuring Interface, Static Route, Security Zone, and Address Book Information on page 81
- Configuring IKE on page 84
- Configuring IPsec on page 86
- Configuring Security Policies on page 87
- Configuring TCP-MSS on page 89
- Configuring the SSG Series Device on page 89

Configuring Interface, Static Route, Security Zone, and Address Book Information

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
set interfaces st0 unit 0 family inet address 10.11.11.24
set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
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 vpn-chicago interfaces st0.0
set security address-book book1 address sunnyvale 10.10.10.0/24
set security address-book book1 attach zone trust
set security address-book book2 address chicago 192.168.168.0/24
set security address-book book2 attach zone vpn-chicago
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure interface, static route, security zone, and address book information:

1. Configure Ethernet interface information.
   
   [edit]
   
   ```
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
   user@host# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
   user@host# set interfaces st0 unit 0 family inet address 10.11.11.24
   ```

2. Configure static route information.
   
   [edit]
   
   ```
   user@host# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
   user@host# set routing-options static route 192.168.168.0/24 next-hop st0.0
   ```

3. Configure the untrust security zone.
   
   [edit]
user@host# edit security zones security-zone untrust

4. Assign an interface to the security zone.
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/3.0

5. Specify allowed system services for the security zone.
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services ike

6. Configure the trust security zone.
   [edit]
   user@host# edit security zones security-zone trust

7. Assign an interface to the trust security zone.
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/0.0

8. Specify allowed system services for the trust security zone.
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-services all

9. Configure an address book and attach a zone to it.
   [edit security address-book book1]
   user@host# set address sunnyvale 10.10.10.0/24
   user@host# set attach zone trust

10. Configure the vpn-chicago security zone.
    [edit]
    user@host# edit security zones security-zone vpn-chicago

11. Assign an interface to the security zone.
    [edit security zones security-zone vpn-chicago]
    user@host# set interfaces st0.0

12. Configure another address book and attach a zone to it.
    [edit security address-book book2]
    user@host# set address chicago 192.168.168.0/24
    user@host# set attach zone vpn-chicago

Results  From configuration mode, confirm your configuration by entering the show interfaces,
          show routing-options, show security zones, and show security address-book commands.
          If the output does not display the intended configuration, repeat the configuration
          instructions in this example to correct it.

          [edit]
          user@host# show interfaces
          ge-0/0/0 [ 
          unit 0 { 
          family inet { 
          address 10.10.10.1/24; 
          } 
          ]


```
} ge-0/0/3 {
    unit 0 {
        family inet {
            address 1.1.1.2/30
        }
    }
}
}
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 1.1.1.1;
    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 {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn-chicago {
    interfaces {
        st0.0;
    }
}
[edit]
user@host# show security address-book
book1 {
    address sunnyvale 10.10.10.0/24;
    attach {
        zone trust;
    }
}
```
If you are done configuring the device, enter **commit** from configuration mode.

### Configuring IKE

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```shell
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 395psksecr3t
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 2.2.2.2
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   ```shell
   [edit security ike]
   user@host# set proposal ike-phase1-proposal
   ```

2. Define the IKE proposal authentication method.
   ```shell
   [edit security ike proposal ike-phase1-proposal]
   user@host# set authentication-method pre-shared-keys
   ```

3. Define the IKE proposal Diffie-Hellman group.
   ```shell
   [edit security ike proposal ike-phase1-proposal]
   user@host# set dh-group group2
   ```

4. Define the IKE proposal authentication algorithm.
   ```shell
   [edit security ike proposal ike-phase1-proposal]
   user@host# set authentication-algorithm sha1
   ```

5. Define the IKE proposal encryption algorithm.
   ```shell
   [edit security ike proposal ike-phase1-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```
6. Create an IKE Phase 1 policy.
   
   [edit security ike]
   user@host# set policy ike-phase1-policy

7. Set the IKE Phase 1 policy mode.
   
   [edit security ike policy ike-phase1-policy]
   user@host# set mode main

8. Specify a reference to the IKE proposal.
   
   [edit security ike policy ike-phase1-policy]
   user@host# set proposals ike-phase1-proposal

9. Define the IKE Phase 1 policy authentication method.
   
   [edit security ike policy ike-phase1-policy]
   user@host# set pre-shared-key ascii-text 395psksecr3t

10. Create an IKE Phase 1 gateway and define its external interface.
    
    [edit security ike]
    user@host# set gateway gw-chicago external-interface ge-0/0/3.0

11. Define the IKE Phase 1 policy reference.
    
    [edit security ike gateway gw-chicago]
    user@host# set ike-policy ike-phase1-policy

12. Define the IKE Phase 1 gateway address.
    
    [edit security ike gateway gw-chicago]
    user@host# set address 2.2.2.2

**Results**

From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [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 {
      mode main;
      proposals ike-phase1-proposal;
      pre-shared-key ascii-text "$9$9VMTp1RvWLdwYKMJDkmF3yIKM87Vb2oZjws5F"; ## SECRET-DATA
    }
    gateway gw-chicago {
      ike-policy ike-phase1-policy;
      address 2.2.2.2;
      external-interface ge-0/0/3.0;
    }

If you are done configuring the device, enter `commit` from configuration mode.
Configuring IPsec

**CLI Quick Configuration**
To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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 ike-vpn-chicago ike gateway gw-chicago
set security ipsec vpn ike-vpn-chicago ike ipsec-policy ipsec-phase2-policy
set security ipsec vpn ike-vpn-chicago bind-interface st0.0
```

**Step-by-Step Procedure**
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   ```
   [edit]
   user@host# set security ipsec proposal ipsec-phase2-proposal
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```

5. Create the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set policy ipsec-phase2-policy
   ```

6. Specify the IPsec Phase 2 proposal reference.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set proposals ipsec-phase2-proposal
   ```

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set perfect-forward-secrecy keys group2
   ```

8. Specify the IKE gateway.
   
   ```
   [edit security ipsec]
   ```
user@host# set vpn ike-vpn-chicago ike gateway gw-chicago

9. Specify the IPsec Phase 2 policy.
   [edit security ipsec]
   user@host# set vpn ike-vpn-chicago ike ipsec-policy ipsec-phase2-policy

10. Specify the interface to bind.
    [edit security ipsec]
    user@host# set vpn ike-vpn-chicago bind-interface st0.0

Results  From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [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 ike-vpn-chicago {
    bind-interface st0.0;
    ike {
    gateway gw-chicago;
    ipsec-policy ipsec-phase2-policy;
    }
    }

    If you are done configuring the device, enter `commit` from configuration mode.

Configuring Security Policies

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

    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
destinyation-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

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the vpn-chicago zone.

   [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. Create the security policy to permit traffic from the vpn-chicago zone to the trust zone.

   [edit security policies from-zone vpn-chicago to-zone trust]
   user@host# set policy vpn-chi-tr match source-address chicago
   user@host# set policy vpn-chi-tr match destination-address sunnyvale
   user@host# set policy vpn-chi-tr match application any
   user@host# set policy vpn-chi-tr then permit

Results

From configuration mode, confirm your configuration by entering the show security policies command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show security policies
from-zone trust to-zone vpn-chicago {
   policy vpn-tr-vpn {
      match {
         source-address sunnyvale;
         destination-address chicago;
         application any;
      }
      then {
         permit;
      }
   }
}
from-zone vpn-chicago to-zone trust {
   policy vpn-tr-vpn {
      match {
         source-address chicago;
         destination-address sunnyvale;
         application any;
      }
   }
}
If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring TCP-MSS

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

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

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure TCP-MSS information:

1. Configure TCP-MSS information.
   ```
   [edit]
   user@host# set security flow tcp-mss ipsec-vpn mss 1350
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show security flow` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring the SSG Series Device

**CLI Quick Configuration**

For reference, the configuration for the SSG Series device is provided. For information about configuring SSG Series devices, see the *Concepts and Examples ScreenOS Reference Guide*, which is located at [http://www.juniper.net/techpubs](http://www.juniper.net/techpubs).

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI.

```
set zone name vpn-chicago
set interface ethernet0/6 zone Trust
```
Verification

To confirm that the configuration is working properly, perform these tasks:

- **Verifying the IKE Phase 1 Status** on page 90
- **Verifying the IPsec Phase 2 Status** on page 92
- **Reviewing Statistics and Errors for an IPsec Security Association** on page 93
- **Testing Traffic Flow Across the VPN** on page 94

### Verifying the IKE Phase 1 Status

**Purpose**
Verify the IKE Phase 1 status.

**Action**

**NOTE:** Before starting the verification process, you need to send traffic from a host in the 10.10.10/24 network to a host in the 192.168.168/24 network. For route-based VPNs, traffic can be initiated by the SRX Series device through the tunnel. We recommend that when testing IPsec tunnels, test traffic be sent from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate a ping from 10.10.10.10 to 192.168.168.10.

From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
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
```
user@host> show security ike security-associations index 1 detail
IKE peer 2.2.2.2, Index 1,
  Role: Responder, State: UP
  Initiator cookie: 744a594d957dd513, Responder cookie: 1e1307db82f58387
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 1.1.1.2:500, Remote: 2.2.2.2:500
  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
  Phase 2 negotiations in progress: 0

Meaning
The show security ike security-associations command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- Index—This value is unique for each IKE SA, which you can use in the show security ike security-associations index detail command to get more information about the SA.
- Remote Address—Verify that the remote IP address is correct.
- State
  - UP—The Phase 1 SA has been established.
  - DOWN—There was a problem establishing the Phase 1 SA.
- Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The show security ike security-associations index 1 detail command lists additional information about the security association with an index number of 1:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Role information
NOTE: Troubleshooting is best performed on the peer using the responder role.

- Initiator and responder information
- Number of IPsec SAs created
- Number of Phase 2 negotiations in progress

### Verifying the IPsec Phase 2 Status

**Purpose**

Verify the IPsec Phase 2 status.

**Action**

From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
user@host> show security ipsec security-associations
total configured sa: 2
   ID   Gateway      Port  Algorithm       SPI      Life:sec/kb  Mon vsys
<16384 2.2.2.2    500   ESP:aes-128/sha1  76d64d1d 3363/ unlim   -   0
>16384 2.2.2.2    500   ESP:aes-128/sha1  a1024ee2 3363/ unlim   -   0

user@host> show security ipsec security-associations index 16384 detail
Virtual-system: Root
Local Gateway: 1.1.1.2, Remote Gateway: 2.2.2.2
Local Identity: ipv4_subnet(any:0,[0..7]=10.10.10.0/24)
Remote Identity: ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
DF-bit: clear
Direction: inbound, SPI: 1993755933, AUX-SPI: 0
Hard lifetime: Expires in 3352 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2775 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -

Anti-replay service: enabled, Replay window size: 32
```

Direction: outbound, SPI: 2701283042, AUX-SPI: 0
Hard lifetime: Expires in 3352 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2775 seconds
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -

Anti-replay service: enabled, Replay window size: 32

**Meaning**

The output from the `show security ipsec security-associations` command lists the following information:
- The ID number is 16384. Use this value with the `show security ipsec security-associations index` command to get more information about this particular SA.

- There is one IPsec SA pair using port 500, which indicates that no NAT-traversal is implemented. (NAT-traversal uses port 4500 or another random high-number port.)

- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3363/ unlim value indicates that the Phase 2 lifetime expires in 3363 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.

- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U indicates that monitoring is up, and D indicates that monitoring is down.

- The virtual system (vsys) is the root system, and it always lists 0.

The output from the `show security ipsec security-associations index 16384 detail` command lists the following information:

- The local identity and remote identity make up the proxy ID for the SA.

  A proxy ID mismatch is one of the most common causes for a Phase 2 failure. If no IPsec SA is listed, confirm that Phase 2 proposals, including the proxy ID settings, are correct for both peers. For route-based VPNs, the default proxy ID is local=0.0.0.0/0, remote=0.0.0.0/0, and service=any. Issues can occur with multiple route-based VPNs from the same peer IP. In this case, a unique proxy ID for each IPsec SA must be specified. For some third-party vendors, the proxy ID must be manually entered to match.

- Another common reason for Phase 2 failure is not specifying the ST interface binding. If IPsec cannot complete, check the kmd log or set traceoptions.

---

**Reviewing Statistics and Errors for an IPsec Security Association**

**Purpose**
Review ESP and authentication header counters and errors for an IPsec security association.

**Action**
From operational mode, enter the `show security ipsec statistics index index_number` command, using the index number of the VPN for which you want to see statistics.

```
user@host> show security ipsec statistics index 16384
ESP Statistics:
Encrypted bytes:                920
Decrypted bytes:                6208
Encrypted packets:               5
Decrypted packets:               87
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

You can also use the `show security ipsec statistics` command to review statistics and errors for all SAs.

To clear all IPsec statistics, use the `clear security ipsec statistics` command.

**Meaning** If you see packet loss issues across a VPN, you can run the `show security ipsec statistics` or `show security ipsec statistics detail` command several times to confirm that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

## Testing Traffic Flow Across the VPN

### Purpose
Verify the traffic flow across the VPN.

### Action
You can use the `ping` command from the SRX Series device to test traffic flow to a remote host PC. Make sure that you specify the source interface so that the route lookup is correct and the appropriate security zones are referenced during policy lookup.

From operational mode, enter the `ping` command.

```
ssg-> 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
```

You can also use the `ping` command from the SSG Series device.

```
user@host> ping 10.10.10.10 from ethernet0/6
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 1 seconds from ethernet0/6
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=4/4/5 ms
```

### Meaning
If the `ping` command fails from the SRX Series or SSG Series device, there might be a problem with the routing, security policies, end host, or encryption and decryption of ESP packets.

### Related Documentation
- [VPN Overview on page 3](#)
- [Example: Configuring a Hub-and-Spoke VPN on page 189](#)
- [Example: Configuring a Policy-Based VPN on page 143](#)
- [IPsec VPN Feature Guide for Security Devices](#)
Example: Configuring a Route-Based VPN for IKEv2

Supported Platforms  LN Series, SRX Series

This example shows how to configure a route-based IPsec VPN to allow data to be securely transferred between a branch office and a corporate office.

- Requirements on page 95
- Overview on page 95
- Configuration on page 97
- Verification on page 107

Requirements

This example uses the following hardware:

- SRX240 device
- SSG140 device

Before you begin, read “VPN Overview” on page 3.

Overview

In this example, you configure a route-based VPN for a branch office in Chicago, Illinois, because you want to conserve tunnel resources but still get granular restrictions on VPN traffic. Users in the Chicago office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

In this example, you configure interfaces, an IPv4 default route, security zones, and address books. Then you configure IKE Phase 1, IPsec Phase 2, a security policy, and TCP-MSS parameters. See Table 17 on page 95 through Table 21 on page 97 for specific configuration parameters used in this example.

Table 17: Interface, Static Route, Security Zone, and Address Book Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/0.0</td>
<td>10.10.10.1/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3.0</td>
<td>1.1.1.2/30</td>
</tr>
<tr>
<td></td>
<td>st0.0 (tunnel interface)</td>
<td>10.11.11.10/24</td>
</tr>
<tr>
<td>Static routes</td>
<td>0.0.0.0/0 (default route)</td>
<td>The next hop is 1.1.1.1.</td>
</tr>
<tr>
<td></td>
<td>192.168.168.0/24</td>
<td>The next hop is st0.0.</td>
</tr>
<tr>
<td>Security zones</td>
<td>trust</td>
<td>• All system services are allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/0.0 interface is bound to this zone.</td>
</tr>
</tbody>
</table>
### Table 17: Interface, Static Route, Security Zone, and Address Book Information (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>untrust</td>
<td>• IKE is the only allowed system service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/3.0 interface is bound to this zone.</td>
</tr>
<tr>
<td></td>
<td>vpn-chicago</td>
<td>The st0.0 interface is bound to this zone.</td>
</tr>
<tr>
<td>Address book entries</td>
<td>sunnyvale</td>
<td>• This address is for the trust zone's address book.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The address for this address book entry is 10.10.10.0/24.</td>
</tr>
<tr>
<td></td>
<td>chicago</td>
<td>• This address is for the untrust zone's address book.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The address for this address book entry is 192.168.168.0/24.</td>
</tr>
</tbody>
</table>

### Table 18: IKE Phase 1 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ike-phase1-proposal</td>
<td>• Authentication method: pre-shared-keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Diffie-Hellman group: group2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: sha1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: aes-128-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ike-phase1-policy</td>
<td>• Mode: main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proposal reference: ike-phase1-proposal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IKE Phase 1 policy authentication method: pre-shared-key ascii-text</td>
</tr>
<tr>
<td>Gateway</td>
<td>gw-chicago</td>
<td>• IKE policy reference: ike-phase1-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External interface: ge-0/0/3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gateway address: 2.2.2.2</td>
</tr>
</tbody>
</table>

### Table 19: IPsec Phase 2 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ipsec-phase2-proposal</td>
<td>• Protocol: esp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: hmac-sha1-96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: aes-128-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ipsec-phase2-policy</td>
<td>• Proposal reference: ipsec-phase2-proposal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PFS: Diffie-Hellman group2</td>
</tr>
<tr>
<td>VPN</td>
<td>ipsec-vpn-chicago</td>
<td>• IKE gateway reference: gw-chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPsec policy reference: ipsec-phase2-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Bind to interface: st0.0</td>
</tr>
</tbody>
</table>
Table 20: Security Policy Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| The security policy permits traffic from the trust zone to the vpn-chicago zone. | vpn-tr-chi | • Match criteria:  
  • source-address sunnyvale  
  • destination-address chicago  
  • application any  
  • Action: permit |
| The security policy permits traffic from the vpn-chicago zone to the trust zone. | vpn-chi-tr | • Match criteria:  
  • source-address chicago  
  • destination-address sunnyvale  
  • application any  
  • Action: permit |

Table 21: TCP-MSS Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP-MSS is negotiated as part of the TCP three-way handshake and limits the maximum size of a TCP segment to better fit the MTU limits on a network. For VPN traffic, the IPsec encapsulation overhead, along with the IP and frame overhead, can cause the resulting ESP packet to exceed the MTU of the physical interface, which causes fragmentation. Fragmentation increases bandwidth and device resources.</td>
<td>MSS value: 1350</td>
</tr>
</tbody>
</table>

**NOTE:** We recommend a value of 1350 as the starting point for most Ethernet-based networks with an MTU of 1500 or greater. You might need to experiment with different TCP-MSS values to obtain optimal performance. For example, you might need to change the value if any device in the path has a lower MTU, or if there is any additional overhead such as PPP or Frame Relay.

**Configuration**

- Configuring Interface, Static Route, Security Zone, and Address Book Information on page 98
- Configuring IKE on page 100
- Configuring IPsec on page 102
- Configuring Security Policies on page 104
- Configuring TCP-MSS on page 105
- Configuring the SSG Series Device on page 106
### Configuring Interface, Static Route, Security Zone, and Address Book Information

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
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
```

### Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure interface, static route, security zone, and address book information:

1. **Configure Ethernet interface information.**
   
   [edit]
   ```
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
   user@host# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
   user@host# set interfaces st0 unit 0 family inet address 10.11.11.10/24
   ```

2. **Configure static route information.**
   
   [edit]
   ```
   user@host# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
   user@host# set routing-options static route 192.168.168.0/24 next-hop st0.0
   ```

3. **Configure the untrust security zone.**
   
   [edit]
   ```
   user@host# edit security zones security-zone untrust
   ```

4. **Assign an interface to the security zone.**
   
   [edit security zones security-zone untrust]
   ```
   user@host# set interfaces ge-0/0/3.0
   ```

5. **Specify allowed system services for the security zone.**
   
   [edit security zones security-zone untrust]
   ```
   user@host# set host-inbound-traffic system-services ike
   ```

6. **Configure the trust security zone.**
   
   [edit]
   ```
   user@host# edit security zones security-zone trust
   ```
7. Assign an interface to the trust security zone.
   
   ```
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/0.0
   ```

8. Specify allowed system services for the trust security zone.

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

9. Configure the address book entry for the trust security zone.

   ```
   [edit security zones security-zone trust]
   user@host# set address-book address sunnyvale 10.10.10.0/24
   ```

10. Configure the vpn-chicago security zone.

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

11. Assign an interface to the security zone.

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

12. Configure the address book entry for the vpn-chicago zone.

    ```
    [edit security zones security-zone vpn-chicago]
    user@host# set address-book address chicago 192.168.168.0/24
    ```

Results From configuration mode, confirm your configuration by entering the `show interfaces`, `show routing-options`, and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    ```
    [edit]
    user@host# show interfaces
    ge-0/0/0 { 
    unit 0 { 
    family inet { 
    address 10.10.10.1/24; 
    } 
    } 
    } 
    ge-0/0/3 { 
    unit 0 { 
    family inet { 
    address 1.1.1.2/30
    } 
    } 
    } 
    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 1.1.1.1;
    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 10.10.10.0/24;
    }
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone vpn-chicago {
    host-inbound-traffic {
        address-book {
            address chicago 192.168.168.0/24;
        }
    }
    interfaces {
        st0.0;
    }
}

If you are done configuring the device, enter commit from configuration mode.

Configuring IKE

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

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 395psksecr3t
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 2.2.2.2
set security ike gateway gw-chicago version v2-only

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   
   [edit security ike]
   
   user@host# set proposal ike-phase1-proposal

2. Define the IKE proposal authentication method.
   
   [edit security ike proposal ike-phase1-proposal]
   
   user@host# set authentication-method pre-shared-keys

3. Define the IKE proposal Diffie-Hellman group.
   
   [edit security ike proposal ike-phase1-proposal]
   
   user@host# set dh-group group2

4. Define the IKE proposal authentication algorithm.
   
   [edit security ike proposal ike-phase1-proposal]
   
   user@host# set authentication-algorithm sha1

5. Define the IKE proposal encryption algorithm.
   
   [edit security ike proposal ike-phase1-proposal]
   
   user@host# set encryption-algorithm aes-128-cbc

6. Create an IKE Phase 1 policy.
   
   [edit security ike]
   
   user@host# set policy ike-phase1-policy

7. Specify a reference to the IKE proposal.
   
   [edit security ike policy ike-phase1-policy]
   
   user@host# set proposals ike-phase1-proposal

8. Define the IKE Phase 1 policy authentication method.
   
   [edit security ike policy ike-phase1-policy]
   
   user@host# set pre-shared-key ascii-text 395psksecr3t

9. Create an IKE Phase 1 gateway and define its external interface.
   
   [edit security ike]
   
   user@host# set gateway gw-chicago external-interface ge-0/0/3.0

10. Define the IKE Phase 1 policy reference.

    [edit security ike gateway gw-chicago]
    
    user@host# set ike-policy ike-phase1-policy
11. Define the IKE Phase 1 gateway address.
   
   [edit security ike gateway gw-chicago]
   user@host# set address 2.2.2.2

12. Define the IKE Phase 1 gateway version.
   
   [edit security ike gateway gw-chicago]
   user@host# set version v2-only

Results

From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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 "$9$9VMTp1RvWLdwYKMJDkmF3yIkm87Vb2oZjws$F"; ## SECRET-DATA
}
gateway gw-chicago {
    ike-policy ike-phase1-policy;
    address 2.2.2.2;
    external-interface ge-0/0/3.0;
    version v2-only;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring IPsec

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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
```
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   ```
   [edit]
   user@host# set security ipsec proposal ipsec-phase2-proposal
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```

5. Create the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set policy ipsec-phase2-policy
   ```

6. Specify the IPsec Phase 2 proposal reference.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set proposals ipsec-phase2-proposal
   ```

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set perfect-forward-secrecy keys group2
   ```

8. Specify the IKE gateway.
   
   ```
   [edit security ipsec]
   user@host# set vpn ipsec-vpn-chicago ike gateway gw-chicago
   ```

9. Specify the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set vpn ipsec-vpn-chicago ike ipsec-policy ipsec-phase2-policy
   ```

10. Specify the interface to bind.
    
    ```
    [edit security ipsec]
    user@host# set vpn ipsec-vpn-chicago bind-interface st0.0
    ```

Results

From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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;
  }
}

If you are done configuring the device, enter commit from configuration mode.

Configuring Security Policies

CLI Quick Configuration
To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

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

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the vpn-chicago zone.

   [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
2. Create the security policy to permit traffic from the vpn-chicago zone to the trust zone.

   [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

Results  From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   [edit]
   user@host# show security policies
   from-zone trust to-zone vpn-chicago {
     policy vpn-tr-vpn {
       match {
         source-address sunnyvale;
         destination-address chicago;
         application any;
       }
       then {
         permit;
       }
     }
   }
   }
   from-zone vpn-chicago to-zone trust {
     policy vpn-tr-vpn {
       match {
         source-address chicago;
         destination-address sunnyvale;
         application any;
       }
       then {
         permit;
       }
     }
   }

If you are done configuring the device, enter `commit` from configuration mode.

### Configuring TCP-MSS

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

```
set security flow tcp-mss ipsec-vpn mss 1350
```
Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure TCP-MSS information:

1. Configure TCP-MSS information.

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

Results
From configuration mode, confirm your configuration by entering the show security flow command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

If you are done configuring the device, enter commit from configuration mode.

Configuring the SSG Series Device

CLI Quick Configuration
For reference, the configuration for the SSG Series device is provided. For information about configuring SSG Series devices, see the Concepts & Examples ScreenOS Reference Guide, which is located at http://www.juniper.net/techpubs.

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI.

```
set zonename 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 2.2.2.2/30
set interface ethernet0/0 route
set interface tunnel.1 ip 10.11.11.12/24
set flow tcp-mss 1350
set address Trust “192.168.168-net” 192.168.168.0 255.255.255.0
set address vpn-chicago “10.10.10-net” 10.10.10.0 255.255.255.0
set ike gateway corp-ike address 1.1.1.2 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” “10.10.10-net” “ANY” permit
```
Verification

To confirm that the configuration is working properly:

- Verifying the IKE Phase 1 Status on page 107
- Verifying the IPsec Phase 2 Status on page 108
- Reviewing Statistics and Errors for an IPsec Security Association on page 110
- Testing Traffic Flow Across the VPN on page 110

Verifying the IKE Phase 1 Status

Purpose

Verify the IKE Phase 1 status.

Action

NOTE: Before starting the verification process, you need to send traffic from a host in the 10.10.10/24 network to a host in the 192.168.168/24 network. For route-based VPNs, traffic can be initiated by the SRX Series device through the tunnel. We recommend that when testing IPsec tunnels, test traffic be sent from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate a ping from 10.10.10.10 to 192.168.168.10.

From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
1       2.2.2.2         UP     744a594d957dd513  1e1307db82f58387  IKEv2

user@host> show security ike security-associations index 1 detail
IKE peer 2.2.2.2, Index 1,  
Role: Responder, State: UP  
Initiator cookie: 744a594d957dd513, Responder cookie: 1e1307db82f58387  
Exchange type: IKEv2, Authentication method: Pre-shared-keys  
Local: 1.1.1.2:500, Remote: 2.2.2.2:500  
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
```
Meaning  The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- Index—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index detail` command to get more information about the SA.
- Remote Address—Verify that the remote IP address is correct.
- State
  - UP—The Phase 1 SA has been established.
  - DOWN—There was a problem establishing the Phase 1 SA.
- Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets).
- IKE policy parameters.
- Preshared key information.
- Phase 1 proposal parameters (must match on both peers).

The `show security ike security-associations index 1 detail` command lists additional information about the SA with an index number of 1:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Role information

NOTE: Troubleshooting is best performed on the peer using the responder role.

- Initiator and responder information
- Number of IPsec SAs created

Verifying the IPsec Phase 2 Status

Purpose  Verify the IPsec Phase 2 status.
Action

From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
user@host> show security ipsec security-associations
total configured sa: 2
  ID    Gateway     Port  Algorithm       SPI      Life:sec/kb  Mon vsys
<16384 2.2.2.2    500   ESP:aes-128/sha1   76d64d1d 3363/ unlim   -   0
>16384 2.2.2.2    500   ESP:aes-128/sha1   a1024ee2 3363/ unlim   -   0
```

```
user@host> show security ipsec security-associations index16384 detail
  Virtual-system: Root
  Local Gateway: 1.1.1.2, Remote Gateway: 2.2.2.2
  Local Identity: ipv4_subnet(any:0,[0..7]=10.10.10.0/24)
  Remote Identity: ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
  Version: IKEv2

  DF-bit: clear
  Direction: inbound, SPI: 1993755933, AUX-SPI: 0
  Hard lifetime: Expires in 3352 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2775 seconds
  Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -

  Anti-replay service: enabled, Replay window size: 32

  Direction: outbound, SPI: 2701283042, AUX-SPI: 0
  Hard lifetime: Expires in 3352 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2775 seconds
  Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -

  Anti-replay service: enabled, Replay window size: 32
```

Meaning

The output from the `show security ipsec security-associations` command lists the following information:

- The ID number is 16384. Use this value with the `show security ipsec security-associations index` command to get more information about this particular SA.
- There is one IPsec SA pair using port 500.
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3363/ unlim value indicates that the Phase 2 lifetime expires in 3363 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, because Phase 2 is not dependent on Phase 1 after the VPN is up.
- The vsys is the root system, and it is always listed as 0.
- The IKEv2 allows connections from a version 2 peer and will initiate a version 2 negotiation.

The output from the `show security ipsec security-associations index16384 detail` command lists the following information:
• The local identity and remote identity make up the proxy ID for the SA.

A proxy ID mismatch is one of the most common causes for a Phase 2 failure. If no IPsec SA is listed, confirm that Phase 2 proposals, including the proxy ID settings, are correct for both peers. For route-based VPNs, the default proxy ID is local=0.0.0.0/0, remote=0.0.0.0/0, and service=any. Issues can occur with multiple route-based VPNs from the same peer IP. In this case, a unique proxy ID for each IPsec SA must be specified. For some third-party vendors, the proxy ID must be manually entered to match.

• Another common reason for Phase 2 failure is not specifying the ST interface binding. If IPsec cannot complete, check the kmd log or set traceoptions.

Reviewing Statistics and Errors for an IPsec Security Association

Purpose
Review ESP and authentication header counters and errors for an IPsec SA.

Action
From operational mode, enter the `show security ipsec statistics index index_number` command, using the index number of the VPN for which you want to see statistics.

```
user@host> show security ipsec statistics index 16384
```

ESP Statistics:
- Encrypted bytes: 920
- Decrypted bytes: 6208
- Encrypted packets: 5
- Decrypted packets: 87

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

You can also use the `show security ipsec statistics` command to review statistics and errors for all SAs.

To clear all IPsec statistics, use the `clear security ipsec statistics` command.

Meaning
If you see packet loss issues across a VPN, you can run the `show security ipsec statistics` or `show security ipsec statistics detail` command several times to confirm that the encrypted and decrypted packet counters are incrementing. You should also check that the other error counters are incrementing.

Testing Traffic Flow Across the VPN

Purpose
Verify the traffic flow across the VPN.

Action
You can use the `ping` command from the SRX Series device to test traffic flow to a remote host PC. Make sure that you specify the source interface so that the route lookup is correct and the appropriate security zones are referenced during policy lookup.
From operational mode, enter the ping command.

```
ssg-> 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
```

You can also use the ping command from the SSG Series device.

```
user@host> ping 10.10.10.10 from ethernet0/6
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 1 seconds from ethernet0/6
!!!!!
Success Rate is 100 percent (5/5), round-trip time min/avg/max=4/4/5 ms
```

**Meaning**
If the ping command fails from the SRX Series or SSG Series device, there might be a problem with the routing, security policies, end host, or encryption and decryption of ESP packets.

**Related Documentation**
- VPN Overview on page 3
- Example: Configuring a Hub-and-Spoke VPN on page 189
- Example: Configuring a Policy-Based VPN on page 143
- Understanding Internet Key Exchange Version 2 on page 22
- IPSec VPN Feature Guide for Security Devices

**Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device**

**Supported Platforms**
J Series, LN Series, SRX Series

This example shows how to configure a route-based VPN with a responder behind a NAT device to allow data to be securely transferred between a branch office and the corporate office.

- Requirements on page 111
- Overview on page 112
- Configuration on page 116
- Verification on page 132

**Requirements**
Before you begin, read “VPN Overview” on page 3.
Overview

In this example, you configure a route-based VPN for a branch office in Chicago, Illinois, because you want to conserve tunnel resources but still get granular restrictions on VPN traffic. Users in the Chicago office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

Figure 20 on page 113 shows an example of a topology for route-based VPN with only the responder behind a NAT device.
Figure 20: Route-Based VPN Topology with Only the Responder Behind a NAT Device
In this example, you configure interfaces, routing options, security zones, and security policies for both an initiator in Chicago and a responder in Sunnyvale. Then you configure IKE Phase 1 and IPsec Phase 2 parameters.

Packets sent from the initiator with a destination address 1.1.1.1/32 are translated to the destination address 71.1.1.1/32 on the NAT device.

See Table 22 on page 114 through Table 24 on page 115 for specific configuration parameters used for the initiator in the examples.

Table 22: Interface, Routing Options, Zones, and Security Policies for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/1</td>
<td>1.0.0.1/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3</td>
<td>33.1.1.24</td>
</tr>
<tr>
<td></td>
<td>st0.1 (tunnel interface)</td>
<td>31.1.2.24</td>
</tr>
<tr>
<td>Static routes</td>
<td>32.1.1.0/24</td>
<td>The next hop is st0.1</td>
</tr>
<tr>
<td></td>
<td>1.1.1.32</td>
<td>The next hop is 1.0.0.2</td>
</tr>
</tbody>
</table>
| Security zones| untrust       | • Only IKE system service is allowed.  
|               |               | • The ge-0/0/1.0 and the st0.1 interfaces are bound to this zone.  
|               | trust         | • All system services are allowed.  
|               |               | • All protocols are allowed.  
|               |               | • The ge-0/0/3.0 interface is bound to this zone.  |
| Security policies | to-sunnyvale | Permit traffic from 33.1.1.1/24 in the trust zone to 32.1.1.1/24 in the untrust zone.  |
|               | from-sunnyvale | Permit traffic from 32.1.1.1/24 in the untrust zone to 33.1.1.1/24 in the trust zone.  |

Table 23: IKE Phase 1 Configuration Parameters for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal | ike_prop | • Authentication method: pre-shared-keys  
|          |       | • Diffie-Hellman group: group2  
|          |       | • Authentication algorithm: sha1  
|          |       | • Encryption algorithm: 3des-cbc  |
| Policy   | ike_pol | • Mode: main  
|          |        | • Proposal reference: ike_prop  
|          |        | • IKE Phase 1 policy authentication method: pre-shared-key ascii-text  |
### Table 23: IKE Phase 1 Configuration Parameters for the Initiator (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Gateway   | gw1    | • IKE policy reference: ike_pol  
|           |        | • External interface: ge-0/0/1.0  
|           |        | • Gateway address: 1.1.1.1  
|           |        | • Local peer (initiator): branch_natt1@juniper.net  
|           |        | • Remote peer (responder): responder_natt1@juniper.net |

### Table 24: IPsec Phase 2 Configuration Parameters for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal  | ipsec_prop | • Protocol: esp  
|           |        | • Authentication algorithm: hmac-sha1-96  
|           |        | • Encryption algorithm: 3des-cbc |
| Policy    | ipsec_pol | • Proposal reference: ipsec_prop  
|           |        | • Perfect forward secrecy (PFS) keys: group2  
| VPN       | vpn1   | • IKE gateway reference: gw1  
|           |        | • IPsec policy reference: ipsec_pol  
|           |        | • Bind to interface: st0.1  
|           |        | • Establish tunnels immediately |

See Table 25 on page 115 through Table 27 on page 116 for specific configuration parameters used for the responder in the examples.

### Table 25: Interface, Routing Options, Zones, and Security Policies for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/2</td>
<td>71.1.1.24/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3</td>
<td>32.1.1.24/24</td>
</tr>
<tr>
<td></td>
<td>st0.1 (tunnel interface)</td>
<td>31.1.1.1/24</td>
</tr>
<tr>
<td>Static routes</td>
<td>0.0.0.0/0 (default route)</td>
<td>The next hop is 71.1.2.0</td>
</tr>
<tr>
<td></td>
<td>33.11.0/24</td>
<td>The next hop is st0.1.0</td>
</tr>
</tbody>
</table>
| Security zones  | untrust         | • Only IKE system service is allowed.  
|                 |                 | • The ge-0/0/2.0 and the st0.1 interfaces are bound to this zone.  
|                 | trust           | • All system services are allowed.  
|                 |                 | • All protocols are allowed.  
|                 |                 | • The ge-0/0/3.0 interface is bound to this zone. |
Table 25: Interface, Routing Options, Zones, and Security Policies for the Responder (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security policies</td>
<td>to-chicago</td>
<td>Permit traffic from 32.1.1.1/24 in the trust zone to 33.1.1.1/24 in the untrust zone.</td>
</tr>
<tr>
<td></td>
<td>from-chicago</td>
<td>Permit traffic from 33.1.1.1/24 in the untrust zone to 32.1.1.1/24 in the trust zone.</td>
</tr>
</tbody>
</table>

Table 26: IKE Phase 1 Configuration Parameters for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal| ike_prop| • Authentication method: pre-shared-keys  
• Diffie-Hellman group: group2  
• Authentication algorithm: sha1  
• Encryption algorithm: 3des-cbc |
| Policy  | ike_pol| • Mode: main  
• Proposal reference: ike_prop  
• IKE Phase 1 policy authentication method: pre-shared-key ascii-text |
| Gateway | gw1| • IKE policy reference: ike_pol  
• External interface: ge-0/0/2.0  
• Gateway address: 1.0.0.1  
• Local peer (responder): responder_natt1@juniper.net  
• Remote peer (initiator): branch_natt1@juniper.net |

Table 27: IPsec Phase 2 Configuration Parameters for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal| ipsec_prop| • Protocol: esp  
• Authentication algorithm: hmac-sha1-96  
• Encryption algorithm: 3des-cbc |
| Policy  | ipsec_pol| • Proposal reference: ipsec_prop  
• PFS keys: group2 |
| VPN     | vpn1| • IKE gateway reference: gw1  
• IPsec policy reference: ipsec_pol  
• Bind to interface: st0.1  
• Establish tunnels immediately |

Configuration

- Configuring Interface, Routing Options, Security Zones, and Security Policies for the Initiator on page 117
- Configuring IKE for the Initiator on page 120
To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
set interfaces ge-0/0/1 unit 0 family inet address 1.0.0.1/24
set interfaces ge-0/0/3 unit 0 family inet address 33.1.1.1/24
set interfaces st0 unit 1 family inet address 31.1.1.2/24
set routing-options static route 32.1.1.0/24 next-hop st0.1
set routing-options static route 1.1.1.1/32 next-hop 1.0.0.2
set security zones security-zone untrust host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces st0.1
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 address-book book1 address Chicago-lan 33.1.1.1/24
set security address-book book1 attach zone trust
set security address-book book2 address Sunnyvale-lan 32.1.1.1/24
set security address-book book2 attach zone untrust
set security policies from-zone trust to-zone untrust policy to-sunnyvale match source-address Chicago-lan
set security policies from-zone trust to-zone untrust policy to-sunnyvale match destination-address Sunnyvale-lan
set security policies from-zone trust to-zone untrust policy to-sunnyvale match any
set security policies from-zone trust to-zone untrust policy to-sunnyvale then permit
set security policies from-zone untrust to-zone trust policy from-sunnyvale match source-address Sunnyvale-lan
set security policies from-zone untrust to-zone trust policy from-sunnyvale match destination-address Chicago-lan
set security policies from-zone untrust to-zone trust policy from-sunnyvale match application any
set security policies from-zone untrust to-zone trust policy from-sunnyvale then permit
```

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure interface, static route, security zone, and security policy information:

1. Configure Ethernet interface information.

```plaintext
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet address 1.0.0.1/24
```
user@host# set interfaces ge-0/0/3 unit 0 family inet address 33.1.1.1/24
user@host# set interfaces st0 unit 1 family inet address 31.1.1.2/24

2. Configure static route information.
   [edit]
   user@host# set routing-options static route 32.1.1.0/24 next-hop st0.1
   user@host# set routing-options static route 1.1.1.1/32 next-hop 1.0.0.2

3. Configure the untrust security zone.
   [edit]
   user@host# set security zones security-zone untrust

4. Assign interfaces to the untrust security zone.
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/1.0
   user@host# set interfaces st0.1

5. Specify allowed system services for the untrust security zone.
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services ike

6. Configure the trust security zone.
   [edit]
   user@host# set security zones security-zone trust host-inbound-traffic protocols all

7. Assign an interface to the trust security zone.
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/3.0

8. Specify allowed system services for the trust security zone.
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-services all

9. Configure address books.
    [edit security address-book]
    user@host# set book1 address Chicago-lan 33.1.1.1/24
    user@host# set book1 attach zone trust
    user@host# set book2 address Sunnyvale-lan 32.1.1.1/24
    user@host# set book2 attach zone untrust

10. Create security policies.
    [edit security security-policies from-zone trust to-zone untrust]
        user@host# set policy to-sunnyvale match source-address Chicago-lan
        user@host# set policy to-sunnyvale match destination-address Sunnyvale-lan
        user@host# set policy to-sunnyvale match application any
        user@host# set policy to-sunnyvale then permit

    [edit security security-policies from-zone untrust to-zone trust]
        user@host# set policy from-sunnyvale match source-address Sunnyvale-lan
        user@host# set policy from-sunnyvale match destination-address Chicago-lan
        user@host# set policy from-sunnyvale match application any
        user@host# set policy from-sunnyvale then permit
Results From configuration mode, confirm your configuration by entering the **show interfaces**, **show routing-options**, **show security zones**, **show security address-book**, and **show security policies** commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show interfaces
ge-0/0/1 {
  unit 0 {
    family inet {
      address 1.0.0.1/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 33.1.1.1/24;
    }
  }
}
st0 {
  unit 1 {
    family inet {
      address 31.1.1.2/24
    }
  }
}
[edit]
user@host# show routing-options
static {
  route 32.1.1.0/24 next-hop st0.1;
  route 1.1.1.32 next-hop 1.0.0.2;
}
[edit]
user@host# show security zones
security-zone untrust {
  host-inbound-traffic {
    system-services {
      ike;
    }
  }
  interfaces {
    st0.1;
    ge-0/0/1.0;
  }
}
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
```
interfaces {  
ge-0/0/3.0;
}
[edit]
[edit]
user@host# show security address-book
book1 {  
  address Chicago-lan 33.1.1.1/24;
  attach {  
    zone trust;
  }
}
book2 {  
  address Sunnyvale-lan 32.1.1.1/24;
  attach {  
    zone untrust;
  }
}
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
  policy to-sunnyvale {
    match {
      source-address Chicago-lan;
      destination-address Sunnyvale-lan;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone untrust to-zone trust {
  policy from-sunnyvale {
    match {
      source-address Sunnyvale-lan;
      destination-address Chicago-lan;
      application any;
    }
    then {
      permit;
    }
  }
}

If you are done configuring the device, enter commit from configuration mode.

