



Junos[®] OS

System Basics: Security Services Configuration Guide

Release
15.1



Modified: 2016-07-26

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Junos[®] OS System Basics: Security Services Configuration Guide

15.1

Copyright © 2016, Juniper Networks, Inc.

All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

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	IPsec Overview	3
	IPsec Overview	3
	IPsec Requirements for Junos-FIPS	3
	IPsec Configuration for an ES PIC Overview	4
	ES Tunnel Interface Configuration for a Layer 3 VPN	4
	IPsec Tunnel Traffic Configuration Overview	4
Chapter 2	Security Associations and IKE Overview	7
	Security Associations Overview	7
	IKE Key Management Protocol Overview	8
Chapter 3	Digital Certificates Overview	9
	Digital Certificates Overview	9
Part 2	Configuration	
Chapter 4	Configuring IPsec for an ES PIC	13
	Configuring Minimum Manual Security Associations for IPsec on an ES PIC	13
	Configuring Minimum IKE Requirements for IPsec on an ES PIC	14
	Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC	14
	Configuring Security Associations for IPsec on an ES PIC	15
	Configuring the Description for an SA	16
	Configuring IPsec Transport Mode	16
	Configuring IPsec Tunnel Mode	16
	Configuring Manual IPsec Security Associations for an ES PIC	17
	Configuring the Processing Direction	18
	Configuring the Protocol for a Manual SA	19
	Configuring the Security Parameter Index	19

Configuring the Auxiliary Security Parameter Index	19
Configuring the Authentication Algorithm and Key	20
Configuring the Encryption Algorithm and Key	20
Configuring Dynamic IPsec Security Associations	21
Enabling Dynamic IPsec Security Associations	21
Configuring Manual IPsec Security Associations for an ES PIC	22
Configuring the Processing Direction	22
Configuring the Protocol for a Manual SA	23
Configuring the Security Parameter Index	24
Configuring the Auxiliary Security Parameter Index	24
Configuring the Authentication Algorithm and Key	25
Configuring the Encryption Algorithm and Key	25
Configuring Dynamic IPsec Security Associations	26
Configuring an IKE Proposal for Dynamic SAs	26
Configuring the Authentication Algorithm for an IKE Proposal	27
Configuring the Authentication Method for an IKE Proposal	27
Configuring the Description for an IKE Proposal	28
Configuring the Diffie-Hellman Group for an IKE Proposal	28
Configuring the Encryption Algorithm for an IKE Proposal	28
Configuring the Lifetime for an IKE SA	29
Example: Configuring an IKE Proposal	29
Configuring an IKE Policy for Preshared Keys	29
Configuring the Description for an IKE Policy	30
Configuring the Mode for an IKE Policy	30
Configuring the Preshared Key for an IKE Policy	30
Associating Proposals with an IKE Policy	31
Example: Configuring an IKE Policy	31
Configuring an IPsec Proposal for an ES PIC	32
Configuring the Authentication Algorithm for an IPsec Proposal	32
Configuring the Description for an IPsec Proposal	33
Configuring the Encryption Algorithm for an IPsec Proposal	33
Configuring the Lifetime for an IPsec SA	33
Configuring the Protocol for a Dynamic IPsec SA	34
Configuring the IPsec Policy for an ES PIC	34
Configuring Perfect Forward Secrecy	34
Example: Configuring an IPsec Policy	35
Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode	36
Configuring the SA Direction	37
Configuring the IPsec SPI	38
Configuring the IPsec Key	38
Example: Configuring Internal IPsec	39