**Configuring IKE for the Initiator**

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.
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 "juniper"  
set security ike gateway gw1 ike-policy ike_pol  
set security ike gateway gw1 address 1.1.1.1  
set security ike gateway gw1 local-identity user-at-hostname branch_natt1@juniper.net  
set security ike gateway gw1 remote-identity user-at-hostname responder_natt1@juniper.net  
set security ike gateway gw1 external-interface ge-0/0/1.0

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   
   [edit security ike]
   user@host# set proposal ike_prop

2. Define the IKE proposal authentication method.
   
   [edit security ike proposal ike_prop]
   user@host# set authentication-method pre-shared-keys

3. Define the IKE proposal Diffie-Hellman group.
   
   [edit security ike proposal ike_prop]
   user@host# set dh-group group2

4. Define the IKE proposal authentication algorithm.
   
   [edit security ike proposal ike_prop]
   user@host# set authentication-algorithm sha1

5. Define the IKE proposal encryption algorithm.
   
   [edit security ike proposal ike_prop]
   user@host# set encryption-algorithm 3des-cbc

6. Create an IKE Phase 1 policy.
   
   [edit security ike]
   user@host# set policy ike_pol

7. Set the IKE Phase 1 policy mode.
   
   [edit security ike policy ike_pol]
   user@host# set mode main

8. Specify a reference to the IKE proposal.
   
   [edit security ike policy ike_pol]
   user@host# set proposals ike_prop

9. Define the IKE Phase 1 policy authentication method.
10. Create an IKE Phase 1 gateway and define its external interface.

```
[edit security ike gateway gw1]
user@host# set external-interface ge-0/0/1.0
```

11. Define the IKE Phase 1 policy reference.

```
[edit security ike gateway gw1]
user@host# set ike-policy ike_pol
```

12. Define the IKE Phase 1 gateway address.

```
[edit security ike gateway gw1]
user@host# set address 1.1.1.1
```

13. Set local-identity of the local peer.

```
[edit security ike gateway gw1]
user@host# set local-identity user-at-hostname branch_natt1@juniper.net
```

14. Set remote-identity of the responder. This is the IKE identifier.

```
[edit security ike gateway gw1]
user@host# set remote-identity user-at-hostname responder_natt1@juniper.net
```

15. Define the external interface.

```
[edit security ike gateway gw1]
user@host# set external-interface ge-0/0/1.0
```

Results From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# 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 “juniper”;
}
gateway gw1 {
    ike-policy ike_pol;
    address 1.1.1.1;
    local-identity user-at-hostname branch_natt1@juniper.net;
    remote-identity user-at-hostname responder_natt1@juniper.net;
    external-interface ge-0/0/1.0;
}
```

If you are done configuring the device, enter `commit` from configuration mode.
Configuring IPsec for the Initiator

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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 st0.1
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
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   ```
   [edit]
   user@host# set security ipsec proposal ipsec_prop
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set encryption-algorithm 3des-cbc
   ```

5. Create the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set policy ipsec_pol
   ```

6. Specify IPsec Phase 2 to use perfect forward secrecy (PFS).
   
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set perfect-forward-secrecy keys group2
   ```

7. Specify the IPsec Phase 2 proposal reference.
   
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set proposals ipsec_prop
   ```

8. Specify the IKE gateway.
9. Specify the IPsec Phase 2 policy.

   [edit security ipsec]
   user@host# set vpn vpn1 ike gateway gw1

   [edit security ipsec]
   user@host# set vpn vpn1 ike ipsec-policy ipsec_pol

10. Specify the interface to bind.

    [edit security ipsec]
    user@host# set vpn vpn1 bind-interface st0.1

11. Specify that the tunnel be brought up immediately without waiting for a verification packet to be sent.

    [edit security ipsec]
    user@host# set vpn vpn1 establish-tunnels immediately

Results  From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

    [edit]
    user@host# 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 st0.1;
      ike {
        gateway gw1;
        ipsec-policy ipsec_pol;
      }
      establish-tunnels immediately;
      proposals ipsec_prop;
    }

If you are done configuring the device, enter `commit` from configuration mode.

Configuring Interfaces, Routing Options, Security Zones, and Security Policies for the Responder

CLI Quick Configuration  To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your
Step-by-Step Procedure  
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure interface, static route, security zones, policies and gateways:

1. Configure Ethernet interface information.
   ```
   [edit]
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 71.1.1.1/24
   user@host# set interfaces ge-0/0/3 unit 0 family inet address 32.1.1.1/24
   user@host# set interfaces st0 unit 1 family inet address 31.1.1.1/24
   ```

2. Configure static route information.
   ```
   [edit]
   user@host# set routing-options static route 0.0.0.0/0 next-hop 71.1.1.2
   user@host# set routing-options static route 33.1.1.0/24 next-hop st0.1
   ```

3. Configure the untrust security zone.
   ```
   [edit]
   user@host# set security zones security-zone untrust
   ```

4. Assign interfaces to the untrust security zone.
   [edit security zones security-zone untrust]
   user@host# set security zones security-zone untrust interfaces ge-0/0/2.0
   user@host# set security zones security-zone untrust interfaces st0.1

5. Specify allowed system services for the untrust security zone.
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services like

6. Configure the trust security zone.
   [edit]
   user@host# set security zones security-zone trust host-inbound-traffic protocols all

7. Assign an interface to the trust security zone.
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/3.0

8. Specify allowed system services for the trust security zone.
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-services all

9. Configure address books.
   [edit security address-book]
   user@host# set book1 address Sunnyvale-lan 32.1.1.1/24
   user@host# set book1 attach zone trust
   user@host# set book2 address Chicago-lan 33.1.1.1/24
   user@host# set book2 attach zone untrust

10. Create security policies.
    [edit security security-policies from-zone trust to-zone untrust]
    user@host# set policy to-chicago match source-address Sunnyvale-lan
    user@host# set policy to-chicago match destination-address Chicago-lan
    user@host# set policy to-chicago match application any
    user@host# set policy to-chicago then permit

    [edit security security-policies from-zone untrust to-zone trust]
    user@host# set policy from-chicago match source-address Chicago-lan
    user@host# set policy from-chicago match destination-address Sunnyvale-lan
    user@host# set policy from-chicago match application any
    user@host# set policy from-chicago then permit

**Results**
From configuration mode, confirm your configuration by entering the show interfaces, show routing-options, show security zones, show security address-book, and show security policies commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[edit]
user@host# show interfaces
ge-0/0/2 {
   unit 0 {
      family inet {
address 71.1.1.1/24;
}
}
} ge-0/0/3 {
unit 0 {
  family inet {
    address 32.1.1.1/24;
  }
}
} st0 {
  unit 1 {
    family inet {
      address 31.1.1.1/24
    }
  }
}
[edit]
user@host# show routing-options
static {
  route 0.0.0.0/0 next-hop 71.1.1.2;
  route 33.1.1.0/24 next-hop st0.1;
}
[edit]
user@host# show security zones
security-zone untrust {
  host-inbound-traffic {
    system-services {
      ike;
    }
  }
  interfaces {
    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 address-book
book1 {
  address Sunnyvale-lan 32.1.1.1/24;
  attach {
zone trust;
}
}
book2 {
    address Chicago-lan 33.1.1.1/24;
    attach {
        zone untrust;
    }
}
}
[edit]
user@host# show security policies
from-zone trust to-zone untrust {
    policy to-chicago {
        match {
            source-address Sunnyvale-lan;
            destination-address Chicago-lan;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone untrust to-zone trust {
    policy from-chicago {
        match {
            source-address Chicago-lan;
            destination-address Sunnyvale-lan;
            application any;
        }
        then {
            permit;
        }
    }
}

If you are done configuring the device, enter commit from configuration mode.

**Configuring IKE for the Responder**

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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 juniper
set security ike gateway gw1 ike-policy ike_pol
set security ike gateway gw1 address 1.0.0.1
set security ike gateway gw1 local-identity user-at-hostname responder_natt1@juniper.net
```
set security ike gateway gw1 remote-identity user-at-hostname branch_natt1@juniper.net
set security ike gateway gw1 external-interface ge-0/0/2.0

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   ```
   [edit security ike]
   user@host# set proposal ike_prop
   ```
2. Define the IKE proposal authentication method.
   ```
   [edit security ike proposal ike_prop]
   user@host# set authentication-method pre-shared-keys
   ```
3. Define the IKE proposal Diffie–Hellman group.
   ```
   [edit security ike proposal ike_prop]
   user@host# set dh-group group2
   ```
4. Define the IKE proposal authentication algorithm.
   ```
   [edit security ike proposal ike_prop]
   user@host# set authentication-algorithm sha1
   ```
5. Define the IKE proposal encryption algorithm.
   ```
   [edit security ike proposal ike_prop]
   user@host# set encryption-algorithm 3des-cbc
   ```
6. Create an IKE Phase 1 policy.
   ```
   [edit security ike]
   user@host# set policy ike_pol
   ```
7. Set the IKE Phase 1 policy mode.
   ```
   [edit security ike policy ike_pol]
   user@host# set mode main
   ```
8. Specify a reference to the IKE proposal.
   ```
   [edit security ike policy ike_pol]
   user@host# set proposals ike_prop
   ```
9. Define the IKE Phase 1 policy authentication method.
    ```
    [edit security ike policy ike_pol]
    user@host# set pre-shared-key ascii-text "juniper"
   ```
10. Create an IKE Phase 1 gateway and define its external interface.
    ```
    [edit security ike gateway gw1]
    user@host# set external-interface ge-0/0/2.0
    ```
11. Define the IKE Phase 1 policy reference.
    ```
    [edit security ike gateway gw1]
    user@host# set ike-policy ike_pol
    ```
12. Define the IKE Phase 1 gateway address.

   [edit security ike gateway gw1]
   user@host# set address 1.0.0.1


   [edit security ike gateway gw1]
   user@host# set local-identity user-at-hostname responder_natt1@juniper.net

14. Set remote-identity of the responder. This is the IKE identifier.

   [edit security ike gateway gw1]
   user@host# set remote-identity user-at-hostname branch_natt1@juniper.net

Results   From configuration mode, confirm your configuration by entering the show security ike
command. If the output does not display the intended configuration, repeat the
instructions in this example to correct the configuration.

   [edit]
   user@host# 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 juniper;
   }
   gateway gw1 {
      ike-policy ike_pol;
      address 1.0.0.1;
      local-identity user-at-hostname "responder_natt1@juniper.net";
      remote-identity user-at-hostname "branch_natt1@juniper.net";
      external-interface ge-0/0/2.0;
   }

If you are done configuring the device, enter commit from configuration mode.

Configuring IPsec for the Responder

CLI Quick Configuration   To quickly configure this section of the example, copy the following commands, paste
them into a text file, remove any line breaks, change any details necessary to match your
network configuration, and then copy and paste the commands into the CLI at the [edit]
hierarchy level.

   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 st0.1
   set security ipsec vpn vpn1 ike gateway gw1
To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   ```
   [edit]
   user@host# set security ipsec proposal ipsec_prop
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set encryption-algorithm 3des-cbc
   ```

5. Create the IPsec Phase 2 policy.
   ```
   [edit security ipsec]
   user@host# set policy ipsec_pol
   ```

6. Specify IPsec Phase 2 to use perfect forward secrecy (PFS).
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set perfect-forward-secrecy keys group2
   ```

7. Specify the IPsec Phase 2 proposal reference.
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set proposals ipsec_prop
   ```

8. Specify the IKE gateway.
   ```
   [edit security ipsec]
   user@host# set security ipsec vpn vpn1 ike gateway gw1
   ```

9. Specify the IPsec Phase 2 policy.
   ```
   [edit security ipsec]
   user@host# set vpn vpn1 ike ipsec-policy ipsec_pol
   ```

10. Specify the interface to bind.
    ```
        [edit security ipsec]
        user@host# set vpn vpn1 bind-interface st0.1
    ```

11. Specify that the tunnel be brought up immediately without waiting for a verification packet to be sent.
    ```
        [edit security ipsec]
    ```
user@host# set vpn vpn1 establish-tunnels immediately

**Results**  From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# 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 st0.1;
    ike {
        gateway gw1;
        ipsec-policy ipsec_pol;
    }
    establish-tunnels immediately;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying the IKE Phase 1 Status for the Initiator on page 132
- Verifying IPsec Security Associations for the Initiator on page 134
- Verifying the IKE Phase 1 Status for the Responder on page 135
- Verifying IPsec Security Associations for the Responder on page 137

**Verifying the IKE Phase 1 Status for the Initiator**

**Purpose**  Verify the IKE Phase 1 status.

**Action**  

**NOTE:** Before starting the verification process, you must send traffic from a host in the 33.1.1.0 network to a host in the 32.1.1.0 network. For route-based VPNs, traffic can be initiated by the SRX Series device through the tunnel. We recommend that when testing IPsec tunnels, test traffic be sent from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate a ping operation from 33.1.1.2 to 32.1.1.2.
From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index  State  Initiator cookie  Responder cookie  Mode           Remote Address
106321  UP     d31d6833108fd69f  9ddfe2ce133086aa  Main           1.1.1.1

user@host> show security ike security-associations index 1 detail
IKE peer 1.1.1.1, Index 106321
Initiator cookie: d31d6833108fd69f, Responder cookie: 9ddfe2ce133086aa
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 1.0.0.1:500, Remote: 1.1.1.1:500
Lifetime: Expires in 28785 seconds
Peer ike-id: responder_natt1@juniper.net
Xauth assigned IP: responder_natt1@juniper.net
Algorithms:
  Authentication        : hmac-sha1-96
  Encryption            : 3des-cbc
  Pseudo random function: hmac-sha1
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Flags: IKE SA is created
IPSec security associations: 2 created, 0 deleted
Phase 2 negotiations in progress: 0
```

### Meaning

The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- **Index**—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index index_number detail` command to get more information about the SA.
- **Remote address**—Verify that the remote IP address is correct and that port 500 is being used for peer-to-peer communication.
- **Role initiator state**
  - **Up**—The Phase 1 SA has been established.
  - **Down**—There was a problem establishing the Phase 1 SA.
  - Both peers in the IPSec SA pair are using port 500.
- Peer IKE ID—Verify the remote address is correct.
- Local identity and remote identity—Verify these are correct.
- Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The `show security ike security-associations` command lists additional information about security associations:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Role information

![NOTE: Troubleshooting is best performed on the peer using the responder role.](image)

- Initiator and responder information
- Number of IPsec SAs created
- Number of Phase 2 negotiations in progress

### Verifying IPsec Security Associations for the Initiator

**Purpose**

Verify the IPsec status.

**Action**

From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
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 ac23df79 2532/ unlim   -   root 500  1.1.1.1
>131073 ESP:3des/sha1 cbc9281a 2532/ unlim   -   root 500  1.1.1.1

user@host> show security ipsec security-associations detail
Virtual-system: root
Local Gateway: 1.0.0.1, Remote Gateway: 1.1.1.1
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)
```
Meaning

The output from the `show security ipsec security-associations` command lists the following information:

- The remote gateway has a NAT address of 1.1.1.1.
- Both peers in the IPsec SA pair are using port 500.
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 2532/`unlim` value indicates that the Phase 2 lifetime expires in 2532 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.
- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, `U` indicates that monitoring is up, and `D` indicates that monitoring is down.
- The virtual system (`vsys`) is the root system, and it always lists 0.

Verifying the IKE Phase 1 Status for the Responder

Purpose

Verify the IKE Phase 1 status.

Action

From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index State Initiator cookie Responder cookie Mode Remote Address
5802591 UP d31d6833108fd69f 9ddfe2ce133086aa Main 1.0.0.1

user@host> show security ike security-associations index 1 detail
IKE peer 1.0.0.1, Index 5802591, Role: Responder, State: UP
Initiator cookie: d31d6833108fd69f, Responder cookie: 9ddfe2ce133086aa
Exchange type: Main, Authentication method: Pre-shared-keys
```
Local: 71.1.1.1:500, Remote: 1.0.0.1:500
Lifetime: Expires in 25704 seconds
Peer ike-id: branch_natt1@juniper.net
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication : hmac-sha1-96
  Encryption : 3des-cbc
  Pseudo random function: hmac-sha1
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Flags: IKE SA is created
IPSec security associations: 8 created, 2 deleted
Phase 2 negotiations in progress: 0
Negotiation type: Quick mode, Role: Responder, Message ID: 0
Local: 71.1.1.1:500, Remote: 1.0.0.1:500
Local identity: responder_natt1@juniper.net
Remote identity: branch_natt1@juniper.net
Flags: IKE SA is created

Meaning

The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- Index—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index detail` command to get more information about the SA.
- Remote address—Verify that the remote IP address is correct and that port 500 is being used for peer-to-peer communication.
- Role responder state
  - Up—The Phase 1 SA has been established.
  - Down—There was a problem establishing the Phase 1 SA.
  - Peer IKE ID—Verify the address is correct.
  - Local identity and remote identity—Verify these addresses are correct.
- Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The `show security ike security-associations` command lists additional information about security associations:
• Authentication and encryption algorithms used
• Phase 1 lifetime
• Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
• Role information

**NOTE:** Troubleshooting is best performed on the peer using the responder role.

• Initiator and responder information
• Number of IPsec SAs created
• Number of Phase 2 negotiations in progress

---

**Verifying IPsec Security Associations for the Responder**

**Purpose**  Verify the IPsec status.

**Action**  From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
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 a5224cd9 3571/ unlim   -   root 500  1.0.0.1
>131073 ESP:3des/sha1 82a86a07 3571/ unlim   -   root 500  1.0.0.1

user@host> show security ipsec security-associations detail
Virtual-system: root
   Local Gateway: 71.1.1.1, Remote Gateway: 1.0.0.1
   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
   Direction: inbound, SPI: a5224cd9, AUX-SPI: 0
                   , VPN Monitoring: -
   Hard lifetime: Expires in 3523 seconds
   Lifesize Remaining: Unlimited
   Soft lifetime: Expires in 2923 seconds
   Mode: Tunnel, Type: dynamic, State: installed
   Anti-replay service: counter-based enabled, Replay window size: 64
   Direction: outbound, SPI: 82a86a07, AUX-SPI: 0
                   , VPN Monitoring: -
   Hard lifetime: Expires in 3523 seconds
   Lifesize Remaining: Unlimited
   Soft lifetime: Expires in 2923 seconds
   Mode: Tunnel, Type: dynamic, State: installed
   Anti-replay service: counter-based enabled, Replay window size: 64
```
Meaning

The output from the `show security ipsec security-associations` command lists the following information:

- The remote gateway has an IP address of 1.0.0.1.
- Both peers in the IPsec SA pair are using port 500.
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3571/unlim value indicates that the Phase 2 lifetime expires in 3571 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.
- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U indicates that monitoring is up, and D indicates that monitoring is down.
- The virtual system (vsys) is the root system, and it always lists 0.

The output from the `show security ipsec security-associations index index_id detail` command lists the following information:

- The local identity and remote identity make up the proxy ID for the SA.
  
  A proxy ID mismatch is one of the most common causes for a Phase 2 failure. If no IPsec SA is listed, confirm that Phase 2 proposals, including the proxy ID settings, are correct for both peers. For route-based VPNs, the default proxy ID is local=0.0.0.0/0, remote=0.0.0.0/0, and service=any. Issues can occur with multiple route-based VPNs from the same peer IP. In this case, a unique proxy ID for each IPsec SA must be specified. For some third-party vendors, the proxy ID must be manually entered to match.

- Another common reason for Phase 2 failure is not specifying the ST interface binding. If IPsec cannot complete, check the kmd log or set traceoptions.

Related Documentation

- VPN Overview on page 3
- Understanding NAT-T on page 23
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device on page 160
- IPsec VPN Feature Guide for Security Devices

Example: Configuring an st0 Interface in a Virtual Router

Supported Platforms

J Series, LN Series, SRX Series

This example shows how to configure an st0 interface in a virtual router.

- Requirements on page 139
- Overview on page 139
requirements

before you begin, configure the interfaces and assign the interfaces to security zones. see security zones and interfaces overview.

overview

in this example, you perform the following operations:

• configure the interfaces.
• configure ike phase 1 proposals.
• configure ike policies, and reference the proposals.
• configure an ike gateway, and reference the policy.
• configure phase 2 proposals.
• configure policies, and reference the proposals.
• configure autkey ike, and reference the policy and gateway.
• configure the security policy.
• configure the routing instance.
• configure the vpn bind to tunnel interface.
• configure the routing options.

configuration

cli quick configuration

to quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the cli at the [edit] hierarchy level.

set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.2/30
set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/30
set interfaces st0 unit 0 family inet address 3.3.3.2/30
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
"$9$xFU-b2ZUF5Qn4aQn/CI7-V"
set security ike gateway first ike-policy first_ikepol
set security ike gateway first address 4.4.4.2
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
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure an st0 in a VR:

1. Configure the interfaces.
   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 1.1.1.2/30
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 2.2.2.2/30
   user@host# set interfaces st0 unit 0 family inet address 3.3.3.2/30
   ```

2. Configure Phase 1 of the IPsec tunnel.
   ```
   [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
   ```

3. Configure the IKE policies, and reference the proposals.
   ```
   [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
     "$S9$xFU-b2ZUH5Qn4aQn/CBI7-V"
   ```

4. Configure the IKE gateway, and reference the policy.
   ```
   [edit security ike]
   user@host# set gateway first ike-policy first_ikepol
   user@host# set gateway first address 4.4.4.2
   user@host# set gateway first external-interface ge-0/0/0.0
   ```

5. Configure Phase 2 of the IPsec tunnel.
   ```
   [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
   ```

6. Configure the policies, and reference the proposals.
   ```
   [edit security ipsec]
   user@host# set policy first_ipsecpol perfect-forward-secrecy keys group1
   user@host# set policy first_ipsecpol proposals first_ipsecpol
   ```
7. Configure AutoKey IKE, and reference the policy and gateway.

    [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

8. Configure the VPN bind to tunnel interface.

    [edit security ipsec]
    user@host# set vpn first_vpn bind-interface st0.0

9. Configure the security policy.

    [edit security policies]
    user@host# set default-policy permit-all

10. Configure the st0 in the routing instance.

    [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

11. Configure the routing options.

    [edit routing-instances VR1 routing-options]
    user@host# set static route 6.6.6.0/24 next-hop st0.0

Results  From configuration mode, confirm your configuration by entering the show security and show routing-instances commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    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 asci-text "$9$xFU-b2ZUH5Qn4aQn/CB17-V"; ## SECRET-DATA
        }
        gateway first {
            ike-policy first_ikepol;
            address 4.4.4.2;
            external-interface ge-0/0/0.0;
        }
    }
    ipsec {
        proposal first_ipsecpol {
            protocol esp;
            authentication-algorithm hmac-md5-96;
            encryption-algorithm 3des-cbc;
        }
    }
policy first_ipsecpol {
    perfect-forward-secrecy {
        keys group1;
    }
    proposals first_ipsecprop;
}
vpn first_vpn {
    bind-interface st0.0;
    ike {
        gateway first;
        ipsec-policy first_ipsecpol;
    }
    establish-tunnels immediately;
}
policies {
    default-policy {
        permit-all;
    }
}

user@host# show routing-instances
VR1 {
    instance-type virtual-router;
    interface ge-0/0/1.0;
    interface st0.0;
    routing-options {
        static {
            route 6.6.6.0/24 next-hop st0.0;
        }
    }
}

If you are done configuring the device, enter commit from configuration mode.

Verification

To confirm that the configuration is working properly, perform this task:

- Verifying an st0 interface in the Virtual Router on page 142

Verifying an st0 interface in the Virtual Router

Purpose Verify the st0 interface in the virtual router.

Action From operational mode, enter the show interfaces st0.0 detail command. The number listed for routing table corresponds to the order that the routing tables in the show route all command.

Related Documentation

- IPsec VPN Feature Guide for Security Devices
CHAPTER 14

Policy-Based VPN

- Example: Configuring a Policy-Based VPN on page 143
- Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device on page 160

Example: Configuring a Policy-Based VPN

Supported Platforms

J Series, LN Series, SRX Series

This example shows how to configure a policy-based IPsec VPN to allow data to be securely transferred between a branch office and the corporate office.

- Requirements on page 143
- Overview on page 143
- Configuration on page 147
- Verification on page 156

Requirements

This example uses the following hardware:

- SRX240 device
- SSG140 device

Before you begin, read “VPN Overview” on page 3.

Overview

In this example, you configure a policy-based VPN for a branch office in Chicago, Illinois, because you do not need to conserve tunnel resources or configure many security policies to filter traffic through the tunnel. Users in the Chicago office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

Figure 21 on page 144 shows an example of a policy-based VPN topology. In this topology, the SRX Series device is located in Sunnyvale, and an SSG Series device (or it can be another third-party device) is located in Chicago.
IKE IPsec tunnel negotiation occurs in two phases. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA). In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel. Just as there are two phases to tunnel negotiation, there are two phases to tunnel configuration.
In this example, you configure interfaces, an IPv4 default route, security zones, and address books. Then you configure IKE Phase 1, IPsec Phase 2, security policy, and TCP-MSS parameters. See Table 28 on page 145 through Table 32 on page 147.

Table 28: Interface, Security Zone, and Address Book Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/0.0</td>
<td>10.10.10.1/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3.0</td>
<td>1.1.1.2/30</td>
</tr>
</tbody>
</table>
| Security zones  | trust         | • All system services are allowed.  
                  |                | • The ge-0/0/0.0 interface is bound to this zone.  |
|                 | untrust       | • IKE is the only allowed system service.  
                  |                | • The ge-0/0/3.0 interface is bound to this zone.  |
| Address book entries | sunnyvale | • This address is an entry in the address book book1, which is attached to a zone called trust.  
                  |                | • The address for this address book entry is 10.10.10.0/24.  |
|                 | chicago       | • This address is an entry in the address book book2, which is attached to a zone called ch.  
                  |                | • The address for this address book entry is 192.168.168.0/24.  |

Table 29: IKE Phase 1 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal        | ike-phase1-proposal | • Authentication method: pre-shared-keys  
                  |                     | • Diffie-Hellman group: group2  
                  |                     | • Authentication algorithm: sha1  
                  |                     | • Encryption algorithm: aes-128-cbc |
| Policy          | ike-phase1-policy   | • Mode: main  
                  |                     | • Proposal reference: ike-phase1-proposal  
                  |                     | • IKE Phase 1 policy authentication method: pre-shared-key ascii-text |
| Gateway         | gw-chicago          | • IKE policy reference: ike-phase1-policy  
                  |                     | • External interface: ge-0/0/3.0  
                  |                     | • Gateway address: 2.2.2.2 |
Table 30: IPsec Phase 2 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal| ipsec-phase2-proposal | • Protocol: esp  
• Authentication algorithm: hmac-sha1-96  
• Encryption algorithm: aes-128-cbc |
| Policy  | ipsec-phase2-policy   | • Proposal reference: ipsec-phase2-proposal  
• PFS: Diffie-Hellman group2 |
| VPN     | ike-vpn-chicago       | • IKE gateway reference: gw-chicago  
• IPsec policy reference: ipsec-phase2-policy |

Table 31: Security Policy Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| This security policy permits traffic from the trust zone to the untrust zone. | vpn-tr-untr  | • Match criteria:  
• source-address sunnyvale  
• destination-address chicago  
• application any  
• Permit action: tunnel ipsec-vpn ike-vpn-chicago  
• Permit action: tunnel pair-policy vpn-untr-tr |
| This security policy permits traffic from the untrust zone to the trust zone. | vpn-untr-tr  | • Match criteria:  
• source-address chicago  
• destination-address sunnyvale  
• application any  
• Permit action: tunnel ipsec-vpn ike-vpn-chicago  
• Permit action: tunnel pair-policy vpn-tr-untr |
| This security policy permits all traffic from the trust zone to the untrust zone. | permit-any | • Match criteria:  
• source-address any  
• source-destination any  
• application any  
• Action: permit |

NOTE: You must put the vpn-tr-untr policy before the permit-any security policy. Junos OS performs a security policy lookup starting at the top of the list. If the permit-any policy comes before the vpn-tr-untr policy, all traffic from the trust zone will match the permit-any policy and be permitted. Thus, no traffic will ever match the vpn-tr-untr policy.
Table 32: TCP-MSS Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSS value: 1350</td>
<td>TCP-MSS is negotiated as part of the TCP three-way handshake and limits the maximum size of a TCP segment to better fit the maximum transmission unit (MTU) limits on a network. This is especially important for VPN traffic, as the IPSec encapsulation overhead, along with the IP and frame overhead, can cause the resulting Encapsulating Security Payload (ESP) packet to exceed the MTU of the physical interface, thus causing fragmentation. Fragmentation results in increased use of bandwidth and device resources.</td>
</tr>
<tr>
<td>NOTE: We recommend a value of 1350 as the starting point for most Ethernet-based networks with an MTU of 1500 or greater. You might need to experiment with different TCP-MSS values to obtain optimal performance. For example, you might need to change the value if any device in the path has a lower MTU, or if there is any additional overhead such as PPP or Frame Relay.</td>
<td></td>
</tr>
</tbody>
</table>

Configuration

**Configuring Basic Network, Security Zone, and Address Book Information**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
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 address-book book1 address sunnyvale 10.10.10.0/24
set security address-book book1 attach zone trust
set security address-book book2 address chicago 192.168.168.0/24
set security address-book book2 attach zone untrust
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure basic network, security zone, and address book information:

1. Configure Ethernet interface information.
   ```
   [edit]
   user@host# set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
   user@host# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
   ```

2. Configure static route information.
   ```
   [edit]
   user@host# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
   ```

3. Configure the untrust security zone.
4. Assign an interface to the security zone.
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/3.0

5. Specify allowed system services for the security zone.
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services ike

6. Configure the trust security zone.
   [edit]
   user@host# edit security zones security-zone trust

7. Assign an interface to the security zone.
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/0.0

8. Specify allowed system services for the security zone.
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-services all

9. Create an address book and attach it to a zone.
   [edit security address-book book1]
   user@host# set address sunnyvale 10.10.10.0/24
   user@host# set attach zone trust

10. Create another address book and attach it to a zone.
    [edit security address-book book2]
    user@host# set address chicago 192.168.168.0/24
    user@host# set attach zone untrust

Results  From configuration mode, confirm your configuration by entering the show interfaces, show routing-options, show security zones, and show security address-book commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [edit]
    user@host# show interfaces
    ge-0/0/0 { unit 0 { family inet { address 10.10.10.1/24; } } } ge-0/0/3 { unit 0 { family inet { address 1.1.1.2/30 } } }
[edit]
user@host# show routing-options
static {
  route 0.0.0.0/0 next-hop 1.1.1.1;
}

[edit]
user@host# 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;
  }
}

[edit]
user@host# show security address-book
book1 {
  address sunnyvale 10.10.10.0/24;
  attach {
    zone trust;
  }
}

book2 {
  address chicago 192.168.168.0/24;
  attach {
    zone untrust;
  }
}

If you are done configuring the device, enter **commit** from configuration mode.

**Configuring IKE**

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set security ike proposal ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ike-phase1-proposal dh-group group2
```
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode

To configure IKE:

1. Create the IKE Phase 1 proposal.
   ```bash
   [edit security ike]
   user@host# set proposal ike-phase1-proposal
   ```

2. Define the IKE proposal authentication method.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@host# set authentication-method pre-shared-keys
   ```

3. Define the IKE proposal Diffie-Hellman group.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@host# set dh-group group2
   ```

4. Define the IKE proposal authentication algorithm.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@host# set authentication-algorithm sha1
   ```

5. Define the IKE proposal encryption algorithm.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```

6. Create an IKE Phase 1 policy.
   ```bash
   [edit security ike]
   user@host# set policy ike-phase1-policy
   ```

7. Set the IKE Phase 1 policy mode.
   ```bash
   [edit security ike policy ike-phase1-policy]
   user@host# set mode main
   ```

8. Specify a reference to the IKE proposal.
   ```bash
   [edit security ike policy ike-phase1-policy]
   user@host# set proposals ike-phase1-proposal
   ```

9. Define the IKE Phase 1 policy authentication method.
   ```bash
   [edit security ike policy ike-phase1-policy]
   user@host# set pre-shared-key ascii-text 395psksecr3t
   ```

10. Create an IKE Phase 1 gateway and define its external interface.
    ```bash
    [edit security ike]
    ```

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 395psksecr3t
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 2.2.2.2
11. Define the IKE Phase 1 policy reference.
   
   ```
   [edit security ike gateway gw-chicago]
   user@host# set ike-policy ike-phase1-policy
   ```

12. Create an IKE Phase 1 gateway and define its external interface.
   
   ```
   [edit security ike gateway gw-chicago]
   user@host# set gateway gw-chicago external-interface ge-0/0/3.0
   ```

13. Define the IKE Phase 1 policy reference.
   
   ```
   [edit security ike gateway gw-chicago]
   user@host# set ike-policy ike-phase1-policy
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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 {
    mode main;
    proposals ike-phase1-proposal;
    pre-shared-key ascii-text "$9$9VMTp1RvWLDwYKMDkmF3yiKM87Vb2oZjws5F"; ## SECRET-DATA
}
gateway gw-chicago {
    ike-policy ike-phase1-policy;
    address 2.2.2.2;
    external-interface ge-0/0/3.0;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

### Configuring IPsec

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
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
set security ipsec vpn ike-vpn-chicago ike gateway gw-chicago
set security ipsec vpn ike-vpn-chicago ike ipsec-policy ipsec-phase2-policy
```
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   ```
   [edit]
   user@host# set security ipsec proposal ipsec-phase2-proposal
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```

5. Create the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set policy ipsec-phase2-policy
   ```

6. Specify the IPsec Phase 2 proposal reference.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set proposals ipsec-phase2-proposal
   ```

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set perfect-forward-secrecy keys group2
   ```

8. Specify the IKE gateway.
   
   ```
   [edit security ipsec]
   user@host# set vpn ike-vpn-chicago ike gateway gw-chicago
   ```

9. Specify the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@host# set vpn ike-vpn-chicago ike ipsec-policy ipsec-phase2-policy
   ```

Results

From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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 ike-vpn-chicago {
  ike {
    gateway gw-chicago;
    ipsec-policy ipsec-phase2-policy;
  }
}

If you are done configuring the device, enter commit from configuration mode.

**Configuring Security Policies**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
set security policies from-zone trust to-zone untrust policy vpn-tr-untr match source-address sunnyvale
set security policies from-zone trust to-zone untrust policy vpn-tr-untr match destination-address chicago
set security policies from-zone trust to-zone untrust policy vpn-tr-untr match application any
set security policies from-zone trust to-zone untrust policy vpn-tr-untr then permit tunnel ipsec-vpn ike-vpn-chicago
set security policies from-zone trust to-zone untrust policy vpn-tr-untr then permit tunnel pair-policy vpn-untr-tr
set security policies from-zone untrust to-zone trust policy vpn-untr-tr match source-address chicago
set security policies from-zone untrust to-zone trust policy vpn-untr-tr match destination-address sunnyvale
set security policies from-zone untrust to-zone trust policy vpn-untr-tr match application any
set security policies from-zone untrust to-zone trust policy vpn-untr-tr then permit tunnel ipsec-vpn ike-vpn-chicago
set security policies from-zone untrust to-zone trust policy vpn-untr-tr then permit tunnel pair-policy 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 vpn-tr-untr before policy permit-any
```

Copyright © 2016, Juniper Networks, Inc.
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the untrust zone.

   ```
   [edit security policies from-zone trust to-zone untrust]
   user@host# set policy vpn-tr-untr match source-address sunnyvale
   user@host# set policy vpn-tr-untr match destination-address chicago
   user@host# set policy vpn-tr-untr match application any
   user@host# set policy vpn-tr-untr then permit tunnel ipsec-vpn ike-vpn-chicago
   user@host# set policy vpn-tr-untr then permit tunnel pair-policy vpn-untr-tr
   ```

2. Create the security policy to permit traffic from the untrust zone to the trust zone.

   ```
   [edit security policies from-zone untrust to-zone trust]
   user@host# set policy vpn-untr-tr match source-address sunnyvale
   user@host# set policy vpn-untr-tr match destination-address chicago
   user@host# set policy vpn-untr-tr match application any
   user@host# set policy vpn-untr-tr then permit tunnel ipsec-vpn ike-vpn-chicago
   user@host# set policy vpn-untr-tr then permit tunnel pair-policy vpn-tr-untr
   ```

3. Create the security policy to permit traffic from the trust zone to the untrust zone.

   ```
   [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. Reorder the security policies so that the vpn-tr-untr security policy is placed above the permit-any security policy.

   ```
   [edit security policies from-zone trust to-zone untrust]
   user@host# insert policy vpn-tr-untr before policy permit-any
   ```

Results

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies from-zone trust to-zone untrust [ policy vpn-tr-untr {
  match {
    source-address sunnyvale;
    destination-address chicago;
    application any;
  }
  then {
    permit {
      tunnel {
        ipsec-vpn ike-vpn-chicago;
        pair-policy vpn-untr-tr;
      }
    }
  }
}
```
policy permit-any {
    match {
        source-address any;
        destination-address any;
        application any;
    }
    then {
        permit
    }
}
from-zone untrust to-zone trust {
    policy vpn-untr-tr {
        match {
            source-address chicago;
            destination-address sunnyvale;
            application any;
        }
        then {
            permit {
                tunnel {
                    ipsec-vpn ike-vpn-chicago;
                    pair-policy vpn-tr-untr;
                }
            }
        }
    }
}

If you are done configuring the device, enter `commit` from configuration mode.

**Configuring TCP-MSS**

**CLI Quick Configuration**
To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

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

**Step-by-Step Procedure**
To configure TCP-MSS information:

1. Configure TCP-MSS information.
   
   ```
   [edit]
   user@host# set security flow tcp-mss ipsec-vpn mss 1350
   ```

**Results**
From configuration mode, confirm your configuration by entering the `show security flow` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
user@host# show security flow
tcp-mss {
ipsec-vpn {
mss 1350;
}
}

If you are done configuring the device, enter **commit** from configuration mode.

**Configuring the SSG Series Device**

For reference, the configuration for the SSG Series device is provided. For information about configuring SSG Series devices, see the *Concepts and Examples ScreenOS Reference Guide*, which is located at [http://www.juniper.net/techpubs](http://www.juniper.net/techpubs).

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI.

```
set interface ethernet0/6 zone Trust
set interface ethernet0/0 zone Untrust
set interface ethernet0/6 ip 192.168.168.1/24
set interface ethernet0/6 route
set interface ethernet0/0 ip 2.2.2.2/30
set interface ethernet0/0 route
set flow tcp-mss 1350
set address Trust "local-net" 192.168.168.0 255.255.255.0
set address Untrust "corp-net" 10.10.10.0 255.255.255.0
set ike gateway corp-ike address 1.1.1.2
Main outgoing-interface ethernet0/0
preshare 395psksecr3t
sec-level standard
set vpn corp-vpn gateway corp-ike replay tunnel idletime 0 sec-level standard
set policy id 11 from Trust to Untrust "local-net" "corp-net" "ANY" tunnel vpn "corp-vpn"
pair-policy 10
set policy id 10 from Untrust to Trust "corp-net" "local-net" "ANY" tunnel vpn "corp-vpn"
pair-policy 11
set policy id 1 from Trust to Untrust "ANY" "ANY" "ANY" nat src permit
set route 0.0.0.0/0 interface ethernet0/0 gateway 2.2.2.1
```

**Verification**

To confirm that the configuration is working properly, perform these tasks:

- Verifying the IKE Phase 1 Status on page 156
- Verifying the IPsec Phase 2 Status on page 158
- Reviewing Statistics and Errors for an IPsec Security Association on page 159

**Verifying the IKE Phase 1 Status**

Verify the IKE Phase 1 status.
NOTE: Before starting the verification process, you need to send traffic from a host in the 10.10.10/24 network to a host in the 192.168.168/24 network. For policy-based VPNs, a separate host must generate the traffic; traffic initiated from the SRX Series device will not match the VPN policy. We recommend that the test traffic be from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate ping from 10.10.10.10 to 192.168.168.10.

From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
4       2.2.2.2         UP     5e1db3f9d50b0de6  e50865d9ebf134f8  Main

user@host> show security ike security-associations index 4 detail
IKE peer 2.2.2.2, Index 4, Role: Responder, State: UP
Initiator cookie: Seldb3f9d50b0de6, Responder cookie: e50865d9ebf134f8
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 1.1.1.2:500, Remote: 2.2.2.2:500
Lifetime: Expires in 28770 seconds
Algorithms:
  Authentication        : sha1
  Encryption            : aes-128-cbc
  Pseudo random function: hmac-sha1
Traffic statistics:
  Input bytes    :                 852
  Output bytes   :                 856
  Input packets  :                   5
  Output packets :                   4
Flags: Caller notification sent
IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0
```

Meaning: The `show security ike security-associations` command lists all active IKE Phase 1 security associations (SAs). If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- **Index**—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index index_number detail` command to get more information about the SA.
- **Remote Address**—Verify that the remote IP address is correct.
- **State**
  - **UP**—The Phase 1 SA has been established.
  - **DOWN**—There was a problem establishing the Phase 1 SA.
- **Mode**—Verify that the correct mode is being used.
Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The `show security ike security-associations index 1 detail` command lists additional information about the security association with an index number of 1:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Initiator and responder role information

**NOTE:** Troubleshooting is best performed on the peer using the responder role.

- Number of IPsec SAs created
- Number of Phase 2 negotiations in progress

### Verifying the IPsec Phase 2 Status

**Purpose**
Verify the IPsec Phase 2 status.

**Action**
From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
user@host> show security ipsec security-associations
  total configured sa:  2
  ID   Gateway      Port  Algorithm       SPI       Life:sec/kb Mon vsys
<2   2.2.2.2       500   ESP:aes-128/sha1  a63eb26f 3565/ unlim   -   0
>2   2.2.2.2       500   ESP:aes-128/sha1  a1024ed9 3565/ unlim   -   0
```

```
user@host> show security ipsec security-associations index 2 detail
  Virtual-system: Root
  Local Gateway: 1.1.1.2, Remote Gateway: 2.2.2.2
  Local Identity: ipv4_subnet(any:0,[0..7]=10.10.10.0/24)
  Remote Identity: ipv4_subnet(any:0,[0..7]=192.168.168.0/24)
  DF-bit: clear
  Policy-name: vpnpolicy-unt-tr
  Direction: inbound, SPI: 2789126767, AUX-SPI: 0
  Hard lifetime: Expires in 3558 seconds
  Lifesize Remaining: Unlimited
  Soft lifetime: Expires in 2986 seconds
  Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: -
```
Meaning

The output from the `show security ipsec security-associations` command lists the following information:

- The ID number is 2. Use this value with the `show security ipsec security-associations index` command to get more information about this particular SA.

- There is one IPsec SA pair using port 500, which indicates that no NAT traversal is implemented. (NAT traversal uses port 4500 or another random high number port.)

- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3565/unlim value indicates that the Phase 2 lifetime expires in 3565 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.

- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U (up) or D (down) is listed.

- The virtual system (vsys) is the root system, and it always lists 0.

The output from the `show security ipsec security-associations index 16384 detail` command lists the following information:

- The local identity and remote identity make up the proxy ID for the SA.

A proxy ID mismatch is one of the most common reasons for a Phase 2 failure. For policy-based VPNs, the proxy ID is derived from the security policy. The local address and remote address are derived from the address book entries, and the service is derived from the application configured for the policy. If Phase 2 fails because of a proxy ID mismatch, you can use the policy to confirm which address book entries are configured. Verify that the addresses match the information being sent. Check the service to ensure that the ports match the information being sent.

### Reviewing Statistics and Errors for an IPsec Security Association

**Purpose**

Review ESP and authentication header counters and errors for an IPsec security association.

**Action**

From operational mode, enter the `show security ipsec statistics index index_number` command, using the index number of the VPN for which you want to see statistics.

```
user@host> show security ipsec statistics index 2
```
ESP Statistics:
- Encrypted bytes: 920
- Decrypted bytes: 6208
- Encrypted packets: 5
- Decrypted packets: 87

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

You can also use the `show security ipsec statistics` command to review statistics and errors for all SAs.

To clear all IPsec statistics, use the `clear security ipsec statistics` command.

**Meaning**
If you see packet loss issues across a VPN, you can run the `show security ipsec statistics` or `show security ipsec statistics detail` command several times to confirm that the encrypted and decrypted packet counters are incrementing. You should also check if the other error counters are incrementing.

**Related Documentation**
- VPN Overview on page 3
- Example: Configuring a Route-Based VPN on page 77
- Example: Configuring a Hub-and-Spoke VPN on page 189
- IPsec VPN Feature Guide for Security Devices

**Example: Configuring a Policy-Based VPN with Both an Initiator and a Responder Behind a NAT Device**

**Supported Platforms**
J Series, LN Series, SRX Series

This example shows how to configure a policy-based VPN with both an initiator and a responder behind a NAT device to allow data to be securely transferred between a branch office and the corporate office.

- Requirements on page 160
- Overview on page 161
- Configuration on page 166
- Verification on page 181

**Requirements**
Before you begin, read “VPN Overview” on page 3.
Overview

In this example, you configure a policy-based VPN for a branch office in Chicago, Illinois, because you want to conserve tunnel resources but still get granular restrictions on VPN traffic. Users in the branch office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

In this example, you configure interfaces, routing options, security zones, security policies for both an initiator and a responder.

Figure 22 on page 162 shows an example of a topology for a VPN with both an initiator and a responder behind a NAT device.
Figure 22: Policy-Based VPN Topology with Both an Initiator and a Responder Behind a NAT Device

**Trust zone**
- 10.1.99.2

**SRX Series device**
- Chicago (initiator)
  - ge-0/0/2.0
  - 10.1.99.1/24
  - ge-0/0/0.1
  - 12.168.99.100/24
  - ge-0/0/0.1
  - 12.168.99.1

**NAT router**
- ge-0/0/2.0
  - 1.1.100.2

**Internet**
- ge-0/0/2.0
  - 1.1.100.1

**SRX Series device**
- Sunnyvale (responder)
  - ge-0/0/2.0
  - 13.168.11.100/24
  - ge-0/0/0.1
  - 13.168.11.1

**NAT router**
- ge-0/0/2.0
  - 1.1.100.1

**Trust zone**
- 10.2.99.2

Policy-based tunnel
In this example, you configure interfaces, an IPv4 default route, and security zones. Then you configure IKE Phase 1, including local and remote peers, IPsec Phase 2, and the security policy. Note in the example above, the responder’s private IP address 13.168.11.1 is hidden by the NAT device and mapped to public IP address 1.1.100.1.

See Table 33 on page 163 through Table 36 on page 164 for specific configuration parameters used for the initiator in the examples.

Table 33: Interface, Routing Options, and Security Zones for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/1</td>
<td>12.168.99.100/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/2</td>
<td>10.1.99.1/24</td>
</tr>
<tr>
<td>Static routes</td>
<td>10.2.99.0/24</td>
<td>The next hop is 12.168.99.1.</td>
</tr>
<tr>
<td></td>
<td>13.168.11.0/24</td>
<td>The next hop is 12.168.99.1.</td>
</tr>
<tr>
<td></td>
<td>1.1.100.0/24</td>
<td>12.168.99.1</td>
</tr>
</tbody>
</table>
| Security zones   | trust       | • All system services are allowed.  
                  |              | • All protocols are allowed.  
                  |              | • The ge-0/0/2.0 interface is bound to this zone.  
|                  | untrust     | • All system services are allowed.  
                  |              | • All protocols are allowed.  
                  |              | • The ge-0/0/1.0 interface is bound to this zone.  |

Table 34: IKE Phase 1 Configuration Parameters for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal         | ike_prop | • Authentication method: pre-shared-keys  
                  |       | • Diffie-Hellman group: group2  
                  |       | • Authentication algorithm: md5  
                  |       | • Encryption algorithm: 3des-cbc  |
| Policy           | ike_pol | • Mode: main  
                  |       | • Proposal reference: ike_prop  
                  |       | • IKE Phase 1 policy authentication method: pre-shared-key ascii-text  |
| Gateway          | gate   | • IKE policy reference: ike_pol  
                  |       | • External interface: ge-0/0/1.0  
                  |       | • Gateway address: 1.1.100.23  
                  |       | • Local peer is inet 11.11.11.11  
                  |       | • Remote peer is inet 44.44.44.44  |
### Table 35: IPsec Phase 2 Configuration Parameters for the Initiator

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ipsec_prop</td>
<td>• Protocol: esp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: hmac-md5-96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: 3des-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ipsec_pol</td>
<td>• Proposal reference: ipsec_prop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perfect forward secrecy (PFS): group1</td>
</tr>
<tr>
<td>VPN</td>
<td>first_vpn</td>
<td>• IKE gateway reference: gate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPsec policy reference: ipsec_pol</td>
</tr>
</tbody>
</table>

### Table 36: Security Policy Configuration Parameters for the Initiator

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>The security policy permits tunnel traffic from the trust zone to the untrust zone.</td>
<td>pol1</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• destination-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Action: permit tunnel ipsec-vpn first_vpn</td>
</tr>
<tr>
<td>The security policy permits tunnel traffic from the untrust zone to the trust zone.</td>
<td>pol1</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• destination-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Action: permit tunnel ipsec-vpn first_vpn</td>
</tr>
</tbody>
</table>

See Table 37 on page 164 through Table 40 on page 166 for specific configuration parameters used for the responder in the examples.

### Table 37: Interface, Routing Options, and Security Zones for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/2</td>
<td>13.168.11.100/24</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/3</td>
<td>10.2.99.1/24</td>
</tr>
<tr>
<td>Static routes</td>
<td>10.1.99.0/24 (default route)</td>
<td>The next hop is 13.168.11.1.</td>
</tr>
<tr>
<td></td>
<td>12.168.99.0/24</td>
<td>The next hop is 13.168.11.1.</td>
</tr>
<tr>
<td></td>
<td>1.1.100.0/24</td>
<td>13.168.11.1</td>
</tr>
</tbody>
</table>
### Table 37: Interface, Routing Options, and Security Zones for the Responder (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security zones</td>
<td>trust</td>
<td>• All system services are allowed.</td>
</tr>
<tr>
<td></td>
<td>untrust</td>
<td>• All system services are allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• All protocols are allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/3.0 interface is bound to this zone.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The ge-0/0/2.0 interface is bound to this zone.</td>
</tr>
</tbody>
</table>

### Table 38: IKE Phase 1 Configuration Parameters for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ike_prop</td>
<td>• Authentication method: pre-shared-keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Diffie-Hellman group: group2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: md5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: 3des-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ike_pol</td>
<td>• Mode: main</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Proposal reference: ike_prop</td>
</tr>
<tr>
<td>Gateway</td>
<td>gate</td>
<td>• IKE policy reference: ike_pol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• External interface: ge-0/0/2.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gateway address: 1.1.100.22</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Always send dead-peer detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Local peer is inet 44.44.44.44</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Remote peer is inet 11.11.11</td>
</tr>
</tbody>
</table>

### Table 39: IPsec Phase 2 Configuration Parameters for the Responder

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposal</td>
<td>ipsec_prop</td>
<td>• Protocol: esp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Authentication algorithm: hmac-md5-96</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Encryption algorithm: 3des-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ipsec_pol</td>
<td>• Proposal reference: ipsec_prop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perfect forward secrecy (PFS): group1</td>
</tr>
<tr>
<td>VPN</td>
<td>first_vpn</td>
<td>• IKE gateway reference: gate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPsec policy reference: ipsec_pol</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Establish tunnels immediately</td>
</tr>
</tbody>
</table>
### Table 40: Security Policy Configuration Parameters for the Responder

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| The security policy permits tunnel traffic from the trust zone to the untrust zone. | pol1 | • Match criteria:  
  • source-address any  
  • destination-address any  
  • application any  
  • Action: permit tunnel ipsec-vpn first_vpn |
| The security policy permits tunnel traffic from the untrust zone to the trust zone. | pol1 | • Match criteria:  
  • source-address any  
  • destination-address any  
  • application any  
  • Action: permit tunnel ipsec-vpn first_vpn |

### Configuration

- Configuring Interface, Routing Options, and Security Zones for the Initiator on page 166
- Configuring IKE for the Initiator on page 168
- Configuring IPsec for the Initiator on page 170
- Configuring Security Policies for the Initiator on page 172
- Configuring Interface, Routing Options, and Security Zones for the Responder on page 173
- Configuring IKE for the Responder on page 176
- Configuring IPsec for the Responder on page 178
- Configuring Security Policies for the Responder on page 180

### CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
[edit]
set interfaces ge-0/0/1 unit 0 family inet address 12.168.99.100/24
set interfaces ge-0/0/2 unit 0 family inet address 10.1.99.1/24
set routing-options static route 10.2.99.0/24 next-hop 12.168.99.1
set routing-options static route 13.168.11.0/24 next-hop 12.168.99.1
set routing-options static route 1.1.100.0/24 next-hop 12.168.99.1
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-0/0/0.0
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
```
**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure interfaces, static routes, and security zones:

1. Configure Ethernet interface information.
   ```
   [edit]
   user@host# set interfaces ge-0/0/1 unit 0 family inet address 12.168.99.100/24
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 10.1.99.1/24
   ```

2. Configure static route information.
   ```
   [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 13.168.11.0/24 next-hop 12.168.99.1
   ```

3. Configure the trust security zone.
   ```
   [edit]
   user@host# set security zones security-zone trust host-inbound-traffic protocols all
   ```

4. Assign an interface to the trust security zone.
   ```
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/2.0
   ```

5. Specify system services for the trust security zone.
   ```
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-services all
   ```

6. Configure the untrust security zone.
   ```
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic protocols all
   ```

7. Assign an interface to the untrust security zone.
   ```
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/1.0
   ```

8. Specify system services for the untrust security zone.
   ```
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services all
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show interfaces`, `show routing-options`, and `show security zones` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show interfaces ge-0/0/1 {
    unit 0 {
        family inet {
            address 12.168.99.100/24;
        }
    }
}
```
If you are done configuring the device, enter **commit** from configuration mode.

### Configuring IKE for the Initiator

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.
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 main
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "juniper"
set security ike gateway gate ike-policy ike_pol
set security ike gateway gate address 1.1.100.23
set security ike gateway gate external-interface ge-0/0/1.0
set security ike gateway gate local-identity inet 11.11.11.11
set security ike gateway gate remote-identity inet 44.44.44.44

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   
   [edit security ike]
   user@host# set proposal ike_prop

2. Define the IKE proposal authentication method.
   
   [edit security ike proposal ike_prop]
   user@host# set authentication-method pre-shared-keys

3. Define the IKE proposal Diffie-Hellman group.
   
   [edit security ike proposal ike_prop]
   user@host# set dh-group group2

4. Define the IKE proposal authentication algorithm.
   
   [edit security ike proposal ike_prop]
   user@host# set authentication-algorithm md5

5. Define the IKE proposal encryption algorithm.
   
   [edit security ike proposal ike_prop]
   user@host# set encryption-algorithm 3des-cbc

6. Create an IKE Phase 1 policy.
   
   [edit security ike policy ]
   user@host# set policy ike_pol

7. Set the IKE Phase 1 policy mode.
   
   [edit security ike policy ike_pol]
   user@host# set mode main

8. Specify a reference to the IKE proposal.
   
   [edit security ike policy ike_pol]
   user@host# set proposals ike_prop

9. Define the IKE Phase 1 policy authentication method.
   
   [edit security ike policy ike_pol pre-shared-key]
Set an ASCII text value for "juniper".

10. Create an IKE Phase 1 gateway and define its external interface.

    ```
    [edit security ike]
    user@host# set gateway ge-0/0/1.0
    ```

11. Create an IKE Phase 1 gateway address.

    ```
    [edit security ike gateway]
    set gate address 1.1.100.23
    ```

12. Define the IKE Phase 1 policy reference.

    ```
    [edit security ike gateway]
    set gate ike-policy ike_pol
    ```

13. Set `local-identity` for the local peer.

    ```
    [edit security ike gateway]
    user@host# set local-identity inet 11.11.11
    ```

14. Set `remote-identity` for the responder. This is the responder's local identity.

    ```
    [edit security ike gateway]
    user@host# set remote-identity inet 44.44.44.44
    ```

**Results**  From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

    ```
    [edit]
    user@host# show security ike
    proposal ike_prop {
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm md5;
        encryption-algorithm 3des-cbc;
    }
    policy ike_pol {
        mode main;
        proposals ike_prop;
        pre-shared-key ascii-text "juniper";
    }
    gateway gate {
        ike-policy ike_pol;
        address 1.1.100.23;
        local-identity 11.11.11.11;
        remote-identity 44.44.44.44;
        external-interface ge-0/0/1.0;
    }
    ```

If you are done configuring the device, enter `commit` from configuration mode.

### Configuring IPsec for the Initiator

**CLI Quick Configuration**  To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your
network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
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
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   ```
   [edit]
   user@host# set security ipsec proposal ipsec_prop
   ```
2. Specify the IPsec Phase 2 proposal protocol.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set protocol esp
   ```
3. Specify the IPsec Phase 2 proposal authentication algorithm.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set authentication-algorithm hmac-md5-96
   ```
4. Specify the IPsec Phase 2 proposal encryption algorithm.
   ```
   [edit security ipsec proposal ipsec_prop]
   user@host# set encryption-algorithm 3des-cbc
   ```
5. Specify the IPsec Phase 2 proposal reference.
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set proposals ipsec_prop
   ```
6. Specify IPsec Phase 2 to use perfect forward secrecy (PFS) group1.
   ```
   [edit security ipsec policy ipsec_pol]
   user@host# set perfect-forward-secrecy keys group1
   ```
7. Specify the IKE gateway.
   ```
   [edit security ipsec]
   user@host# set vpn first_vpn ike gateway gate
   ```
8. Specify the IPsec Phase 2 policy.
   ```
   [edit security ipsec]
   user@host# set vpn first_vpn ike ipsec-policy ipsec_pol
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.
[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;
    }
}

If you are done configuring the device, enter `commit` from configuration mode.

**Configuring Security Policies for the Initiator**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
set security policies from-zone trust to-zone untrust policy pol1 match source-address any
set security policies from-zone trust to-zone untrust policy pol1 match destination-address any
set security policies from-zone trust to-zone untrust policy pol1 match application any
set security policies from-zone trust to-zone untrust policy pol1 then permit tunnel
    ipsec-vpn first_vpn
set security policies from-zone untrust to-zone trust policy pol1 match source-address any
set security policies from-zone untrust to-zone trust policy pol1 match destination-address any
set security policies from-zone untrust to-zone trust policy pol1 match application any
set security policies from-zone untrust to-zone trust policy pol1 then permit tunnel
    ipsec-vpn first_vpn
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the untrust zone.

```plaintext
[edit]
user@host# set 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
```
2. Create the security policy to permit traffic from the untrust zone to the trust zone.

[edit security policies from-zone untrust to-zone trust]
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

Results

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

[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 {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
      tunnel {
        ipsec-vpn first_vpn;
      }
    }
  }
}

If you are done configuring the device, enter `commit` from configuration mode.

Configuring Interface, Routing Options, and Security Zones for the Responder

CLI Quick Configuration

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure interfaces, static routes, security zones, and security policies:

1. Configure Ethernet interface information.
   
```
   [edit]
   user@host# set interfaces ge-0/0/2 unit 0 family inet address 13.168.11.100/24
   user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.2.99.1/24
   ```

2. Configure static route information.
   
```
   [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 12.168.99.0/24 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. Configure the untrust security zone.
   
```
   [edit]
   user@host# set security zones security-zone untrust host-inbound-traffic system-services all
   ```

4. Assign an interface to the untrust security zone.
   
```
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/2.0
   ```

5. Specify allowed system services for the untrust security zone.
   
```
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-services all
   ```

6. Configure the trust security zone.
   
```
   [edit]
   user@host# set security zones security-zone trust host-inbound-traffic protocols all
   ```

7. Assign an interface to the trust security zone.
   
```
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/3.0
   ```

8. Specify allowed system services for the trust security zone.
   
```
   [edit security zones security-zone trust]
   ```
user@host# set host-inbound-traffic system-services all

**Results**  From configuration mode, confirm your configuration by entering the `show interfaces`, `show routing-options`, and `show security zones` commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```yaml
[edit]
user@host# show interfaces
ge-0/0/2 {
  unit 0 {
    family inet {
      address 13.168.11.100/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 10.2.99.1/244;
    }
  }
}

[edit]
user@host# show routing-options
static {
  route 10.1.99.0/24 next-hop 13.168.11.1;
  route 12.168.99.0/24 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 {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
    ge-0/0/2.0;
  }
}
security-zone trust {
  host-inbound-traffic {
    system-services {
      all;
    }
    protocols {
      all;
    }
  }
  interfaces {
```
If you are done configuring the device, enter `commit` from configuration mode.

### Configuring IKE for the Responder

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```plaintext
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 main
set security ike policy ike_pol proposals ike_prop
set security ike policy ike_pol pre-shared-key ascii-text "juniper"
set security ike gateway gate ike-policy ike_pol
set security ike gateway gate address 1.1.100.22
set security ike gateway gate dead-peer-detection probe-idle-tunnel
set security ike gateway gate external-interface ge-0/0/2.0
set security ike gateway gate local-identity inet 44.44.44.44
set security ike gateway gate remote-identity inet 11.11.11.11
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IKE:

1. Create the IKE Phase 1 proposal.
   ```plaintext
   [edit security ike]
   user@host# set proposal ike-phase1-proposal
   ```

2. Define the IKE proposal authentication method.
   ```plaintext
   [edit security ike proposal ike_prop]
   user@host# set authentication-method pre-shared-key
   ```

3. Define the IKE proposal Diffie-Hellman group.
   ```plaintext
   [edit security ike proposal ike_prop]
   user@host# set dh-group group2
   ```

4. Define the IKE proposal authentication algorithm.
   ```plaintext
   [edit security ike proposal ike_prop]
   user@host# set authentication-algorithm md5
   ```

5. Define the IKE proposal encryption algorithm.
   ```plaintext
   [edit security ike proposal ike_prop]
   user@host# set encryption-algorithm 3des-cbc
   ```

6. Create an IKE Phase 1 policy.
7. Set the IKE Phase 1 policy mode.
   [edit security ike policy ike_pol]
   user@host# set mode main

8. Specify a reference to the IKE proposal.
   [edit security ike policy ike_pol]
   user@host# set proposals ike_prop

9. Define the IKE Phase 1 policy authentication method.
   [edit security ike policy ike_pol proposals ike_prop set security ike policy ike_pol
   pre-shared-key]
   user@host# set ascii-text "juniper"

10. Create an IKE Phase 1 gateway and define its external interface.
    [edit security ike]
    user@host# set security ike gateway gate external-interface ge-0/0/2.0

11. Define the IKE Phase 1 policy reference.
    [edit security ike gateway]
    user@host# set gate ike-policy ike_pol

12. Create an IKE Phase 1 gateway address.
    [edit security ike gateway]
    user@host# set gate address 1.1.100.22

13. Set local-identity for the local peer (initiator).
    [edit security ike gateway gate]
    user@host# set local-identity inet 44.44.44.44

14. Set remote-identity for the responder. This is the responder’s local identity.
    [edit security ike gateway gate]
    user@host# set remote-identity inet 11.11.11.11

15. Set dead peer detection to detect whether the peer is up or down.
    [edit security ike gateway gate]
    user@host# set dead-peer-detection probe idle-tunnel

Results  From configuration mode, confirm your configuration by entering the show security ike
command. If the output does not display the intended configuration, repeat the
instructions in this example to correct the configuration.

    [edit]
    user@host# show security ike
    proposal ike_prop {
      authentication-method pre-shared-keys;
      dh-group group2;
      authentication-algorithm md5;
      encryption-algorithm 3des-cbc;
    }
    policy ike_pol {
mode main;
proposals ike_prop;
pre-shared-key ascii-text "juniper";
}
gateway gate {
ike-policy ike_pol;
address 1.1.100.22;
dead-peer-detection probe-idle-tunnel;
external-interface ge-0/0/2.0;
local-identity inet 44.44.44.44;
remote-identity inet 11.11.11.11;
}

If you are done configuring the device, enter commit from configuration mode.

Configuring IPsec for the Responder

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set security ipsec proposal ipsec_prop
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
set security ipsec vpn first_vpn establish-tunnels immediately
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   [edit]
   user@host# set security ipsec proposal ipsec_prop

2. Specify the IPsec Phase 2 proposal protocol.
   
   [edit security security ipsec proposal ipsec_prop]
   user@host# set protocol esp

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   [edit security ipsec proposal ipsec_prop]
   user@host# set authentication-algorithm hmac-md5-96

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   [edit security ipsec proposal ipsec_prop]
   user@host# set encryption-algorithm 3des-cbc

5. Set IPsec Phase 2 to use perfect forward secrecy (PFS) group1.
6. Create the IPsec Phase 2 policy.
   [edit security ipsec]
   user@host# set policy ipsec_pol

7. Specify the IPsec Phase 2 proposal reference.
   [edit security ipsec policy ipsec_pol]
   user@host# set proposals ipsec_prop

8. Specify the IKE gateway.
   [edit security ipsec]
   user@host# set vpn first_vpn ike gateway gate

9. Specify the IPsec Phase 2 policy.
   [edit security ipsec]
   user@host# set vpn first_vpn ike ipsec-policy ipsec_pol

10. Specify that the tunnel be brought up immediately without a verification packet.
    [edit security ipsec]
    user@host# set security ipsec vpn first_vpn establish-tunnels immediately

**Results** From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

    [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;
            establish-tunnels immediately;
        }
    }

If you are done configuring the device, enter **commit** from configuration mode.
**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set security policies from-zone trust to-zone untrust policy pol1 match source-address any
set security policies from-zone trust to-zone untrust policy pol1 match destination-address any
set security policies from-zone trust to-zone untrust policy pol1 match application any
set security policies from-zone trust to-zone untrust policy pol1 then permit tunnel ipsec-vpn first_vpn
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the untrust zone.
   
   ```
   [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. Create the security policy to permit traffic from the untrust zone to the trust zone.
   
   ```
   [edit security policies from-zone untrust to-zone trust]
   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
   ```

**Results**

From configuration mode, confirm your configuration by entering the `show security policies` command. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
If you are done configuring the device, enter commit from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the IKE Phase 1 Status for the Initiator on page 181
- Verifying IPsec Security Associations for the Initiator on page 183
- Verifying the IKE Phase 1 Status for the Responder on page 184
- Verifying IPsec Security Associations for the Responder on page 186

**Verifying the IKE Phase 1 Status for the Initiator**

**Purpose**
Verify the IKE Phase 1 status.

**Action**

NOTE: Before starting the verification process, you must send traffic from a host in the 10.1.99.0 network to a host in the 10.2.99.0 network. For route-based VPNs, traffic can be initiated by the SRX Series device through the tunnel. We recommend that when testing IPsec tunnels, test traffic be sent from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate a ping operation from 10.1.99.2 to 10.2.99.2.
From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index  State  Initiator cookie  Responder cookie  Mode           Remote Address
5137403 UP     b3a24bc00e963c51  7bf96bcc6230e484  Main           1.1.100.23

user@host> show security ike security-associations index 1 detail
Index  State  Initiator cookie  Responder cookie  Mode           Remote Address
1400579286 UP  487cfb570908425c  7710c8487f9ff20c  Main           1.1.100.22
```

```
{primary:node0}[edit]
root@poway# run show security ike security-associations detail
node0:

IKE peer 1.1.100.22, Index 1400579286,
   Location: FPC 5, PIC 0, KMD-Instance 4
   Role: Initiator, State: UP
   Initiator cookie: 487cfb570908425c, Responder cookie: 7710c8487f9ff20c
   Exchange type: Main, Authentication method: Pre-shared-keys
   Local: 13.168.11.100:4500, Remote: 1.1.100.22:4500
   Lifetime: Expires in 28622 seconds
   Peer ike-id: 44.44.44.44
   Xauth user-name: not available
   Xauth assigned IP: 0.0.0.0
   Algorithms:
      Authentication        : hmac-md5-96
      Encryption            : 3des-cbc
      Pseudo random function: hmac-md5
   Traffic statistics:
      Input bytes : 0
      Output bytes : 0
      Input packets: 0
      Output packets: 0
   IPSec security associations: 0 created, 0 deleted
   Phase 2 negotiations in progress: 0
```

**Meaning**  
The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- **Index**—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index index_number detail` command to get more information about the SA.
- **Remote address**—Verify that the remote IP address is correct and that port 4500 is being used for peer-to-peer communication.
- **Role initiator state**
  - **Up**—The Phase 1 SA has been established.
  - **Down**—There was a problem establishing the Phase 1 SA.
Both peers in the IPsec SA pair are using port 4500, which indicates that NAT-T is implemented. (NAT-T uses port 4500 or another random high-numbered port.)

Peer IKE ID—Verify the remote (responder) address is correct. In this example, the address is 44.44.44.44.

Local identity and remote identity—Verify these are correct.

Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The `show security ike security-associations` command lists additional information about security associations:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Role information

---

**NOTE:** Troubleshooting is best performed on the peer using the responder role.

- Initiator and responder information
- Number of IPsec SAs created
- Number of Phase 2 negotiations in progress

### Verifying IPsec Security Associations for the Initiator

**Purpose**  
Verify the IPsec status.

**Action**  
From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
user@host> show security ipsec security-associations
Total active tunnels: 1
ID  Algorithm     SPI         Life:sec/kb  Mon vsys Port  Gateway
<2  ESP:3des/md5  2bf24122   3390/ unlim   -   root 4500  1.1.100.23
>2  ESP:3des/md5  2baef146   3390/ unlim   -   root 4500  1.1.100.23
user@host> show security ipsec security-associations detail
```
Local Gateway: 12.168.99.100, 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
Policy-name: pol1
Location: FPC 5, PIC 0, KMD-Instance 4
Direction: inbound, SPI: 2bf24122, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3388 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2801 seconds
Mode: Tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Local Gateway: 12.168.99.100, 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
Policy-name: pol1
Location: FPC 5, PIC 0, KMD-Instance 4
Direction: outbound, SPI: 2baef146, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3388 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2801 seconds
Mode: Tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Meaning The output from the `show security ipsec security-associations` command lists the following information:

- The remote gateway has a NAT address of 1.1.100.23.
- Both peers in the IPsec SA pair are using port 4500, which indicates that NAT-T is implemented. (NAT-T uses port 4500 or another random high-numbered port.)
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3390/ unlimited value indicates that the Phase 2 lifetime expires in 3390 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.
- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U indicates that monitoring is up, and D indicates that monitoring is down.
- The virtual system (vsys) is the root system, and it always lists 0.

Verifying the IKE Phase 1 Status for the Responder

Purpose Verify the IKE Phase 1 status.

Action From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
```
The `show security ike security-associations index 1 detail` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- **Index**—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index detail` command to get more information about the SA.

- **Remote address**—Verify that the remote IP address is correct and that port 4500 is being used for peer-to-peer communication.

- **Role responder state**
  - **Up**—The Phase 1 SA has been established.
  - **Down**—There was a problem establishing the Phase 1 SA.
  - **Peer IKE ID**—Verify the local (initiator) address for the peer is correct. In this example, the address is 11.11.11.11.
  - **Local identity and remote identity**—Verify these are correct.

- **Mode**—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:
• External interfaces (the interface must be the one that receives IKE packets)
• IKE policy parameters
• Preshared key information
• Phase 1 proposal parameters (must match on both peers)

The show security ike security-associations command lists additional information about security associations:

• Authentication and encryption algorithms used
• Phase 1 lifetime
• Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
• Role information

NOTE: Troubleshooting is best performed on the peer using the responder role.

• Initiator and responder information
• Number of IPsec SAs created
• Number of Phase 2 negotiations in progress

Verifying IPsec Security Associations for the Responder

Purpose  Verify the IPsec status.

Action  From operational mode, enter the show security ipsec security-associations command. After obtaining an index number from the command, use the show security ipsec security-associations index index_number detail command.

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 a5224cd9 3571/ unlim   -   root 4500  1.0.0.1
>131073 ESP:3des/sha1 82a86a07 3571/ unlim   -   root 4500  1.0.0.1

user@host> show security ipsec security-associations detail
Virtual-system: root
Local Gateway: 71.1.1.1, Remote Gateway: 1.0.0.1
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
Direction: inbound, SPI: a5224cd9, AUX-SPI: 0
, VPN Monitoring: -
Hard lifetime: Expires in 3523 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2923 seconds
Mode: Tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: 82a86a07, AUX-SPI: 0, VPN Monitoring: -
Hard lifetime: Expires in 3523 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2923 seconds
Mode: Tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Meaning
The output from the `show security ipsec security-associations` command lists the following information:

- The remote gateway has a NAT address of 1.0.0.1.
- Both peers in the IPsec SA pair are using port 4500, which indicates that NAT-T is implemented. (NAT-T uses port 4500 or another random high-numbered port.)
- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3571/ unlim value indicates that the Phase 2 lifetime expires in 3571 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.
- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U indicates that monitoring is up, and D indicates that monitoring is down.
- The virtual system (vsys) is the root system, and it always lists 0.

Related Documentation
- VPN Overview on page 3
- Understanding NAT-T on page 23
- Example: Configuring a Route-Based VPN with Only the Responder Behind a NAT Device on page 111
- IPsec VPN Feature Guide for Security Devices
CHAPTER 15

Hub-and-Spoke VPN

- Example: Configuring a Hub-and-Spoke VPN on page 189

Example: Configuring a Hub-and-Spoke VPN

Supported Platforms

| J Series, LN Series, SRX Series |

This example shows how to configure a hub-and-spoke IPsec VPN for an enterprise-class deployment.

- Requirements on page 189
- Overview on page 189
- Configuration on page 195
- Verification on page 215

Requirements

This example uses the following hardware:

- SRX240 device
- SRX5800 device
- SSG140 device

Before you begin, read “VPN Overview” on page 3.

Overview

This example describes how to configure a hub-and-spoke VPN typically found in branch deployments. The hub is the corporate office, and there are two spokes—a branch office in Sunnyvale, California, and a branch office in Westford, Massachusetts. Users in the branch offices will use the VPN to securely transfer data with the corporate office.

Figure 23 on page 190 shows an example of a hub-and-spoke VPN topology. In this topology, an SRX5800 device is located at the corporate office. An SRX240 device is located at the Westford branch, and an SSG140 device is located at the Sunnyvale branch.

Copyright © 2016, Juniper Networks, Inc.
In this example, you configure the corporate office hub, the Westford spoke, and the Sunnyvale spoke. First you configure interfaces, IPv4 static and default routes, security zones, and address books. Then you configure IKE Phase 1 and IPsec Phase 2 parameters, and bind the st0.0 interface to the IPsec VPN. On the hub, you configure st0.0 for multipoint and add a static NHTB table entry for the Sunnyvale spoke. Finally, you configure security policy and TCP-MSS parameters. See Table 41 on page 190 through Table 45 on page 195 for specific configuration parameters used in this example.

Table 41: Interface, Security Zone, and Address Book Information

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub</td>
<td>Interfaces</td>
<td>ge-0/0/0.0</td>
<td>10.10.10.1/24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ge-0/0/3.0</td>
<td>1.1.1.2/30</td>
</tr>
<tr>
<td></td>
<td></td>
<td>st0</td>
<td>10.11.10.24</td>
</tr>
<tr>
<td>Spoke</td>
<td>Interfaces</td>
<td>ge-0/0/0.0</td>
<td>3.3.3.2/30</td>
</tr>
</tbody>
</table>
## Table 41: Interface, Security Zone, and Address Book Information (continued)

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ge-0/0/3.0</td>
<td>192.168.178.1/24</td>
<td></td>
</tr>
</tbody>
</table>
| Hub          | Security zones     | trust     | • All system services are allowed.  
• The ge-0/0/0.0 interface is bound to this zone. |
|              | st0                | 10.11.11.12/24 |
|              | Security zones     | untrust   | • IKE is the only allowed system service.  
• The ge-0/0/3.0 interface is bound to this zone. |
|              | vpn                |           | The st0.0 interface is bound to this zone. |
| Spoke        | Security zones     | trust     | • All system services are allowed.  
• The ge-0/0/3.0 interface is bound to this zone. |
|              | untrust            |           | • IKE is the only allowed system service.  
• The ge-0/0/0.0 interface is bound to this zone. |
|              | vpn                |           | The st0.0 interface is bound to this zone. |
| Hub          | Address book entries | local-net | • This address is for the trust zone's address book.  
• The address for this address book entry is 10.10.10.0/24. |
|              | sunnyvale-net      |           | • This address book is for the vpn zone's address book.  
• The address for this address book entry is 192.168.168.0/24. |
|              | westford-net       |           | • This address is for the vpn zone's address book.  
• The address for this address book entry is 192.168.178.0/24. |
### Table 41: Interface, Security Zone, and Address Book Information (continued)

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoke</td>
<td>Address book entries</td>
<td>local-net</td>
<td>- This address is for the trust zone’s address book.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The address for this address book entry is 192.168.168.0/24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>corp-net</td>
<td>- This address is for the vpn zone’s address book.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The address for this address book entry is 10.10.10.0/24.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sunnyvale-net</td>
<td>- This address is for the vpn zone’s address book.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- The address for this address book entry is 192.168.168.0/24.</td>
</tr>
</tbody>
</table>

### Table 42: IKE Phase 1 Configuration Parameters

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub</td>
<td>Proposal</td>
<td>ike-phase1-proposal</td>
<td>- Authentication method: pre-shared-keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Diffie-Hellman group: group2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Authentication algorithm: sha1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Encryption algorithm: aes-128-cbc</td>
</tr>
<tr>
<td>Policy</td>
<td>ike-phase1-policy</td>
<td></td>
<td>- Mode: main</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Proposal reference: ike-phase1-proposal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- IKE Phase 1 policy authentication method: pre-shared-key ascii-text</td>
</tr>
<tr>
<td>Gateway</td>
<td>gw-westford</td>
<td></td>
<td>- IKE policy reference: ike-phase1-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- External interface: ge-0/0/3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Gateway address: 3.3.3.2</td>
</tr>
<tr>
<td></td>
<td>gw-sunnyvale</td>
<td></td>
<td>- IKE policy reference: ike-phase1-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- External interface: ge-0/0/3.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Gateway address: 2.2.2.2</td>
</tr>
</tbody>
</table>
### Table 42: IKE Phase 1 Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Spoke        | Proposal  | ike-phase1-proposal | • Authentication method: pre-shared-keys  
|              |           |                   | • Diffie-Hellman group: group2  
|              |           |                   | • Authentication algorithm: sha1  
|              |           |                   | • Encryption algorithm: aes-128-cbc |
| Policy       |           | ike-phase1-policy  | • Mode: main  
|              |           |                   | • Proposal reference: ike-phase1-proposal  
|              |           |                   | • IKE Phase 1 policy authentication method: pre-shared-key ascii-text |
| Gateway      |           | gw-corporate      | • IKE policy reference: ike-phase1-policy  
|              |           |                   | • External interface: ge-0/0/0.0  
|              |           |                   | • Gateway address: 1.1.1.2 |

### Table 43: IPsec Phase 2 Configuration Parameters

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Hub          | Proposal  | ipsec-phase2-proposal | • Protocol: esp  
|              |           |               | • Authentication algorithm: hmac-sha1-96  
|              |           |               | • Encryption algorithm: aes-128-cbc |
| Policy       |           | ipsec-phase2-policy | • Proposal reference: ipsec-phase2-proposal  
|              |           |               | • PFS: Diffie-Hellman group2 |
| VPN          | vpn-sunnyvale |               | • IKE gateway reference: gw-sunnyvale  
|              |           |               | • IPsec policy reference: ipsec-phase2-policy  
|              |           |               | • Bind to interface: st0.0 |
|              | vpn-westford |               | • IKE gateway reference: gw-westford  
|              |           |               | • IPsec policy reference: ipsec-phase2-policy  
|              |           |               | • Bind to interface: st0.0 |
| Spoke        | Proposal  | ipsec-phase2-proposal | • Protocol: esp  
|              |           |               | • Authentication algorithm: hmac-sha1-96  
|              |           |               | • Encryption algorithm: aes-128-cbc |
| Policy       |           | ipsec-phase2-policy | • Proposal reference: ipsec-phase2-proposal  
|              |           |               | • PFS: Diffie-Hellman group2 |
Table 43: IPsec Phase 2 Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VPN</td>
<td>vpn-corporate</td>
<td>• IKE gateway reference: gw-corporate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• IPsec policy reference: ipsec-phase2-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Bind to interface: st0.0</td>
</tr>
</tbody>
</table>

Table 44: Security Policy Configuration Parameters

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub</td>
<td>The security policy permits traffic from the trust zone to the vpn zone.</td>
<td>local-to-spokes</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address local-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address sunnyvale-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address westford-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td>The security policy permits traffic from the vpn zone to the trust zone.</td>
<td>spokes-to-local</td>
<td>Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address sunnyvale-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address westford-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address local-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td>The security policy permits intrazone traffic.</td>
<td>spoke-to-speak</td>
<td>Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td>Spoke</td>
<td>The security policy permits traffic from the trust zone to the vpn zone.</td>
<td>to-corp</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address local-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address corp-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address sunnyvale-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td>Spoke</td>
<td>The security policy permits traffic from the vpn zone to the trust zone.</td>
<td>from-corp</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address corp-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address sunnyvale-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• destination-address local-net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
</tbody>
</table>
Table 44: Security Policy Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Hub or Spoke</th>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The security policy permits traffic from the untrust zone to the trust zone.</td>
<td>permit-any</td>
<td>Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source-destination any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Permit action: source-nat interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>By specifying <strong>source-nat interface</strong>, the SRX Series device translates the source IP address and port for outgoing traffic, using the IP address of the egress interface as the source IP address and a random high-number port for the source port.</td>
</tr>
</tbody>
</table>

Table 45: TCP-MSS Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCC-MSS is negotiated as part of the TCP three-way handshake and limits the maximum size of a TCP segment to better fit the MTU limits on a network. For VPN traffic, the IPsec encapsulation overhead, along with the IP and frame overhead, can cause the resulting ESP packet to exceed the MTU of the physical interface, which causes fragmentation. Fragmentation results in increased use of bandwidth and device resources.</td>
<td>MSS value: 1350</td>
</tr>
</tbody>
</table>

**NOTE:** The value of 1350 is a recommended starting point for most Ethernet-based networks with an MTU of 1500 or greater. You might need to experiment with different TCP-MSS values to obtain optimal performance. For example, you might need to change the value if any device in the path has a lower MTU, or if there is any additional overhead such as PPP or Frame Relay.

**Configuration**

- Configuring Basic Network, Security Zone, and Address Book Information for the Hub on page 196
- Configuring IKE for the Hub on page 199
- Configuring IPsec for the Hub on page 201
- Configuring Security Policies for the Hub on page 203
- Configuring TCP-MSS for the Hub on page 205
- Configuring Basic Network, Security Zone, and Address Book Information for the Westford Spoke on page 206
- Configuring IKE for the Westford Spoke on page 209
- Configuring IPsec for the Westford Spoke on page 211
- Configuring Security Policies for the Westford Spoke on page 212
- Configuring TCP-MSS for the Westford Spoke on page 214
- Configuring the Sunnyvale Spoke on page 214
Configuring Basic Network, Security Zone, and Address Book Information for the Hub

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```bash
set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
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 1.1.1.1
set routing-options static route 192.168.168.0/24 next-hop 10.11.11.11
set routing-options static route 192.168.178.0/24 next-hop 10.11.11.12
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 untrust interfaces st0.0
set security-zones security-zone untrust host-inbound-traffic system-services all
set security-zones security-zone untrust vpn interfaces st0.0
set security-address-book book1 address local-net 10.10.10.0/24
set security-address-book book1 attach zone trust
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
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure basic network, security zone, and address book information for the hub:

1. Configure Ethernet interface information.
   ```
   [edit]
   user@hub# set interfaces ge-0/0/0 unit 0 family inet address 10.10.10.1/24
   user@hub# set interfaces ge-0/0/3 unit 0 family inet address 1.1.1.2/30
   user@hub# set interfaces st0 unit 0 family inet address 10.11.11.10/24
   ```

2. Configure static route information.
   ```
   [edit]
   user@hub# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1
   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. Configure the untrust security zone.
   ```
   [edit]
   user@hub# set security-zones security-zone untrust
   ```

4. Assign an interface to the untrust security zone.
   ```
   [edit security-zones security-zone untrust]
   user@hub# set interfaces ge-0/0/3.0
   ```

5. Specify allowed system services for the untrust security zone.
   ```
   [edit security-zones security-zone untrust]
   ```
6. Configure the trust security zone.
   ```
   [edit]
   user@hub# edit security zones security-zone trust
   ```

7. Assign an interface to the trust security zone.
   ```
   [edit security zones security-zone trust]
   user@hub# set interfaces ge-0/0/0
   ```

8. Specify allowed system services for the trust security zone.
   ```
   [edit security zones security-zone trust]
   user@hub# set host-inbound-traffic system-services all
   ```

9. Create an address book and attach a zone to it.
   ```
   [edit security address-book book1]
   user@hub# set address local-net 10.10.10.0/24
   user@hub# set attach zone trust
   ```

10. Configure the vpn security zone.
    ```
    [edit]
    user@hub# edit security zones security-zone vpn
    ```

11. Assign an interface to the vpn security zone.
    ```
    [edit security zones security-zone vpn]
    user@hub# set interfaces st0
    ```

12. Create another address book and attach a zone to it.
    ```
    [edit security address-book book2]
    user@hub# set address sunnyvale-net 192.168.168.0/24
    user@hub# set address westford-net 192.168.178.0/24
    user@hub# set attach zone vpn
    ```

**Results**

From configuration mode, confirm your configuration by entering the `show interfaces`, `show routing-options`, `show security zones`, and `show security address-book` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@hub# show interfaces
ge-0/0/0 {
  unit 0 {
    family inet {
      address 10.10.10.1/24;
    }
  }
}
ge-0/0/3 {
  unit 0 {
    family inet {
      address 1.1.1.2/30
    }
  }
}
```


```conf
st0{
    unit 0 {
        family inet {
            address 10.11.11.10/24
        }
    }
}

[edit]
user@hub# show routing-options
static {
    route 0.0.0.0/0 next-hop 1.1.1.1;
    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;
}
```
If you are done configuring the device, enter commit from configuration mode.

**Configuring IKE for the Hub**

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```bash
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 395psksecre3t
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 3.3.3.2
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 2.2.2.2
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IKE for the hub:

1. Create the IKE Phase 1 proposal.
   ```bash
   [edit security ike]
   user@hub# set proposal ike-phase1-proposal
   ```

2. Define the IKE proposal authentication method.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@hub# set authentication-method pre-shared-keys
   ```

3. Define the IKE proposal Diffie–Hellman group.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@hub# set dh-group group2
   ```

4. Define the IKE proposal authentication algorithm.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@hub# set authentication-algorithm sha1
   ```

5. Define the IKE proposal encryption algorithm.
   ```bash
   [edit security ike proposal ike-phase1-proposal]
   user@hub# set encryption-algorithm aes-128-cbc
   ```
6. Create an IKE Phase 1 policy.
   
   ```
   [edit security ike]
   user@hub# set policy ike-phase1-policy
   ```

7. Set the IKE Phase 1 policy mode.
   
   ```
   [edit security ike policy ike-phase1-policy]
   user@hub# set mode main
   ```

8. Specify a reference to the IKE proposal.
   
   ```
   [edit security ike policy ike-phase1-policy]
   user@hub# set proposals ike-phase1-proposal
   ```

9. Define the IKE Phase 1 policy authentication method.
   
   ```
   [edit security ike policy ike-phase1-policy]
   user@hub# set pre-shared-key ascii-text 395psksecr3t
   ```

10. Create an IKE Phase 1 gateway and define its external interface.
    
    ```
    [edit security ike]
    user@hub# set gateway gw-westford external-interface ge-0/0/3.0
    ```

11. Define the IKE Phase 1 policy reference.
    
    ```
    [edit security ike]
    user@hub# set gateway gw-westford ike-policy ike-phase1-policy
    ```

12. Define the IKE Phase 1 gateway address.
    
    ```
    [edit security ike]
    user@hub# set gateway gw-westford address 3.3.3.2
    ```

13. Create an IKE Phase 1 gateway and define its external interface.
    
    ```
    [edit security ike]
    user@hub# set gateway gw-sunnyvale external-interface ge-0/0/3.0
    ```

14. Define the IKE Phase 1 policy reference.
    
    ```
    [edit security ike gateway]
    user@hub# set gateway gw-sunnyvale ike-policy ike-phase1-policy
    ```

15. Define the IKE Phase 1 gateway address.
    
    ```
    [edit security ike gateway]
    user@hub# set gateway gw-sunnyvale address 2.2.2.2
    ```

**Results**

From configuration mode, confirm your configuration by entering the `show security ike` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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 "$9$9VMTP1RvWLdwYKMDkJF3yIKM87Vb2oZjws5F"; ## SECRET-DATA
}
gateway gw-sunnyvale {
    ike-policy ike-phase1-policy;
    address 2.2.2.2;
    external-interface ge-0/0/3.0;
}
gateway gw-westford {
    ike-policy ike-phase1-policy;
    address 3.3.3.2;
    external-interface ge-0/0/3.0;
}

If you are done configuring the device, enter commit from configuration mode.