Chapter 5	Configuring Digital Certificates for ES and AS PICs	41
	Configuration Statements for Setting Up Digital Certificates for an ES PIC	41
	Obtaining a Certificate from a Certificate Authority for an ES PIC	42
	Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router	43
	Example: Requesting a CA Digital Certificate	43
	Generating a Private and Public Key Pair for Digital Certificates for an ES PIC	43
	Obtaining a Signed Certificate from the CA for an ES PIC	44
	Configuring Digital Certificates for an ES PIC	45
	Configuring the Certificate Authority Properties for an ES PIC	46
	Specifying the Certificate Authority Name	46
	Configuring the Certificate Revocation List	46
	Configuring the Type of Encoding Your CA Supports	47
	Specifying an Enrollment URL	47
	Specifying a File to Read the Digital Certificate	47
	Specifying an LDAP URL	47
	Configuring the Cache Size	48
	Configuring the Negative Cache	48
	Configuring the Number of Enrollment Retries	48
	Configuring the Maximum Number of Peer Certificates	49
	Configuring the Path Length for the Certificate Hierarchy	49
	Configuring an IKE Policy for Digital Certificates for an ES PIC	49
	Configuring the Type of Encoding Your CA Supports	50
	Configuring the Identity to Define the Remote Certificate Name	50
	Specifying the Certificate Filename	50
	Specifying the Private and Public Key File	50
	Associating the Configured Security Association with a Logical Interface	51
	Configuring Digital Certificates for Adaptive Services Interfaces	51
	Configuring the Certificate Authority Properties	53
	Specifying the CA Profile Name	53
	Specifying an Enrollment URL	53
	Specifying the Enrollment Properties	54
	Configuring the Certificate Revocation List	54
	Specifying an LDAP URL	54
	Configuring the Interval Between CRL Updates	55
	Overriding Certificate Verification if CRL Download Fails	55
	Managing Digital Certificates	55
	Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers	56
	Generating a Public/Private Key Pair	56
	Generating and Enrolling a Local Digital Certificate	56
	Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA	57
	Specify the Certificate ID	59
	Specify the CA Profile	59
	Specify the Challenge Password	59
	Specify the Reenroll Trigger Time	59
	Specify the Regenerate Key Pair	59
	Specify the Validity Period	60

	Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA	60
	Specify the Certificate ID	61
	Specify the CA Profile	61
	Specify the Challenge Password	62
	Specify the Reenroll Trigger Time	62
	Specify the Regenerate Key Pair	62
	Specify the Validity Period	62
Chapter 6	Configuring Traffic Filters and Tracing Operations	63
	Example: Configuring an Outbound Traffic Filter	63
	Example: Applying an Outbound Traffic Filter	64
	Example: Configuring an Inbound Traffic Filter for a Policy Check	64
	Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check	66
	Configuring Tracing Operations for Security Services	67
	Configuring Tracing Operations for IPsec Events for Adaptive Services PICs	68
Chapter 7	Configuring Authentication Key Updates	71
	Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols	71
	Configuring Authentication Key Updates	71
	Configuring BGP and LDP for Authentication Key Updates	72
Chapter 8	Configuring Keys for SSH and SSL	73
	Configuring SSH Host Keys for Secure Copying of Data	73
	Configuring SSH Known Hosts	74
	Configuring Support for SCP File Transfer	74
	Updating SSH Host Key Information	75
	Retrieving Host Key Information Manually	75
	Importing Host Key Information from a File	75
	Importing SSL Certificates for Junos XML Protocol Support	75
	global (DDoS)	77
	logical-interface (DDoS Flow Detection)	78
	no-flow-logging (DDoS Flow Detection)	79
	physical-interface (DDoS Flow Detection)	80
	priority (DDoS)	81
	protocols (DDoS)	82
	recover-time (DDoS)	91
	subscriber (DDoS Flow Detection)	92
	timeout-active-flows (DDoS Flow Detection)	93
	traceoptions (DDoS)	94
	violation-report-rate (DDoS Flow Detection)	96
Chapter 9	Configuration Statements	97
	[edit security] Hierarchy Level	99
	algorithm (Authentication Keychain)	102
	algorithm (Junos FIPS)	103
	authentication (Security IPsec)	104
	authentication-algorithm (Security IKE)	105
	authentication-algorithm (Security IPsec)	106