Configuring IPsec for the Hub

CLI Quick Configuration
To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```bash
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 keysgroup2
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
```

Step-by-Step Procedure
The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec for the hub:

1. Create an IPsec Phase 2 proposal.
   ```bash
   [edit]
   user@hub# set security ipsec proposal ipsec-phase2-proposal
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   ```bash
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@hub# set protocol esp
   ```
3. Specify the IPsec Phase 2 proposal authentication algorithm.
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@hub# set authentication-algorithm hmac-sha1-96

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@hub# set encryption-algorithm aes-128-cbc

5. Create the IPsec Phase 2 policy.
   [edit security ipsec]
   user@hub# set policy ipsec-phase2-policy

6. Specify the IPsec Phase 2 proposal reference.
   [edit security ipsec policy ipsec-phase2-policy]
   user@hub# set proposals ipsec-phase2-proposal

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   [edit security ipsec policy ipsec-phase2-policy]
   user@hub# set perfect-forward-secrecy keys group2

8. Specify the IKE gateways.
   [edit security ipsec]
   user@hub# set vpn vpn-westford ike gateway gw-westford
   user@hub# set vpn vpn-sunnyvale ike gateway gw-sunnyvale

9. Specify the IPsec Phase 2 policies.
   [edit security ipsec]
   user@hub# set vpn vpn-westford ike ipsec-policy ipsec-phase2-policy
   user@hub# set vpn vpn-sunnyvale ike ipsec-policy ipsec-phase2-policy

10. Specify the interface to bind.
    [edit security ipsec]
        user@hub# set vpn vpn-westford bind-interface st0.0
        user@hub# set vpn vpn-sunnyvale bind-interface st0.0

11. Configure the st0 interface as multipoint.
    [edit]
        user@hub# set interfaces st0 unit 0 multipoint

12. Add static NHTB table entries for the Sunnyvale and Westford offices.
    [edit]
        user@hub# set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.11 ipsec-vpn
        user@hub# set interfaces st0 unit 0 family inet next-hop-tunnel 10.11.11.12 ipsec-vpn

Results From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [edit]
    user@hub# show security ipsec
proposals 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-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;
  }
}

If you are done configuring the device, enter commit from configuration mode.

Configuring Security Policies for the Hub

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

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

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies for the hub:

1. Create the security policy to permit traffic from the trust zone to the vpn zone.

   [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. Create the security policy to permit traffic from the vpn zone to the trust zone.

   [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 destination-address any
   user@hub# set policy spokes-to-local then permit

3. Create the security policy to permit intrazone traffic.

   [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 destination-address any
   user@hub# set policy spoke-to-spoke then permit

Results

From configuration mode, confirm your configuration by entering the show security policies command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[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;
        }
    }
}

If you are done configuring the device, enter commit from configuration mode.

### Configuring TCP-MSS for the Hub

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the [edit] hierarchy level.

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

**Step-by-Step Procedure**

To configure TCP-MSS information for the hub:

1. Configure TCP-MSS information.

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

**Results**

From configuration mode, confirm your configuration by entering the `show security flow` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
```
user@hub# show security flow
tcp-mss {
    ipsec-vpn {
        mss 1350;
    }
}
```
If you are done configuring the device, enter `commit` from configuration mode.

**Configuring Basic Network, Security Zone, and Address Book Information for the Westford Spoke**

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```plaintext
set interfaces ge-0/0/0 unit 0 family inet address 3.3.3.2/30
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 3.1.1.1
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-0/0/0/0.0
set security-zones security-zone untrust host-inbound-traffic system-services ike
set security-zones security-zone untrust 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
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure basic network, security zone, and address book information for the Westford spoke:

1. Configure Ethernet interface information.
   ```plaintext
   [edit]
   user@spoke# set interfaces ge-0/0/0/0 unit 0 family inet address 3.3.3.2/30
   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. Configure static route information.
   ```plaintext
   [edit]
   user@spoke# set routing-options static route 0.0.0.0/0 next-hop 3.1.1.1
   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. Configure the untrust security zone.
   ```plaintext
   [edit]
   user@spoke# set security-zones security-zone untrust
   ```

4. Assign an interface to the security zone.
   ```plaintext
   [edit security-zones security-zone untrust]
   user@spoke# set interfaces ge-0/0/0/0
   ```
5. Specify allowed system services for the untrust security zone.
   [edit security zones security-zone untrust]
   user@spoke# set host-inbound-traffic system-services ike

6. Configure the trust security zone.
   [edit]
   user@spoke# edit security zones security-zone trust

7. Assign an interface to the trust security zone.
   [edit security zones security-zone trust]
   user@spoke# set interfaces ge-0/0/3.0

8. Specify allowed system services for the trust security zone.
   [edit security zones security-zone trust]
   user@spoke# set host-inbound-traffic system-services all

9. Configure the vpn security zone.
   [edit]
   user@spoke# edit security zones security-zone vpn

10. Assign an interface to the vpn security zone.
    [edit security zones security-zone vpn]
    user@spoke# set interfaces st0.0

11. Create an address book and attach a zone to it.
    [edit security address-book book1]
    user@spoke# set address local-net 192.168.178.0/24
    user@spoke# set attach zone trust

12. Create another address book and attach a zone to it.
    [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

Results

From configuration mode, confirm your configuration by entering the show interfaces, show routing-options, show security zones, and show security address-book commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@spoke# show interfaces
ge-0/0/0 {  
  unit 0 {  
    family inet {  
      address 3.3.3.2/30;  
    }
  }
}  
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 1.1.1.1;
  route 192.168.168.0/24 next-hop 10.11.11.11;
  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;
}
}

If you are done configuring the device, enter commit from configuration mode.

### Configuring IKE for the Westford Spoke

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set security ike proposal ike-phase1-proposal
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 395psksecr3t
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 1.1.1.2
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IKE for the Westford spoke:

1. Create the IKE Phase 1 proposal.
   ```
   [edit security ike]
   user@spoke# set proposal ike-phase1-proposal
   ```
2. Define the IKE proposal authentication method.
   ```
   [edit security ike proposal ike-phase1-proposal]
   user@spoke# set authentication-method pre-shared-keys
   ```
3. Define the IKE proposal Diffie–Hellman group.
   ```
   [edit security ike proposal ike-phase1-proposal]
   user@spoke# set dh-group group2
   ```
4. Define the IKE proposal authentication algorithm.
   ```
   [edit security ike proposal ike-phase1-proposal]
   user@spoke# set authentication-algorithm sha1
   ```
5. Define the IKE proposal encryption algorithm.
   ```
   [edit security ike proposal ike-phase1-proposal]
   user@spoke# set encryption-algorithm aes-128-cbc
   ```
6. Create an IKE Phase 1 policy.
7. Set the IKE Phase 1 policy mode.

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

8. Specify a reference to the IKE proposal.

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

9. Define the IKE Phase 1 policy authentication method.

    [edit security ike policy ike-phase1-policy]
    user@spoke# set pre-shared-key ascii-text "$9$9VMTp1RvWLdwYKMJDkmF3yIKM87Vb2oZjws5F";

10. Create an IKE Phase 1 gateway and define its external interface.

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

11. Define the IKE Phase 1 policy reference.

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

12. Define the IKE Phase 1 gateway address.

    [edit security ike]
    user@spoke# set gateway gw-corporate address 1.1.1.2

Results  From configuration mode, confirm your configuration by entering the show security ike command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

    [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 "$9$9VMTp1RvWLdwYKMJDkmF3yIKM87Vb2oZjws5F"; ##
        SECRET-DATA
    }
    gateway gw-corporate {
        ike-policy ike-phase1-policy;
        address 1.1.1.2;
        external-interface ge-0/0/0.0;
    }

If you are done configuring the device, enter commit from configuration mode.
Configuring IPsec for the Westford Spoke

**CLI Quick Configuration**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
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
```

**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure IPsec for the Westford spoke:

1. Create an IPsec Phase 2 proposal.
   
   ```
   [edit]
   user@spoke# set security ipsec proposal ipsec-phase2-proposal
   ```

2. Specify the IPsec Phase 2 proposal protocol.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@spoke# set protocol esp
   ```

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@spoke# set authentication-algorithm hmac-sha1-96
   ```

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   ```
   [edit security ipsec proposal ipsec-phase2-proposal]
   user@spoke# set encryption-algorithm aes-128-cbc
   ```

5. Create the IPsec Phase 2 policy.
   
   ```
   [edit security ipsec]
   user@spoke# set policy ipsec-phase2-policy
   ```

6. Specify the IPsec Phase 2 proposal reference.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@spoke# set proposals ipsec-phase2-proposal
   ```

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   
   ```
   [edit security ipsec policy ipsec-phase2-policy]
   user@host# set perfect-forward-secrecy keys group2
   ```

8. Specify the IKE gateway.
   
   ```
   [edit security ipsec]
   ```
9. Specify the IPsec Phase 2 policy.
   ```
   [edit security ipsec]
   user@spoke# set vpn vpn-corporate ike gateway gw-corporate
   ```

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

**Results**

From configuration mode, confirm your configuration by entering the `show security ipsec` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[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;
   }
}
```  

If you are done configuring the device, enter `commit` from configuration mode.

**Configuring Security Policies for the Westford Spoke**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
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

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies for the Westford spoke:

1. Create the security policy to permit traffic from the trust zone to the vpn zone.

   [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. Create the security policy to permit traffic from the vpn zone to the trust zone.

   [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 destination-address corp-net
   user@spoke# set policy spokes-to-local match application any
   user@spoke# set policy spokes-to-local then permit

Results

From configuration mode, confirm your configuration by entering the show security policies command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   [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;
   }
If you are done configuring the device, enter **commit** from configuration mode.

### Configuring TCP-MSS for the Westford Spoke

#### CLI Quick Configuration

To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

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

#### Step-by-Step Procedure

To configure TCP-MSS for the Westford spoke:

1. Configure TCP-MSS information.

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

#### Results

From configuration mode, confirm your configuration by entering the **show security flow** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring the Sunnyvale Spoke

#### CLI Quick Configuration

This example uses an SSG Series device for the Sunnyvale spoke. For reference, the configuration for the SSG Series device is provided. For information about configuring SSG Series devices, see the *Concepts and Examples ScreenOS Reference Guide*, which is located at [http://www.juniper.net/techpubs](http://www.juniper.net/techpubs).

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI.

```
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 2.2.2.2/30
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 1.1.1.2 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 2.2.2.1

Verification

To confirm that the configuration is working properly, perform these tasks:

- Verifying the IKE Phase 1 Status on page 215
- Verifying the IPsec Phase 2 Status on page 217
- Verifying Next-Hop Tunnel Bindings on page 218
- Verifying Static Routes for Remote Peer Local LANs on page 219
- Reviewing Statistics and Errors for an IPsec Security Association on page 219
- Testing Traffic Flow Across the VPN on page 220

Verifying the IKE Phase 1 Status

Purpose

Verify the IKE Phase 1 status.

Action

NOTE: Before starting the verification process, you need to send traffic from a host in the 10.10.10/24 network to a host in the 192.168.168/24 and 192.168.178/24 networks to bring the tunnels up. For route-based VPNs, you can send traffic initiated from the SRX Series device through the tunnel. We recommend that when testing IPsec tunnels, you send test traffic from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate a ping from 10.10.10.10 to 192.168.168.10.
From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@hub> show security ike security-associations
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
6       3.3.3.2         UP     94906ae2263bbd8e  1c35e4c3fc54d6d3  Main
7       2.2.2.2         UP     7e7a1c0367dfed73c  f284221c656a5fbc  Main

user@hub> show security ike security-associations index 6 detail
IKE peer 3.3.3.2, Index 6,
  Role: Responder, State: UP
  Initiator cookie: 94906ae2263bbd8e, Responder cookie: 1c35e4c3fc54d6d3
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 1.1.1.2:500, Remote: 3.3.3.2:500
  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: 1.1.1.2:500, Remote: 3.3.3.2:500
    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
```

Meaning

The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- **Index**—This value is unique for each IKE SA, which you can use in the `show security ike security-associations index index_number detail` command to get more information about the SA.
- **Remote Address**—Verify that the remote IP address is correct.
- **State**
  - **UP**—The Phase 1 SA has been established.
  - **DOWN**—There was a problem establishing the Phase 1 SA.
- **Mode**—Verify that the correct mode is being used.

Verify that the following information is correct in your configuration:

- **External interfaces (the interface must be the one that receives IKE packets)**
- **IKE policy parameters**
• Preshared key information
• Phase 1 proposal parameters (must match on both peers)

The `show security ike security-associations index 1 detail` command lists additional information about the security association with an index number of 1:

• Authentication and encryption algorithms used
• Phase 1 lifetime
• Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
• Initiator and responder role information

---

**NOTE:** Troubleshooting is best performed on the peer using the responder role.

---

• Number of IPsec SAs created
• Number of Phase 2 negotiations in progress

### Verifying the IPsec Phase 2 Status

**Purpose**  
Verify the IPsec Phase 2 status.

**Action**  
From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```
user@hub> show security ipsec security-associations
total configured sa: 4

ID    Gateway          Port  Algorithm          SPI      Life:sec/kb  Mon vsys
<16384 2.2.2.2         500   ESP:aes-128/sha1   b2fc36f8 3364/ unlim   -   0
>16384 2.2.2.2         500   ESP:aes-128/sha1   5d73929e 3364/ unlim   -   0

ID    Gateway          Port  Algorithm          SPI      Life:sec/kb  Mon vsys
<16385 3.3.3.2         500   ESP:3des/sha1      70f79c67 28756/unlim   -   0
>16385 3.3.3.2         500   ESP:3des/sha1      80f4126d 28756/unlim   -   0
```

```
user@hub> show security ipsec security-associations index 16385 detail
Virtual-system: Root
Local Gateway: 1.1.1.2, Remote Gateway: 3.3.3.2
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: -

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: -

Anti-replay service: enabled, Replay window size: 32

Meaning
The output from the `show security ipsec security-associations` command lists the following information:

- The ID number is 16385. Use this value with the `show security ipsec security-associations index` command to get more information about this particular SA.

- There is one IPsec SA pair using port 500, which indicates that no NAT-traversal is implemented. (NAT-traversal uses port 4500 or another random high-number port.)

- The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 28756/unlim value indicates that the Phase 2 lifetime expires in 28756 seconds, and that no lifesize has been specified, which indicates that it is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.

- VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U indicates that monitoring is up, and D indicates that monitoring is down.

- The virtual system (vsys) is the root system, and it always lists 0.

The output from the `show security ipsec security-associations index 16385 detail` command lists the following information:

- The local identity and remote identity make up the proxy ID for the SA.

A proxy ID mismatch is one of the most common causes for a Phase 2 failure. If no IPsec SA is listed, confirm that Phase 2 proposals, including the proxy ID settings, are correct for both peers. For route-based VPNs, the default proxy ID is local=0.0.0.0/0, remote=0.0.0.0/0, and service=any. Issues can occur with multiple route-based VPNs from the same peer IP. In this case, a unique proxy ID for each IPsec SA must be specified. For some third-party vendors, the proxy ID must be manually entered to match.

- Another common reason for Phase 2 failure is not specifying the ST interface binding. If IPsec cannot complete, check the kmd log or set traceoptions.

Verifying Next-Hop Tunnel Bindings

Purpose
After Phase 2 is complete for all peers, verify the next-hop tunnel bindings.

Action
From operational mode, enter the `show security ipsec next-hop-tunnels` command.

```
user@hub> show security ipsec next-hop-tunnels
```
Next-hop gateway | interface | IPSec VPN name | Flag
---|---|---|---
10.11.11.11 | st0.0 | sunnyvale-vpn | Static
10.11.11.12 | st0.0 | westford-vpn | Auto

**Meaning**
The next-hop gateways are the IP addresses for the st0 interfaces of all remote spoke peers. The next hop should be associated with the correct IPSec VPN name. If no NHTB entry exists, there is no way for the hub device to differentiate which IPSec VPN is associated with which next hop.

The Flag field has one of the following values:

- **Static**— NHTB was manually configured in the st0.0 interface configurations, which is required if the peer is not an SRX Series device.
- **Auto**— NHTB was not configured, but the entry was automatically populated into the NHTB table during Phase 2 negotiations between two SRX Series devices

There is no NHTB table for any of the spoke sites in this example. From the spoke perspective, the st0 interface is still a point-to-point link with only one IPSec VPN binding.

---

**Verifying Static Routes for Remote Peer Local LANs**

**Purpose**
Verify that the static route references the spoke peer’s st0 IP address.

**Action**
From operational mode, enter the `show route` command.

```plaintext
user@hub> show route 192.168.168.10
inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.168.0/24  *[Static/5] 00:08:33
  > to 10.11.11.11 via st0.0

user@hub> show route 192.168.178.10
inet.0: 9 destinations, 9 routes (9 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
192.168.178.0/24  *[Static/5] 00:04:04
  > to 10.11.11.12 via st0.0
```

The next hop is the remote peer’s st0 IP address, and both routes point to st0.0 as the outgoing interface.

---

**Reviewing Statistics and Errors for an IPsec Security Association**

**Purpose**
Review ESP and authentication header counters and errors for an IPsec security association.

**Action**
From operational mode, enter the `show security ipsec statistics index` command.

```plaintext
user@hub> show security ipsec statistics index 16385
ESP Statistics:
  Encrypted bytes: 920
  Decrypted bytes: 6208
  Encrypted packets: 5
```
Decrypted packets: 87

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

You can also use the **show security ipsec statistics** command to review statistics and errors for all SAs.

To clear all IPsec statistics, use the **clear security ipsec statistics** command.

**Meaning**
If you see packet loss issues across a VPN, you can run the **show security ipsec statistics** or **show security ipsec statistics detail** command several times to confirm that the encrypted and decrypted packet counters are incrementing. You should also check whether the other error counters are incrementing.

**Testing Traffic Flow Across the VPN**

**Purpose**
Verify the traffic flow across the VPN.

**Action**
You can use the **ping** command from the SRX Series device to test traffic flow to a remote host PC. Make sure that you specify the source interface so that the route lookup is correct and the appropriate security zones are referenced during policy lookup.

From operational mode, enter the **ping** command.

```
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
```

You can also use the **ping** command from the SSG Series device.

```
user@hub> ping 10.10.10.10 from ethernet0/6
Type escape sequence to abort
Sending 5, 100-byte ICMP Echos to 10.10.10.10, 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

**Meaning**  If the **ping** command fails from the SRX Series or SSG Series device, there might be a problem with the routing, security policies, end host, or encryption and decryption of ESP packets.

**Related Documentation**
- [Understanding Hub-and-Spoke VPNs on page 33](#)
- [Example: Configuring a Route-Based VPN on page 77](#)
- [Example: Configuring a Policy-Based VPN on page 143](#)
- [IPsec VPN Feature Guide for Security Devices](#)
CHAPTER 16

Loopback Interface for High Availability VPN

- Example: Configuring Redundancy Groups for Loopback Interfaces on page 223

**Example: Configuring Redundancy Groups for Loopback Interfaces**

**Supported Platforms**

| LN Series, SRX Series |

This example shows how to configure a redundancy group (RG) for a loopback interface in order to prevent VPN failure. Redundancy groups are used to bundle interfaces into a group for failover purpose in a chassis cluster setup.

- Requirements on page 223
- Overview on page 223
- Configuration on page 225
- Verification on page 228

**Requirements**

This example uses the following hardware and software:

- A pair of supported chassis cluster SRX Series devices
- An SSG140 device or equivalent
- Two switches
- Junos OS Release 12.1x44-D10 for SRX Series Services Gateways

Before you begin:

Understand chassis cluster redundant Ethernet interfaces. See *Understanding Chassis Cluster Redundant Ethernet Interfaces*.

**Overview**

An Internet Key Exchange (IKE) gateway needs an external interface to communicate with a peer device. In a chassis cluster setup, the node on which the external interface is active selects a Services Processing Unit (SPU) to support the VPN tunnel. IKE and IPsec
packets are processed on that SPU. Therefore, the active external interface decides the anchor SPU.

In a chassis cluster setup, this external interface can be the reth interface or a standalone interface. These interfaces can go down when the physical interfaces are down. Therefore, you can configure loopback interfaces to reach the peer gateway as they are alternate physical interfaces. Loopback interfaces can be configured on any redundancy group. This redundancy group configuration is only checked for VPN packets, because only VPN packets must find the anchor SPU through the active interface.

NOTE: You must configure lo0.x in customer virtual router, since lo0.0 is in default virtual router and only one loopback interface is allowed in one virtual router.

Figure 24 on page 225 shows an example of a loopback chassis cluster VPN topology. In this topology, the SRX Series chassis cluster device is located in Sunnyvale, California. The SRX Series chassis cluster device works as a single gateway in this setup. The SSG Series device (or a third-party device) is located in Chicago, Illinois. This device acts as a peer device to the SRX chassis cluster and it helps to build a VPN tunnel.
Figure 24: Loopback Interface for Chassis Cluster VPN

### Configuration

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network.
configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```
set interfaces lo0 redundant-pseudo-interface-options redundancy-group 1
set interfaces lo0 unit 1 family inet address 3.3.3.3/30
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 "$9$STheLNsYoUjqM8oGDkTQ/Ct"
set security ike gateway t-ike-gate ike-policy ike-policy1
set security ike gateway t-ike-gate address 2.2.2.2
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
set security ipsec vpn t-ike-vpn ike proxy-identity remote 192.168.168.1/24
set security ipsec vpn t-ike-vpn ike ipsec-policy vpn-policy1
```

**Step-by-Step Procedure**

To configure a redundancy group for a loopback interface:

1. Configure the loopback interface in one redundancy group.
   ```
   [edit interfaces]
   user@host# set lo0 redundant-pseudo-interface-options redundancy-group 1
   ```

2. Configure the IP address for the loopback interface.
   ```
   [edit interfaces]
   user@host# set lo0 unit 1 family inet address 3.3.3.3/30
   ```

3. Configure routing options.
   ```
   [edit routing-instances]
   user@host# set vr1 instance-type virtual-router
   user@host# set vr1 interface lo0.1
   user@host# set vr1 interface reth0.0
   user@host# set vr1 interface reth1.0
   user@host# set vr1 interface st0.0
   user@host# set vr1 routing-options static route 192.168.168.1/24 next-hop st0.0
   ```

4. Configure the loopback interface as an external interface for the IKE gateway.
   ```
   [edit security ike]
Configure an IPsec proposal.

```
[edit security ipsec]
user@host# set proposal p2-std-p1 authentication-algorithm hmac-sha1-96
data-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
```

Results  From configuration mode, confirm your configuration by entering the show interfaces lo0, show routing-instances, show security ike, and show security ipsec commands. If the output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

```
[edit]
user@host# show interfaces lo0
unit 1 {
  family inet {
    address 3.3.3.3/30;
  }
}
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 "$9$STheLNsYoUjQmBGoGkTQ/Ct";
    }
    gateway t-ike-gate {
        ike-policy ike-policy1;
        address 2.2.2.2;
        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;
        }
    }

If you are done configuring the device, enter commit from configuration mode.

Verification

**Verifying the Configuration**

**Purpose**
Verify that the configuration for redundancy groups for loopback interfaces is correct.
**Action**  
From operational mode, enter the `show chassis cluster interfaces` command.

```
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
```

**Meaning**  
The `show chassis cluster interfaces` command displays the chassis cluster interfaces information. If the status of the Redundant-pseudo-interface Information field shows the lo0 interface as Up and the status of the Redundant-ethernet Information field shows reth0, reth1, and reth2 fields as Up then your configuration is correct.

**Related Documentation**  
•  Understanding Loopback Interface for a High Availability VPN on page 35
IPv6 IPsec

IPv6 IPsec Configuration Overview on page 231
Example: Configuring Dual Stack Tunnels over an External Interface on page 232
Example: Configuring an IPv6 IPsec Manual VPN on page 242
Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN on page 244

IPv6 IPsec Configuration Overview

- IPv6 IPsec Configuration Overview on page 231
- Example: Configuring Dual Stack Tunnels over an External Interface on page 232
- Example: Configuring an IPv6 IPsec Manual VPN on page 242
- Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN on page 244

IPv6 IPsec Configuration Overview

Supported Platforms

J Series, LN Series, SRX Series

Juniper Networks supports manual and autokey IKE with preshared keys configurations for IPv6 IPsec VPN.

- Manual VPN—In a manual VPN configuration, the secret keys and security associations (SAs) are manually configured on the tunnel endpoints using the manual key mechanism. To create an IPv6 IPsec manual VPN, see "Example: Configuring an IPv6 IPsec Manual VPN" on page 242.

- AutoKey IKE VPN—In an autoKey IKE VPN configuration, the secret keys and SAs are automatically created using the autoKey IKE mechanism. To set up an IPv6 autoKey IKE VPN, two phases of negotiations are required—Phase 1 and Phase 2.
  - Phase 1—In this phase, the participants establish a secure channel for negotiating the IPsec SAs. For more information on Phase 1 negotiations, see "Understanding Phase 1 of IKE Tunnel Negotiation" on page 18.
  - Phase 2—In this phase, the participants negotiate the IPsec SAs for authenticating and encrypting the IPv6 data packets. For more information on Phase 2 negotiations, see "Understanding Phase 2 of IKE Tunnel Negotiation" on page 20.

To create an IPv6 autoKey IKE policy-based VPN, see "Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN" on page 244.

Related Documentation

- Understanding IPv6 IKE and IPsec Packet Processing on page 44
- Example: Configuring an IPv6 IPsec Manual VPN on page 242
- Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN on page 244
- IPsec VPN Feature Guide for Security Devices
Example: Configuring Dual Stack Tunnels over an External Interface

Supported Platforms
SRX Series

This example shows how to configure parallel IPv4 and IPv6 tunnels over a single external physical interface to a peer for route-based site-to-site VPNs.

- Requirements on page 232
- Overview on page 232
- Configuration on page 235
- Verification on page 239

Requirements

Before you begin, read “Understanding Dual Stack Tunnels over an External Interface” on page 43.

NOTE: The configuration shown in this example is only supported with route-based site-to-site VPNs.

Overview

In this example, a redundant Ethernet interface on the local device supports parallel IPv4 and IPv6 tunnels to a peer device:

- The IPv4 tunnel carries IPv6 traffic; it operates in IPv6-in-IPv4 tunnel mode. The secure tunnel interface st0.0 bound to the IPv4 tunnel is configured with family inet6 only.
- The IPv6 tunnel carries both IPv4 and IPv6 traffic; it operates in both IPv4-in-IPv6 and IPv6-in-IPv6 tunnel modes. The secure tunnel interface st0.1 bound to the IPv6 tunnel is configured with both family inet and family inet6.

Table 46 on page 232 shows the Phase 1 options used in this example. The Phase 1 option configuration includes two IKE gateway configurations, one to the IPv6 peer and the other to the IPv4 peer.

Table 46: Phase 1 Options for Dual Stack Tunnel Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE proposal</td>
<td>ike_proposal</td>
</tr>
<tr>
<td>Authentication method</td>
<td>Preshared keys</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>MD5</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>3DES CBC</td>
</tr>
<tr>
<td>Lifetime</td>
<td>3600 seconds</td>
</tr>
</tbody>
</table>
Table 46: Phase 1 Options for Dual Stack Tunnel Configuration (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE policy</td>
<td>ike_policy</td>
</tr>
<tr>
<td>Mode</td>
<td>Aggressive</td>
</tr>
<tr>
<td>IKE proposal</td>
<td>ike_proposal</td>
</tr>
<tr>
<td>Preshared key</td>
<td>ASCII text</td>
</tr>
<tr>
<td>IPv6 IKE gateway</td>
<td>ike_gw_v6</td>
</tr>
<tr>
<td>IKE policy</td>
<td>ike_policy</td>
</tr>
<tr>
<td>Gateway address</td>
<td>2000::2</td>
</tr>
<tr>
<td>External interface</td>
<td>reth1.0</td>
</tr>
<tr>
<td>IKE version</td>
<td>IKEv2</td>
</tr>
<tr>
<td>IPv4 IKE gateway</td>
<td>ike_gw_v4</td>
</tr>
<tr>
<td>IKE policy</td>
<td>ike_policy</td>
</tr>
<tr>
<td>Gateway address</td>
<td>20.0.0.2</td>
</tr>
<tr>
<td>External interface</td>
<td>reth1.0</td>
</tr>
</tbody>
</table>

Table 47 on page 233 shows the Phase 2 options used in this example. The Phase 2 option configuration includes two VPN configurations, one for the IPv6 tunnel and the other for the IPv4 tunnel.

Table 47: Phase 2 Options for Dual Stack Tunnel Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec proposal</td>
<td>ipsec_proposal</td>
</tr>
<tr>
<td>Protocol</td>
<td>ESP</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>HMAC SHA-1 96</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>3DES CBC</td>
</tr>
<tr>
<td>IPsec policy</td>
<td>ipsec_policy</td>
</tr>
<tr>
<td>Proposal</td>
<td>ipsec_proposal</td>
</tr>
<tr>
<td>IPv6 VPN</td>
<td>test_s2s_v6</td>
</tr>
</tbody>
</table>
Table 47: Phase 2 Options for Dual Stack Tunnel Configuration (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind interface</td>
<td>st0.1</td>
</tr>
<tr>
<td>IKE gateway</td>
<td>ike_gw_v6</td>
</tr>
<tr>
<td>IKE IPsec policy</td>
<td>ipsec_policy</td>
</tr>
<tr>
<td>Establish tunnels</td>
<td>Immediately</td>
</tr>
<tr>
<td>IPv4 VPN</td>
<td>test_s2s_v4</td>
</tr>
<tr>
<td>Bind interface</td>
<td>st0.0</td>
</tr>
<tr>
<td>IKE gateway</td>
<td>ike_gw_4</td>
</tr>
<tr>
<td>IKE IPsec policy</td>
<td>ipsec_policy</td>
</tr>
</tbody>
</table>

The following static routes are configured in the IPv6 routing table:

- Route IPv6 traffic to 3000::1/128 through st0.0.
- Route IPv6 traffic to 3000::2/128 through st0.1.

A static route is configured in the default (IPv4) routing table to route IPv4 traffic to 30.0.0.0/24 through st0.1.

**NOTE:** Flow-based processing of IPv6 traffic must be enabled with the `mode flow-based` configuration option at the `[edit security forwarding-options family inet6]` hierarchy level.

**Topology**

In Figure 25 on page 235, the SRX Series device A supports IPv4 and IPv6 tunnels to device B. IPv6 traffic to 3000::1/128 is routed through the IPv4 tunnel, while IPv6 traffic to 3000::2/128 and IPv4 traffic to 30.0.0.0/24 are routed through the IPv6 tunnel.
**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```plaintext
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 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 "S9ShLyeWNdsJGiLxGik-zFcyl"
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
```
To configure dual stack tunnels:

1. Configure the external interface.

```
[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. Configure the secure tunnel interfaces.

```
[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. Configure Phase 1 options.

```
[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 "$9$hdeWNg1LxGik.zFcyI"
```

```
[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. Configure Phase 2 options.
[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. Configure static routes.

[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


[edit security forwarding-options]
user@host# set family inet6 mode flow-based

Results  From configuration mode, confirm your configuration by entering the `show interfaces`, `show security ike`, `show security ipsec`, `show routing-options`, and `show security forwarding-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.
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 asciitext "$9$hdLyeWNdsJGlXGk.zFcy!"; ## 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;
    }
}

If you are done configuring the device, enter commit from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying IKE Phase 1 Status on page 239
- Verifying IPsec Phase 2 Status on page 240
- Verifying Routes on page 240

Verifying IKE Phase 1 Status

Purpose
Verify the IKE Phase 1 status.

Action
From operational mode, enter the show security ike security-associations command.

<table>
<thead>
<tr>
<th>Index</th>
<th>State</th>
<th>Initiator cookie</th>
<th>Responder cookie</th>
<th>Mode</th>
<th>Remote Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1081812113</td>
<td>UP</td>
<td>51d9e6df8a929624</td>
<td>7bc15bb40781a902</td>
<td>IKEv2</td>
<td>2000::2</td>
</tr>
<tr>
<td>1887118424</td>
<td>UP</td>
<td>d80b55b949b54f0a</td>
<td>b75ecc815529ae8f</td>
<td>Aggressive</td>
<td>20.0.0.2</td>
</tr>
</tbody>
</table>
Meaning

The `show security ike security-associations` command lists all active IKE Phase 1 SAs. If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration. Phase 1 proposal parameters must match on the peer devices.

Verifying IPsec Phase 2 Status

Purpose

Verify the IPsec Phase 2 status.

Action

From operational mode, enter the `show security ipsec security-associations` command.

```
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
```

Meaning

The `show security ipsec security-associations` command lists all active IKE Phase 2 SAs. If no SAs are listed, there was a problem with Phase 2 establishment. Check the IKE policy parameters and external interface settings in your configuration. Phase 2 proposal parameters must match on the peer devices.

Verifying Routes

Purpose

Verify active routes.

Action

From operational mode, enter the `show route` command.

```
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: 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
Local via reth1.0

Meaning  The `show route` command lists active entries in the routing tables.

Related Documentation  •  Understanding Dual Stack Tunnels over an External Interface on page 43
  •  Understanding VPN Tunnel Modes on page 37
  •  IPsec VPN Feature Guide for Security Devices
Example: Configuring an IPv6 IPsec Manual VPN

Supported Platforms

J Series, LN Series, SRX Series

This example shows how to configure an IPv6 IPsec manual VPN.

• Requirements on page 242
• Overview on page 242
• Configuration on page 242
• Verification on page 244

Requirements

Before you begin:

• Understand how VPNs work. See “VPN Overview” on page 3.
• Understand IPv6 IPsec packet processing. See “Understanding IPv6 IKE and IPsec Packet Processing” on page 44.

Overview

In a Manual VPN configuration, the secret keys are manually configured on the two IPsec endpoints.

In this example, you:

• Configure the authentication parameters for a VPN named vpn-sunnyvale.
• Configure the encryption parameters for vpn-sunnyvale.
• Specify the outgoing interface for the SA.
• Specify the IPv6 address of the peer.
• Define the IPsec protocol. Select the ESP protocol because the configuration includes both authentication and encryption.
• Configure a security parameter index (SPI).

Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
set security ipsec vpn vpn-sunnyvale manual authentication algorithm hmac-md5–96
key ascii-text 1111111111111111
set security ipsec vpn vpn-sunnyvale manual encryption algorithm 3des-cbc key ascii-text 111111111111111111111111
set security ipsec vpn vpn-sunnyvale manual external-interface ge-0/0/14.0
set security ipsec vpn vpn-sunnyvale manual gateway 1212::1112
set security ipsec vpn vpn-sunnyvale manual protocol esp
```
set security ipsec vpn vpn-sunnyvale manual spi 12435

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security algorithms:

1. Configure the authentication parameters.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set authentication algorithm hmac-md5–96 key ascii-text 111111111111111111111111
   ```

2. Configure the encryption parameters.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set encryption algorithm 3des-cbc key ascii-text 111111111111111111111111
   ```

3. Specify the outgoing interface for the SA.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set external-interface ge-0/0/14.0
   ```

4. Specify the IPv6 address of the peer.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set gateway 1212::1112
   ```

5. Define the IPsec protocol.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set protocol esp
   ```

6. Configure an SPI.

   ```
   [edit security ipsec vpn vpn-sunnyvale manual]
   user@host# set spi 12435
   ```

Results

From configuration mode, confirm your configuration by entering the `show security ipsec vpn vpn-sunnyvale` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
[user@host]show security ipsec vpn vpn-sunnyvale manual {
  gateway 1212::1112 ;
  external-interface ge-0/0/14.0 ;
  protocol esp ;
  spi 12435 ;
  authentication {
    algorithm hmac-md5-96 ;
    key ascii-text $9$P5369Ap01R3nSreK8LZUDImfTz36CtmP01REyrs2goUjHqm" ;## SECRET DATA
  }
  encryption {
    algorithm 3des-cbc ;
    key ascii-text $9$DRimfTz36tmP01REyrs2goUjHqmfQFUD/CtpB1xN-V24aZU" ;## SECRET DATA
  }
}
```
Verification

To confirm that the configuration is working properly, perform this task:

- Verifying Security Algorithms on page 244

### Verifying Security Algorithms

**Purpose**

Determine if security algorithms are applied or not.

**Action**

From operational mode, enter the `show security ipsec security-associations` command.

**Related Documentation**

- Understanding IPv6 IKE and IPsec Packet Processing on page 44
- IPv6 IPsec Configuration Overview on page 231
- Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN on page 244
- IPsec VPN Feature Guide for Security Devices

---

**Example: Configuring an IPv6 AutoKey IKE Policy-Based VPN**

**Supported Platforms**

J Series, LN Series, SRX100, SRX210, SRX240, SRX650

This example shows how to configure a policy-based IPv6 AutoKey IKE VPN to allow IPv6 data to be securely transferred between the branch office and the corporate office.

---

**NOTE:** IPv6 policy-based VPNs are supported only on standalone branch SRX Series devices.

- Requirements on page 244
- Overview on page 245
- Configuration on page 249
- Verification on page 258

**Requirements**

This example uses the following hardware:

- SRX240 device

Before you begin:

- Understand how VPNs work. See “VPN Overview” on page 3.
- Understand IPv6 IKE and IPsec packet processing. See “Understanding IPv6 IKE and IPsec Packet Processing” on page 44.
Overview

In this example, you configure an IPv6 IKE policy-based VPN for a branch office in Chicago, Illinois, because you do not need to conserve tunnel resources or configure many security policies to filter traffic through the tunnel. Users in the Chicago office will use the VPN to connect to their corporate headquarters in Sunnyvale, California.

Figure 26 on page 246 shows an example of an IPv6 IKE policy-based VPN topology. In this topology, one SRX Series device is located in Sunnyvale, and another SRX Series device (this can be a second SRX Series device or a third-party device) is located in Chicago.
In this example, you configure interfaces, an IPv6 default route, security zones, and address books. Then you configure IKE Phase 1, IPsec Phase 2, a security policy, and TCP-MSS parameters. See Table 48 on page 247 through Table 52 on page 249.
### Table 48: Interface, Security Zone, and Address Book Information

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interfaces</td>
<td>ge-0/0/14.0</td>
<td>1212::1111/64</td>
</tr>
<tr>
<td></td>
<td>ge-0/0/15.0</td>
<td>1111::1111/64</td>
</tr>
</tbody>
</table>
| Security zones| trust        | • All system services are allowed.  
                |               | • The ge-0/0/14.0 interface is bound to this zone. |
|               | untrust      | • IKE is the only allowed system service.  
                |               | • The ge-0/0/15.0 interface is bound to this zone. |
| Address book entries | sunnyvale    | • This address is for the trust zone’s address book.  
                          |               | • The address for this address book entry is 1212::abcd/64. |
|               | chicago      | • This address is for the untrust zone’s address book.  
                          |               | • The address for this address book entry is 1111::abcd/128. |

### Table 49: IPv6 IKE Phase 1 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal      | ipv6-ike-phase1-proposal    | • Authentication method: pre-shared-keys  
                |               | • Diffie-Hellman group: group2  
                |               | • Authentication algorithm: sha1  
                |               | • Encryption algorithm: aes-128-cbc |
| Policy        | ipv6-ike-phase1-policy      | • Mode: Aggressive  
                |               | • Proposal reference: ipv6-ike-phase1-proposal  
                |               | • IKE Phase 1 policy authentication method: pre-shared-key ascii-text |
| Gateway       | gw-chicago                  | • IKE policy reference: ipv6-ike-phase1-policy  
                |               | • External interface: ge-0/0/15.0  
                |               | • Gateway address: 1111::1112/64 |

### Table 50: IPv6 IPsec Phase 2 Configuration Parameters

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
</table>
| Proposal      | ipv6-ipsec-phase2-proposal  | • Protocol: esp  
                |               | • Authentication algorithm: hmac-sha1-96  
                |               | • Encryption algorithm: aes-128-cbc |
Table 50: IPv6 IPsec Phase 2 Configuration Parameters (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy</td>
<td>ipv6-ipsec-phase2-policy</td>
<td>• Proposal reference: ipv6-ipsec-phase2-proposal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PFS: Diffie-Hellman group2</td>
</tr>
<tr>
<td>VPN</td>
<td>ipv6-ike-vpn-chicago</td>
<td>• IKE gateway reference: gw-chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IPsec policy reference: ipv6-ipsec-phase2-policy</td>
</tr>
</tbody>
</table>

Table 51: Security Policy Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Name</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>This security policy permits traffic from the trust zone to the untrust zone.</td>
<td>ipv6-vpn-tr-untr</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-address sunnyvale</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• destination-address chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit action: tunnel ipsec-vpn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit action: tunnel pair-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipv6-ike-vpn-chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipv6-vpn-untr-tr</td>
</tr>
<tr>
<td>This security policy permits traffic from the untrust zone to the trust zone.</td>
<td>ipv6-vpn-untr-tr</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-address chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• destination-address sunnyvale</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit action: tunnel ipsec-vpn</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Permit action: tunnel pair-policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipv6-ike-vpn-chicago</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ipv6-VPN-tr-untr</td>
</tr>
<tr>
<td>This security policy permits all traffic from the trust zone to the untrust zone.</td>
<td>permit-any</td>
<td>• Match criteria:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-address any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source-destination any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• application any</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Action: permit</td>
</tr>
</tbody>
</table>

NOTE: You must put the ipv6-VPN-tr-untr policy before the permit-any security policy. Junos OS performs a security policy lookup starting at the top of the list. If the permit-any policy comes before the ipv6-VPN-tr-untr policy, all traffic from the trust zone will match the permit-any policy and be permitted. Thus, no traffic will ever match the ipv6-VPN-tr-untr policy.
Table 52: TCP-MSS Configuration Parameters

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Configuration Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSS value: 1350</td>
<td>TCP-MSS is negotiated as part of the TCP three-way handshake and limits the maximum size of a TCP segment to better fit the MTU limits on a network. This is especially important for VPN traffic, as the IPsec encapsulation overhead, along with the IP and frame overhead, can cause the resulting ESP packet to exceed the MTU of the physical interface, thus causing fragmentation. Fragmentation results in increased use of bandwidth and device resources.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>We recommend a value of 1350 as the starting point for most Ethernet-based networks with an MTU of 1500 or greater. You might need to experiment with different TCP-MSS values to obtain optimal performance. For example, you might need to change the value if any device in the path has a lower MTU, or if there is any additional overhead such as PPP or Frame Relay.</td>
</tr>
</tbody>
</table>

**Configuration**

**Configuring Basic Network, Security Zone, and Address Book Information**

- CLI Quick Configuration
  - To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
set interfaces ge-0/0/14 unit 0 family inet6 address 1212::1111/64  
set interfaces ge-0/0/15 unit 0 family inet6 address 1111::1111/64  
set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1  
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 1212::abcd/64  
set security address-book book1 attach zone trust  
set security address-book book2 address chicago 1111::abcd/64  
set security address-book book2 attach zone untrust
```

- Step-by-Step Procedure
  - The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure basic network, security zone, and address book information:

1. Configure Ethernet interface information.
   - `[edit]`
   - `user@host# set interfaces ge-0/0/14 unit 0 family inet6 address 1212::1111/64`
   - `user@host# set interfaces ge-0/0/15 unit 0 family inet6 address 1111::1111/64`

2. Configure static route information.
   - `[edit]`
   - `user@host# set routing-options static route 0.0.0.0/0 next-hop 1.1.1.1`

3. Configure the untrust security zone.
   - `[edit]`
   - `user@host# edit security zones security-zone untrust`
4. Assign an interface to the untrust security zone.
   
   [edit security zones security-zone untrust]
   user@host# set interfaces ge-0/0/15.0

5. Specify allowed system services for the untrust security zone.
   
   [edit security zones security-zone untrust]
   user@host# set host-inbound-traffic system-servicesike

6. Configure the trust security zone.
   
   [edit]
   user@host# edit security zones security-zone trust

7. Assign an interface to the trust security zone.
   
   [edit security zones security-zone trust]
   user@host# set interfaces ge-0/0/14.0

8. Specify allowed system services for the trust security zone.
   
   [edit security zones security-zone trust]
   user@host# set host-inbound-traffic system-servicesall

9. Create an address book and attach a zone to it.
   
   [edit security address-book book1]
   user@host# set address sunnyvale 1212::abcd/64
   user@host# set attach zone trust

10. Create another address book and attach a zone to it.
    
    [edit security address-book book2]
    user@host# set address chicago 1111::abcd/64
    user@host# set attach zone untrust

**Results**

From configuration mode, confirm your configuration by entering the `show interfaces`, `show routing-options`, `show security zones`, and `show security address-book` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces
ge-0/0/14 {
  unit 0 {
    family inet6 {
      address 1212::1111/64;
    }
  }
}
ge-0/0/15 {
  unit 0 {
    family inet6 {
      address 1111::1111/64;
    }
  }
}
[edit]
```
user@host# show routing-options
static {
    route 0.0.0.0/0 next-hop 1.1.1.1;
}

[edit]
user@host# show security zones
security-zone untrust {
    host-inbound-traffic {
        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 1212::abcd/64;
    attach {
        zone trust;
    }
}
book2 {
    address chicago 1111::abcd/64;
    attach {
        zone untrust;
    }
}

If you are done configuring the device, enter commit from configuration mode.

Configuring IKE

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

set security ike proposal ipv6-ike-phase1-proposal authentication-method pre-shared-keys
set security ike proposal ipv6-ike-phase1-proposal dh-group group2
set security ike proposal ipv6-ike-phase1-proposal authentication-algorithm sha1
set security ike proposal ipv6-ike-phase1-proposal encryption-algorithm aes-128-cbc
set security ike policy ipv6-ike-phase1-policy mode aggressive
To configure IKE:

1. Create the IKE Phase 1 proposal.
   ```
   [edit security ike]
   user@host# set proposal ipv6-ike-phase1-proposal
   ```

2. Define the IKE proposal authentication method.
   ```
   [edit security ike proposal ipv6-ike-phase1-proposal]
   user@host# set authentication-method pre-shared-keys
   ```

3. Define the IKE proposal Diffie-Hellman group.
   ```
   [edit security ike proposal ipv6-ike-phase1-proposal]
   user@host# set dh-group group2
   ```

4. Define the IKE proposal authentication algorithm.
   ```
   [edit security ike proposal ipv6-ike-phase1-proposal]
   user@host# set authentication-algorithm sha1
   ```

5. Define the IKE proposal encryption algorithm.
   ```
   [edit security ike proposal ipv6-ike-phase1-proposal]
   user@host# set encryption-algorithm aes-128-cbc
   ```

6. Create an IKE Phase 1 policy.
   ```
   [edit security ike]
   user@host# set policy ipv6-ike-phase1-policy
   ```

7. Set the IKE Phase 1 policy mode.
   ```
   [edit security ike policy ipv6-ike-phase1-policy]
   user@host# set mode aggressive
   ```

8. Specify a reference to the IKE proposal.
   ```
   [edit security ike policy ipv6-ike-phase1-policy]
   user@host# set proposals ipv6-ike-phase1-proposal
   ```

9. Define the IKE Phase 1 policy authentication method.
   ```
   [edit security ike policy ipv6-ike-phase1-policy]
   user@host# set pre-shared-key ascii-text 1111111111111111
   ```

10. Create an IKE Phase 1 gateway and define its external interface.
    ```
        [edit security ike]
        user@host# set gateway gw-chicago external-interface ge-0/0/15.0
    ```

11. Define the IKE Phase 1 policy reference.
[edit security ike gateway gw-chicago]
user@host# set ike-policy ipv6-ike-phase1-policy

12. Assign an IP address to the IKE Phase 1 gateway.

[edit security ike gateway gw-chicago]
user@host# set address 1111::1112

Results From configuration mode, confirm your configuration by entering the show security ike command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[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 "$9$jrHP5QFn/ApPfBIEhr1Yg4aDik.P5z3Dj9ApulI7—dbgoJGD";
  ### SECRET-DATA
}

gateway gw-chicago {
  ike-policy ipv6-ike-phase1-policy;
  address 1111::1112;
  external-interface ge-0/0/15.0;
}

If you are done configuring the device, enter commit from configuration mode.

Configuring IPsec

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

set security ipsec proposal ipv6-ipsec-phase2-proposal protocol esp
set security ipsec proposal ipv6-ipsec-phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal ipv6-ipsec-phase2-proposal encryption-algorithm aes-128-cbc
set security ipsec policy ipv6-ipsec-phase2-policy proposals ipv6-ipsec-phase2-proposal
set security ipsec policy ipv6-ipsec-phase2-policy perfect-forward-secrecy keys group2
set security ipsec vpn ipv6-ike-vpn-chicago ike gateway gw-chicago
set security ipsec vpn ipv6-ike-vpn-chicago ike ipv6-ipsec-policy ipsec-phase2-policy
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure IPsec:

1. Create an IPsec Phase 2 proposal.
   
   [edit]
   user@host# set security ipsec proposal ipv6-ipsec-phase2-proposal

2. Specify the IPsec Phase 2 proposal protocol.
   
   [edit security ipsec proposal ipv6-ipsec-phase2-proposal]
   user@host# set protocol esp

3. Specify the IPsec Phase 2 proposal authentication algorithm.
   
   [edit security ipsec proposal ipv6-ipsec-phase2-proposal]
   user@host# set authentication-algorithm hmac-sha1-96

4. Specify the IPsec Phase 2 proposal encryption algorithm.
   
   [edit security ipsec proposal ipv6-ipsec-phase2-proposal]
   user@host# set encryption-algorithm aes-128-cbc

5. Create the IPsec Phase 2 policy.
   
   [edit security ipsec]
   user@host# set policy ipv6-ipsec-phase2-policy

6. Specify the IPsec Phase 2 proposal reference.
   
   [edit security ipsec policy ipv6-ipsec-phase2-policy]
   user@host# set proposals ipv6-ipsec-phase2-proposal

7. Specify IPsec Phase 2 PFS to use Diffie-Hellman group 2.
   
   [edit security ipsec policy ipv6-ipsec-phase2-policy]
   user@host# set perfect-forward-secrecy keys group2

8. Specify the IKE gateway.
   
   [edit security ipsec]
   user@host# set vpn ipv6-ike-vpn-chicago ike gateway gw-chicago

9. Specify the IPsec Phase 2 policy.
   
   [edit security ipsec]
   user@host# set vpn ipv6-ike-vpn-chicago ike policy ipv6-ipsec-phase2-policy

Results

From configuration mode, confirm your configuration by entering the show security ipsec command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show security ipsec
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;
    }
}

If you are done configuring the device, enter `commit` from configuration mode.

**Configuring Security Policies**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level.

```plaintext
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
```

Copyright © 2016, Juniper Networks, Inc.
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure security policies:

1. Create the security policy to permit traffic from the trust zone to the untrust zone.

   [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. Create the security policy to permit traffic from the untrust zone to the trust zone.

   [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. Create the security policy to permit traffic from the trust zone to the untrust zone.

   [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. Reorder the security policies so that the vpn-tr-untr security policy is placed above the permit-any security policy.

   [edit security policies from-zone trust to-zone untrust]
   user@host# insert policy ipv6-vpn-tr-untr before policy permit-any

Results

From configuration mode, confirm your configuration by entering the show security policies command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   [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;
        }
      }
    }
  }
}

If you are done configuring the device, enter commit from configuration mode.

Configuring TCP-MSS

To quickly configure this section of the example, copy the following command, paste it into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the [edit] hierarchy level.

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

Step-by-Step Procedure

To configure TCP-MSS information:

1. Configure TCP-MSS information.

```
[edit]
user@host# set security flow tcp-mss ipsec-vpn mss 1350
```
Results  From configuration mode, confirm your configuration by entering the `show security flow` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

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

If you are done configuring the device, enter `commit` from configuration mode.

Verification  To confirm that the configuration is working properly, perform these tasks:

- Verifying the IKE Phase 1 Status on page 258
- Verifying the IPsec Phase 2 Status on page 260

Verifying the IKE Phase 1 Status  Purpose  Verify the IKE Phase 1 status.

Action  NOTE: Before starting the verification process, you need to send traffic from a host in Sunnyvale to a host in Chicago. For policy-based VPNs, a separate host must generate the traffic; traffic initiated from the SRX Series device will not match the VPN policy. We recommend that the test traffic be from a separate device on one side of the VPN to a second device on the other side of the VPN. For example, initiate ping from 1212::abcd/64 to 1111::abcd/128.

From operational mode, enter the `show security ike security-associations` command. After obtaining an index number from the command, use the `show security ike security-associations index index_number detail` command.

```
user@host> show security ike security-associations
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
5      1111::1112        UP     e48efd6a444853cf  0d09c59aaf7b20be  Aggressive

user@host> show security ike security-associations index 5 detail
IKE peer 1111::1112, Index 5,
  Role: Initiator, State: UP
  Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aaf7b20be
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 1111::1111:500, Remote: 1111::1112:500
  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: 1111::1111:500, Remote: 1111::1112:500
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

Meaning

The show security ike security-associations command lists all active IKE Phase 1 security associations (SAs). If no SAs are listed, there was a problem with Phase 1 establishment. Check the IKE policy parameters and external interface settings in your configuration.

If SAs are listed, review the following information:

- Index—This value is unique for each IKE SA, which you can use in the show security ike security-associations index index_number detail command to get more information about the SA.
- Remote Address—Verify that the remote IP address is correct.
- State
  - UP—The Phase 1 SA has been established.
  - DOWN—There was a problem establishing the Phase 1 SA.
- Mode—Verify that the correct mode is being used.

Verify that the following are correct in your configuration:

- External interfaces (the interface must be the one that receives IKE packets)
- IKE policy parameters
- Preshared key information
- Phase 1 proposal parameters (must match on both peers)

The show security ike security-associations index 5 detail command lists additional information about the security association with an index number of 5:

- Authentication and encryption algorithms used
- Phase 1 lifetime
- Traffic statistics (can be used to verify that traffic is flowing properly in both directions)
- Initiator and responder role information
NOTE: Troubleshooting is best performed on the peer using the responder role.

- Number of IPsec SAs created
- Number of Phase 2 negotiations in progress

### Verifying the IPsec Phase 2 Status

**Purpose**
Verify the IPsec Phase 2 status.

**Action**
From operational mode, enter the `show security ipsec security-associations` command. After obtaining an index number from the command, use the `show security ipsec security-associations index index_number detail` command.

```bash
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   1111::1112
2    ESP:aes-128/sha1 9a4db486 3597/ unlim   -   root 500   1111::1112

user@host> show security ipsec security-associations index 2 detail
Virtual-system: Root
Local Gateway: 111::1111, Remote Gateway: 1111::1112
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
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
Anti-replay service: counter-based enabled, Replay window size: 64
```

**Meaning**
The output from the `show security ipsec security-associations` command lists the following information:

- The ID number is 2. Use this value with the `show security ipsec security-associations index` command to get more information about this particular SA.

- There is one IPsec SA pair using port 500, which indicates that no NAT-traversal is implemented. (NAT-traversal uses port 4500 or another random high-number port.)
The SPIs, lifetime (in seconds), and usage limits (or lifesize in KB) are shown for both directions. The 3597/unlim value indicates that the Phase 2 lifetime expires in 3597 seconds, and that no lifesize has been specified, which indicates that the lifetime is unlimited. Phase 2 lifetime can differ from Phase 1 lifetime, as Phase 2 is not dependent on Phase 1 after the VPN is up.

VPN monitoring is not enabled for this SA, as indicated by a hyphen in the Mon column. If VPN monitoring is enabled, U (up) or D (down) is listed.

The virtual system (vsys) is the root system, and it always lists 0.

The output from the `show security ipsec security-associations index 2 detail` command lists the following information:

- The local and remote identities make up the proxy ID for the SA.

  A proxy ID mismatch is one of the most common reasons for a Phase 2 failure. For policy-based VPNs, the proxy ID is derived from the security policy. The local and remote addresses are derived from the address book entries, and the service is derived from the application configured for the policy. If Phase 2 fails because of a proxy ID mismatch, you can use the policy to confirm which address book entries are configured. Verify that the addresses match the information being sent. Check the service to ensure that the ports match the information being sent.

  **NOTE:** For some third-party vendors, the proxy ID must be manually entered to match.

---

**Related Documentation**

- Understanding IPv6 IKE and IPsec Packet Processing on page 44
- IPv6 IPsec Configuration Overview on page 231
- Example: Configuring an IPv6 IPsec Manual VPN on page 242
- IPsec VPN Feature Guide for Security Devices
CHAPTER 18

Traffic Selectors

- Example: Configuring Traffic Selectors in a Route-Based VPN on page 263

Example: Configuring Traffic Selectors in a Route-Based VPN

Supported Platforms SRX Series

This example shows how to configure traffic selectors for a route-based VPN.

- Requirements on page 263
- Overview on page 263
- Configuration on page 266
- Verification on page 275

Requirements

Before you begin, read "Understanding Traffic Selectors in Route-Based VPNs" on page 51.

NOTE: The configuration shown in this example is supported only with route-based VPNs with IKEv1.

Overview

This example configures traffic selectors to allow traffic to flow between subnetworks on an SRX650 and subnetworks on an SRX3400.

Table 53 on page 263 shows the traffic selectors used in this example. Traffic selectors are configured with other Phase 2 options (shown in Table 55 on page 265).

Table 53: Traffic Selector Configurations

<table>
<thead>
<tr>
<th>SRX650 Traffic Selector Name</th>
<th>Local IP</th>
<th>Remote IP</th>
<th>SRX3400 Traffic Selector Name</th>
<th>Local IP</th>
<th>Remote IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS1-ipv6</td>
<td>10::0/64</td>
<td>20::0/64</td>
<td>TS1-ipv6</td>
<td>20::0/64</td>
<td>10::0/64</td>
</tr>
</tbody>
</table>

Copyright © 2016, Juniper Networks, Inc.
### Table 53: Traffic Selector Configurations (continued)

<table>
<thead>
<tr>
<th>Traffic Selector Name</th>
<th>SRX650</th>
<th>SRX3400</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Remote IP</td>
<td>Remote IP</td>
</tr>
<tr>
<td>TS2-ipv4</td>
<td>20.1.0.0/16</td>
<td>10.1.1.0/24</td>
</tr>
<tr>
<td>TS3-ipv4</td>
<td>20.1.1.0/24</td>
<td>10.1.1.0/24</td>
</tr>
</tbody>
</table>

Table 54 on page 264 shows the Phase 1 options used in this example. The Phase 1 option configuration on each device includes an IKE gateway configuration to the IPv6 peer.

### Table 54: Phase 1 Options for Traffic Selector Configurations

<table>
<thead>
<tr>
<th>Option</th>
<th>SRX650</th>
<th>SRX3400</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE proposal</td>
<td>phase1_psk_proposal</td>
<td>phase1_psk_proposal</td>
</tr>
<tr>
<td>Authentication method</td>
<td>preshared keys</td>
<td>preshared keys</td>
</tr>
<tr>
<td>DH group</td>
<td>group2</td>
<td>group2</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>SHA 1</td>
<td>SHA 1</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>3DES CBC</td>
<td>3DES CBC</td>
</tr>
<tr>
<td>Lifetime</td>
<td>180 seconds</td>
<td>180 seconds</td>
</tr>
<tr>
<td>IKE policy</td>
<td>ike_psk_policy</td>
<td>ike_psk_policy</td>
</tr>
<tr>
<td>Mode</td>
<td>main</td>
<td>main</td>
</tr>
<tr>
<td>Proposal</td>
<td>phase1_psk_proposal</td>
<td>phase1_psk_proposal</td>
</tr>
<tr>
<td>Preshared key</td>
<td>ASCII text</td>
<td>ASCII text</td>
</tr>
<tr>
<td>IKE gateway</td>
<td>ike-gateway-to-he-srx</td>
<td>ike-gateway-to-branch-srx</td>
</tr>
<tr>
<td>IKE policy</td>
<td>ike_psk_policy</td>
<td>ike_psk_policy</td>
</tr>
<tr>
<td>Gateway address</td>
<td>2000::2</td>
<td>2000::1</td>
</tr>
<tr>
<td>External interface</td>
<td>ge-0/0/1.0</td>
<td>ge-0/0/1.0</td>
</tr>
<tr>
<td>Local address</td>
<td>2000::1</td>
<td>2000::2</td>
</tr>
<tr>
<td>IKE version</td>
<td>v1-only (default)</td>
<td>v1-only</td>
</tr>
</tbody>
</table>
Table 55 on page 265 shows the Phase 2 options used in this example. Traffic selectors shown in Table 53 on page 263 are configured with the Phase 2 options.

### Table 55: Phase 2 Options for Traffic Selector Configurations

<table>
<thead>
<tr>
<th>Option</th>
<th>SRX650</th>
<th>SRX3400</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec proposal</td>
<td>phase2-proposal</td>
<td>phase2-proposal</td>
</tr>
<tr>
<td>Protocol</td>
<td>ESP</td>
<td>ESP</td>
</tr>
<tr>
<td>Authentication algorithm</td>
<td>HMAC SHA-1 96</td>
<td>HMAC SHA-1 96</td>
</tr>
<tr>
<td>Encryption algorithm</td>
<td>DES CBC</td>
<td>DES CBC</td>
</tr>
<tr>
<td>IPSec policy</td>
<td>ipsec-policy</td>
<td>ipsec-policy</td>
</tr>
<tr>
<td>Proposal</td>
<td>phase2-proposal</td>
<td>phase2-proposal</td>
</tr>
<tr>
<td>VPN</td>
<td>ipsec-vpn-to-he-srx</td>
<td>ipsec-vpn-to-branch-srx</td>
</tr>
<tr>
<td>Bind interface</td>
<td>st0.1</td>
<td>st0.1</td>
</tr>
<tr>
<td>IKE gateway</td>
<td>ike-gateway-to-he-srx</td>
<td>ike-gateway-to-branch-srx</td>
</tr>
<tr>
<td>IPSec policy</td>
<td>ipsec-policy</td>
<td>ipsec-policy</td>
</tr>
</tbody>
</table>

**NOTE:** On both devices, flow-based processing of IPv6 traffic must be enabled with the mode flow-based configuration option at the [edit security forwarding-options family inet6] hierarchy level.

### Topology

In Figure 27 on page 265, an IPv6 VPN tunnel carries both IPv4 and IPv6 traffic between the SRX650 and the SRX3400 devices. That is, the tunnel operates in both IPv4-in-IPv6 and IPv6-in-IPv6 tunnel modes.

### Figure 27: Traffic Selector Configuration Example
Configuration

- Configuring the SRX650 on page 266
- Configuring the SRX3400 on page 270

**Configuring the SRX650**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level and then enter commit from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet6 address 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 inet6 address 10.1.1.1/24
set security ike proposal phase1_psk_proposal authentication-method pre-shared-keys
set security ike proposal phase1_psk_proposal dh-group group2
set security ike proposal phase1_psk_proposal authentication-algorithm sha1
set security ike proposal phase1_psk_proposal encryption-algorithm 3des-cbc
set security ike proposal phase1_psk_proposal lifetime-seconds 180
set security ike policy ike_psk_policy mode main
set security ike policy ike_psk_policy proposals phase1_psk_proposal
set security ike policy ike_psk_policy pre-shared-key ascii-text "$9$49oDkST39TOfnORcLXwYgoUjk.PQ36"
set security ike gateway ike-gateway-to-he-srx ike-policy ike_psk_policy
set security ike gateway ike-gateway-to-he-srx address 2000::2
set security ike gateway ike-gateway-to-he-srx external-interface ge-0/0/1.0
set security ike gateway ike-gateway-to-he-srx local-address 2000::1
set security ipsec proposal phase2-proposal protocol esp
set security ipsec proposal phase2-proposal authentication-algorithm hmac-sha1-96
set security ipsec proposal phase2-proposal encryption-algorithm 3des-cbc
set security ipsec policy ipsec_policy proposals phase2-proposal
set security ipsec vpn ipsec-vpn-to-he-srx bind-interface st0.1
set security ipsec vpn ipsec-vpn-to-he-srx ike ipsec-policy ipsec_policy
set security ipsec vpn ipsec-vpn-to-he-srx ike gateway ike-gateway-to-he-srx
set security ipsec vpn ipsec-vpn-to-he-srx traffic-selector TS1-ipv6 local-ip 10::/64
  remote-ip 20::/64
set security ipsec vpn ipsec-vpn-to-he-srx traffic-selector TS2-ipv4 local-ip 10.1.1.0/24
  remote-ip 20.1.1.0/16
set security ipsec vpn ipsec-vpn-to-he-srx traffic-selector TS3-ipv4 local-ip 10.1.1.0/24
  remote-ip 20.1.1.0/24
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 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 st0.1
set security policies default-policy permit-all
```
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode in the CLI User Guide.

To configure traffic selectors:

1. Configure the external interface.
   ```
   [edit interfaces]
   user@host# set ge-0/0/1 unit 0 family inet6 address 2000::1/64
   ```

2. Configure the secure tunnel interface.
   ```
   [edit interfaces]
   user@host# set st0 unit 1 family inet
   user@host# set st0 unit 1 family inet6
   ```

3. Configure the internal interface.
   ```
   [edit interfaces]
   user@host# set ge-1/0/1 unit 0 family inet address 10.1.1.1/24
   user@host# set ge-1/0/1 unit 0 family inet6 address 10::1/64
   ```

4. Configure Phase 1 options.
   ```
   [edit security ike proposal phase1_psk_proposal]
   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
   user@host# set lifetime-seconds 180
   ```

   ```
   [edit security ike policy ike_psk_policy]
   user@host# set mode main
   user@host# set proposals phase1_psk_proposal
   user@host# set pre-shared-key ascii-text
   "$9S49oDk5T39tOFnORclLXwYgoUjk.PQ36"
   ```

   ```
   [edit security ike gateway ike-gateway-to-he-srx]
   user@host# set ike-policy ike_psk_policy
   user@host# set address 2000::2
   user@host# set external-interface ge-0/0/1.0
   user@host# set local-address 2000::1
   ```

5. Configure Phase 2 options.
   ```
   [edit security ipsec proposal phase2-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 phase2-proposal
   ```

   ```
   [edit security ipsec vpn ipsec-vpn-to-he-srx]
   user@host# set bind-interface st0.1
   user@host# set ike gateway ike-gateway-to-he-srx
   ```

   [edit security forwarding-options]
   user@host# set family inet6 mode flow-based

7. Configure security zones and the security policy.

   [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 all
   user@host# set host-inbound-traffic protocols all
   user@host# set interfaces st0.1
   user@host# set interfaces ge-0/0/1.0

   [edit security policies]
   user@host# set default-policy permit-all

Results  From configuration mode, confirm your configuration by entering the `show interfaces`, `show security ike`, `show security ipsec`, `show security forwarding-options`, `show security zones`, and `show security policies` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

   [edit]
   user@host# show interfaces
   ge-0/0/1 { unit 0 { family inet6 { address 2000::1/64; } }
   ge-1/0/1 { unit 0 { family inet { address 10.1.1.1/24; }
   family inet6 { address 10::1/64; }
   }
   st0 { unit 1 { family inet; family inet6; }
   } }
[edit]
user@host# show security ike
proposal phase1_psk_proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 180;
}
policy ike_psk_policy {
    mode main;
    proposals phase1_psk_proposal;
    pre-shared-key asci-text "$9$49oDkST39tOFnORcILXwYgoUjk.PQ36"; ## SECRET-DATA
}
gateway ike-gateway-to-he-srx {
    ike-policy ike_psk_policy;
    address 2000::2;
    external-interface ge-0/0/1.0;
    local-address 2000::1;
}
[edit]
user@host# show security ipsec
proposal phase2-proposal {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm 3des-cbc;
}
policy ipsec_policy {
    proposals phase2-proposal;
}
vpn ipsec-vpn-to-he-srx {
    bind-interface st0.1;
    ike {
        ipsec-policy ipsec_policy;
        gateway ike-gateway-to-he-srx;
    }
    traffic-selector TS1-ipv6 {
        local-ip 10::0/64;
        remote-ip 20::0/64;
    }
    traffic-selector TS2-ipv4 {
        local-ip 10.11.0/24;
        remote-ip 20.1.0.0/16;
    }
    traffic-selector TS3-ipv4 {
        local-ip 10.11.0/24;
        remote-ip 20.1.0/24;
    }
}
[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;
    }
}
security-zone untrust {
    host-inbound-traffic {
        system-services {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}
[edit]
user@host# show security policies
default-policy {
    permit-all;
}

If you are done configuring the device, enter commit from configuration mode.

**Configuring the SRX3400**

To quickly configure this section of the example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the [edit] hierarchy level and then enter commit from configuration mode.

```
set interfaces ge-0/0/1 unit 0 family inet6 address 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 20.1.1.1/24
set interfaces ge-1/0/1 unit 0 family inet6 address 20::1/64
set interfaces ge-1/1/1 unit 0 family inet address 20.1.2.1/24
set security ike proposal phase1_psk_proposal authentication-method pre-shared-keys
set security ike proposal phase1_psk_proposal dh-group group2
set security ike proposal phase1_psk_proposal authentication-algorithm sha1
set security ike proposal phase1_psk_proposal encryption-algorithm 3des-cbc
```
**Step-by-Step Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure traffic selectors:

1. Configure the external interface.
   
   ```
   [edit interfaces]  
   user@host# set ge-0/0/1 unit 0 family inet6 address 2000::2/64  
   ```

2. Configure the secure tunnel interface.
   
   ```
   [edit interfaces]  
   user@host# set st0 unit 1 family inet  
   user@host# set st0 unit 1 family inet6  
   ```

3. Configure the internal interfaces.
   
   ```
   [edit interfaces]  
   user@host# set ge-1/0/1 unit 0 family inet address 20.1.1.1/24  
   user@host# set ge-1/0/1 unit 0 family inet6 address 20::1/64  
   user@host# set ge-1/1/1 unit 0 family inet address 20.1.2.1/24  
   ```
4. Configure Phase 1 options.

```plaintext
[edit security ike proposal phase1_psk_proposal]
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
user@host# set lifetime-seconds 180
```

```plaintext
[edit security ike policy ike_psk_policy]
user@host# set mode main
user@host# set proposals phase1_psk_proposal
user@host# set pre-shared-key ascii-text
"$9$49oDk5T39tOFnORcLXwYgoUjk.4Q36"
```

```plaintext
[edit security ike gateway ike-gateway-to-branch-srx]
user@host# set ike-policy ike_psk_policy
user@host# set address 2000::1
user@host# set external-interface ge-0/0/1.0
user@host# set local-address 2000::2
```

5. Configure Phase 2 options.

```plaintext
[edit security ipsec proposal phase2-proposal]
user@host# set protocol esp
user@host# set authentication-algorithm hmac-sha1-96
user@host# set encryption-algorithm 3des-cbc
```

```plaintext
[edit security ipsec policy ipsec_policy]
user@host# set proposals phase2-proposal
```

```plaintext
[edit security ipsec vpn ipsec-vpn-to-branch-srx]
user@host# set bind-interface st0.1
user@host# set ike gateway ike-gateway-to-branch-srx
user@host# set ike-policy ipsec_policy
user@host# set traffic-selector TS1-ipv6 local-ip 20::0/64 remote-ip 10::0/64
user@host# set traffic-selector TS2-ipv4 local-ip 20.1.0.0/16 remote-ip 10.1.1.0/24
user@host# set traffic-selector TS3-ipv4 local-ip 20.1.1.0/24 remote-ip 10.1.1.0/24
```


```plaintext
[edit security forwarding-options]
user@host# set family inet6 mode flow-based
```

7. Configure security zones and the security policy.

```plaintext
[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
user@host# set interfaces ge-1/1/1.0
```

```plaintext
[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 st0.1
```
user@host# set interfaces ge-0/0/1.0

[edit security policies]
user@host# set default-policy permit-all

**Results**

From configuration mode, confirm your configuration by entering the `show interfaces`, `show security ike`, `show security ipsec`, `show security forwarding-options`, `show security zones`, and `show security policies` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        family inet6 {
            address 2000::2/64;
        }  
    }
    }  
ge-1/0/1 {
    unit 0 {
        family inet {
            address 20.1.1.1/24;
        }
        family inet6 {
            address 20::1/64;
        }
    }
    }
    }
ge-1/1/1 {
    unit 0 {
        family inet {
            address 20.1.2.1/24;
        }
    }
    }
}
st0 {
    unit 1 {
        family inet;
        family inet6;
    }
}
[edit]
user@host# show security ike
proposal phase1_psk_proposal {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 180;
}  
policy ike_psk_policy {
    mode main;
    proposals phase1_psk_proposal;
pre-shared-key ascii-text "$9$49oDkST39tOFnORcILxwYgoUjk.PQ36"; ##
SECRET-DATA
}
gateway ike-gateway-to-branch-srx {
  ike-policy ike_psk_policy;
  address 2000::1;
  external-interface ge-0/0/1.0;
  local-address 2000::2;
}
[edit]
user@host# show security ipsec
proposal phase2-proposal {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm 3des-cbc;
}
policy ipsec_policy {
  proposals phase2-proposal;
}
vpn ipsec-vpn-to-branch-srx {
  bind-interface st0.1;
  ike {
    ipsec-policy ipsec_policy;
    gateway ike-gateway-to-branch-srx;
  }
  traffic-selector TS1-ipv6 {
    local-ip 20::0/64;
    remote-ip 10::0/64;
  }
  traffic-selector TS2-ipv4 {
    local-ip 20.1.0.0/16;
    remote-ip 10.1.1.0/24;
  }
  traffic-selector TS3-ipv4 {
    local-ip 20.1.1.0/24;
    remote-ip 10.1.1.0/24;
  }
}
[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 {
            all;
        }
        protocols {
            all;
        }
    }
    interfaces {
        st0.1;
        ge-0/0/1.0;
    }
}

[edit]
user@host# show security policies
default-policy {
    permit-all;
}

If you are done configuring the device, enter commit from configuration mode.

Verification

Confirm that the configuration is working properly.

- Verifying IPsec Phase 2 Status on page 275
- Verifying Routes on page 277

Verifying IPsec Phase 2 Status

Purpose

Verify the IPsec Phase 2 status.

Action

From operational mode, enter the show security ipsec security-associations command.

user@host> show security ipsec security-associations
Total active tunnels: 3
ID   Algorithm       SPI      Life:sec/kb Mon lsys Port  Gateway
<268173313 ESP:des/ sha1 3d75aeff 2984/ unlim -  root 500   2000::2
>268173313 ESP:des/ sha1 a468fece 2984/ unlim -  root 500   2000::2
<268173316 ESP:des/ sha1 417f3cea 3594/ unlim -  root 500   2000::2
>268173316 ESP:des/ sha1 a4344027 3594/ unlim -  root 500   2000::2
<268173317 ESP:des/ sha1 cc9fb573 3556/ unlim -  root 500   2000::2
>268173317 ESP:des/ sha1 a4bde69b 3556/ unlim -  root 500   2000::2

From operational mode, enter the show security ipsec security-associations detail command.

user@host> show security ipsec security-associations detail
ID: 268173313 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS1-ipv6
Local Identity: ipv6(10::10::ffff:ffff:ffff:ffff)
Remote Identity: ipv6(20::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
Hard lifetime: Expires in 2976 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2354 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: a468fece, AUX-SPI: 0
Hard lifetime: Expires in 2976 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2354 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

ID: 268173316 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS2-ipv4
Local Identity: ipv4(10.1.1.0-10.1.1.255)
Remote Identity: ipv4(20.1.0.0-20.1.255.255)
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
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: a4344027, AUX-SPI: 0
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

ID: 268173317 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS3-ipv4
Local Identity: ipv4(10.1.1.0-10.1.1.255)
Remote Identity: ipv4(20.1.1.0-20.1.1.255)
Meaning

The `show security ipsec security-associations` command lists all active IKE Phase 2 SAs. If no SAs are listed, there was a problem with Phase 2 establishment. Check the IKE policy parameters and external interface settings in your configuration. Phase 2 proposal parameters must match on the peer devices.

Verifying Routes

Purpose

Verify active routes

Action

From operational mode, enter the `show route` command.

```
user@host> show route
inet.0: 24 destinations, 24 routes (24 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.1.0.0/16    *[Static/5] 00:00:32  
               > via st0.1
20.1.1.0/24    *[Static/5] 00:00:32  
               > via st0.1
20::/64        *[Static/5] 00:00:34  
               > via st0.1
```

Meaning

The `show route` command lists active entries in the routing tables. Routes to the remote IP address configured in each traffic selector should be present with the correct st0 interface.

Related Documentation

- Understanding Traffic Selectors in Route-Based VPNs on page 51
- IPSec VPN Feature Guide for Security Devices
CHAPTER 19

VPN Alarms

- Example: Setting an Audible Alert as Notification of a Security Alarm on page 279
- Example: Generating Security Alarms in Response to Potential Violations on page 280

Example: Setting an Audible Alert as Notification of a Security Alarm

**Supported Platforms**  LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX650

This example shows how to configure a device to generate a system alert beep when a new security event occurs. By default, alarms are not audible.

- Requirements on page 279
- Overview on page 279
- Configuration on page 279
- Verification on page 280

**Requirements**

No special configuration beyond device initialization is required before configuring this feature.

**Overview**

In this example, you set an audible beep to be generated in response to a security alarm.

**Configuration**

**Step-by-Step Procedure**

To set an audible alarm:

1. Enable security alarms.
   
   [edit]
   
   user@host# edit security alarms

2. Specify that you want to be notified of security alarms with an audible beep.
   
   [edit security alarms]
   
   user@host# set audible

3. If you are done configuring the device, commit the configuration.
   
   [edit security alarms]
   
   user@host# commit
Verification

To verify the configuration is working properly, enter the `show security alarms detail` command.

Related Documentation

- *IPsec VPN Feature Guide for Security Devices*

Example: Generating Security Alarms in Response to Potential Violations

Supported Platforms

LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX650

This example shows how to configure the device to generate a system alarm when a potential violation occurs. By default, no alarm is raised when a potential violation occurs.

- Requirements on page 280
- Overview on page 280
- Configuration on page 280
- Verification on page 282

Requirements

No special configuration beyond device initialization is required before configuring this feature.

Overview

In this example, you configure an alarm to be raised when:

- The number of authentication failures exceeds 6.
- The cryptographic self-test fails.
- The non-cryptographic self-test fails.
- The key generation self-test fails.
- The number of encryption failures exceeds 10.
- The number of decryption failures exceeds 1.
- The number of IKE Phase 1 failures exceeds 10.
- The number of IKE Phase 2 failure exceeds 1.
- A replay attack occurs.

Configuration

**CLI Quick Configuration**

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the `[edit]` hierarchy level.

```
set security alarms potential-violation authentication 6
```
Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see Using the CLI Editor in Configuration Mode.

To configure alarms in response to potential violations:

1. Enable security alarms.
   
   [edit]
   user@host# edit security alarms

2. Specify that an alarm should be raised when an authentication failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set authentication 6

3. Specify that an alarm should be raised when a cryptographic self-test failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set cryptographic-self-test

4. Specify that an alarm should be raised when a non-cryptographic self-test failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set non-cryptographic-self-test

5. Specify that an alarm should be raised when a key generation self-test failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set key-generation-self-test

6. Specify that an alarm should be raised when an encryption failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set encryption-failures threshold 10

7. Specify that an alarm should be raised when a decryption failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set decryption-failures threshold 1

8. Specify that an alarm should be raised when an IKE Phase 1 failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set ike-phase1-failures threshold 10

9. Specify that an alarm should be raised when an IKE Phase 2 failure occurs.
   
   [edit security alarms potential-violation]
   user@host# set ike-phase2-failures threshold 1

10. Specify that an alarm should be raised when a replay attack occurs.
[edit security alarms potential-violation]
user@host# set replay-attacks

**Results**  From configuration mode, confirm your configuration by entering the `show security alarms` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# 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;
}
```

If you are done configuring the device, enter **commit** from configuration mode.

**Verification**

To confirm that the configuration is working properly, from operational mode, enter the `show security alarms` command.

**Related Documentation**
- Understanding VPN Alarms and Auditing on page 59
- Example: Setting an Audible Alert as Notification of a Security Alarm on page 279
- *IPsec VPN Feature Guide for Security Devices*
CHAPTER 20

VPN Peer Availability

- Example: Configuring Global SPI and VPN Monitoring Features on page 283

**Example: Configuring Global SPI and VPN Monitoring Features**

**Supported Platforms**

- J Series, LN Series, SRX Series

**Requirements**

- Requirements on page 283
- Overview on page 283
- Configuration on page 283

**Overview**

Before you begin, understand global SPI and VPN monitoring features. See “Understanding Global SPI and VPN Monitoring Features” on page 63.

In this example, you configure the device to detect and respond five times to a bad IPsec SPI before deleting the SA and initiating a new one. You also configure the device to monitor the VPN by sending ICMP requests to the peer every 15 seconds, and to declare the peer unreachable after 15 unsuccessful pings.

**Configuration**

**Step-by-Step Procedure**

To configure global VPN settings in the CLI editor:

1. Specify global VPN settings.

   ```
   [edit]
   user@host# set security ike respond-bad-spi 5
   user@host# set security ipsec vpn-monitor-options interval 15 threshold 15
   ```

**Related Documentation**

- Example: Configuring a Policy-Based VPN on page 143
- Example: Configuring a Route-Based VPN on page 77
- IPsec VPN Feature Guide for Security Devices
CHAPTER 21

VPN Session Affinity

- Enabling VPN Session Affinity on page 285
- Accelerating the IPsec VPN Traffic Performance on page 287

Enabling VPN Session Affinity

**Supported Platforms**

LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

By default, VPN session affinity is disabled on SRX Series devices. Enabling VPN session affinity can improve VPN throughput under certain conditions. This section describes how to use the CLI to enable VPN session affinity.

Determine if clear-text sessions are being forwarded to IPsec tunnel sessions on a different SPU. Use the `show security flow session` command to display session information about clear-text sessions.

```
user@host> show security flow session
Flow Sessions on FPC3 PIC0:

Session ID: 60000001, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/6204 --> 23.0.21.6/41264;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 60000002, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 60000003, Policy name: self-traffic-policy/1, Timeout: 58, Valid
In: 23.0.21.6/500 --> 23.0.21.11/500;udp, If: .local., Pkts: 105386, Bytes: 12026528
Out: 23.0.21.11/500 --> 23.0.21.6/500;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: 26.0.20.156/23 --> 22.0.20.155/53051;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: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 120000002, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0
```
Session ID: 120031730, Policy name: default-policy-00/2, Timeout: 1764, Valid
In: 22.0.20.155/53051 --> 26.0.20.156/23;tcp, If: ge-0/0/1.0, Pkts: 44, Bytes: 2399
Out: 26.0.20.156/23 --> 22.0.20.155/53051;tcp, If: st0.0, Pkts: 35, Bytes: 2449
Total sessions: 3

In the example, there is a tunnel session on FPC 3, PIC 0 and a clear-text session on FPC 6, PIC 0. A forwarding session (session ID 60017354) is set up on FPC 3, PIC 0.

To enable VPN session affinity:

1. In configuration mode, use the `set` command to enable VPN session affinity.
   
   ```
   [edit]
   user@host# set security flow load-distribution session-affinity ipsec
   ```

2. Check your changes to the configuration before committing.
   
   ```
   [edit]
   user@host# commit check
   ```

3. Commit the configuration.
   
   ```
   [edit]
   user@host# commit
   ```

After enabling VPN session affinity, use the `show security flow session` command to display session information about clear-text sessions.

```
user@host> show security flow session
Flow Sessions on FPC3 PIC0:

Session ID: 60000001, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/6352 --> 23.0.21.6/7927;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 60000002, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 60000003, Policy name: self-traffic-policy/1, Timeout: 56, Valid
In: 23.0.21.6/500 --> 23.0.21.11/500;udp, If: .local..0, Pkts: 105425, Bytes: 12031144
Out: 23.0.21.11/500 --> 23.0.21.6/500;udp, If: ge-0/0/2.0, Pkts: 106503, Bytes: 12110680

Session ID: 60017387, Policy name: default-policy-00/2, Timeout: 1796, Valid
In: 22.0.20.155/53053 --> 26.0.20.156/23;tcp, If: ge-0/0/1.0, Pkts: 10, Bytes: 610
Out: 26.0.20.156/23 --> 22.0.20.155/53053;tcp, If: st0.0, Pkts: 9, Bytes: 602
Total sessions: 4

Flow Sessions on FPC6 PIC0:

Session ID: 120000001, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

Session ID: 120000002, Policy name: N/A, Timeout: N/A, Valid
In: 23.0.21.11/0 --> 23.0.21.6/0;esp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0
Total sessions: 2

After VPN session affinity is enabled, the clear-text session is always located on FPC 3, PIC 0.
Accelerating the IPsec VPN Traffic Performance

Supported Platforms  
SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

You can accelerate the IPsec VPN performance by configuring the performance acceleration parameter. By default, VPN performance acceleration is disabled on SRX Series devices. Enabling the VPN performance acceleration can improve the VPN throughput with VPN session affinity enabled.

This topic describes how to use the CLI to enable VPN performance acceleration.

NOTE: To enable performance acceleration, you must ensure that cleartext sessions and IPsec tunnel sessions are established on the same Services Processing Unit (SPU). For more information on enabling the session affinity, see “Understanding VPN Session Affinity” on page 65.

To enable IPsec VPN performance acceleration:

1. Use the set command to enable VPN session affinity.
   
   [edit]
   user@host# set security flow load-distribution session-affinity ipsec

2. Use the set command to enable IPsec performance acceleration.
   
   [edit]
   user@host# set security flow ipsec-performance-acceleration

3. Check your changes to the configuration before committing.
   
   [edit]
   user@host# commit check

4. Commit the configuration.
   
   [edit]
   user@host# commit

After enabling VPN performance acceleration, use the show security flow status command to display flow status.

Flow forwarding mode:
   Inet forwarding mode: flow based
   Inet6 forwarding mode: drop
   MPLS forwarding mode: drop
   ISO forwarding mode: drop
Flow trace status
   Flow tracing status: off
Flow session distribution
   Distribution mode: Hash-based
   Flow packet ordering
Ordering mode: Hardware
Flow ipsec performance acceleration: on

Related Documentation

- Understanding VPN Session Affinity on page 65
- Enabling VPN Session Affinity on page 285
- ipsec-performance-acceleration (Security Flow) on page 354
- show security flow status
- IPsec VPN Feature Guide for Security Devices
CHAPTER 22

IKE Configuration Statements

- Security Configuration Statement Hierarchy on page 290
- [edit security ike] Hierarchy Level on page 291
- address (Security IKE Gateway) on page 293
- always-send on page 294
- authentication-algorithm (Security IKE) on page 295
- authentication-method on page 296
- certificate on page 297
- connections-limit on page 298
- container on page 299
- dead-peer-detection on page 300
- dh-group (Security IKE) on page 301
- distinguished-name (Security) on page 302
- dynamic (Security) on page 303
- encryption-algorithm (Security IKE) on page 304
- external-interface (Security IKE Gateway) on page 305
- gateway (Security IKE) on page 306
- general-ikeid on page 307
- hostname on page 307
- ike (Security) on page 308
- ike (Security IPsec VPN) on page 310
- ike-policy (Security Gateway) on page 311
- ike-user-type on page 312
- inet (Security Dynamic Peer) on page 313
- inet6 (Security IKE Gateway) on page 313
- interval (Security IKE) on page 314
- lifetime-seconds (Security IKE) on page 314
- local-address on page 315
- local-certificate (Security) on page 316
Security Configuration Statement Hierarchy

Supported Platforms J Series, LN Series, SRX Series

Use the statements in the security configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones. Statements that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the [edit security] hierarchy.

- [edit security address-book] Hierarchy Level
- [edit security alarms] Hierarchy Level on page 378
- [edit security alg] Hierarchy Level
- [edit security analysis] Hierarchy Level
• [edit security application-firewall] Hierarchy Level
• [edit security application-tracking] Hierarchy Level
• [edit security certificates] Hierarchy Level
• [edit security datapath-debug] Hierarchy Level
• [edit security dynamic-VPN] Hierarchy Level
• [edit security firewall-authentication] Hierarchy Level
• [edit security flow] Hierarchy Level
• [edit security forwarding-options] Hierarchy Level
• [edit security forwarding-process] Hierarchy Level
• [edit security gprs] Hierarchy Level
• [edit security group-VPN] Hierarchy Level
• [edit security idp] Hierarchy Level
• [edit security ike] Hierarchy Level on page 291
• [edit security ipsec] Hierarchy Level on page 337
• [edit security log] Hierarchy Level
• [edit security nat] Hierarchy Level
• [edit security pki] Hierarchy Level
• [edit security policies] Hierarchy Level
• [edit security resource-manager] Hierarchy Level
• [edit security screen] Hierarchy Level
• [edit security softwires] Hierarchy Level
• [edit security ssh-known-hosts] Hierarchy Level
• [edit security traceoptions] Hierarchy Level
• [edit security user-identification] Hierarchy Level
• [edit security utm] Hierarchy Level
• [edit security zones] Hierarchy Level

Related Documentation

• Master Administrator for Logical Systems Feature Guide for Security Devices
• CLI User Guide

[edit security ike] Hierarchy Level

Supported Platforms
J Series, LN Series, SRX Series

```
security {
ike {
```
gateway gateway-name {
    address [ip-address-or-hostname];
    dead-peer-detection {
        (always-send | optimized | probe-idle-tunnel);
        interval seconds;
        threshold number;
    }
    dynamic {
        connections-limit number;
        (distinguished-name <container container-string> <wildcard wildcard-string> | hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
        ike-user-type (group-ike-id | shared-ike-id);
    }
    external-interface external-interface-name;
    general-ikeid;
    ike-policy policy-name;
    local-address (ipv4-address | ipv6-address);
    local-identity {
        (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
    }
    nat-keepalive seconds;
    no-nat-traversal;
    remote-identity {
        (distinguished-name <container container-string> <wildcard wildcard-string> | hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
    }
    version (v1-only | v2-only);
    xauth {
        access-profile profile-name;
    }
}

policy policy-name {
    certificate {
        local-certificate certificate-id;
        peer-certificate-type (pkcs7 | x509-signature);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
}

proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha-384 | sha1);
    authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc | suiteb-gcm-128 | suiteb-gcm-256);
    lifetime-seconds seconds;
}

respond-bad-spi <max-responses>;
traceoptions {
address (Security IKE Gateway)

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax** `address [ip-address-or-hostname];`

**Hierarchy Level**
- `[edit security group-vpn member ike gateway gateway-name]`
- `[edit security ike gateway gateway-name]`


**Description** Specify the IPv4 or IPv6 address or the hostname of the primary Internet Key Exchange (IKE) gateway and up to four backup gateways.

**Options** `ip-address-or-hostname`—IPv4 or IPv6 address or hostname of an IKE gateway.

**Required Privilege**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
## always-send

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>J Series, LN Series, SRX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>always-send;</td>
</tr>
<tr>
<td>Hierarchy Level</td>
<td>[edit security ike gateway gateway-name dead-peer-detection]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 8.5.</td>
</tr>
<tr>
<td>Description</td>
<td>Instructs the device to send dead peer detection (DPD) requests regardless of whether there is outgoing IPsec traffic to the peer.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>security—To view this statement in the configuration. security-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• Dynamic VPN Feature Guide for SRX Series Gateway Devices</td>
</tr>
<tr>
<td></td>
<td>• Group VPN Feature Guide for Security Devices</td>
</tr>
<tr>
<td></td>
<td>• IPsec VPN Feature Guide for Security Devices</td>
</tr>
</tbody>
</table>
**authentication-algorithm (Security IKE)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`authentication-algorithm (md5 | sha-256 | sha-384 | sha1);`

**Hierarchy Level**  
[edit security ike proposal *proposal-name*]

**Release Information**  

**Description**  
Configure the Internet Key Exchange (IKE) authentication algorithm.

**NOTE:** The device does not delete existing IPsec SAs when you update the `authentication-algorithm` configuration in the IKE proposal. The device deletes existing IPsec SAs when you update the `authentication-algorithm` configuration in the IPsec proposal.

**Options**  
`authentication-algorithm`—Hash algorithm that authenticates packet data. It can be one of the following algorithms:

- `md5`—Produces a 128-bit digest.
- `sha-256`—Produces a 256-bit digest. This option is not supported on group VPNs.
- `sha-384`—Produces a 384-bit digest. This option is not supported on group VPNs.
- `sha1`—Produces a 160-bit digest.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- *AutoVPN Feature Guide for SRX Series Gateway Devices*
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*
- *IPsec VPN Feature Guide for Security Devices*
**authentication-method**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  
```
authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
```

**Hierarchy Level**  [edit security ike proposal *proposal-name*]

**Release Information**  

**Description**  Specify the method the device uses to authenticate the source of Internet Key Exchange (IKE) messages. The *pre-shared-keys* option refers to a preshared key, which is a key for encryption and decryption that both participants must have before beginning tunnel negotiations. The other options refer to types of digital signatures, which are certificates that confirm the identity of the certificate holder.

---

**NOTE:** The device does not delete existing IPsec SAs when you update the authentication-method configuration in the IKE proposal.

---

**Options**

- **dsa-signatures**—Specify that the Digital Signature Algorithm (DSA) is used. This option is not supported on dynamic VPNs.

- **ecdsa-signatures-256**—Specify that the Elliptic Curve DSA (ECDSA) using the 256-bit elliptic curve secp256r1, as specified in the Federal Information Processing Standard (FIPS) Digital Signature Standard (DSS) 186-3, is used. This option is not supported on group VPNs.

- **ecdsa-signatures-384**—Specify that the ECDSA using the 384-bit elliptic curve secp384r1, as specified in the FIPS DSS 186-3, is used. This option is not supported on group VPNs.

- **pre-shared-keys**—Specify that a preshared key, which is a secret key shared between the two peers, is used during authentication to identify the peers to each other. The same key must be configured for each peer. This is the default method.

- **rsa-signatures**—Specify that a public key algorithm, which supports encryption and digital signatures, is used. This option is not supported on dynamic VPNs.

**Required Privilege Level**  
- security—to view this statement in the configuration.
- security-control—to add this statement to the configuration.

**Related Documentation**

- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
certificate

Supported Platforms  J Series, LN Series, SRX Series

Syntax  certificate {
  local-certificate certificate-id;
  peer-certificate-type (pkcs7 | x509-signature);
}

Hierarchy Level  [edit security group-vpn member ike policy policy-name]
                 [edit security group-vpn server ike policy policy-name]
                 [edit security ike policy policy-name]


Description  Specify usage of a digital certificate to authenticate the virtual private network (VPN) initiator and recipient. (This statement is not supported on dynamic VPN implementations.)

Options  The remaining statements are explained separately.

Required Privilege Level  security—To view this statement in the configuration.
                         security-control—To add this statement to the configuration.

Related Documentation  • AutoVPN Feature Guide for SRX Series Gateway Devices
                         • Group VPN Feature Guide for Security Devices
                         • IPsec VPN Feature Guide for Security Devices
connections-limit

Supported Platforms  J Series, LN Series, SRX Series

Syntax  connections-limit number;

Hierarchy Level  [edit security ike gateway gateway-name dynamic]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Configure the number of concurrent connections that the group profile supports. When the maximum number of connections is reached, no more dynamic virtual private network (VPN) endpoints dialup users attempting to access an IPsec VPN are allowed to begin Internet Key Exchange (IKE) negotiations.

Options  number—Maximum number of concurrent connections allowed.

Required Privilege Level  security—To view this statement in the configuration. security-control—To add this statement to the configuration.

Related Documentation  • IPsec VPN Feature Guide for Security Devices
• Network Monitoring and Troubleshooting Guide for Security Devices
• System Log Monitoring and Troubleshooting Guide for Security Devices
container

Supported Platforms  J Series, LN Series, SRX Series

Syntax  container container-string;

Hierarchy Level  [edit security group-vpn server gateway gateway-name dynamic distinguished-name]
                 [edit security ike gateway gateway-name dynamic distinguished-name]


Description  Specify that the value in the identity fields of a dynamic virtual private network (VPN) endpoint user’s distinguished name exactly match the values in the group IKE user’s distinguished name. The order of the identity fields in the fields of the distinguished name strings must be identical when matching. (This statement is not supported on dynamic VPN implementations.)

Options  container-string—Distinguished name identity value to be matched. For example, cn=admin, ou=eng, o=juniper, dc=net.

NOTE: Add a space between each container string. For example, edit security ike gateway jsr_gateway dynamic distinguished-name container o=juniper, ou=eng;

Required Privilege  Level  security—To view this statement in the configuration.
                              security-control—To add this statement to the configuration.

Related Documentation  • AutoVPN Feature Guide for SRX Series Gateway Devices
                               • Group VPN Feature Guide for Security Devices
                               • IPsec VPN Feature Guide for Security Devices
                               • Network Monitoring and Troubleshooting Guide for Security Devices
                               • System Log Monitoring and Troubleshooting Guide for Security Devices
dead-peer-detection

Supported Platforms  J Series, LN Series, SRX Series

Syntax  
```plaintext
dead-peer-detection {
  (always-send | optimized | probe-idle-tunnel);
  interval seconds;
  threshold number;
}
```

Hierarchy Level  [edit security ike gateway gateway-name]


Description  Enable the device to use dead peer detection (DPD). DPD is a method used by devices to verify the current existence and availability of IPsec peers. A device performs this verification by sending encrypted IKE Phase 1 notification payloads (R-U-THERE messages) to a peer and waiting for DPD acknowledgements (R-U-THERE-ACK messages) from the peer.

Options  The remaining statements are explained separately.

Required Privilege
Level  security—To view this statement in the configuration.
      security-control—To add this statement to the configuration.

Related Documentation
• AutoVPN Feature Guide for SRX Series Gateway Devices
• Dynamic VPN Feature Guide for SRX Series Gateway Devices
• Group VPN Feature Guide for Security Devices
• IPsec VPN Feature Guide for Security Devices
**dh-group (Security IKE)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);

**Hierarchy Level**  
[edit security ike proposal proposal-name]

**Release Information**  

**Description**  
Specify the IKE Diffie-Hellman group.

---

**NOTE:** The device does not delete existing IPsec SAs when you update the dh-group configuration in the IKE proposal.

---

**Options**  
dh-group—Diffie-Hellman group for key establishment.

- group1—768-bit Modular Exponential (MODP) algorithm.
- group14—2048-bit MODP group. This option is not supported on dynamic VPN implementations.
- group19—256-bit random Elliptic Curve Groups modulo a Prime (ECP groups) algorithm. This option is not supported on group VPN implementations.
- group2—1024-bit MODP algorithm.
- group20—384-bit random ECP groups algorithm. This option is not supported on group VPN implementations.
- group24—2048-bit MODP Group with 256-bit prime order subgroup. This option is not supported on group VPN implementations.
- group5—1536-bit MODP algorithm.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices  
- IPsec VPN Feature Guide for Security Devices
distinguished-name (Security)

Supported Platforms  
J Series, LN Series, SRX Series

Syntax  
distinguished-name <container container-string> <wildcard wildcard-string>

Hierarchy Level  
[edit security group-vpn server ike gateway gateway-name]
[edit security ike gateway gateway-name dynamic]

Release Information  
Statement introduced in Junos OS Release 8.5. Support for group-vpn server hierarchy added in Junos OS Release 10.2.

Description  
Specify a distinguished name as the identifier for the remote gateway with a dynamic IP address. (This statement is not supported on dynamic VPN implementations.)

Options  
The remaining statements are explained separately.

Required Privilege  
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
**dynamic (Security)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
dynamic {
  connections-limit number;
  (distinguished-name <container container-string> <wildcard wildcard-string> | hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);  
  ike-user-type (group-ike-id | shared-ike-id);
}

**Hierarchy Level**  
[edit security ike gateway gateway-name]

**Release Information**  

**Description**  
Specify the identifier for the remote gateway with a dynamic IPv4 or IPv6 address. Use this statement to set up a VPN with a gateway that has an unspecified IPv4 or IPv6 address.

**Options**  
The remaining statements are explained separately.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices  
- IPsec VPN Feature Guide for Security Devices
encryption-algorithm (Security IKE)

Supported Platforms
J Series, LN Series, SRX Series

Syntax
encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);

Hierarchy Level
[edit security group-vpn member ike proposal proposal-name]
[edit security group-vpn server ike proposal proposal-name]
[edit security ike proposal proposal-name]

Release Information
Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2.

Description
Configure an encryption algorithm for an IKE proposal.

NOTE: The device does not delete existing IPsec SAs when you update the encryption-algorithm configuration in the IKE proposal.

Options
- 3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long.
- aes-192-cbc—AES 192-bit encryption algorithm.
- aes-256-cbc—AES 256-bit encryption algorithm.
- des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.

Required Privilege Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
- Network Monitoring and Troubleshooting Guide for Security Devices
- System Log Monitoring and Troubleshooting Guide for Security Devices
### external-interface (Security IKE Gateway)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```
external-interface external-interface-name;
```

**Hierarchy Level**  
```
[edit security ike gateway gateway-name]
```

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the outgoing interface for IKE SAs. This interface is associated with a zone that acts as its carrier, providing firewall security for it.