authentication-key-chains	108
authentication-method	109
auto-re-enrollment	110
auxiliary-spi (Security IPsec)	111
ca-identity	111
ca-name	112
ca-profile	113
cache-size	114
cache-timeout-negative	115
certificate-id	116
certificates	117
certification-authority	118
challenge-password	119
crl (Adaptive Services Interface)	120
crl (Encryption Interface)	121
description (Authentication Keychain)	121
description (IKE policy)	122
dh-group	122
direction (Junos OS)	123
direction (Junos-FIPS Software)	124
dynamic	125
encoding	126
encryption (Junos OS)	127
encryption (Junos-FIPS Software)	128
encryption-algorithm (Security)	129
enrollment	130
enrollment-retry	131
enrollment-url	131
file	132
identity	132
ike (Security)	133
internal	134
ipsec (Security)	135
key (Authentication Keychain)	137
key (Junos FIPS)	138
key-chain (Security)	139
ldap-url	140
lifetime-seconds (Security)	140
local	141
local-certificate (Security)	142
local-key-pair	142
manual (Junos OS)	143
manual (Junos FIPS)	144
maximum-certificates	145
mode (IKE)	146
mode (IPsec)	147
options (Security)	148
path-length	149
perfect-forward-secrecy (Security)	149

pki	150
policy (Security IKE)	151
policy (Security IPsec)	152
pre-shared-key (Security)	152
proposal (Security IKE)	153
proposal (Security IPsec)	153
proposals	154
protocol (Junos OS)	155
protocol (Junos-FIPS Software)	156
re-enroll-trigger-time-percentage	156
re-generate-keypair	157
refresh-interval	157
retry (Adaptive Services Interface)	158
retry-interval	158
revocation-check	159
secret	160
security-association (Junos OS)	161
security-association (Junos-FIPS Software)	162
spi (Junos OS)	163
spi (Junos-FIPS Software)	163
ssh-known-hosts	164
start-time (Authentication Key Transmission)	165
tolerance	166
traceoptions	167
url (Security)	169
validity-period	169
Security Services Configuration Statements	170

Part 3

Chapter 10

Administration

IPsec Administrative Commands 175

request security pki ca-certificate enroll	176
request security pki ca-certificate load	177
request security pki ca-certificate verify	178
request security pki crl load	179
request security pki generate-certificate-request	180
request security pki local-certificate generate-self-signed	182
request security pki local-certificate enroll	183
request security pki local-certificate verify	185

Chapter 11

IPsec Monitoring Commands 187

clear security pki ca-certificate	188
clear security pki certificate-request	189
clear security pki crl	190
clear security pki key-pair	191
clear security pki local-certificate	192
clear services ipsec-vpn certificates	193
clear services ipsec-vpn ipsec statistics	194
clear services ipsec-vpn ike security-associations	195
clear services ipsec-vpn ipsec security-associations	196

Part 3

Index

Index	199
-------------	-----

List of Figures

Part 1	Overview	
Chapter 1	IPsec Overview	3
	Figure 1: Example: IPsec Tunnel Connecting Security Gateways	5

List of Tables

	About the Documentation	xv
	Table 1: Notice Icons	xvii
	Table 2: Text and Syntax Conventions	xviii
Chapter 9	Configuration Statements	97
	Table 3: Security Services Configuration Statements	170

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:

- M Series
- MX Series
- T Series
- T4000

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.xml;
    }
  }
}
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.xml; }
```


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 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xviii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric metric>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast <i>(string1 string2 string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [community-ids]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

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 of the Juniper Networks TechLibrary site at <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/>.
- 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.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <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

- [IPsec Overview on page 3](#)
- [Security Associations and IKE Overview on page 7](#)
- [Digital Certificates Overview on page 9](#)

CHAPTER 1

IPsec Overview

- [IPsec Overview on page 3](#)
- [IPsec Requirements for Junos-FIPS on page 3](#)
- [IPsec Configuration for an ES PIC Overview on page 4](#)
- [ES Tunnel Interface Configuration for a Layer 3 VPN on page 4](#)
- [IPsec Tunnel Traffic Configuration Overview on page 4](#)

IPsec Overview

IP Security (IPsec) architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides such functionality as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. In addition to IPsec, the Junos OS also supports the Internet Key Exchange (IKE), which defines mechanisms for key generation and exchange, and manages security associations (SAs).

IPsec also defines a security association and key management framework that can be used with any network layer protocol. The SA specifies what protection policy to apply to traffic between two IP-layer entities. IPsec provides secure tunnels between two peers.

For a complete description of the IPsec security suite, see the *IPsec Feature Guide*.

Related Documentation

- [IPsec Configuration for an ES PIC Overview on page 4](#)
- [IPsec Security Associations on page 7](#)

IPsec Requirements for Junos-FIPS

In a Junos-FIPS environment, hardware configurations with two Routing Engines must be configured to use IPsec and a private routing instance for all communications between the Routing Engines. IPsec communication between the Routing Engines and AS II FIPS PICs is also required.

Related Documentation

- [IPsec Security Associations on page 7](#)
- [IKE Key Management Protocol Overview on page 8](#)
- [\[edit security\] Hierarchy Level on page 99](#)

IPsec Configuration for an ES PIC Overview

IP Security (IPsec) provides a secure way to authenticate senders and encrypt IPv4 and IPv6 traffic between network devices, such as routers and hosts. The following sections show how to configure IPsec for an ES PIC.

The key management process (**kmd**) provides IPsec authentication services for ES PICs. The key management process starts only when IPsec is configured on the router.

Related Documentation

- [Configuring Minimum Manual Security Associations for IPsec on an ES PIC on page 13](#)
- [Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC on page 14](#)
- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)
- [Configuring an IKE Proposal for Dynamic SAs on page 26](#)
- [Example: Configuring an IKE Proposal on page 29](#)

ES Tunnel Interface Configuration for a Layer 3 VPN

To configure an ES tunnel interface for a Layer 3 VPN, you need to configure an ES tunnel interface on the provider edge (PE) router and on the customer edge (CE) router. You also need to configure IPsec on the PE and CE routers.

Related Documentation

- [IPsec Tunnel Traffic Configuration Overview on page 4](#)

IPsec Tunnel Traffic Configuration Overview

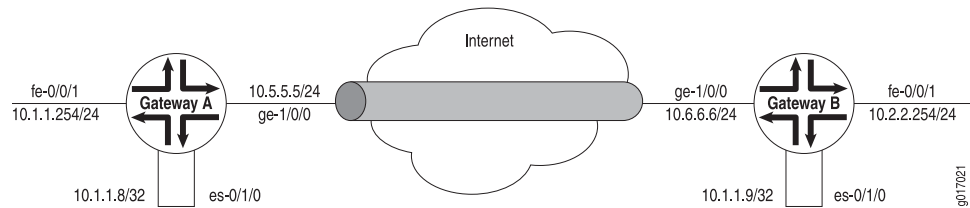
Traffic configuration defines the traffic that must flow through the IPsec tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt off of that LAN or WAN. The inbound filter is applied to the ES PIC to check the policy for traffic coming in from the remote host. Because of the complexity of configuring a router to forward packets, no automatic checking is done to ensure that the configuration is correct. Make sure that you configure the router very carefully.



NOTE: The valid firewall filters statements for IPsec are **destination-port**, **source-port**, **protocol**, **destination-address**, and **source-address**.

In [Figure 1 on page 5](#), Gateway A protects the network **10.1.1.0/24**, and Gateway B protects the network **10.2.2.0/24**. The gateways are connected by an IPsec tunnel.

Figure 1: Example: IPsec Tunnel Connecting Security Gateways



The SA and ES interfaces for Gateway A are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
        key ascii-text 123456789009876543211234;
      }
    }
  }
}
[edit interfaces es-0/1/0]
unit 0 {
  tunnel {
    source 10.5.5.5;
    destination 10.6.6.6;
  }
  family inet {
    ipsec-sa manual-sa1;
    address 10.1.1.8/32 {
      destination 10.1.1.9;
    }
  }
}
```

The SA and ES interfaces for Gateway B are configured as follows:

```
[edit security ipsec]
security-association manual-sa1 {
  manual {
    direction bidirectional {
      protocol esp;
      spi 2312;
      authentication {
        algorithm hmac-md5-96;
        key ascii-text 1234123412341234;
      }
      encryption {
        algorithm 3des-cbc;
      }
    }
  }
}
```

```
        key ascii-text 123456789009876543211234;
    }
}
[edit interfaces es-0/1/0]
unit 0 {
    tunnel {
        source 10.6.6.6;
        destination 10.5.5.5;
    }
    family inet {
        ipsec-sa manual-sa1;
        address 10.1.1.9/32; {
            destination 10.1.1.8;
        }
    }
}
```