**Options**  
`external-interface-name`—Name of the interface to be used to send traffic to the IPsec VPN.

**Required Privilege Level**  
- `security`—To view this statement in the configuration.
- `security-control`—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
gateway (Security IKE)

Supported Platforms  J Series, LN Series, SRX Series

Syntax  

```plaintext
gateway gateway-name {
  address [ip-address-or-hostname];
  dead-peer-detection {
    (always-send | optimized | probe-idle-tunnel);
    interval seconds;
    threshold number;
  }
  dynamic {
    connections-limit number;
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
    ike-user-type (group-ike-id | shared-ike-id);
  }
  external-interface external-interface-name;
  general-ikeid;
  ike-policy policy-name;
  local-address (ipv4-address | ipv6-address);
  local-identity {
    (distinguished-name | hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
  }
  nat-keepalive seconds;
  no-nat-traversal;
  remote-identity {
    (distinguished-name <container container-string> <wildcard wildcard-string> | hostname
    hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
  }
  version (v1-only | v2-only);
  xauth {
    access-profile profile-name;
  }
}
```

Hierarchy Level  [edit security ike]

Release Information  Statement introduced in Junos OS Release 8.5. Support for IPv6 addresses added in

Description  Configure an IKE gateway.

Options  

- `gateway-name` —Name of the gateway.

  The remaining statements are explained separately.

Required Privilege  security—To view this statement in the configuration.

  security-control—To add this statement to the configuration.

Related Documentation  

- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
• IPSec VPN Feature Guide for Security Devices

**general-ikeid**

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax**

```
general-ikeid;
```

**Hierarchy Level**

```
[edit security ike gateway gateway-name]
```

**Release Information** Statement introduced in Junos OS Release 10.4.

**Description** Accept general peer IKE ID.

**Required Privilege Level**

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**

- IPSec VPN Feature Guide for Security Devices

**hostname**

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax**

```
hostname domain-name;
```

**Hierarchy Level**

```
[edit security group-vpn server ike gateway gateway-name dynamic]
[edit security ike gateway gateway-name dynamic]
```

**Release Information** Statement introduced in Junos OS Release 8.5. Support for group-vpn server hierarchy added in Junos OS Release 10.2.

**Description** Unique name by which a network-attached device is known on a network.

**Options**

- `domain-name`—A fully qualified domain name (FQDN).

**Required Privilege Level**

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
ike (Security)

Supported Platforms
J Series, LN Series, SRX Series

Syntax
ike

gateway gateway-name
  address [ip-address-or-hostname];
  dead-peer-detection
    (always-send | optimized | probe-idle-tunnel);
    interval seconds;
    threshold number;
  }
dynamic
  connections-limit number;
  (distinguished-name <container container-string> <wildcard wildcard-string> | hostname domain-name | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
  ike-user-type (group-ike-id | shared-ike-id);
}
external-interface external-interface-name;
general-ikeid;
ike-policy policy-name;
local-identity
  (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
}
nat-keepalive seconds;
no-nat-traversal;
remote-identity
  (distinguished-name <container container-string> <wildcard wildcard-string> | hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
}
version (v1-only | v2-only);
xauth
  access-profile profile-name;
}
policy policy-name
  certificate
    local-certificate certificate-id;
    peer-certificate-type (pkcs7 | x509-signature);
  }
description description;
mode (aggressive | main);
pre-shared-key (ascii-text key | hexadecimal key);
proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
proposals [proposal-name];
}
proposal proposal-name
  authentication-algorithm (md5 | sha-256 | sha-384 | sha1);
  authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384 | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
lifetime-seconds seconds;
}
respond-bad-spi <max-responses>;
traceoptions {
  file {
    filename;
    files number;
    match regular-expression;
    size maximum-file-size;
    (world-readable | no-world-readable);
  }
  flag flag;
  no-remote-trace;
  rate-limit messages-per-second;
}

Hierarchy Level [edit security]


Description Define Internet Key Exchange (IKE) configuration.

Options The remaining statements are explained separately.

Required Privilege Level

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation

- IKE and ESP ALG Feature Guide for Security Devices
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
ike (Security IPsec VPN)

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**
```
ike {
    gateway gateway-name;
    idle-time seconds;
    install-interval seconds;
    ipsec-policy ipsec-policy-name;
    no-anti-replay;
    proxy-identity {
        local ip-prefix;
        remote ip-prefix;
        service (any | service-name);
    }
}
```

**Hierarchy Level**  [edit security ipsec vpn vpn-name]


**Description**  Define an IKE-keyed IPsec VPN.

**Options**  The remaining statements are explained separately.

**Required Privilege**  
- **Level**  
  - security—to view this statement in the configuration.
  - security-control—to add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
### ike-policy (Security Gateway)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
ike-policy *policy-name*;

**Hierarchy Level**  
- [edit security group-vpn member ike gateway *gateway-name*]
- [edit security group-vpn server ike gateway *gateway-name*]
- [edit security ike gateway *gateway-name*]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2.

**Description**  
Specify the IKE policy to be used for the gateway.

**Options**  
- *policy-name* — IKE policy name.

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
## ike-user-type

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>J Series, LN Series, SRX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>ike-user-type (group-ike-id</td>
</tr>
<tr>
<td>Hierarchy Level</td>
<td>[edit security ike gateway gateway-name dynamic]</td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 8.5.</td>
</tr>
<tr>
<td>Description</td>
<td>Configure the type of IKE user for a remote access connection.</td>
</tr>
<tr>
<td>Options</td>
<td>• group-ike-id—E-mail address or fully qualified domain name (FQDN) shared for a group of remote access users so that each one does not need a separate IKE profile configured.</td>
</tr>
<tr>
<td></td>
<td>• shared-ike-id—E-mail address shared for a large number of remote access users so that each one does not need a separate IKE profile configured.</td>
</tr>
<tr>
<td>Required Privilege Level</td>
<td>security—To view this statement in the configuration. security-control—To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>• AutoVPN Feature Guide for SRX Series Gateway Devices</td>
</tr>
<tr>
<td></td>
<td>• Dynamic VPN Feature Guide for SRX Series Gateway Devices</td>
</tr>
<tr>
<td></td>
<td>• Group VPN Feature Guide for Security Devices</td>
</tr>
<tr>
<td></td>
<td>• IPSec VPN Feature Guide for Security Devices</td>
</tr>
</tbody>
</table>
### inet (Security Dynamic Peer)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`inet ip-address;`

**Hierarchy Level**  
`[edit security group-vpn server ike gateway gateway-name dynamic]`
`[edit security ike gateway gateway-name dynamic]`

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for `group-vpn server` hierarchy added in Junos OS Release 10.2.

**Description**  
Specify IP address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

**Options**  
`ip-address`—IP address.

**Required Privilege**  
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

### inet6 (Security IKE Gateway)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`inet6 ipv6-address;`

**Hierarchy Level**  
`[edit security ike gateway gateway-name dynamic]`

**Release Information**  
Statement introduced in Junos OS Release 11.1.

**Description**  
Specify an IPv6 address to identify the dynamic peer. (This statement is not supported on dynamic VPN implementations.)

**Options**  
`ipv6-address`—IPv6 address.

**Required Privilege**  
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**  
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
interval (Security IKE)

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  interval seconds;

**Hierarchy Level**  [edit security ike gateway gateway-name dead-peer-detection]

**Release Information**  Statement introduced in Junos OS Release 8.5.

**Description**  Specify the amount of time that the peer waits for traffic from its destination peer before sending a dead-peer-detection (DPD) request packet.

**Options**  
- *seconds* — Number of seconds that the peer waits before sending a DPD request packet.  
  - **Range:** 10 through 60 seconds  
  - **Default:** 10 seconds

**Required Privilege Level**  
- security—To view this statement in the configuration.  
- security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices

lifetime-seconds (Security IKE)

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  lifetime-seconds seconds;

**Hierarchy Level**  [edit security ike proposal proposal-name]

**Release Information**  Statement introduced in Junos OS Release 8.5. Default value modified in Junos OS Release 10.2.

**Description**  Specify the lifetime (in seconds) of an IKE security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

**Options**  
- *seconds* — Lifetime of the IKE SA.  
  - **Range:** 180 through 86,400 seconds  
  - **Default:** 28,800 seconds

**Required Privilege Level**  
- security—To view this statement in the configuration.  
- security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices  
- Infranet Authentication Feature Guide for Security Devices
**local-address**

**Supported Platforms**  
SRX Series

**Syntax**  
`local-address (ipv4-address | ipv6-address);`

**Hierarchy Level**  
`[edit security ike gateway gateway-name]`

**Release Information**  
Statement introduced in Junos OS Release 12.1X46-D10.

**Description**  
Specify the local gateway address. Multiple addresses in the same address family can be configured on an external physical interface to a VPN peer. If this is the case, we recommend that `local-address` be configured. If there is only one IPv4 and one IPv6 address configured on an external physical interface, `local-address` configuration is not necessary.

---

**NOTE:** `local-address` must be an IP address that is configured on an interface on the SRX Series device. We recommend that `local-address` belong to the external interface of the IKE gateway. If `local-address` does not belong to the external interface of the IKE gateway, the interface must be in the same zone as the external interface of the IKE gateway and an intra-zone security policy must be configured to permit traffic.

local-address and the remote IKE gateway address must be in the same address family, either IPv4 or IPv6.

---

**Options**  
- `ipv4-address`—IPv4 address for the local gateway.
- `ipv6-address`—IPv6 address for the local gateway.

**Required Privilege Level**  
- `view-level`—To view this statement in the configuration.
- `control-level`—To add this statement to the configuration.

**Related Documentation**  
- *IPsec VPN Feature Guide for Security Devices*
### local-certificate (Security)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`local-certificate certificate-id;`

**Hierarchy Level**  
- [edit security group-vpn member ike policy policy-name certificate]
- [edit security group-vpn server ike policy policy-name certificate]
- [edit security ike policy policy-name certificate]

**Release Information**  

**Description**  
Specify a particular certificate when the local device has multiple loaded certificates. (This statement is not supported on dynamic VPN implementations.)

---

**NOTE:** The device deletes existing IKE and IPsec SAs when you update the `local-certificate` configuration in the IKE policy.

---

**Options**  
- **certificate-id** —Name of the specific certificate to be used.

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- *AutoVPN Feature Guide for SRX Series Gateway Devices*
- *Group VPN Feature Guide for Security Devices*
- *IPsec VPN Feature Guide for Security Devices*
local-identity

**Supported Platforms**
J Series, LN Series, SRX Series

**Syntax**
local-identity {
    (distinguished-name | hostname hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);
}

**Hierarchy Level**
- [edit security group-vpn member ike gateway gateway-name]
- [edit security group-vpn server ike gateway gateway-name]
- [edit security ike gateway gateway-name]

**Release Information**
Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2. The inet6 option added in Junos OS Release 11.1. The inet6 option is not supported on the group-vpn hierarchies.

**Description**
Specify the local IKE identity to send in the exchange with the destination peer to establish communication. If you do not configure a local-identity, the device uses the IPv4 or IPv6 address corresponding to the local endpoint by default. (The distinguished-name option is not supported on dynamic VPN implementations.)

**Options**
- **distinguished-name**—Specify identity as the distinguished name (DN) from the certificate. If there is more than one certificate on the device, use the `securityikegateway gateway-name policy policy-name certificate local-certificate certificate-id` statement to specify a certificate.
- **hostname hostname**—Specify identity as a fully qualified domain name (FQDN).
- **inet ip-address**—Specify identity as an IPv4 address.
- **inet6 ipv6-address**—Specify identity as an IPv6 address.
- **user-at-hostname e-mail-address**—Specify identity as an e-mail address.

**Required Privilege Level**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
mode (Security IKE Policy)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
mode (aggressive | main);

**Hierarchy Level**  
[edit security group-vpn member ike policy policy-name]  
[edit security group-vpn server ike policy policy-name]  
[edit security ike policy policy-name]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2.

**Description**  
Define the mode used for Internet Key Exchange (IKE) Phase 1 negotiations. Use aggressive mode only when you need to initiate an IKE key exchange without ID protection, as when a peer unit has a dynamically assigned IP address. (The **main** option is not supported on dynamic VPN implementations.)

---

**NOTE:**
- IKEv2 protocol does not negotiate using mode configuration.
- The device deletes existing IKE and IPsec SAs when you update the mode configuration in the IKE policy.

**Options**
- **aggressive**—Aggressive mode.
- **main**—Main mode. Main mode is the recommended key-exchange method because it conceals the identities of the parties during the key exchange.

**Required Privilege Level**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
### nat-keepalive

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
nat-keepalive seconds;

**Hierarchy Level**  
[edit security ike gateway gateway-name]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Default value changed from 5 seconds to 20 seconds in Junos OS Release 12.1X46-D10.

**Description**  
Specify the interval at which NAT keepalive packets can be sent so that NAT translation continues.

**Options**  
seconds — Maximum interval in seconds at which NAT keepalive packets can be sent.  
*Range:* 1 through 300 seconds.  
*Default:* 20 seconds.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- [IPsec VPN Feature Guide for Security Devices](#)

### no-nat-traversal

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
no-nat-traversal;

**Hierarchy Level**  
[edit security ike gateway gateway-name]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Disables UDP encapsulation of IPsec Encapsulating Security Payload (ESP) packets, otherwise known as Network Address Translation Traversal (NAT-T). NAT-T is enabled by default.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- [IPsec VPN Feature Guide for Security Devices](#)
**optimized (DPD)**

**Supported Platforms**  
SRX Series

**Syntax**  
optimized;

**Hierarchy Level**  
[edit security ike gateway gateway-name dead-peer-detection]

**Release Information**  
Statement introduced in Junos OS Release 12.1X46-D10.

**Description**  
Send dead peer detection (DPD) messages if there is no incoming IKE or IPsec traffic within the configured interval after outgoing packets are sent to the peer. This is the default DPD mode.

**Required Privilege**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices

---

**peer-certificate-type**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
peer-certificate-type (pkcs7 | x509-signature);

**Hierarchy Level**  
[edit security group-vpn member ike policy policy-name certificate]  
[edit security group-vpn server ike policy policy-name certificate]  
[edit security ike policy policy-name certificate]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2.

**Description**  
Specify a preferred type of certificate (PKCS7 or X509). (This statement is not supported on dynamic VPN implementations.)

**Options**  
- pkcs7—Public-Key Cryptography Standard #7.  
- x509-signature—X509 is an ITU-T standard for public key infrastructure.

**Required Privilege**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices
policy (Security IKE)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
policy policy-name {
    certificate {
        local-certificate certificate-id;
        peer-certificate-type (pkcs7 | x509-signature);
    }
    description description;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposal-set (basic | compatible | standard } suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
}

**Hierarchy Level**  
[edit security ike]

**Release Information**  

**Description**  
Configure an IKE policy.

**Options**  
- **policy-name**—Name of the IKE policy. The policy name can be up to 32 alphanumeric characters long.
  
The remaining statements are explained separately.

**Required Privilege Level**  
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
### pre-shared-key (Security IKE Policy)

**Supported Platforms**
- J Series, LN Series, SRX Series

**Syntax**
`pre-shared-key (ascii-text key | hexadecimal key);`

**Hierarchy Level**
- [edit security group-vpn member ike policy policy-name]
- [edit security group-vpn server ike policy policy-name]
- [edit security ike policy policy-name]

**Release Information**

**Description**
Define a preshared key for an IKE policy.

**NOTE:** The device deletes existing IKE and IPsec SAs when you update the pre-shared-key configuration in the IKE policy.

**Options**
- `ascii-text key`—ASCII text key.
- `hexadecimal key`—Hexadecimal key.

**Required Privilege**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

### probe-idle-tunnel

**Supported Platforms**
- SRX Series

**Syntax**
`probe-idle-tunnel;`

**Hierarchy Level**
- [edit security ike gateway gateway-name dead-peer-detection]

**Release Information**
Statement introduced in Junos OS Release 12.1X46-D10.

**Description**
Send dead peer detection (DPD) messages during idle traffic time between peers.

**Required Privilege**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPN Feature Guide for Security Devices
**proposal (Security IKE)**

**Supported Platforms**
J Series, LN Series, SRX Series

**Syntax**

```plaintext
proposal proposal-name {
    authentication-algorithm (md5 | sha-256 | sha-384 | sha1);
    authentication-method (dsa-signatures | ecdsa-signatures-256 | ecdsa-signatures-384 |
                           pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group14 | group19 | group2 | group20 | group24 | group5);
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    lifetime-seconds seconds;
}
```

**Hierarchy Level**
[edit security ike]

**Release Information**
Statement modified in Junos OS Release 8.5. Support for dh-group group14 and
dsa-signatures added in Junos OS Release 11.1. Support for sha-384, ecdsa-signatures-256,
ecdsa-signatures-384, group19, group20, and group24 options added in Junos OS Release
12.1X45-D10.

**Description**
Define an IKE proposal.

**Options**

- **proposal-name**—Name of the IKE proposal. The proposal name can be up to 32
  alphanumeric characters long.

  The remaining statements are explained separately.

**Required Privilege**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- *AutoVPN Feature Guide for SRX Series Gateway Devices*
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*
- *IPsec VPN Feature Guide for Security Devices*
**proposal-set (Security IKE)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```
proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
```

**Hierarchy Level**  
[edit security ike policy *policy-name*]

**Release Information**  

**Description**  
Specify a set of default Internet Key Exchange (IKE) proposals.

**Options**

- **basic**—Basic set of two IKE proposals:
  - Proposal 1—Preshared key, Data Encryption Standard (DES) encryption, and Diffie-Hellman (DH) group 1 and Secure Hash Algorithm 1 (SHA-1) authentication.
  - Proposal 2—Preshared key, DES encryption, and DH group 1 and Message Digest 5 (MD5) authentication.

- **compatible**—Set of four commonly used IKE proposals:
  - Proposal 1—Preshared key, triple DES (3DES) encryption, and Gnutella2 (G2) and SHA-1 authentication.
  - Proposal 2—Preshared key, 3DES encryption, and DH group 2 and MD5 authentication.
  - Proposal 3—Preshared key, DES encryption, and DH group 2 and SHA-1 authentication.
  - Proposal 4—Preshared key, DES encryption, and DH group 2 and MD5 authentication.

- **standard**—Standard set of two IKE proposals:
  - Proposal 1—Preshared key, 3DES encryption, and DH group 2 and SHA-1 authentication.
  - Proposal 2—Preshared key, Advanced Encryption Standard (AES) 128-bit encryption, and DH group 2 and SHA-1 authentication.

- **suiteb-gcm-128**—Provides the following Suite B proposal (this option is not supported on group VPNs):
  - Authentication method—Elliptic Curve Digital Signal Algorithm (ECDSA) 256-bit signatures
  - Diffie-Hellman Group—19
  - Encryption algorithm—Advanced Encryption Standard (AES) 128-bit cipher block chaining (CBC)

**NOTE:** CBC mode is used instead of Galois/Counter Mode (GCM).
- Authentication algorithm—SHA-256
- **suiteb-gcm-256**—Provides the following Suite B proposal (this option is not supported on group VPNs):
  - Authentication method—ECDSA 384-bit signatures
  - Diffie-Hellman Group—20
  - Encryption algorithm—AES 256-bit CBC

---

**NOTE:** CBC mode is used instead of GCM.

- Authentication algorithm—SHA-384

---

**Required Privilege**
- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices

---

**proposals (Security IKE)**

**Supported Platforms**
- J Series, LN Series, SRX Series

**Syntax**
```
proposals [proposal-name];
```

**Hierarchy Level**
- [edit security group-vpn member ike policy policy-name]
- [edit security group-vpn server ike policy policy-name]
- [edit security ike policy policy-name]

**Release Information**

**Description**
- Specify up to four Phase 1 proposals for an IKE policy. If you include multiple proposals, use the same Diffie-Hellman group in all of the proposals.

**Options**
- **proposal-name**—Names of up to four configured Phase 1 proposals.

**Required Privilege**
- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
remote-identity

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```syntax
remote-identity {  
  (distinguished-name <container container-string> <wildcard wildcard-string> | hostname  
    hostname | inet ip-address | inet6 ipv6-address | user-at-hostname e-mail-address);  
}
```

**Hierarchy Level**  
[edit security ike gateway gateway-name]

**Release Information**  
Statement introduced in Junos OS Release 11.4.

**Description**  
Specify the remote IKE identity to exchange with the destination peer to establish communication. If you do not configure a remote-identity, the device uses the IPv4 or IPv6 address corresponding to the remote endpoint by default. (The distinguished-name option is not supported on dynamic VPN implementations.)

---

**NOTE:** For Network Address Translation Traversal (NAT-T), both remote identity and local identity must be configured.

---

**Options**  
- **distinguished-name**—Specify identity as the distinguished name (DN) from the certificate. If there is more than one certificate on the device, use the `security ike gateway gateway-name policy policy-name certificate local-certificate certificate-id`.
  
  Optional container and wildcard strings may be specified:
  
  - **container container-string**—Specify a string for the container.
  - **wildcard wildcard-string**—Specify a string for the wildcard.

- **hostname hostname**—Specify identity as a fully qualified domain name (FQDN).
- **inet ip-address**—Specify identity as an IPv4 address.
- **inet6 ipv6-address**—Specify identity as an IPv6 address.
- **user-at-hostname e-mail-address**—Specify identity as an e-mail address.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
respond-bad-spi

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  
respond-bad-spi max-responses;

**Hierarchy Level**  [edit security ike]

**Release Information**  Statement introduced in Junos OS Release 8.5.

**Description**  Enable response to invalid IPsec Security Parameter Index (SPI) values. If the security associations (SAs) between two peers of an IPsec VPN become unsynchronized, the device resets the state of a peer so that the two peers are synchronized.

**Options**  
*max-responses*—Number of times to respond to invalid SPI values per gateway.  
**Range:** 1 through 30  
**Default:** 5

**Required Privilege Level**  
- security—to view this statement in the configuration.  
- security-control—to add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices
### threshold (Security IKE Gateway)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
threshold number;

**Hierarchy Level**  
[edit security ike gateway gateway-name dead-peer-detection]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the maximum number of unsuccessful dead peer detection (DPD) requests to be sent before the peer is considered unavailable. (This statement is not supported on dynamic VPN implementations.)

**Options**  
**number**—Maximum number of unsuccessful DPD requests to be sent.  
**Range:** 1 through 5  
**Output:** 5

| Required Privilege Level | security—To view this statement in the configuration.  
|                         | security-control—To add this statement to the configuration.  

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices

**NOTE:** The threshold number for the IKEv2 protocol is predefined as 5.
traceoptions (Security IKE)

Supported Platforms  
J Series, LN Series, SRX Series

Syntax  
traceoptions {
    file {
        filename;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    no-remote-trace;
    rate-limit messages-per-second;
}

Hierarchy Level  
[edit security ike]

Release Information  
Statement introduced in Junos OS Release 8.5.

Description  
Configure IKE tracing options.

Options  
- file—Configure the trace file options.
  - filename—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.
  - files number—Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed to trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. The oldest archived file is overwritten.

  If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.

  Range: 2 through 1000 files

  Default: 10 files

  - match regular-expression—Refine the output to include lines that contain the regular expression.

  - size maximum-file-size—Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named trace-file reaches this size, it is renamed trace-file.0. When the trace-file again reaches its maximum size, trace-file.0 is renamed trace-file.1 and trace-file is renamed trace-file.0. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

  If you specify a maximum file size, you also must specify a maximum number of trace files with the files option and filename.

  Syntax: x k to specify KB, x m to specify MB, or x g to specify GB
Range: 10 KB through 1 GB
Default: 128 KB

- **world-readable | no-world-readable**—By default, log files can be accessed only by the user who configures the tracing operation. The **world-readable** option enables any user to read the file. To explicitly set the default behavior, use the **no-world-readable** option.

- **flag**—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.
  - **all**—Trace all iked process modules activity
  - **certificates**—Trace certificate-related activity
  - **config**—Trace configuration download processing
  - **database**—Trace VPN-related database activity
  - **general**—Trace general activity
  - **high-availability**—Trace high-availability operations
  - **ike**—Trace IKE protocol activity
  - **next-hop-tunnels**—Trace next-hop tunnels operations
  - **parse**—Trace VPN parsing activity
  - **policy-manager**—Trace iked callback activity
  - **routing-socket**—Trace routing socket activity
  - **thread**—Trace thread processing
  - **timer**—Trace timer activity
  - **no-remote-trace**—Set remote tracing as disabled.
  - **rate-limit messages-per-second**—Configure the incoming rate of trace messages.

Range: 0 through 4,294,967,295

<table>
<thead>
<tr>
<th>Required Privilege Level</th>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>trace</td>
<td>AutoVPN Feature Guide for SRX Series Gateway Devices</td>
</tr>
<tr>
<td></td>
<td>Dynamic VPN Feature Guide for SRX Series Gateway Devices</td>
</tr>
<tr>
<td></td>
<td>Group VPN Feature Guide for Security Devices</td>
</tr>
<tr>
<td></td>
<td>IPsec VPN Feature Guide for Security Devices</td>
</tr>
</tbody>
</table>
# trusted-ca (Security IKE Policy)

**Supported Platforms**  
LN Series, SRX Series

**Syntax**  
trusted-ca (ca-index | use-all);

**Hierarchy Level**  
[edit security group-vpn member ike policy policy-name certificate]  
[edit security group-vpn server ike policy policy-name certificate]  
[edit security ike policy policy-name certificate]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for `group-vpn` hierarchies added in Junos OS Release 10.2.

**Description**  
Specify the preferred certificate authority (CA) to use when requesting a certificate from the peer. If no value is specified, then no certificate request is sent (although incoming certificates are still accepted). (This statement is not supported on dynamic VPN implementations.)

**Options**  
- **ca-index**—Preferred certificate authority ID for the device to use.
- **use-all**—Device uses all configured certificate authorities.

**Required Privilege Level**  
security—to view this statement in the configuration.  
security-control—to add this statement to the configuration.

**Related Documentation**  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices
**user-at-hostname**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  
`user-at-hostname e-mail-address;`

**Hierarchy Level**  
[edit security group-vpn server ike gateway gateway-name dynamic]
[edit security ike gateway gateway-name dynamic]

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for **group-vpn server** hierarchy added in Junos OS Release 10.2.

**Description**  
Configure an e-mail address. (This statement is not supported on dynamic VPN implementations.)

**Options**  
`e-mail-address`—Valid e-mail address.

**Required Privilege**  
- **Security**—To view this statement in the configuration.
- **Security-Control**—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

**version (Security IKE Gateway)**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  
`version (v1-only | v2-only);`

**Hierarchy Level**  
[edit security ike gateway gateway-name]

**Release Information**  
Statement introduced in Junos OS Release 11.3.

**Description**  
Specify the IKE version to use to initiate the connection.

**Options**  
`v1-only`—The connection must be initiated using IKE version 1. This is the default.
`v2-only`—The connection must be initiated using IKE version 2.

**Required Privilege**  
- **Security**—To view this statement in the configuration.
- **Security-Control**—To add this statement to the configuration.

**Related Documentation**  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
wildcard

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`wildcard string;`

**Hierarchy Level**  
```
[edit security group-vpn server ike gateway gateway-name dynamic distinguished-name]
[edit security ike gateway gateway-name dynamic distinguished-name]
```

**Release Information**  
Statement introduced in Junos OS Release 8.5. Support for `group-vpn server` hierarchy added in Junos OS Release 10.2.

**Description**  
Specify that the values of a dynamic VPN (DVPN) endpoint user's distinguished name's identity fields match the values in the group IKE user's distinguished name's fields. The order of the identity fields in the distinguished name strings does not matter during a match. (This statement is not supported on DVPN implementations.)

**Options**  
`string`—Distinguished name identity values to be matched.

**Values:**  
The DVPN endpoint user's distinguished name's identity field values should be identical to the corresponding values in the group IKE user's distinguished name fields. If a DVPN endpoint user's distinguished name's identity field is null, the same field can have any value in the group IKE user's distinguished name's field.

**Required Privilege**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- [AutoVPN Feature Guide for SRX Series Gateway Devices](#)
- [Group VPN Feature Guide for Security Devices](#)
- [IPsec VPN Feature Guide for Security Devices](#)
xauth

Supported Platforms  J Series, LN Series, SRX Series

Syntax  xauth {
          access-profile profile-name;
        }

Hierarchy Level  [edit security ike gateway gateway-name]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Specify that Extended authentication (XAuth) is performed in addition to IKE authentication for remote users trying to access a VPN tunnel. Include a previously created access profile, created with the edit access profile statement, to specify the access profile to be used for authentication information.

Options  access-profile profile-name—Name of previously created access profile to reference for authentication information.

Required Privilege  Level
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation
• Dynamic VPN Feature Guide for SRX Series Gateway Devices
• Group VPN Feature Guide for Security Devices
• IPsec VPN Feature Guide for Security Devices
CHAPTER 23

IPsec Configuration Statements

- Security Configuration Statement Hierarchy on page 336
- [edit security ipsec] Hierarchy Level on page 337
- algorithm (Security) on page 340
- authentication (Security IPsec) on page 341
- authentication-algorithm (Security IPsec) on page 342
- bind-interface on page 343
- destination-ip (Security IPsec) on page 343
- df-bit on page 344
- encryption (Security) on page 345
- encryption-algorithm (Security IPsec) on page 346
- establish-tunnels on page 347
- external-interface (Security Manual SA) on page 347
- gateway (Security IPsec VPN) on page 348
- gateway (Security Manual SA) on page 348
- idle-time on page 349
- ike (Security IPsec VPN) on page 350
- install-interval on page 351
- ipsec (Security) on page 352
- ipsec-performance-acceleration (Security Flow) on page 354
- ipsec-policy (Security) on page 354
- ipsec-vpn (Security Flow) on page 355
- lifetime-kilobytes on page 355
- lifetime-seconds (Security IPsec) on page 356
- load-distribution on page 356
- local (Security IPsec) on page 357
- manual (Security IPsec) on page 358
- no-anti-replay (Security) on page 359
- optimized on page 359
Use the statements in the security configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones. Statements that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the [edit security] hierarchy.

- [edit security address-book] Hierarchy Level
- [edit security alarms] Hierarchy Level on page 378
- [edit security alg] Hierarchy Level
- [edit security analysis] Hierarchy Level
- [edit security application-firewall] Hierarchy Level
• [edit security application-tracking] Hierarchy Level
• [edit security certificates] Hierarchy Level
• [edit security datapath-debug] Hierarchy Level
• [edit security dynamic-vpn] Hierarchy Level
• [edit security firewall-authentication] Hierarchy Level
• [edit security flow] Hierarchy Level
• [edit security forwarding-options] Hierarchy Level
• [edit security forwarding-process] Hierarchy Level
• [edit security gprs] Hierarchy Level
• [edit security group-vpn] Hierarchy Level
• [edit security idp] Hierarchy Level
• [edit security ike] Hierarchy Level on page 291
• [edit security ipsec] Hierarchy Level on page 337
• [edit security log] Hierarchy Level
• [edit security nat] Hierarchy Level
• [edit security pki] Hierarchy Level
• [edit security policies] Hierarchy Level
• [edit security resource-manager] Hierarchy Level
• [edit security screen] Hierarchy Level
• [edit security softwires] Hierarchy Level
• [edit security ssh-known-hosts] Hierarchy Level
• [edit security traceoptions] Hierarchy Level
• [edit security user-identification] Hierarchy Level
• [edit security utm] Hierarchy Level
• [edit security zones] Hierarchy Level

Related Documentation
  • Master Administrator for Logical Systems Feature Guide for Security Devices
  • CLI User Guide

[edit security ipsec] Hierarchy Level

Supported Platforms
  J Series, LN Series, SRX Series

  security {
  ipsec {
    internal {
      security-association {
manual encryption {
    algorithm 3des-cbc;
    key ascii-text key;
}
}
policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24 | group5);
    proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
} proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm | aes-256-cbc | aes-256-gcm | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
}
security-association sa-name {
    manual {
        direction bidirectional {
            authentication {
                algorithm (hmac-md5-96 | hmac-sha1-96);
                key {
                    ascii-text key;
                    hexadecimal key;
                }
            }
            auxiliary-spi auxiliary-spi-value;
            encryption {
                algorithm (3des-cbc | des-cbc | null);
                key {
                    ascii-text key;
                    hexadecimal key;
                }
            }
            protocol (ah | esp);
            spi spi-value;
        }
        mode transport;
    }
    traceoptions {
        flag flag;
    }
} vpn vpn-name {
    bind-interface interface-name;
    df-bit (clear | copy | set);
    establish-tunnels (immediately | on-traffic);
    ike {
        gateway gateway-name;
    }
}
idle-time seconds;
install-interval seconds;
ipsec-policy ipsec-policy-name;
no-anti-replay;
proxy-identity {
  local ip-prefix;
  remote ip-prefix;
  service (any | service-name);
}
}
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  encryption {
    algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    key (ascii-text key | hexadecimal key);
  }
  external-interface external-interface-name;
  gateway ip-address;
  protocol (ah | esp);
  spi spi-value;
}
traffic-selector traffic-selector-name {
  local-ip ip-address/netmask;
  remote-ip ip-address/netmask;
}
vpn-monitor {
  destination-ip ip-address;
  optimized;
  source-interface interface-name;
}
vpn-monitor-options {
  interval seconds;
  threshold number;
}

Related Documentation

- Security Configuration Statement Hierarchy on page 290
- MPLS Feature Guide for Security Devices
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
algorithm (Security)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);

**Hierarchy Level**  
[edit security ipsec vpn vpn-name manual encryption]

**Release Information**  
Statement modified in Junos OS Release 8.5.

**Description**  
Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration. (This statement is not supported on dynamic VPN implementations.)

**Options**  
- 3des-cbc—3DES-CBC encryption algorithm.
- aes-256-cbc—AES-CBC 256-bit encryption algorithm.
- des-cbc—DES-CBC encryption algorithm.

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
authentication (Security IPsec)

Supported Platforms  J Series, LN Series, SRX Series

Syntax  
```
authentication {
    algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level  [edit security ipsec vpn vpn-name manual]


Description  Configure IPsec authentication parameters for a manual security association. This statement is not supported on dynamic VPN implementations.

Options  
- **algorithm**—Hash algorithm that authenticates packet data. It can be one of the following:
  - hmac-md5-96—Produce a 128-bit digest.
  - hmac-sha-256-128—Produce a 256-bit digest, truncated to 128 bits.
  - hmac-sha-256-96—Produce a 256-bit digest, truncated to 96 bits. This option is not supported on high-end SRX Series devices.
  - hmac-sha1-96—Produce a 160-bit digest.

- **key**—Type of authentication key. It can be one of the following:
  - ascii-text key—ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters.
  - hexadecimal key—Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.

Required Privilege  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation  
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
**authentication-algorithm (Security IPsec)**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  `authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);`

**Hierarchy Level**  `[edit security ipsec proposal proposal-name]`


**Description**  Configure the IPsec authentication algorithm.

**Options**  The hash algorithm to authenticate data can be one of the following:

- `hmac-md5-96`—Produce a 128-bit digest.
- `hmac-sha-256-128`—Produce a 256-bit digest, truncated to 128 bits. This option is not supported on group VPNs.
- `hmac-sha-256-96`—Produce a 256-bit digest, truncated to 96 bits. This option is not supported on group VPNs or high-end SRX Series devices.
- `hmac-sha1-96`—Produce a 160-bit digest.

**Required Privilege**  
- **Level**  security—to view this statement in the configuration.  
- security-control—to add this statement to the configuration.

**Related Documentation**  
- *AutoVPN Feature Guide for SRX Series Gateway Devices*  
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*  
- *IPsec VPN Feature Guide for Security Devices*
### bind-interface

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`bind-interface interface-name;`

**Hierarchy Level**  
`[edit security ipsec vpn vpn-name]`

**Release Information**  
Statement modified in Junos OS Release 8.5.

**Description**  
Configure the tunnel interface to which the route-based virtual private network (VPN) is bound.

**Options**  
`interface-name` — Tunnel interface.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices  
- IPsec VPN Feature Guide for Security Devices

### destination-ip (Security IPsec)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`destination-ip ip-address;`

**Hierarchy Level**  
`[edit security ipsec vpn vpn-name vpn-monitor]`

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the destination of the Internet Control Message Protocol (ICMP) pings. If this statement is used, the device uses the peer’s gateway address by default. (This statement is not supported on dynamic VPN implementations.)

**Options**  
`ip-address` — Destination IP address.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices
### df-bit

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
df-bit (clear | copy | set);

**Hierarchy Level**  
[edit security ipsec vpn vpn-name]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify how the device handles the Don't Fragment (DF) bit in the outer header.

**Options**  
- **clear**—Clear (disable) the DF bit from the outer header. This is the default.
- **copy**—Copy the DF bit to the outer header.
- **set**—Set (enable) the DF bit in the outer header.

**Required Privilege**  
- **level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
encryption (Security)

Supported Platforms  J Series, LN Series, SRX Series

Syntax  
```
encryption {
  algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
  key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level  [edit security ipsec vpn vpn-name manual]

Release Information  Statement modified in Junos OS Release 8.5.

Description  Configure an encryption algorithm and key for a manual Security Association (SA). (This statement is not supported on dynamic VPN implementations.)

Options  
- **algorithm**—Type of encryption algorithm. It can be one of the following:
  - **des-cbc**—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
  - **3des-cbc**—Has block size of 8 bytes (64 bits); its key size is 192 bits long

  **NOTE:** For **3des-cbc**, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.

  - **aes-128-cbc**—Advanced Encryption Standard (AES) 128-bit encryption algorithm.
  - **aes-192-cbc**—Advanced Encryption Standard (AES) 192-bit encryption algorithm.
  - **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption algorithm.

- **key**—Type of encryption key. It can be one of the following:
  - **ascii-text key**—ASCII text key. For the **des-cbc** option, the key contains 8 ASCII characters; for **3des-cbc**, the key contains 24 ASCII characters.
  - **hexadecimal key**—Hexadecimal key. For the **des-cbc** option, the key contains 16 hexadecimal characters; for the **3des-cbc** option, the key contains 48 hexadecimal characters.

Required Privilege Level  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation  
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
- Network Monitoring and Troubleshooting Guide for Security Devices
- System Log Monitoring and Troubleshooting Guide for Security Devices
encryption-algorithm (Security IPsec)

Supported Platforms  J Series, LN Series, SRX Series

Syntax  encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm | aes-256-cbc | aes-256-gcm | des-cbc);

Hierarchy Level  [edit security ipsec proposal proposal-name]


Description  Configure an encryption algorithm.

NOTE: The device deletes existing IPsec SAs when you update the encryption-algorithm configuration in the IPsec proposal.

Options  
- 3des-cbc—Has a block size of 24 bytes; the key size is 192 bits long.
- aes-128-gcm—AES Galois/Counter Mode (GCM) 128-bit encryption algorithm. This option is for IPsec proposals only. This option is not supported on group VPNs.
- aes-192-cbc—AES 192-bit encryption algorithm.
- aes-192-gcm—AES GCM 192-bit encryption algorithm. This option is for IPsec proposals only. This option is not supported on group VPNs.
- aes-256-cbc—AES 256-bit encryption algorithm.
- aes-256-gcm—AES GCM 256-bit encryption algorithm. This option is for IPsec proposals only. This option is not supported on group VPNs.
- des-cbc—Has a block size of 8 bytes; the key size is 48 bits long.

Required Privilege Level  security—to view this statement in the configuration.  security-control—to add this statement to the configuration.

Related Documentation  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
- Network Monitoring and Troubleshooting Guide for Security Devices
- System Log Monitoring and Troubleshooting Guide for Security Devices
### establish-tunnels

- **Supported Platforms**: J Series, LN Series, SRX Series
- **Syntax**: `establish-tunnels (immediately | on-traffic);`
- **Hierarchy Level**: `[edit security ipsec vpn vpn-name]`
- **Description**: Specify when IKE is activated: immediately after VPN information is configured and configuration changes are committed, or only when data traffic flows. In the second case, IKE needs to be negotiated with the peer gateway.
- **Options**:
  - `immediately`—IKE is activated immediately after VPN configuration and configuration changes are committed.
  - `on-traffic`—IKE is activated only when data traffic flows and must be negotiated.
- **Required Privilege Level**: security—To view this statement in the configuration. security-control—To add this statement to the configuration.
- **Related Documentation**:
  - AutoVPN Feature Guide for SRX Series Gateway Devices
  - Dynamic VPN Feature Guide for SRX Series Gateway Devices
  - Group VPN Feature Guide for Security Devices
  - IPsec VPN Feature Guide for Security Devices

### external-interface (Security Manual SA)

- **Supported Platforms**: J Series, LN Series, SRX Series
- **Syntax**: `external-interface external-interface-name;`
- **Hierarchy Level**: `[edit security ipsec vpn vpn-name manual]`
- **Description**: Specify the outgoing interface for the manual SA. (This statement is not supported on dynamic VPN implementations.)
- **Options**:
  - `external-interface-name`—Name of the outgoing interface.
- **Required Privilege Level**: security—To view this statement in the configuration. security-control—To add this statement to the configuration.
- **Related Documentation**:
  - Group VPN Feature Guide for Security Devices
  - IPsec VPN Feature Guide for Security Devices
**gateway (Security IPsec VPN)**

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax** `gateway ip-address;`

**Hierarchy Level** `[edit security ipsec vpn vpn-name ike]`

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the IP address of the peer.

**Options** `ip-address`—IP address of the peer.

**Required Privilege Level**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices

**gateway (Security Manual SA)**

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax** `gateway ip-address;`

**Hierarchy Level** `[edit security ipsec vpn vpn-name manual]`


**Description** For a manual security association, specify the IPv4 or IPv6 address of the peer. (This statement is not supported on dynamic VPN implementations.)

**Options** `ip-address`—IPv4 or IPv6 address of the peer.

**Required Privilege Level**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
idle-time

Supported Platforms  J Series, LN Series, SRX Series

Syntax  idle-time seconds;

Hierarchy Level  [edit security ipsec vpn vpn-name ike]

Release Information  Statement introduced in Junos OS Release 8.5.

Description  Specify the maximum amount of idle time to delete a security association (SA).

Options  seconds — Maximum amount of idle time.
          Range: 60 through 999999 seconds
          Default: To be disabled

Required Privilege Level

security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation

• AutoVPN Feature Guide for SRX Series Gateway Devices
• Dynamic VPN Feature Guide for SRX Series Gateway Devices
• Group VPN Feature Guide for Security Devices
• IPsec VPN Feature Guide for Security Devices
ike (Security IPsec VPN)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
ike {  
gateway gateway-name;  
idle-time seconds;  
install-interval seconds;  
ipsec-policy ipsec-policy-name;  
no-anti-replay;  
proxy-identity {  
  local ip-prefix;  
  remote ip-prefix;  
  service (any | service-name);  
}  
}

**Hierarchy Level**  
[edit security ipsec vpn vpn-name]

**Release Information**  

**Description**  
Define an IKE-keyed IPsec VPN.

**Options**  
The remaining statements are explained separately.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- *AutoVPN Feature Guide for SRX Series Gateway Devices*  
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*  
- *Group VPN Feature Guide for Security Devices*  
- *IPsec VPN Feature Guide for Security Devices*
### install-interval

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>J Series, LN Series, SRX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td><code>install-interval seconds;</code></td>
</tr>
<tr>
<td>Hierarchy Level</td>
<td><code>[edit security ipsec vpn vpn-name ike]</code></td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement introduced in Junos OS Release 8.5.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify the maximum number of seconds to allow for the installation of a rekeyed outbound security association (SA) on the device.</td>
</tr>
<tr>
<td>Options</td>
<td><code>seconds</code> — Maximum amount of idle time.</td>
</tr>
<tr>
<td>Range</td>
<td>0 through 10 seconds</td>
</tr>
<tr>
<td>Required Privilege</td>
<td>security — To view this statement in the configuration.</td>
</tr>
<tr>
<td>Level</td>
<td>security-control — To add this statement to the configuration.</td>
</tr>
<tr>
<td>Related Documentation</td>
<td>- Group VPN Feature Guide for Security Devices</td>
</tr>
<tr>
<td></td>
<td>- IPSec VPN Feature Guide for Security Devices</td>
</tr>
</tbody>
</table>
ipsec (Security)

Supported Platforms J Series, LN Series, SRX Series

Syntax

```plaintext
ipsec {
  policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24 | group5);
    proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
  }
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm | aes-256-cbc | aes-256-gcm | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
  }
  traceoptions {
    flag flag;
  }
  vpn vpn-name {
    bind-interface interface-name;
    df-bit (clear | copy | set);
    establish-tunnels (immediately | on-traffic);
    ike {
      gateway gateway-name;
      idle-time seconds;
      install-interval seconds;
      ipsec-policy ipsec-policy-name;
      no-anti-replay;
      proxy-identity {
        local ip-prefix;
        remote ip-prefix;
        service (any | service-name);
      }
    }
    manual {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      external-interface external-interface-name;
      gateway ip-address;
      protocol (ah | esp);
      spi spi-value;
    }
  }
  traffic-selector traffic-selector-name {
```

```
local-ip ip-address/netmask;
   remote-ip ip-address/netmask;
}
vpn-monitor {
   destination-ip ip-address;
   optimized;
   source-interface interface-name;
}
}
vpn-monitor-options {
   interval seconds;
   threshold number;
}
}

Hierarchy Level  [edit security]

Release Information Statement modified in Junos OS Release 8.5.

Description Define IP Security (IPsec) configuration.

Options The remaining statements are explained separately.

Required Privilege security—To view this statement in the configuration.
Level security-control—To add this statement to the configuration.

Related Documentation • AutoVPN Feature Guide for SRX Series Gateway Devices
• Dynamic VPN Feature Guide for SRX Series Gateway Devices
• IPsec VPN Feature Guide for Security Devices
• Master Administrator for Logical Systems Feature Guide for Security Devices
ipsec-performance-acceleration (Security Flow)

**Supported Platforms** SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

**Syntax**

```
ipsec-performance-acceleration;
```

**Hierarchy Level** [edit security flow]

**Release Information** Statement introduced in Junos OS Release 12.1X46-D10.

**Description** Enables IPsec VPN performance acceleration.

**Options** None.

**Required Privilege**

- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- IPsec VPN Feature Guide for Security Devices
- `show security flow status`

ipsec-policy (Security)

**Supported Platforms** J Series, LN Series, SRX Series

**Syntax**

```
ipsec-policy ipsec-policy-name;
```

**Hierarchy Level** [edit security ipsec vpn vpn-name ike]

**Release Information** Statement introduced in Junos OS Release 8.5.

**Description** Specify the IPsec policy name.

**Options**

- `ipsec-policy-name` — Name of the IPsec policy.

**Required Privilege**

- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
### ipsec-vpn (Security Flow)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```  
ipsec-vpn {  
mss value;  
}  
```

**Hierarchy Level**  
[edit security flow tcp-mss]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the TCP maximum segment size (TCP MSS) for the TCP packets that are about to go into an IPsec VPN tunnel. This value overrides the value specified in the `all-tcp-mss` statement.

**Options**  
- `mss value`—TCP MSS value for TCP packets entering an IPsec VPN tunnel. Value is optional.
  - **Range:** 64 through 65,535 bytes
  - **Default:** 1320 bytes

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices

### lifetime-kilobytes

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```  
lifetime-kilobytes kilobytes;  
```

**Hierarchy Level**  
[edit security ipsec proposal proposal-name]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the lifetime (in kilobytes) of an IPsec security association (SA).

**Options**  
- `kilobytes`—Lifetime of the IPsec security association (SA).
  - **Range:** 64 through 1048576 kilobytes

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices
**lifetime-seconds (Security IPsec)**

**Supported Platforms**
- J Series, LN Series, SRX Series

**Syntax**
```
lifetime-seconds seconds ;
```

**Hierarchy Level**
```
[edit security ipsec proposal proposal-name ]
```

**Release Information**

**Description**
Specify the lifetime (in seconds) of an IPsec security association (SA). When the SA expires, it is replaced by a new SA and security parameter index (SPI) or terminated.

**Options**
- `seconds`—Lifetime of the IPsec SA.
  - **Range:** 180 through 86,400 seconds
  - **Default:** 3600 seconds

**Required Privilege Level**
- `security`—To view this statement in the configuration.
- `security-control`—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

**load-distribution**

**Supported Platforms**
- LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

**Syntax**
```
load distribution {
    session-affinity ipsec;
}
```

**Hierarchy Level**
```
[edit security flow]
```

**Release Information**
Statement introduced in Junos OS Release 11.4R5.

**Description**
Enable load distribution for a data flow.

**Options**
The remaining statements are explained separately.

**Required Privilege Level**
- `security`—To view this statement in the configuration.
- `security-control`—To add this statement to the configuration.

**Related Documentation**
- IPsec VPN Feature Guide for Security Devices
local (Security IPsec)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
`local ip-prefix;`

**Hierarchy Level**  
`[edit security ipsec vpn vpn-name ike proxy-identity]`

**Release Information**  

**Description**  
Specify the local IPv4 or IPv6 address and subnet mask for the proxy identity.

**Options**  
`ip-prefix`—IPv4 or IPv6 address and subnet mask.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices
**manual (Security IPsec)**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**

```
manual {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  encryption {
    algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
    key (ascii-text key | hexadecimal key);
  }
  external-interface external-interface-name;
  gateway ip-address;
  protocol (ah | esp);
  spi spi-value;
}
```

**Hierarchy Level**  `[edit security ipsec vpn vpn-name]`


**Description**  Define a manual IPsec security association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options**  The remaining statements are explained separately.

**Required Privilege Level**

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- *IPsec VPN Feature Guide for Security Devices*
no-anti-replay (Security)

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
no-anti-replay;

**Hierarchy Level**  
[edit security ipsec vpn vpn-name ike]  
[edit security group-vpn server group group-name]

**Release Information**  

**Description**  
Disable the antireplay checking feature of IPsec. By default, antireplay checking is enabled.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
• Group VPN Feature Guide for Security Devices  
• IPsec VPN Feature Guide for Security Devices

optimized

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
optimized;

**Hierarchy Level**  
[edit security ipsec vpn vpn-name vpn-monitor]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify that the device uses traffic patterns as evidence of peer liveliness. If enabled, ICMP requests are suppressed. This feature is disabled by default. (This statement is not supported on dynamic VPN implementations.)

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
• AutoVPN Feature Guide for SRX Series Gateway Devices  
• Group VPN Feature Guide for Security Devices  
• IPsec VPN Feature Guide for Security Devices
peer-certificate-type

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  peer-certificate-type (pkcs7 | x509-signature);

**Hierarchy Level**  
[edit security group-vpn member ike policy policy-name certificate]
[edit security group-vpn server ike policy policy-name certificate]
[edit security ike policy policy-name certificate]

**Release Information**  Statement introduced in Junos OS Release 8.5. Support for group-vpn hierarchies added in Junos OS Release 10.2.

**Description**  Specify a preferred type of certificate (PKCS7 or X509). (This statement is not supported on dynamic VPN implementations.)

**Options**  
- **pkcs7**—Public-Key Cryptography Standard #7.
- **x509-signature**—X509 is an ITU-T standard for public key infrastructure.

**Required Privilege**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- *Group VPN Feature Guide for Security Devices*
- *IPsec VPN Feature Guide for Security Devices*
perfect-forward-secrecy (Security IPsec)

**Supported Platforms**
J Series, LN Series, SRX Series

**Syntax**
perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24 | group5);

**Hierarchy Level**
[edit security ipsec policy policy-name]

**Release Information**

**Description**
Specify Perfect Forward Secrecy (PFS) as the method that the device uses to generate the encryption key. PFS generates each new encryption key independently from the previous key.

---

**NOTE:** The device deletes existing IPsec SAs when you update the perfect-forward-secrecy configuration in the IPsec policy.

---

**Options**
- **group1**—Diffie-Hellman Group 1.
- **group14**—Diffie-Hellman Group 14. This option is not supported on dynamic VPNs.
- **group19**—Diffie-Hellman Group 19. This option is not supported on group VPNs.
- **group2**—Diffie-Hellman Group 2.
- **group20**—Diffie-Hellman Group 20. This option is not supported on group VPNs.
- **group24**—Diffie-Hellman Group 24. This option is not supported on group VPNs.
- **group5**—Diffie-Hellman Group 5.

**Required Privilege Level**
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
policy (Security IPsec)

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  
```
policy policy-name {
    description description;
    perfect-forward-secrecy keys (group1 | group14 | group19 | group2 | group20 | group24 | group5);
    proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);
    proposals [proposal-name];
}
```

**Hierarchy Level**  [edit security ipsec]

**Release Information**  Statement modified in Junos OS Release 8.5. Support for group 14 is added in Junos OS Release 11.1.

**Description**  Define an IPsec policy.

**Options**  
- `policy-name` — Name of the IPsec policy.

The remaining statements are explained separately.

**Required Privilege Level**  
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
proposal (Security IPsec)

Supported Platforms

J Series, LN Series, SRX Series

Syntax

```
proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | aes-128-cbc | aes-128-gcm | aes-192-cbc | aes-192-gcm | aes-256-cbc | aes-256-gcm | des-cbc);
    lifetime-kilobytes kilobytes;
    lifetime-seconds seconds;
    protocol (ah | esp);
}
```

Hierarchy Level

[edit security ipsec]

Release Information

Statement modified in Junos OS Release 8.5.

Description

Define an IPsec proposal.

Options

- `proposal-name`—Name of the IPsec proposal.

The remaining statements are explained separately.

Required Privilege

- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

Related Documentation

- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
**proposal-set (Security IPsec)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
proposal-set (basic | compatible | standard | suiteb-gcm-128 | suiteb-gcm-256);

**Hierarchy Level**  
[edit security ipsec policy policy-name]

**Release Information**  

**Description**  
Define a set of default IPsec proposals.

**Options**
- **basic**—nopfs-esp-des-sha and nopfs-esp-des-md5
- **compatible**—nopfs-esp-3des-sha, nopfs-esp-3des-md5, nopfs-esp-des-sha, and nopfs-esp-des-md5
- **standard**—g2-esp-3des-sha and g2-esp-aes128-sha
- **suiteb-gcm-128**—Provides the following Suite B proposal:
  - Encapsulating Security Payload (ESP) protocol
  - Encryption algorithm—Advanced Encryption Standard Galois/Counter mode (AES-GCM)128-bit
  - Authentication algorithm—None (AES-GCM provides both encryption and authentication)

**NOTE:** This option is not supported on group VPNs.

- **suiteb-gcm-256**—Provides the following Suite B proposal:
  - ESP protocol
  - Encryption algorithm—AES-GCM 256-bit
  - Authentication algorithm—None (AES-GCM provides both encryption and authentication)

**NOTE:** This option is not supported on group VPNs.

**NOTE:** Perfect Forward Secrecy setting in IPsec policy will override the settings in proposal-sets in Release 10.4 and later.
proposals (Security IPsec)

**Supported Platforms**
- J Series, LN Series, SRX Series

**Syntax**
```
proposals [proposal-name];
```

**Hierarchy Level**
```
[edit security ipsec policy policy-name]
```

**Release Information**
Statement modified in Junos OS Release 8.5.

**Description**
Specify one or more proposals for an IPsec policy.

**Options**
- `proposal-name`—Name of a configured proposal.

---

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
**protocol (Security IPsec)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
protocol (ah | esp);

**Hierarchy Level**  
[edit security ipsec proposal *proposal-name* ]

**Release Information**  
Statement modified in Junos OS Release 8.5.

**Description**  
Define the IPsec protocol for a manual or dynamic security association (SA).

---

**NOTE:** The device deletes existing IPsec SAs when you update the encryption-algorithm configuration in the IPsec proposal.

---

**Options**
- `ah`—Authentication Header protocol.
- `esp`—Encapsulating Security Payload (ESP) protocol.

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- IPsec VPN Feature Guide for Security Devices
**protocol (Security IPsec Manual SA)**

<table>
<thead>
<tr>
<th>Supported Platforms</th>
<th>J Series, LN Series, SRX Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax</td>
<td>`protocol (ah</td>
</tr>
<tr>
<td>Hierarchy Level</td>
<td><code>[edit security ipsec vpn vpn-name manual]</code></td>
</tr>
<tr>
<td>Release Information</td>
<td>Statement modified in Junos OS Release 8.5.</td>
</tr>
<tr>
<td>Description</td>
<td>Define the IPsec protocol for the manual security association. (This statement is not supported on dynamic VPN implementations.)</td>
</tr>
</tbody>
</table>
| Options             | • ah—Authentication Header protocol.  
                      • esp—ESP protocol (To use the ESP protocol, you must also use the `tunnel` statement at the `[edit security ipsec security-association sa-name mode]` hierarchy level.) |
| Required Privilege Level | security—To view this statement in the configuration.  
                          security-control—To add this statement to the configuration. |
| Related Documentation | • *Group VPN Feature Guide for Security Devices*  
                          • *IPsec VPN Feature Guide for Security Devices* |
proxy-identity

Supported Platforms  J Series, LN Series, SRX Series

Syntax  
proxy-identity {
  local ip-prefix;
  remote ip-prefix;
  service (all | service-name);
}

Hierarchy Level  [edit security ipsec vpn vpn-name ike]


Description  Optionally specify the IPsec proxy ID to use in negotiations. The default is the identity based on the IKE gateway. If the IKE gateway is an IPv6 site-to-site gateway, the default proxy ID is ::/0. If the IKE gateway is an IPv4 gateway or a dynamic endpoint or dialup gateway, the default proxy ID is 0.0.0.0/0.

Options  The remaining statements are explained separately.

Required Privilege Level  
- security—to view this statement in the configuration.
- security-control—to add this statement to the configuration.

Related Documentation  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
refresh-interval

 Supported Platforms SRX Series
 Syntax refresh-interval hours;
 Hierarchy Level [edit security pki ca-profile ca-profile-name revocation-check crl]
 Release Information Statement introduced in Junos OS Release 8.5.
 Description Specify the amount of time between certificate revocation list (CRL) updates.
 Options number-of-hours—Time interval, in hours, between CRL updates.
 Range: 0 through 8784
 Default: 6
 Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.
 Related Documentation • Security Configuration Statement Hierarchy on page 290
 • [edit security pki] Hierarchy Level
 • crl (Security)

remote (Security IPsec)

 Supported Platforms J Series, LN Series, SRX Series
 Syntax remote ip-prefix;
 Hierarchy Level [edit security ipsec vpn vpn-name ike proxy-identity]
 Description Specify the remote IPv4 or IPv6 address and subnet mask for the proxy identity.
 Options ip-prefix—IPv4 or IPv6 address and subnet mask.
 Required Privilege Level security—To view this statement in the configuration.
 security-control—To add this statement to the configuration.
 Related Documentation • AutoVPN Feature Guide for SRX Series Gateway Devices
 • Dynamic VPN Feature Guide for SRX Series Gateway Devices
 • Group VPN Feature Guide for Security Devices
 • IPsec VPN Feature Guide for Security Devices
**service (Security IPsec)**

**Supported Platforms**  J Series, LN Series, SRX Series

**Syntax**  service (all | service-name);

**Hierarchy Level**  [edit security ipsec vpn vpn-name ike proxy-identity]

**Release Information**  Statement introduced in Junos OS Release 8.5.

**Description**  Specify the service (port and protocol combination) to protect.

**Options**  service-name — Name of the service, as defined with system-services (Interface Host-Inbound Traffic) and system-services (Zone Host-Inbound Traffic).

**Required Privilege Level**  security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices  
- Group VPN Feature Guide for Security Devices  
- IPsec VPN Feature Guide for Security Devices

**session-affinity**

**Supported Platforms**  LN Series, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

**Syntax**  session-affinity ipsec

**Hierarchy Level**  [edit security flow load-distribution]

**Release Information**  Statement introduced in Junos OS Release 11.4R5.

**Description**  Enable VPN session affinity.

**Required Privilege Level**  security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
- IPsec VPN Feature Guide for Security Devices
**source-interface (Security)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
source-interface  *interface-name* ;

**Hierarchy Level**  
[edit security ipsec vpn  *vpn-name* vpn-monitor]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Specify the source interface for ICMP requests (VPN monitoring “hellos”). If no source interface is specified, the device automatically uses the local tunnel endpoint interface. (This statement is not supported on dynamic VPN implementations.)

**Options**  
*interface-name* — Name of the interface for the ICMP requests.

**Required Privilege**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

**spi (Security IPsec)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
spi  *spi-value* ;

**Hierarchy Level**  
[edit security ipsec vpn  *vpn-name* manual]

**Release Information**  
Statement modified in Junos OS Release 8.5.

**Description**  
Configure a security parameter index (SPI) for a security association (SA). (This statement is not supported on dynamic VPN implementations.)

**Options**  
*spi-value* — An arbitrary value that uniquely identifies which security association (SA) to use at the receiving host (the destination address in the packet).

**Range:** 256 through 16639

**Required Privilege**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
**traceoptions (Security IPsec)**

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
traceoptions {
  flag flag;
}

**Hierarchy Level**  
[edit security ipsec]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Configure IPsec tracing options.

---

**NOTE:** Configure IPsec tracing options only when instructed to do so by your Juniper support representative.

---

Trace operations are written to the trace file /var/log/kmd.

**Options**  
- **flag**—To specify more than one trace operation, include multiple flag statements.
  - all—Trace with all flags enabled
  - next-hop-tunnel-binding—Trace next-hop tunnel binding events
  - packet-drops—Trace packet drop activity
  - packet-processing—Trace data packet processing events
  - security-associations—Trace security association (SA) management events

**Required Privilege Level**  
- trace—To view this statement in the configuration.
- trace-control—To add this statement to the configuration.

**Related Documentation**  
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPSec VPN Feature Guide for Security Devices
**traffic-selector**

**Syntax**
traffic-selector traffic-selector-name {
local-ip ip-address/netmask;
remote-ip ip-address/netmask;
}

**Hierarchy Level**
[edit security ipsec vpn vpn-name]

**Release Information**
Statement introduced in Junos OS Release 12.1X46-D10.

**Description**
Configure local and remote IP addresses for a traffic selector.

**Options**
- **local-ip ip-address/netmask**—A local IP address or a local subnetwork protected by the local VPN device.
- **remote-ip ip-address/netmask**—A remote IP address or a remote subnetwork protected by the peer VPN device.

**Required Privilege**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- *IPsec VPN Feature Guide for Security Devices*
vpn (Security)

Supported Platforms  J Series, LN Series, SRX Series

Syntax  
```
vpn vpn-name {
  bind-interface interface-name;
  df-bit (clear | copy | set);
  establish-tunnels (immediately | on-traffic);
  ike {
    gateway gateway-name;
    idle-time seconds;
    install-interval seconds;
    ipsec-policy ipsec-policy-name;
    no-anti-replay;
    proxy-identity {
      local ip-prefix;
      remote ip-prefix;
      service (any | service-name);
    }
  }
  manual {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha-256-128 | hmac-sha-256-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    encryption {
      algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    external-interface external-interface-name;
    gateway ip-address;
    protocol (ah | esp);
    spi spi-value;
  }
  traffic-selector traffic-selector-name {
    local-ip ip-address/netmask;
    remote-ip ip-address/netmask;
  }
  vpn-monitor {
    destination-ip ip-address;
    optimized;
    source-interface interface-name;
  }
}
```

Hierarchy Level  [edit security ipsec]


Description  Configure an IPsec VPN.

Options  
- **vpn-name** — Name of the VPN.
The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices

### vpn-monitor

**Supported Platforms**
- J Series, LN Series, SRX Series

**Syntax**
```
vpn-monitor {
  destination-ip ip-address;
  optimized;
  source-interface interface-name;
}
```

**Hierarchy Level**
- [edit security ipsec vpn vpn-name]

**Release Information**
- Statement introduced in Junos OS Release 8.5.

**Description**
Configure settings for VPN monitoring. This feature cannot be configured simultaneously with the `dead-peer-detection` statement. (This statement is not supported on dynamic VPN implementations.)

**Options**
The remaining statements are explained separately.

**Required Privilege**
- **Level**
  - security—To view this statement in the configuration.
  - security-control—To add this statement to the configuration.

**Related Documentation**
- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
## vpn-monitor-options

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```  
vpn-monitor-options {  
  interval seconds;  
  threshold number;  
}  
```

**Hierarchy Level**  
[edit security ipsec]

**Release Information**  
Statement introduced in Junos OS Release 8.5.

**Description**  
Configure VPN monitoring options. (This statement is not supported on dynamic VPN implementations.)

**Options**

- **interval seconds** — Interval at which to send ICMP requests to the peer.
  
  **Range:** 2 through 3600 seconds  
  **Default:** 10 seconds

- **threshold number** — Number of consecutive unsuccessful pings before the peer is declared unreachable.
  
  **Range:** 1 through 65536 pings  
  **Default:** 10 pings

**Required Privilege Level**  
security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**

- AutoVPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
CHAPTER 24

VPN Alarms Configuration Statements

- Security Configuration Statement Hierarchy on page 377
- [edit security alarms] Hierarchy Level on page 378
- cryptographic-self-test on page 380
- decryption-failures on page 381
- encryption-failures on page 382
- key-generation-self-test on page 383
- ike-phase1-failures on page 384
- ike-phase2-failures on page 385
- non-cryptographic-self-test on page 386
- replay-attacks on page 387

Security Configuration Statement Hierarchy

Supported Platforms  J Series, LN Series, SRX Series

Use the statements in the security configuration hierarchy to configure actions, certificates, dynamic virtual private networks (VPNs), firewall authentication, flow, forwarding options, group VPNs, Intrusion Detection Prevention (IDP), Internet Key Exchange (IKE), Internet Protocol Security (IPsec), logging, Network Address Translation (NAT), public key infrastructure (PKI), policies, resource manager, rules, screens, secure shell known hosts, trace options, user identification, Unified Threat Management (UTM), and zones.

Statements that are exclusive to the J Series and SRX Series devices running Junos OS are described in this section.

Each of the following topics lists the statements at a sub-hierarchy of the [edit security] hierarchy.

- [edit security address-book] Hierarchy Level
- [edit security alarms] Hierarchy Level on page 378
- [edit security alg] Hierarchy Level
- [edit security analysis] Hierarchy Level
- [edit security application-firewall] Hierarchy Level
[edit security application-tracking] Hierarchy Level
[edit security certificates] Hierarchy Level
[edit security datapath-debug] Hierarchy Level
[edit security dynamic-vpn] Hierarchy Level
[edit security firewall-authentication] Hierarchy Level
[edit security flow] Hierarchy Level
[edit security forwarding-options] Hierarchy Level
[edit security forwarding-process] Hierarchy Level
[edit security gprs] Hierarchy Level
[edit security group-vpn] Hierarchy Level
[edit security idp] Hierarchy Level
[edit security ike] Hierarchy Level on page 291
[edit security ipsec] Hierarchy Level on page 337
[edit security log] Hierarchy Level
[edit security nat] Hierarchy Level
[edit security pki] Hierarchy Level
[edit security policies] Hierarchy Level
[edit security resource-manager] Hierarchy Level
[edit security screen] Hierarchy Level
[edit security softwires] Hierarchy Level
[edit security ssh-known-hosts] Hierarchy Level
[edit security traceoptions] Hierarchy Level
[edit security user-identification] Hierarchy Level
[edit security utm] Hierarchy Level
[edit security zones] Hierarchy Level

Related Documentation
- CLI User Guide

[edit security alarms] Hierarchy Level

Supported Platforms
J Series, LN Series, SRX Series

```
security {
alarms {
  audible {
    continuous;
  }
}
```
potential-violation {
  authentication-failures;
  cryptographic-self-test;
  decryption-failures {
    threshold value;
  }
  encryption-failures {
    threshold value;
  }
  idp;
  ike-phase1-failures {
    threshold value;
  }
  ike-phase2-failures {
    threshold value;
  }
  key-generation-self-test;
  non-cryptographic-self-test;
  policy {
    application {
      duration interval;
      size count;
      threshold value;
    }
    destination-ip {
      duration interval;
      size count;
      threshold value;
    }
    policy match {
      duration interval;
      size count;
      threshold value;
    }
    source-ip {
      duration interval;
      size count;
      threshold value;
    }
  }
  replay-attacks {
    threshold value;
  }
  security-log-percent-full percentage;
}

Related Documentation
  • Security Configuration Statement Hierarchy on page 290
  • IPsec VPN Feature Guide for Security Devices
  • IDP Policies Feature Guide for Security Devices
cryptographic-self-test

Supported Platforms | LN Series, SRX Series

Syntax | cryptographic-self-test;

Hierarchy Level | [edit security alarms potential-violation ]

Release Information | Statement introduced in Junos OS Release 11.2.

Description | Raise a security alarm when the device or switch detects a cryptographic self-test failure. Cryptographic self-tests are a set of preoperational tests that are performed after the device or switch is powered on. The self-test run without operator intervention.

Default | No alarm is raised upon failure of a cryptographic self-test.

Required Privilege Level | security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation | • Dynamic VPN Feature Guide for SRX Series Gateway Devices
• Group VPN Feature Guide for Security Devices
• IPsec VPN Feature Guide for Security Devices
**decryption-failures**

**Supported Platforms**
LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650

**Syntax**
```
decryption-failures {
    threshold value;
}
```

**Hierarchy Level**
[edit security alarms potential-violation]

**Release Information**
Statement introduced in Junos OS Release 11.2.

**Description**
Raise a security alarm after exceeding a specified number of decryption failures.

**Default**
Multiple decryption failures do not cause an alarm to be raised.

**Options**
- **failures**—Number of decryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.
  - **Range:** 0 through 1 through 1,000,000,000.
  - **Default:** 1000

**Required Privilege**
- **security**—To view this statement in the configuration.
- **security-control**—To add this statement to the configuration.

**Related Documentation**
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
encryption-failures

Supported Platforms LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650

Syntax encryption-failures {
    threshold value;
}

Hierarchy Level [edit security alarms potential-violation]

Release Information Statement introduced in Junos OS Release 11.2.

Description Raise a security alarm after exceeding a specified number of encryption failures.

Default Multiple encryption failures do not cause an alarm to be raised.

Options failures—Number of encryption failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

Range: 1 through 1000000000.
Default: 1000

Required Privilege Level security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

Related Documentation • Dynamic VPN Feature Guide for SRX Series Gateway Devices
• Group VPN Feature Guide for Security Devices
• IPsec VPN Feature Guide for Security Devices
**key-generation-self-test**

**Supported Platforms**  LN Series, SRX Series

**Syntax**  key-generation-self-test;

**Hierarchy Level**  [edit security alarms potential-violation]

**Release Information**  Statement introduced in Junos OS Release 11.2.

**Description**  Raise a security alarm when the device or switch detects a key generation self-test failure. Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt data. The self-tests run without operator intervention.

**Default**  No alarm is raised upon failure of a key generation self-test.

**Required Privilege Level**  security—To view this statement in the configuration.  
security-control—To add this statement to the configuration.

**Related Documentation**  
• Dynamic VPN Feature Guide for SRX Series Gateway Devices  
• Group VPN Feature Guide for Security Devices  
• IPsec VPN Feature Guide for Security Devices
# ike-phase1-failures

**Supported Platforms**
LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650

**Syntax**
ike-phase1-failures {
    threshold value;
}

**Hierarchy Level**
[edit security alarms potential-violation]

**Release Information**
Statement introduced in Junos OS Release 11.2.

**Description**
Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) Phase 1 failures.

**Default**
Multiple IKE phase 1 failures do not cause an alarm to be raised.

**Options**
- **failures**—Number of IKE phase 1 failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.
  - **Range:** 1 through 1000000000.
  - **Default:** 20

**Required Privilege Level**
- security—To view this statement in the configuration.
- security-control—To add this statement to the configuration.

**Related Documentation**
- *Dynamic VPN Feature Guide for SRX Series Gateway Devices*
- *Group VPN Feature Guide for Security Devices*
- *IPsec VPN Feature Guide for Security Devices*
### ike-phase2-failures

**Supported Platforms**  
LN Series, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650

**Syntax**  
ike-phase2-failures {
  threshold value;
}

**Hierarchy Level**  
[edit security alarms potential-violation]

**Release Information**  
Statement introduced in Junos OS Release 11.2.

**Description**  
Raise a security alarm after exceeding a specified number of Internet Key Exchange (IKE) phase 2 failures.

**Default**  
Multiple IKE phase 2 failures do not cause an alarm to be raised.

**Options**  
* failures—Number of IKE phase 2 failures up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.
  
  **Range:** 1 through 1000000000.
  **Default:** 20

**Required Privilege Level**  
security—To view this statement in the configuration.
security-control—To add this statement to the configuration.

**Related Documentation**  
- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
### non-cryptographic-self-test

**Supported Platforms**  LN Series, SRX Series

**Syntax**  non-cryptographic-self-test;

**Hierarchy Level**  [edit security alarms potential-violation]

**Release Information**  Statement introduced in Junos OS Release 11.2.

**Description**  Raise a security alarm when the device or switch detects a noncryptographic self-test failure. The self-tests run without operator intervention.

**Default**  No alarm is raised upon failure of a noncryptographic self-test.

**Required Privilege**

- **Level**  security—To view this statement in the configuration.
- **security-control—To add this statement to the configuration.**

**Related Documentation**

- Dynamic VPN Feature Guide for SRX Series Gateway Devices
- Group VPN Feature Guide for Security Devices
- IPsec VPN Feature Guide for Security Devices
replay-attacks

Supported Platforms  LN Series, SRX Series

Syntax  replay-attacks {
  threshold value;
}

Hierarchy Level  [edit security alarms potential-violation]

Release Information  Statement introduced in Junos OS Release 11.2.

Description  Raise a security alarm when the device detects a replay attack. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

Default  Replay attacks do not raise security alarms.

Options  
  • threshold value—Number of reply attacks up to which an alarm is not raised. When the configured number is exceeded, an alarm is raised.

  Range: Range: 0 through 100,000,000.

Required Privilege Level  security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

Related Documentation  • Dynamic VPN Feature Guide for SRX Series Gateway Devices
  • Group VPN Feature Guide for Security Devices
  • IPsec VPN Feature Guide for Security Devices
PART 3

Administration

• Operational Commands on page 391
CHAPTER 25

Operational Commands

- clear security ike respond-bad-spi-count
- clear security ike security-associations
- clear security ipsec security-associations
- clear security ipsec statistics
- request security ike debug-disable
- request security ike debug-enable
- show security ike active-peer
- show security ike debug-status
- show security ike pre-shared-key
- show security ike security-associations
- show security ike tunnel-map
- show security ipsec inactive-tunnels
- show security ipsec next-hop-tunnels
- show security ipsec security-associations
- show security ipsec statistics
clear security ike respond-bad-spi-count

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
clear security ike respond-bad-spi-count  
< gateway-name >

**Release Information**  
Command introduced in Junos OS Release 8.5.

**Description**  
Clear information about invalid Internet Key Exchange (IKE) security parameter index (SPI) counters.

**Options**  
- **none**—Clear all invalid SPI counters.
- **gateway-name**—(Optional) Clear the invalid SPI counters for the given gateway.

**Required Privilege Level**  
clear

**Related Documentation**  
- respond-bad-spi on page 327

**List of Sample Output**  
clear security ike respond-bad-spi-count on page 392  
clear security ike respond-bad-spi-count gateway-name1 on page 392

**Output Fields**  
This command produces no output.

**Sample Output**
clear security ike respond-bad-spi-count

```
user@host> clear security ike respond-bad-spi-count
```

**Sample Output**
clear security ike respond-bad-spi-count gateway-name1

```
user@host> clear security ike respond-bad-spi-count gateway-name1
```
# clear security ike security-associations

## Supported Platforms
- J Series
- LN Series
- SRX Series

## Syntax
```
clear security ike security-associations
< peer-address >
< port >
<fpc slot-number>
<index SA-index-number>
<kmd-instance (all | kmd-instance-name)>
<pic slot-number>
port
<family (inet | inet6)>
```

## Release Information

## Description
Clear information about the current Internet Key Exchange security associations (IKE SAs). For IKEv2, the device clears the information about the IKE SAs and the associated IPSec SA.

## Options
- **none**—Clear all IKE SAs.
- **peer-address** — (Optional) Clear IKE SAs for the destination peer at this IP address.
- **fpc slot-number** — Specific to SRX Series devices. Clear information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot.
- **index SA-index-number** — (Optional) Clear the IKE SA with this index number.
- **port** — (Optional) Port number of SA (1 through 65,535).
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC **slot-number** and PIC **slot-number**.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - **kmd-instance-name**—Name of the KMD instance running on the SPU.
- **pic slot-number**—Specific to SRX Series devices. Clear information about existing IKE SAs in this PIC slot.
- **family**— (Optional) Clear IKE SAs by family.
  - **inet**—IPv4 address family.
  - **inet6**—IPv6 address family.

## Required Privilege
- clear
Related Documentation

- show security ike security-associations on page 404

List of Sample Output

clear security ike security-associations on page 394

clear security ike security-associations 1.1.2 port 19405 on page 394

clear security ike security-associations index 8 on page 394

clear security ike security-associations family inet6 on page 394

clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices) on page 394

Output Fields

This command produces no output.

Sample Output

clear security ike security-associations

user@host> clear security ike security-associations

Sample Output

clear security ike security-associations 1.1.2 port 19405

user@host> clear security ike security-associations 1.1.2 port 19405

Sample Output

clear security ike security-associations index 8

user@host> clear security ike security-associations index 8

Sample Output

clear security ike security-associations family inet6

user@host> clear security ike security-associations family inet6

Sample Output

clear security ike security-associations fpc 5 pic 0 kmd-instance all (SRX Series Devices)

user@host> clear security ike security-associations fpc 5 pic 0 kmd-instance all
clear security ipsec security-associations

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
clear security ipsec security-associations  
fpc slot-number  
<index SA-index-number>  
kmd-instance (all | kmd-instance-name )  
pic slot-number  
<fAMILY (inet | inet6)>  

**Release Information**  

**Description**  
Clear information about IPsec security associations (SAs).

**Options**
- none—Clear all IPsec SAs.
- **fpc** slot-number—Specific to SRX Series devices. Clear information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot.
- **index** SA-index-number—(Optional) Clear the IPsec SA with this index number.
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IPsec SAs in the key management process (the daemon, which in this case is KMD) identified by FPC slot-number and PIC slot-number.
  - all—All KMD instances running on the Services Processing Unit (SPU).
  - kmd-instance-name—Name of the KMD instance running on the SPU.
- **pic** slot-number—Specific to SRX Series devices. Clear information about existing IPsec SAs in this PIC slot.
- **family**—(Optional) Clear SAs by family.
  - inet—IPv4 address family.
  - inet6—IPv6 address family.

**Required Privilege Level**  
clear

**Related Documentation**
- show security ipsec security-associations on page 416

**List of Sample Output**
- clear security ipsec security-associations on page 396
- clear security ipsec security-associations index 8 on page 396
- clear security ipsec security-associations family inet6 on page 396

**Output Fields**  
This command produces no output.
Sample Output

`clear security ipsec security-associations`

```
user@host> clear security ipsec security-associations
```

Sample Output

`clear security ipsec security-associations index 8`

```
user@host> clear security ipsec security-associations index 8
```

Sample Output

`clear security ipsec security-associations family inet6`

```
user@host> clear security ipsec security-associations family inet6
```
### clear security ipsec statistics

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```
clear security ike statistics  
   <fpc slot-number>  
   <index SA-index-number>  
   <kmd-instance (all | kmd-instance-name )>  
   <pic slot-number>
```

**Release Information**  

**Description**  
Clear IPsec statistics on the device.

**Options**  
- **none**—Clear all IPsec statistics.
- **fpc slot-number**—Specific to SRX Series devices. Clear statistics about existing IPsec security associations (SAs) in this Flexible PIC Concentrator (FPC) slot.
- **index SA-index-number**—(Optional) Clear the IPsec statistics for the SA with this index number.
- **kmd-instance**—Specific to SRX Series devices. Clear information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC *slot-number* and PIC *slot-number*.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - **kmd-instance-name**—Name of the KMD instance running on the SPU.
- **pic slot-number**—Specific to SRX Series devices. Clear statistics about existing IPsec SAs in this PIC slot.

**Required Privilege**  
`clear`

**Related Documentation**  
- show security ipsec statistics on page 424

**List of Sample Output**  
- clear security ipsec statistics on page 397
- clear security ipsec statistics index 1 on page 398
- clear security ipsec statistics fpc 5 pic 0 (SRX Series devices) on page 398

**Output Fields**  
This command produces no output.

**Sample Output**  
```
clear security ipsec statistics

user@host> clear security ipsec statistics
```
Sample Output

```
clear security ipsec statistics index 1
```

user@host> clear security ipsec statistics index 1

Sample Output

```
clear security ipsec statistics fpc 5 pic 0 (SRX Series devices)
```

user@host> clear security ipsec statistics fpc 5 pic 0
request security ike debug-disable

**Supported Platforms**  LN Series, SRX Series

**Syntax**  request security ike debug-disable

**Release Information**  Command introduced in Release Junos OS 11.4R3.

**Description**  Disable IKE debugging.

**Required Privilege Level**  maintenance

**Related Documentation**
- request security ike debug-enable on page 400
- show security ike debug-status on page 402

**List of Sample Output**  request security ike debug-disable on page 399

**Output Fields**  This command produces no output.

**Sample Output**

request security ike debug-disable

```
user@host> request security ike debug-disable
```
**request security ike debug-enable**

**Supported Platforms**
- LN Series, SRX Series

**Syntax**
```
request security ike debug-enable local local-ip-address remote remote-ip-address
```

**Release Information**
Command introduced in Junos OS Release 11.4R3.

**Description**
Enable IKE debugging.

**Options**
- `local local-ip-address`—The address of the local peer.
- `remote remote-ip-address`—The address of the remote peer.

**Required Privilege Level**
maintenance

**Related Documentation**
- request security ike debug-disable on page 399
- show security ike debug-status on page 402

**List of Sample Output**
request security ike debug-enable local 1.1.1.1 remote 2.2.2.2 on page 400

**Output Fields**
This command produces no output.

**Sample Output**
```
request security ike debug-enable local 1.1.1.1 remote 2.2.2.2

user@host> request security ike debug-enable local 1.1.1.1 remote 2.2.2.2
```
show security ike active-peer

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
show security ike active-peer

**Release Information**  
Command introduced in Junos OS Release 10.4.

**Description**  
This command is used to display the list of connected active users with details about the peer addresses and ports they are using.

**Required Privilege Level**  
view

**Related Documentation**  
- show security ike security-associations on page 404
- show security ipsec security-associations on page 416
- Junos OS VPN Library for Security Devices

**List of Sample Output**  
show security ike active-peer on page 401

**Sample Output**

```
show security ike active-peer

user@host> show security ike active-peer

Remote Address   Port     Peer IKE-ID        XAUTH username   Assigned IP
172.27.6.136     8034     tleungjtac@650a     tleung          10.123.80.225
```

Copyright © 2016, Juniper Networks, Inc.
show security ike debug-status

**Supported Platforms**  LN Series, SRX Series

**Syntax**  show security ike debug-status

**Release Information**  Command introduced in Junos OS Release 11.4R3.

**Description**  Display debug information for currently enabled Internet Key Exchange (IKE).

**Required Privilege**  view

**Related Documentation**
- request security ike debug-disable on page 399
- request security ike debug-enable on page 400

**List of Sample Output**  show security ike debug-status on page 402

**Sample Output**

```
show security ike debug-status
user@host> show security ike debug-status
Enabled
flag: all
level: 15
```
show security ike pre-shared-key

**Supported Platforms**  
J Series, LN Series, SRX Series

**Syntax**  
```
show security ike pre-shared key
<master-key master-key>
<user-id user-id>
```

**Release Information**  
Command introduced in Junos OS Release 8.5.

**Description**  
Display the Internet Key Exchange (IKE) preshared key used by the Virtual Private network (VPN) gateway to authenticate the remote access user.

**Options**  
- **master-key master-key**—(Optional) Master preshared key.
- **user-id user-id**—(Optional) IKE user ID value.

**Required Privilege Level**  
view

**Related Documentation**  
- pre-shared-key (Security IKE Policy) on page 322

**List of Sample Output**  
show security ike pre-shared-key on page 403

**Sample Output**
```
show security ike pre-shared-key
user@host> show security ike pre-shared-key user-id a@juniper.net master-key juniper
Preshared Key:3b33ec3631a561ec5a710f5d02f208033b108bb4
```
show security ike security-associations

Supported Platforms  J Series, LN Series, SRX Series

Syntax  show security ike security-associations
         peer-address
         brief | detail
         fpc slot-number
         index SA-index-number
         kmd-instance (all | kmd-instance-name)
         pic slot-number
         family (inet | inet6)


Description  Display information about Internet Key Exchange security associations (IKE SAs).

Options

- none—Display standard information about existing IKE SAs, including index numbers.
- peer-address—(Optional) Display details about a particular SA based on the IPv4 or IPv6 address of the destination peer. This option and index provide the same level of output.
- brief—(Optional) Display standard information about all existing IKE SAs. (Default)
- detail—(Optional) Display detailed information about all existing IKE SAs.
- fpc slot-number—(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
- index SA-index-number—(Optional) Display information for a particular SA based on the index number of the SA. For a particular SA, display the list of existing SAs by using the command with no options. This option and peer-address provide the same level of output.
- kmd-instance—(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (in this case, it is KMD) identified by FPC slot-number and PIC slot-number. This option is used to filter the output.
  - all—All KMD instances running on the Services Processing Unit (SPU).
  - kmd-instance-name—Name of the KMD instance running on the SPU.
- pic slot-number—(Optional) Specific to SRX Series devices. Display information about existing IKE SAs in this PIC slot. This option is used to filter the output.
- family—(Optional) Display IKE SAs by family. This option is used to filter the output.
  - inet—IPv4 address family.
  - inet6—IPv6 address family.
Required Privilege Level

- view

Related Documentation

- clear security ike security-associations on page 393
- Junos OS VPN Library for Security Devices

List of Sample Output

- show security ike security-associations (IPv4) on page 407
- show security ike security-associations (IPv6) on page 407
- show security ike security-associations detail (Branch SRX Series Devices) on page 408
- show security ike security-associations detail (For High-End SRX Series Devices) on page 408
- show security ike security-associations family inet6 on page 409
- show security ike security-associations index 8 detail on page 409
- show security ike security-associations 1.1.1.2 on page 410
- show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 410

Output Fields

Table 56 on page 405 lists the output fields for the `show security ike security-associations` command. Output fields are listed in the approximate order in which they appear.

Table 56: show security ike security-associations Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE Peer or Remote Address</td>
<td>IP address of the destination peer with which the local peer communicates.</td>
</tr>
<tr>
<td>Index</td>
<td>Index number of an SA. This number is an internally generated number you can use to display information about a single SA.</td>
</tr>
<tr>
<td>Gateway Name</td>
<td>Name of the IKE gateway.</td>
</tr>
<tr>
<td>Location</td>
<td>- FPC—Flexible PIC Concentrator (FPC) slot number.</td>
</tr>
<tr>
<td></td>
<td>- PIC—PIC slot number.</td>
</tr>
<tr>
<td></td>
<td>- KMD-Instance—The name of the KMD instance running on the SPU, identified by FPC slot-number and PIC slot-number. Currently, 4 KMD instances are running on each SPU, and any particular IKE negotiation is carried out by a single KMD instance.</td>
</tr>
<tr>
<td>Role</td>
<td>Part played in the IKE session. The device triggering the IKE negotiation is the initiator, and the device accepting the first IKE exchange packets is the responder.</td>
</tr>
<tr>
<td>State</td>
<td>State of the IKE SAs:</td>
</tr>
<tr>
<td></td>
<td>- DOWN—SA has not been negotiated with the peer.</td>
</tr>
<tr>
<td></td>
<td>- UP—SA has been negotiated with the peer.</td>
</tr>
<tr>
<td>Initiator cookie</td>
<td>Random number, called a cookie, which is sent to the remote node when the IKE negotiation is triggered.</td>
</tr>
</tbody>
</table>
### Table 56: show security ike security-associations Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responder cookie</td>
<td>Random number generated by the remote node and sent back to the initiator as a verification that the packets were received. A cookie is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity.</td>
</tr>
</tbody>
</table>
| Mode or Exchange type | Negotiation method agreed on by the two IPsec endpoints, or peers, used to exchange information between one another. Each exchange type determines the number of messages and the payload types that are contained in each message. The modes, or exchange types, are:  
  - **main**—The exchange is done with six messages. This mode or exchange type encrypts the payload, protecting the identity of the neighbor. The authentication method used is displayed: preshared keys or certificate.  
  - **aggressive**—The exchange is done with three messages. This mode or exchange type does not encrypt the payload, leaving the identity of the neighbor unprotected. |
| Local                 | Address of the local peer.                                                                                                                                                                                      |
| Remote                | Address of the remote peer.                                                                                                                                                                                     |
| Lifetime              | Number of seconds remaining until the IKE SA expires.                                                                                                                                                         |
| Algorithms            | IKE algorithms used to encrypt and secure exchanges between the peers during the IPsec Phase 2 process:                                                                                                           
  - **Authentication**—Type of authentication algorithm used:  
    - **sha1**—Secure Hash Algorithm 1 authentication.  
    - **md5**—MD5 authentication.  
  - **Encryption**—Type of encryption algorithm used:  
    - **aes-256-cbc**—Advanced Encryption Standard (AES) 256-bit encryption.  
    - **aes-192-cbc**—AES192-bit encryption.  
    - **aes-128-cbc**—AES 128-bit encryption.  
    - **3des-cbc**—3 Data Encryption Standard (DES) encryption.  
    - **des-cbc**—DES encryption. |
| Diffie-Hellman group   | Specifies the IKE Diffie-Hellman group.                                                                                                                                                                         |
| Traffic statistics     |                                                                                                                                                                                                            |
|                       | • **Input bytes**—Number of bytes received.  
|                       | • **Output bytes**—Number of bytes transmitted.  
|                       | • **Input packets**—Number of packets received.  
|                       | • **Output packets**—Number of packets transmitted. |
### Table 56: show security ike security-associations Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flags</td>
<td>Notification to the key management process of the status of the IKE negotiation:</td>
</tr>
<tr>
<td></td>
<td>• caller notification sent — Caller program notified about the completion of the</td>
</tr>
<tr>
<td></td>
<td>IKE negotiation.</td>
</tr>
<tr>
<td></td>
<td>• waiting for done — Negotiation is done. The library is waiting for the remote</td>
</tr>
<tr>
<td></td>
<td>end retransmission timers to expire.</td>
</tr>
<tr>
<td></td>
<td>• waiting for remove — Negotiation has failed. The library is waiting for the</td>
</tr>
<tr>
<td></td>
<td>remote end retransmission timers to expire before removing this negotiation.</td>
</tr>
<tr>
<td></td>
<td>• waiting for policy manager — Negotiation is waiting for a response from the</td>
</tr>
<tr>
<td></td>
<td>policy manager.</td>
</tr>
<tr>
<td>IPSec security associations</td>
<td>• number created: The number of SAs created.</td>
</tr>
<tr>
<td></td>
<td>• number deleted: The number of SAs deleted.</td>
</tr>
<tr>
<td>Phase 2 negotiations in progress</td>
<td>Number of Phase 2 IKE negotiations in progress and status information:</td>
</tr>
<tr>
<td></td>
<td>• Negotiation type — Type of Phase 2 negotiation. Junos OS currently supports</td>
</tr>
<tr>
<td></td>
<td>quick mode.</td>
</tr>
<tr>
<td></td>
<td>• Message ID — Unique identifier for a Phase 2 negotiation.</td>
</tr>
<tr>
<td></td>
<td>• Local identity — Identity of the local Phase 2 negotiation. The format is id-</td>
</tr>
<tr>
<td></td>
<td>type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation).</td>
</tr>
<tr>
<td></td>
<td>• Remote identity — Identity of the remote Phase 2 negotiation. The format is id-</td>
</tr>
<tr>
<td></td>
<td>type-name (proto-name:port-number,[0..id-data-len] = iddata-presentation).</td>
</tr>
<tr>
<td></td>
<td>• Flags — Notification to the key management process of the status of the IKE</td>
</tr>
<tr>
<td></td>
<td>negotiation:</td>
</tr>
<tr>
<td></td>
<td>• caller notification sent — Caller program notified about the completion of</td>
</tr>
<tr>
<td></td>
<td>the IKE negotiation.</td>
</tr>
<tr>
<td></td>
<td>• waiting for done — Negotiation is done. The library is waiting for the remote</td>
</tr>
<tr>
<td></td>
<td>end retransmission timers to expire.</td>
</tr>
<tr>
<td></td>
<td>• waiting for remove — Negotiation has failed. The library is waiting for the</td>
</tr>
<tr>
<td></td>
<td>remote end retransmission timers to expire before removing this negotiation.</td>
</tr>
<tr>
<td></td>
<td>• waiting for policy manager — Negotiation is waiting for a response from the</td>
</tr>
<tr>
<td></td>
<td>policy manager.</td>
</tr>
</tbody>
</table>

### Sample Output

**show security ike security-associations (IPv4)**

```plaintext
user@host> show security ike security-associations
Index  Remote Address    State  Initiator cookie     Responder cookie     Mode
      8  1.1.1.2    UP  3a895f8a9f620198     9040753e66d700bb     Main
Index  Remote Address    State  Initiator cookie     Responder cookie     Mode
      9  1.2.1.3     UP  5ba96hfa9f65067   1  70890755b65b80b   d Main
```

**show security ike security-associations (IPv6)**

```plaintext
user@host> show security ike security-associations
Index  State  Initiator cookie  Responder cookie  Mode  Remote Address
      5    UP   e48ef6a444853cf  0d09c59aafbf720be  Aggressive    1212::1112
```
Sample Output

show security ike security-associations detail (Branch SRX Series Devices)

user@host> show security ike security-associations detail
IKE peer 25.191.134.245, Index 2577565, Gateway Name: tropic
  Role: Initiator, State: UP
  Initiator cookie: b869b3424513340a, Responder cookie: 4cb3488cb19397c3
  Exchange type: Main, Authentication method: Pre-shared-keys
  Lifetime: Expires in 169 seconds
  Peer ike-id: 25.191.134.245
  Xauth assigned IP: 0.0.0.0
  Algorithms:
    Authentication : hmac-sha1-96
    Encryption      : aes128-cbc
    Pseudo random function: hmac-sha1
    Diffie-Hellman group : DH-group-5
  Traffic statistics:
    Input bytes :       1012
    Output bytes :      1196
    Input packets:       4
    Output packets:      5
  Flags: IKE SA is created

IPSec security associations: 1 created, 0 deleted
Phase 2 negotiations in progress: 0

Negotiation type: Quick mode, Role: Initiator, Message ID: 0
Local identity: 25.191.134.241
Remote identity: 25.191.134.245
Flags: IKE SA is created

Sample Output

show security ike security-associations detail (For High-End SRX Series Devices)

user@host> show security ike security-associations detail
IKE peer 1.1.1.2, Index 914039858, Gateway Name: tropic
  Location: FPC 3, PIC 1, KMD-Instance 3
  Role: Initiator, State: UP
  Initiator cookie: 219a697652bdde37, Responder cookie: b49c30b229d36bcd
  Exchange type: Aggressive, Authentication method: Pre-shared-keys
  Local: 1.1.1.1:500, Remote: 1.1.1.2:500
  Lifetime: Expires in 26297 seconds
  Peer ike-id: 1.1.1.2
  Xauth user-name: not available
  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-5
  Traffic statistics:
    Input bytes :        0
    Output bytes :       0
    Input packets:       0
    Output packets:      0
  Flags: IKE SA is created

IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1
Sample Output
show security ike security-associations family inet6

user@host> show security ike security-associations family inet6
IKE peer 1212::1112, Index 5, Gateway Name: tropic
Role: Initiator, State: UP
Initiator cookie: e48efd6a444853cf, Responder cookie: 0d09c59aaf870be
Exchange type: Aggressive, Authentication method: Pre-shared-keys
Local: 1212::1111:500, Remote: 1212::1112:500
Lifetime: Expires in 19518 seconds
Peer ike-id: not valid
Xauth assigned IP: 0.0.0.0
Algorithms:
  Authentication : sha1
  Encryption : 3des-cbc
  Pseudo random function: hmac-sha1
  Diffie-Hellman group : DH-group-5
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: 1212::1111:500, Remote: 1212::1112:500
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

Sample Output
show security ike security-associations index 8 detail

user@host> show security ike security-associations index 8 detail
IKE peer 1.1.1.2, Index 8, Gateway Name: tropic
Role: Responder, State:UP
Initiator cookie: 3a895f8a9f620198, Responder cookie: 9040753e66d700bb
Exchange type: main, Authentication method: Pre-shared-keys
Local: 1.1.1.1:500, Remote: 1.1.1.2:500
Lifetime: Expired in 381 seconds
Algorithms:
  Authentication: md5
  Encryption: 3des-cbc
  Pseudo random function: hmac-md5
  Diffie-Hellman group : DH-group-5
Traffic statistics:
  Input bytes: 11268
  Output bytes: 6940
  Input packets: 57
  Output packets: 57
Flags: Caller notification sent
IPSec security associations: 0 created, 0 deleted
Phase 2 negotiations in progress: 1

Negotiation type: Quick mode, Role: Responder, Message ID: 1765792815
Local: 1.1.1.1:500, Remote: 1.1.1.2:500
Local identity: No Id
Remote identity: No Id
Flags: Caller notification sent, Waiting for remove

Sample Output
show security ike security-associations 1.1.1.2

```
user@host> show security ike security-associations 1.1.1.2
Index  State  Initiator cookie  Responder cookie  Mode    Remote Address
     8    UP    3a895f8a9f620198  9040753e66d700bb  Main        1.1.1.2
```

Sample Output
show security ike security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

```
user@host> show security ike security-associations fpc 6 pic 1 kmd-instance all
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
1728053250  1.1.1.2    UP    fc959afd1070d10b  bdeb7e8c1ea99483  Main
```
show security ike tunnel-map

**Supported Platforms**
LN Series, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800

**Syntax**
show security ike tunnel-map <brief | summary>

**Release Information**
Command introduced in Junos OS Release 12.1x44-D10.

**Description**
Display the tunnel mapping on different Services Processing Units (SPUs).

**Options**
- brief | summary — (Optional) Display the specified level of output.

**Required Privilege**
view

**Related Documentation**
- show security ike security-associations on page 404
- show security ipsec security-associations on page 416
- Junos OS VPN Library for Security Devices

**List of Sample Output**
- show security ike tunnel-map on page 411
- show security ike tunnel-map summary on page 411

**Sample Output**

show security ike tunnel-map

```
user@host> show security ike tunnel-map
node0: Gateway ID Gateway Name FPC PIC IKED Instance
     2     ike_gw1     4     0       1
     3     ike_gw2     7     0       1
     4     ike_gw3     7     0       2
     5     ike_gw4     4     0       2
```

show security ike tunnel-map summary

```
user@host> show security ike tunnel-map summary
node0: FPC PIC SPU Load
     4     0     2
     7     0     2
```
**show security ipsec inactive-tunnels**

**Supported Platforms**
- LN Series, SRX Series

**Syntax**
```
show security ipsec inactive-tunnels
brief | detail
family (inet | inet6)
fpc slot-number
index index-number
kmd-instance (all | kmd-instance-name)
pic slot-number
vpn-name vpn-name
```

**Release Information**
- Command introduced in Junos OS Release 11.4R3.

**Description**
Display security information about the inactive tunnel.

**Options**
- **none**—Display information about all inactive tunnels.
- **brief | detail**—(Optional) Display the specified level of output.
- **family**—(Optional) Display the inactive tunnel by family. This option is used to filter the output.
  - **inet**—IPv4 address family.
  - **inet6**—IPv6 address family.
- **fpc slot-number**—(Optional) Specific to SRX Series devices. Display information about inactive tunnels in the Flexible PIC Concentrator (FPC) slot.
- **index index-number**—(Optional) Display detailed information about the specified inactive tunnel identified by this index number. For a list of all inactive tunnels with their index numbers, use the command with no options.
- **kmd-instance**—(Optional) Specific to SRX Series devices. Display information about inactive tunnels in the key management process (in this case, it is KMD) identified by FPC slot-number and PIC slot-number.
  - **all**—All KMD instances running on the Services Processing Unit (SPU).
  - **kmd-instance-name**—Name of the KMD instance running on the SPU.
- **pic slot-number**—Specific to SRX Series devices. Display information about inactive tunnels in the PIC slot.
- **vpn-name vpn-name**—(Optional) Name of the VPN.

**NOTE:** The fpc slot-number, kmd-instance (all | kmd-instance-name), and pic slot-number parameters apply to SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices only.
Required Privilege Level  view

Related Documentation
- show security ipsec security-associations on page 416
- show security ipsec inactive-tunnels on page 414
- show security ipsec inactive-tunnels index 131073 on page 414

List of Sample Output  show security ipsec inactive-tunnels on page 414
show security ipsec inactive-tunnels index 131073 on page 414

Output Fields  Table 57 on page 413 lists the output fields for the show security ipsec inactive-tunnels command. Output fields are listed in the approximate order in which they appear.

Table 57: show security ipsec inactive-tunnels Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total inactive tunnels</td>
<td>Total number of inactive IPsec tunnels.</td>
</tr>
<tr>
<td>Total inactive tunnels which establish immediately</td>
<td>Total number of inactive IPsec tunnels that can establish a session immediately.</td>
</tr>
<tr>
<td>ID</td>
<td>Identification number of the inactive tunnel. You can use this number to get more information about the inactive tunnel.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the remote gateway.</td>
</tr>
<tr>
<td>Port</td>
<td>If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500.</td>
</tr>
<tr>
<td>Nego#</td>
<td>Number of IPsec negotiations.</td>
</tr>
<tr>
<td>Fail#</td>
<td>Number of IPsec negotiation failures.</td>
</tr>
<tr>
<td>Def-Del#</td>
<td>Number of deferred deletions of a dial-up IPsec VPN.</td>
</tr>
<tr>
<td>Flag</td>
<td>Internal flag depicting the state of the tunnel, used for debugging purposes.</td>
</tr>
<tr>
<td>Virtual system</td>
<td>Virtual system to which the VPN belongs.</td>
</tr>
<tr>
<td>VPN name</td>
<td>Name of the IPsec VPN.</td>
</tr>
<tr>
<td>Local gateway</td>
<td>Gateway address of the local system.</td>
</tr>
<tr>
<td>Remote gateway</td>
<td>Gateway address of the remote system.</td>
</tr>
<tr>
<td>Local identity</td>
<td>Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN).</td>
</tr>
<tr>
<td>Remote identity</td>
<td>IP address of the destination peer gateway.</td>
</tr>
<tr>
<td>Version</td>
<td>Version of IKE.</td>
</tr>
</tbody>
</table>
**Table 57: show security ipsec inactive-tunnels Output Fields (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF-bit</td>
<td>State of the don't fragment bit: set or clear.</td>
</tr>
<tr>
<td>Bind-interface</td>
<td>The tunnel interface to which the route-based VPN is bound.</td>
</tr>
<tr>
<td>Policy-name</td>
<td>Name of the applicable policy.</td>
</tr>
<tr>
<td>Tunnel Down Reason</td>
<td>Reason for which the tunnel is inactive.</td>
</tr>
</tbody>
</table>

**Sample Output**

**show security ipsec inactive-tunnels**

```
user@host> show security ipsec inactive-tunnels
Total inactive tunnels: 5
Total inactive tunnels with establish immediately: 1
ID     Port  Nego#  Fail#  Flag      Gateway          Tunnel Down Reason
2      500   0      0      604829                     SA not initiated
3      500   0      0      600829    12.2.3.110       SA not initiated
131073 500   419    0      600a29    12.2.2.110       P1 SA deleted
131074 500   0      0      600a29    12.2.2.110       SA not initiated
131075 500   0      0      600a29    12.2.4.110       SA not initiated
```

**Sample Output**

**show security ipsec inactive-tunnels index 131073**

```
user@host> show security ipsec inactive-tunnels index 131073
ID: 131073 Virtual-system: root, VPN Name: tropic
   Local Gateway: 12.2.2.109, Remote Gateway: 12.2.2.110
   Local Identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
   Remote Identity: ipv4_subnet(any:0,[0..7]=30.1.1.0/24)
   Version: IKEv1
   DF-bit: clear
   Bind-interface: st0.3

   Port: 500, Nego#: 0, Fail#: 0, Def-Del#: 0 Flag: 600a29
   Tunnel Down Reason: SA not initiated
```
show security ipsec next-hop-tunnels

Supported Platforms J Series, LN Series, SRX Series

Syntax show security ipsec next-hop-tunnels < interface-name interface-name >

Release Information Command introduced in Junos OS Release 8.5.

Description Display security information about the secure tunnel interface.

Options

• none—Display information about all secure tunnel interface.

• interface-name interface-name—(Optional) Name of the secure tunnel logical interface.

Required Privilege view

Related Documentation

• show security ipsec security-associations on page 416

• Junos OS VPN Library for Security Devices

List of Sample Output show security ipsec next-hop-tunnels on page 415

Output Fields Table 58 on page 415 lists the output fields for the show security ipsec next-hop-tunnels command. Output fields are listed in the approximate order in which they appear.

Table 58: show security ipsec next-hop-tunnels Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the next gateway.</td>
<td>Next-hop gateway</td>
</tr>
<tr>
<td>Name of the secure tunnel logical interface.</td>
<td>Interface</td>
</tr>
<tr>
<td>Name of the IPsec VPN tunnel.</td>
<td>IPsec VPN name</td>
</tr>
<tr>
<td>Static—IP address manually configured.</td>
<td>Flag</td>
</tr>
<tr>
<td>Auto—IP address obtained from the remote peer automatically.</td>
<td></td>
</tr>
</tbody>
</table>

Sample Output

show security ipsec next-hop-tunnels

user@host> show security ipsec next-hop-tunnels

<table>
<thead>
<tr>
<th>Next-hop gateway</th>
<th>interface</th>
<th>IPsec VPN name</th>
<th>Flag</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1.1.2</td>
<td>st0.0</td>
<td>autokey</td>
<td>Static</td>
</tr>
<tr>
<td>11.1.1.3</td>
<td>st0.0</td>
<td>pbd-4-6</td>
<td>Auto</td>
</tr>
</tbody>
</table>
show security ipsec security-associations

Supported Platforms  J Series, LN Series, SRX Series

Syntax  

show security ipsec security-associations  
brief | detail  
fpc slot-number  
index SA-index-number  
kmd-instance (all | kmd-instance-name)  
pic slot-number>  
family (inet | inet6)  
vpn-name vpn-name <traffic-selector traffic-selector-name>


Description  Display information about the IPsec security associations (SAs).

Options  

• none—Display information about all SAs.
  • brief | detail—(Optional) Display the specified level of output.
  • fpc slot-number—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
  • index SA-index-number—(Optional) Display detailed information about the specified SA identified by this index number. To obtain a list of all SAs that includes their index numbers, use the command with no options.
  • kmd-instance—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in the key management process (in this case, it is KMD) identified by the FPC slot-number and PIC slot-number. This option is used to filter the output.
    • all—All KMD instances running on the Services Processing Unit (SPU).
    • kmd-instance-name—Name of the KMD instance running on the SPU.
  • pic slot-number—(Optional) Specific to SRX Series devices. Display information about existing IPsec SAs in this PIC slot. This option is used to filter the output.
    • family—(Optional) Display SAs by family. This option is used to filter the output.
      • inet—IPv4 address family.
      • inet6—IPv6 address family.
  • vpn-name vpn-name—Name of the VPN. If configured, traffic-selector traffic-selector-name can optionally be specified.
**Required Privilege Level**  
- view

**Related Documentation**  
- [MPLS Feature Guide for Security Devices](#)
- [clear security ipsec security-associations on page 395](#)
- [Junos OS VPN Library for Security Devices](#)
- [Master Administrator for Logical Systems Feature Guide for Security Devices](#)

**List of Sample Output**  
- show security ipsec security-associations (IPv4) on page 420
- show security ipsec security-associations (IPv6) on page 420
- show security ipsec security-associations index 5 on page 420
- show security ipsec security-associations brief on page 421
- show security ipsec security-associations detail on page 421
- show security ipsec security-associations family inet6 on page 423
- show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices) on page 423

**Output Fields**  
Table 59 on page 417 lists the output fields for the `show security ipsec security-associations` command. Output fields are listed in the approximate order in which they appear.

### Table 59: show security ipsec security-associations

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total active tunnels</td>
<td>Total number of active IPsec tunnels.</td>
</tr>
<tr>
<td>ID</td>
<td>Index number of the SA. You can use this number to get additional information about the SA.</td>
</tr>
<tr>
<td>VPN name</td>
<td>IPsec name for VPN.</td>
</tr>
<tr>
<td>Gateway</td>
<td>IP address of the remote gateway.</td>
</tr>
<tr>
<td>Port</td>
<td>If Network Address Translation (NAT) is used, this value is 4500. Otherwise, it is the standard IKE port, 500.</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Cryptography used to secure exchanges between peers during the IKE Phase 2 negotiations includes:</td>
</tr>
<tr>
<td></td>
<td>- An authentication algorithm used to authenticate exchanges between the peers. Options are hmac-md5-95, hmac-shal-96, or ESP.</td>
</tr>
<tr>
<td></td>
<td>- An encryption algorithm used to encrypt data traffic. Options are 3des-cbc, aes-128-cbc, aes-192-cbc, aes-256-cbc, or des-cbc.</td>
</tr>
<tr>
<td>SPI</td>
<td>Security parameter index (SPI) identifier. An SA is uniquely identified by an SPI. Each entry includes the name of the VPN, the remote gateway address, the SPIs for each direction, the encryption and authentication algorithms, and keys. The peer gateways each have two SAs, one resulting from each of the two phases of negotiation: Phase 1 and Phase 2.</td>
</tr>
</tbody>
</table>
Table 59: show security ipsec security-associations (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life: sec/kb</td>
<td>The lifetime of the SA, after which it expires, expressed either in seconds or kilobytes.</td>
</tr>
<tr>
<td>Sta</td>
<td>State has two options, <strong>Installed</strong> and <strong>Not Installed</strong>.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Installed</strong>—The SA is installed in the SA database.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Installed</strong>—The SA is not installed in the SA database.</td>
</tr>
<tr>
<td></td>
<td>For transport mode, the value of State is always <strong>Installed</strong>.</td>
</tr>
<tr>
<td>Mon</td>
<td>The Mon field refers to VPN monitoring status. If VPN monitoring is enabled, then this field displays <strong>U</strong> (up) or <strong>D</strong> (down). A hyphen (-) means VPN monitoring is not enabled for this SA.</td>
</tr>
<tr>
<td>vsys or Virtual-system</td>
<td>The root system.</td>
</tr>
<tr>
<td>Tunnel index</td>
<td>Numeric identifier of the specific IPsec tunnel for the SA.</td>
</tr>
<tr>
<td>Local gateway</td>
<td>Gateway address of the local system.</td>
</tr>
<tr>
<td>Remote gateway</td>
<td>Gateway address of the remote system.</td>
</tr>
<tr>
<td>Traffic selector</td>
<td>Name of the traffic selector.</td>
</tr>
<tr>
<td>Local identity</td>
<td>Identity of the local peer so that its partner destination gateway can communicate with it. The value is specified as an IP address, fully qualified domain name, e-mail address, or distinguished name (DN).</td>
</tr>
<tr>
<td>Remote identity</td>
<td>IP address of the destination peer gateway.</td>
</tr>
<tr>
<td>DF-bit</td>
<td>State of the don’t fragment bit: <strong>set</strong> or <strong>cleared</strong>.</td>
</tr>
<tr>
<td>Bind interface</td>
<td>The tunnel interface to which VPN is bound.</td>
</tr>
<tr>
<td>Policy-name</td>
<td>Name of the applicable policy.</td>
</tr>
<tr>
<td>Location</td>
<td><strong>FPC</strong>—Flexible PIC Concentrator (FPC) slot number.</td>
</tr>
<tr>
<td></td>
<td><strong>PIC</strong>—PIC slot number.</td>
</tr>
<tr>
<td></td>
<td><strong>KMD-Instance</strong>—The name of the KMD instance running on the SPU, identified by FPC slot-number and PIC slot-number. Currently, 4 KMD instances running on each SPU, and any particular IPsec negotiation is carried out by a single KMD instance.</td>
</tr>
<tr>
<td>Direction</td>
<td>Direction of the SA; it can be inbound or outbound.</td>
</tr>
<tr>
<td>AUX-SPI</td>
<td>Value of the auxiliary security parameter index(SPI).</td>
</tr>
<tr>
<td></td>
<td>• When the value is <strong>AH</strong> or <strong>ESP</strong>, AUX-SPI is always 0.</td>
</tr>
<tr>
<td></td>
<td>• When the value is <strong>AH+ESP</strong>, AUX-SPI is always a positive integer.</td>
</tr>
</tbody>
</table>
## Table 59: show security ipsec security-associations (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mode</strong></td>
<td>Mode of the SA:</td>
</tr>
<tr>
<td>• transport</td>
<td>Protects host-to-host connections.</td>
</tr>
<tr>
<td>• tunnel</td>
<td>Protects connections between security gateways.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>Type of the SA:</td>
</tr>
<tr>
<td>• manual</td>
<td>Security parameters require no negotiation. They are static and are configured</td>
</tr>
<tr>
<td></td>
<td>by the user.</td>
</tr>
<tr>
<td>• dynamic</td>
<td>Security parameters are negotiated by the IKE protocol. Dynamic SAs are not</td>
</tr>
<tr>
<td></td>
<td>supported in transport mode.</td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>State of the SA:</td>
</tr>
<tr>
<td>• Installed</td>
<td>The SA is installed in the SA database.</td>
</tr>
<tr>
<td>• Not Installed</td>
<td>The SA is not installed in the SA database.</td>
</tr>
<tr>
<td></td>
<td>For transport mode, the value of State is always installed.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>Protocol supported.</td>
</tr>
<tr>
<td></td>
<td>Transport mode supports Encapsulation Security Protocol (ESP) and Authentication</td>
</tr>
<tr>
<td></td>
<td>Header (AH).</td>
</tr>
<tr>
<td></td>
<td>Tunnel mode supports ESP and AH.</td>
</tr>
<tr>
<td></td>
<td>• Authentication—Type of authentication used.</td>
</tr>
<tr>
<td></td>
<td>• Encryption—Type of encryption used.</td>
</tr>
<tr>
<td><strong>Soft lifetime</strong></td>
<td>The soft lifetime informs the IPsec key management system that the SA is about to</td>
</tr>
<tr>
<td></td>
<td>expire.</td>
</tr>
<tr>
<td></td>
<td>Each lifetime of an SA has two display options, hard and soft, one of which must</td>
</tr>
<tr>
<td></td>
<td>be present for a dynamic SA. This allows the key management system to negotiate a</td>
</tr>
<tr>
<td></td>
<td>new SA before the hard lifetime expires.</td>
</tr>
<tr>
<td></td>
<td>• Expires in seconds—Number of seconds left until the SA expires.</td>
</tr>
<tr>
<td><strong>Hard lifetime</strong></td>
<td>The hard lifetime specifies the lifetime of the SA.</td>
</tr>
<tr>
<td></td>
<td>• Expires in seconds—Number of seconds left until the SA expires.</td>
</tr>
<tr>
<td><strong>Lifesize Remaining</strong></td>
<td>The lifesize remaining specifies the usage limits in kilobytes. If there is no</td>
</tr>
<tr>
<td></td>
<td>lifesize specified, it shows unlimited.</td>
</tr>
<tr>
<td></td>
<td>• Expires in kilobytes—Number of kilobytes left until the SA expires.</td>
</tr>
<tr>
<td><strong>Anti-replay service</strong></td>
<td>State of the service that prevents packets from being replayed. It can be Enabled</td>
</tr>
<tr>
<td></td>
<td>or Disabled.</td>
</tr>
<tr>
<td><strong>Replay window size</strong></td>
<td>Configured size of the antireplay service window. It can be 32 or 64 packets. If</td>
</tr>
<tr>
<td></td>
<td>the replay window size is 0, the antireplay service is disabled.</td>
</tr>
<tr>
<td></td>
<td>The antireplay window size protects the receiver against replay attacks by rejecting</td>
</tr>
<tr>
<td></td>
<td>old or duplicate packets.</td>
</tr>
</tbody>
</table>
Table 59: show security ipsec security-associations (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bind-interface</td>
<td>The tunnel interface to which the route-based VPN is bound.</td>
</tr>
</tbody>
</table>

Sample Output

show security ipsec security-associations (IPv4)

```
user@host> show security ipsec security-associations
Total active tunnels: 1

<table>
<thead>
<tr>
<th>ID</th>
<th>Gateway</th>
<th>Port</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec/kb</th>
<th>Mon vsys</th>
<th>Port</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>131075</td>
<td>11.0.28.241</td>
<td>500</td>
<td>ESP:3des/sha1</td>
<td>86758ff0</td>
<td>6918/ unlim</td>
<td>-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>131075</td>
<td>11.0.28.241</td>
<td>500</td>
<td>ESP:3des/sha1</td>
<td>3183ff26</td>
<td>6918/ unlim</td>
<td>-</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

Sample Output

show security ipsec security-associations (IPv6)

```
user@host> show security ipsec security-associations
Total active tunnels: 1

<table>
<thead>
<tr>
<th>ID</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec/kb</th>
<th>Mon vsys</th>
<th>Port</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>131074</td>
<td>ESP:3des/sha1</td>
<td>14caf1d9</td>
<td>3597/ unlim</td>
<td>-</td>
<td>root</td>
<td>1212::1112</td>
</tr>
<tr>
<td>131074</td>
<td>ESP:3des/sha1</td>
<td>9a4db486</td>
<td>3597/ unlim</td>
<td>-</td>
<td>root</td>
<td>1212::1112</td>
</tr>
</tbody>
</table>
```

Sample Output

show security ipsec security-associations index 5

```
user@host> show security ipsec security-associations index 5
ID: 131073 Virtual-system: root, VPN Name: tropic
Local gateway: 1.1.1.1, Remote gateway: 1.1.1.2
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: st0.3
Policy-name: my-policy

Direction: inbound, SPI: 494001027, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Soft lifetime: Expired
Hard lifetime: Expired in 130 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64

Direction: inbound, SPI: 1498711950, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Soft lifetime: Expires in 40 seconds
Hard lifetime: Expires in 175 seconds
Lifesize Remaining: Unlimited
Anti-replay service: Enabled, Replay window size: 64
```
Sample Output

show security ipsec security-associations brief

```
user@host> show security ipsec security-associations brief
Total active tunnels: 2
ID Gateway Port Algorithm SPI Life:sec/kb Mon vsys
<16384 1.1.1.1 500 ESP:3des/sha1 af88baa 28795/unlim D 0
>16384 1.1.1.1 500 ESP:3des/sha1 f4e3e5f4 28795/unlim D 0
```

Sample Output

show security ipsec security-associations detail

```
user@host> show security ipsec security-associations detail
ID: 131073 Virtual-system: root, VPN Name: tropic
Local Gateway: 1.1.1.2, Remote Gateway: 1.1.1.1
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: st0.3
Direction: inbound, SPI: 184060842, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Anti-replay service: enabled, Replay window size: 32
Direction: outbound, SPI: 4108576244, AUX-SPI: 0
Hard lifetime: Expires in 28785 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expired
Mode: tunnel, Type: dynamic, State: installed, VPN Monitoring: DOWN
Anti-replay service: enabled, Replay window size: 32
```

Sample Output

show security ipsec security-associations detail (SRX Series Devices)

```
user@host> show security ipsec security-associations detail
ID: 268173313 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS1-ipv6
Local Identity: ipv6(10::-10::ffff:ffff:ffff:ffff)
Remote Identity: ipv6(20::-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
Hard lifetime: Expires in 2976 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2354 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: a468fece, AUX-SPI: 0
Hard lifetime: Expires in 2976 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2354 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
ID: 268173316 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS2-ipv4
Local Identity: ipv4(10.1.1.0-10.1.1.255)
Remote Identity: ipv4(20.1.1.0-20.1.1.255)
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
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: a4344027, AUX-SPI: 0
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
ID: 268173317 Virtual-system: root, VPN Name: ipsec-vpn-to-he-srx
Local Gateway: 2000::1, Remote Gateway: 2000::2
Traffic Selector Name: TS3-ipv4
Local Identity: ipv4(10.1.1.0-10.1.1.255)
Remote Identity: ipv4(20.1.1.0-20.1.1.255)
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: cc9fb573, AUX-SPI: 0
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Direction: outbound, SPI: a4344027, AUX-SPI: 0
Hard lifetime: Expires in 3586 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2948 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64
Hard lifetime: Expires in 3548 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2925 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: a4bde69b, AUX-SPI: 0

Hard lifetime: Expires in 3548 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2925 seconds
Mode: Tunnel(0 0), Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Sample Output
show security ipsec security-associations family inet6

user@host> show security ipsec security-associations family inet6
Virtual-system: root
Local Gateway: 1212::1111, Remote Gateway: 1212::1112
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

Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Direction: outbound, SPI: 9a4db486, AUX-SPI: 0

Hard lifetime: Expires in 3440 seconds
Lifesize Remaining: Unlimited
Soft lifetime: Expires in 2813 seconds
Mode: tunnel, Type: dynamic, State: installed
Anti-replay service: counter-based enabled, Replay window size: 64

Sample Output
show security ipsec security-associations fpc 6 pic 1 kmd-instance all (SRX Series Devices)

user@host> show security ipsec security-associations fpc 6 pic 1 kmd-instance all
Total active tunnels: 1

<table>
<thead>
<tr>
<th>ID</th>
<th>Gateway</th>
<th>Port</th>
<th>Algorithm</th>
<th>SPI</th>
<th>Life:sec/kb</th>
<th>Mon vsys</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;2</td>
<td>1.1.1.2</td>
<td>500</td>
<td>ESP:3des/shal</td>
<td>67a7d25d</td>
<td>28280/unlim</td>
<td>0</td>
</tr>
<tr>
<td>&gt;2</td>
<td>1.1.1.2</td>
<td>500</td>
<td>ESP:3des/shal</td>
<td>a23bc8d9</td>
<td>28280/unlim</td>
<td>0</td>
</tr>
</tbody>
</table>
show security ipsec statistics

Supported Platforms  J Series, LN Series, SRX Series

Syntax  show security ipsec statistics
        <fpc  slot-number >
        <index  SA-index-number >
        <kmd-instance  kmd-instance-name >
        pic  slot-number


Description  Display standard IPsec statistics.

Options  • none—Display statistics about all IPsec security associations (SAs).
         • fpc slot-number —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this Flexible PIC Concentrator (FPC) slot. This option is used to filter the output.
         • index SA-index-number —(Optional) Display statistics for the SA with this index number.
         • kmd-instance kmd-instance-name —Specific to SRX Series devices. Display information about existing IKE SAs in the key management process (the daemon, which in this case is KMD) identified by FPC slot-number and PIC slot-number. This option is used to filter the output.
           • all—All KMD instances running on the Services Processing Unit (SPU).
           • kmd-instance-name—Name of the KMD instance running on the SPU.
         • pic slot-number —Specific to SRX Series devices. Display statistics about existing IPsec SAs in this PIC slot. This option is used to filter the output.

Required Privilege Level  view

Related Documentation  • MPLS Feature Guide for Security Devices
                       • clear security ipsec statistics on page 397

List of Sample Output  show security ipsec statistics on page 425
                      show security ipsec statistics index 5 on page 426
                      show security ipsec statistics fpc 6 pic 1 (SRX Series devices) on page 426

Output Fields  Table 60 on page 424 lists the output fields for the show security ipsec statistics command. Output fields are listed in the approximate order in which they appear.

Table 60: show security ipsec statistics Output Fields

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual-system</td>
<td>The root system.</td>
</tr>
</tbody>
</table>
### Table 60: show security ipsec statistics Output Fields (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Field Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ESP Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Encrypted bytes</strong>—Total number of bytes encrypted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Decrypted bytes</strong>—Total number of bytes decrypted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Encrypted packets</strong>—Total number of packets encrypted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Decrypted packets</strong>—Total number of packets decrypted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td><strong>AH Statistics</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>Input bytes</strong>—Total number of bytes received by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Output bytes</strong>—Total number of bytes transmitted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Input packets</strong>—Total number of packets received by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Output packets</strong>—Total number of packets transmitted by the local system across the IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td></td>
</tr>
<tr>
<td>• <strong>AH authentication failures</strong>—Total number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Replay errors</strong>—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window.</td>
<td></td>
</tr>
<tr>
<td>• <strong>ESP authentication failures</strong>—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets.</td>
<td></td>
</tr>
<tr>
<td>• <strong>ESP decryption failures</strong>—total number of ESP decryption errors.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Bad headers</strong>—Total number of invalid headers detected.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Bad trailers</strong>—Total number of invalid trailers detected.</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Output

**show security ipsec statistics**

```
user@host> show security ipsec statistics
Virtual-system: Root
ESP Statistics:
    Encrypted bytes: 0
    Decrypted bytes: 0
    Encrypted packets: 0
    Decrypted packets: 0
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
```
Sample Output
show security ipsec statistics index 5

```
user@host> show security ipsec statistics index 5
Virtual-system: Root
SA index: 5
ESP Statistics:
  Encrypted bytes: 0
  Decrypted bytes: 0
  Encrypted packets: 0
  Decrypted packets: 0
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
```

Sample Output
show security ipsec statistics fpc 6 pic 1 (SRX Series devices)

```
user@host> show security ipsec statistics fpc 6 pic 1
ESP Statistics:
  Encrypted bytes: 536408
  Decrypted bytes: 696696
  Encrypted packets: 1246
  Decrypted packets: 888
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
```
PART 4

Index

- Index on page 429
Index

Symbols
#, comments in configuration statements........................xviii
( ), in syntax descriptions..............................................xviii
3DES.................................................................................9
< >, in syntax descriptions................................................xviii
[ ], in configuration statements......................................xviii
{ }, in configuration statements.....................................xviii
| (pipe), in syntax descriptions....................................xviii

A
address statement..........................................................293
Advanced IKE Gateway..................................................293
Advanced Encryption Standard (AES).............................9
aggressive mode...................................................................20
algorithm statement..........................................................340
always-send statement....................................................294
attacks
replay...............................................................................21
audible-alarm....................................................................279
authentication
algorithms........................................................................8
authentication statement....................................................341
authentication-algorithm statement.................................295, 342
datif-authentication-method statement............................296
AutoKey IKE VPN.............................................................7
management......................................................................7

B
bind-interface statement..................................................343
braces, in configuration statements.................................xviii
brackets
angle, in syntax descriptions.............................................xviii
square, in configuration statements...................................xviii

C
certificate statement.......................................................297
certificates.......................................................................7
clear security ike respond-bad-spi-count
command............................................................................392
clear security ike security-associations
command...........................................................................393
clear security ipsec security-associations
command...........................................................................395
clear security ipsec statistics command..........................397
commits, in configuration statements..............................xviii
connections-limit statement..........................................298
container statement..........................................................299
conventions
text and syntax..............................................................xvii
cryptographic-self-test statement....................................380
curly braces, in configuration statements.........................xviii
customer support.............................................................xix
contacting JTAC...............................................................xix

D
Data Encryption Standard (DES).........................................9
dead peer detection.........................................................61, 62
dead-peer-detection statement..........................................300
decryption-failures statement............................................381
des....................................................................................9
destination-ip statement..................................................343
df-bit statement................................................................344
dh-group statement..........................................................301
Diffie-Hellman.................................................................7
distinguished-name statement.........................................302
documentation
comments on..................................................................xix
dual stack tunnels.............................................................43
dual stack tunnels configuration example........................232
dynamic statement...........................................................303

E
encryption algorithms......................................................9
encryption statement......................................................345
encryption-algorithm statement.......................................304, 346
decryption-failures statement............................................382
esp...................................................................................8, 9
establish-tunnels statement............................................347
external-interface statement
(IKE Gateway).................................................................305, 332
(Manual Security Association).........................................347

F
firewall filters
statistics

clearing............................................................................404
font conventions.............................................................xvii
PFS...........................................................................................................21
Phase 1.........................................................................................................18
   proposals.................................................................18
   proposals, predefined..................................................18
Phase 2.........................................................................................................20
   proposals............................................................................20
   proposals, predefined..................................................20
policy statement
   (IKE).................................................................................................321
policy-based VPN...........................................................................31
policy-based VPN configuration example.........................................143
policy-based VPN with both initiator and responder
   behind NAT configuration example........................................160
potential-violation...........................................................................280
   authentication........................................................................280
   decryption..............................................................................280
   encryption..............................................................................280
   ikephase1.............................................................................280
   ikephase2.............................................................................280
   replayattack..........................................................................280
   self-test.................................................................................280
pre-shared-key statement.................................................................322
preshared key....................................................................................7
probe-idle-tunnel statement..............................................................322
proposal statement...........................................................................323
   proposals.............................................................................323
   proposals, predefined.......................................................323
proposal-set statement
   (IKE).................................................................................................324
   (IPsec)..............................................................................................364
proposals
   Phase 1.......................................................................................18
   Phase 2.......................................................................................20
proposal statement...........................................................................325
protocol statement
   (IPsec)..............................................................................................366
   (Manual Security Association)..............................................367
proxy ID.............................................................................................51
   See also traffic selector
proxy IDs...........................................................................................20
proxy-identity statement.................................................................368
R
remote IKE ID
   configuring..............................................................................75
remote statement..............................................................................369
remote-identity
   configuring..............................................................................75
remote-identity statement...............................................................326
replay protection.............................................................................21
replay-attacks statement.................................................................387
request security ike debug-disable command...............................399
request security ike debug-enable command...............................400
respond-bad-spi statement.............................................................327
route-based VPN..............................................................................27
route-based VPN configuration example...........................................27
route-based VPN with only responder behind NAT
   configuration example.........................................................111
RRI..........................................................................................................53
S
SA parameters.....................................................................................9
SAs.....................................................................................................20
Secure Hash Algorithm-1.................................................................20
security
   alarms......................................................................................380
   Security Configuration Statement
      Hierarchy..................................................................................290
   service statement
         (Security IPsec).................................................................370
session affinity
   VPN...............................................................................................65
   session-affinity statement........................................................370
   SHA-1.........................................................................................8
show security ike active-peer command...........................................401
show security ike debug-status command.......................................402
show security ike pre-shared-key command....................................403
show security ike security-associations
   command.....................................................................................404
show security ike tunnel-map............................................................411
show security ipsec inactive-tunnels
   command.....................................................................................412
show security ipsec next-hop-tunnels
   command.....................................................................................415
show security ipsec security-associations
   command.....................................................................................416
show security ipsec statistics command.........................................424
source-interface statement..............................................................371
SPC
   VPN support.................................................................................25
   spi statement.............................................................................371
   SPUs
      VPN session affinity.............................................................65
SRX Services Gateways
   distributed VPNs........................................................................24
support, technical See technical support
syntax conventions........................................................................xvii
technical support
  contacting JTAC..............................................................xix
threshold statement........................................................................328
traceoptions statement
  (IKE).................................................................................329
  (IPsec)..............................................................................372
traffic selector................................................................................51
  and overlapping IP addresses...................................54
  and RRI...............................................................................53
  configuring............................................................................263
traffic-selector statement.............................................................373
transport mode...............................................................................11
Triple DES.....................................................................................9
trusted-ca statement.....................................................................331
tunnel mode
  overview..............................................................................11
user-at hostname statement.......................................................332
virtual router..............................................................................28, 138
  configure st0 interface.................................................138
  support in route-based VPNS........................................28
VPN monitoring...........................................................................61
vno statement.............................................................................374
vpn-monitor statement..............................................................375
vpn-monitor-options statement..................................................376
VPNs
  aggressive mode....................................................................20
  AutoKey IKE...............................................................7
  Diffie-Hellman exchange...............................................7
  Diffie-Hellman groups....................................................7
  enabling session affinity..............................................285
  hub-and-spoke configuration example.......................189
  main mode...........................................................................19
  Phase 1...............................................................................18
  Phase 2..............................................................................20
  policy-based.......................................................................31
  policy-based configuration example............................143
  policy-based initiator responder and behind
    NAT configuration example......................................160
  replay protection..............................................................21
  route-based......................................................................27
  route-based configuration example............................77, 95
  route-based responder behind NAT
    configuration example...............................................111
  session affinity....................................................................65
wildcard statement.......................................................................333
xauth statement...........................................................................334