**Related
Documentation**

- [Example: Configuring an Outbound Traffic Filter on page 63](#)
- [Example: Applying an Outbound Traffic Filter on page 64](#)
- [Example: Configuring an Inbound Traffic Filter for a Policy Check on page 64](#)
- [ES Tunnel Interface Configuration for a Layer 3 VPN on page 4](#)

CHAPTER 2

Security Associations and IKE Overview

- [Security Associations Overview on page 7](#)
- [IKE Key Management Protocol Overview on page 8](#)

Security Associations Overview

To use IPsec security services, you create SAs between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. There are two types of SAs: manual and dynamic.

- Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. Manual SAs statically define the Security Parameter Index (SPI) values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.
- Dynamic SAs require additional configuration. With dynamic SAs, you configure IKE first and then the SA. IKE creates dynamic security associations; it negotiates SAs for IPsec. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway. This connection is then used to dynamically agree upon keys and other data used by the dynamic IPsec SA. The IKE SA is negotiated first and then used to protect the negotiations that determine the dynamic IPsec SAs.
- Set up user-level tunnels or SAs, including tunnel attribute negotiations and key management. These tunnels can also be refreshed and terminated on top of the same secure channel.

The Junos OS implementation of IPsec supports two modes of security (transport mode and tunnel mode).

Related Documentation

- [IKE Key Management Protocol Overview on page 8](#)
- [IPsec System Requirements for Junos-FIPS on page 3](#)
- [\[edit security\] Hierarchy Level on page 99](#)

IKE Key Management Protocol Overview

IKE is a key management protocol that creates dynamic SAs; it negotiates SAs for IPsec. An IKE configuration defines the algorithms and keys used to establish a secure connection with a peer security gateway.

IKE does the following:

- Negotiates and manages IKE and IPsec parameters
- Authenticates secure key exchange
- Provides mutual peer authentication by means of shared secrets (not passwords) and public keys
- Provides identity protection (in main mode)

IKE occurs over two phases. In the first phase, it negotiates security attributes and establishes shared secrets to form the bidirectional IKE SA. In the second phase, inbound and outbound IPsec SAs are established. The IKE SA secures the exchanges in the second phase. IKE also generates keying material, provides Perfect Forward Secrecy, and exchanges identities.

Related Documentation

- [IPsec Security Associations on page 7](#)
- [IPsec System Requirements for Junos-FIPS on page 3](#)
- [\[edit security\] Hierarchy Level on page 99](#)

CHAPTER 3

Digital Certificates Overview

- [Digital Certificates Overview on page 9](#)

Digital Certificates Overview

A digital certificate provides a way of authenticating users through a trusted third-party called a certificate authority (CA). The CA validates the identity of a certificate holder and “signs” the certificate to attest that it has not been forged or altered.

A certificate includes the following information:

- The distinguished name (DN) of the owner. A DN is a unique identifier and consists of a fully qualified name including the common name (CN) of the owner, the owner’s organization, and other distinguishing information.
- The public key of the owner.
- The date on which the certificate was issued.
- The date on which the certificate expires.
- The distinguished name of the issuing CA.
- The digital signature of the issuing CA.

The additional information in a certificate allows recipients to decide whether to accept the certificate. The recipient can determine if the certificate is still valid based on the expiration date. The recipient can check whether the CA is trusted by the site based on the issuing CA.

With a certificate, a CA takes the owner’s public key, signs that public key with its own private key, and returns this to the owner as a certificate. The recipient can extract the certificate (containing the CA’s signature) with the owner’s public key. By using the CA’s public key and the CA’s signature on the extracted certificate, the recipient can validate the CA’s signature and owner of the certificate.

When you use digital certificates, your first step is to send in a request to obtain a certificate from your CA. You then configure digital certificates and a digital certificate IKE policy. Finally, you obtain a digitally signed certificate from a CA.



NOTE: Certificates without an alternate subject name are not appropriate for IPsec services.

**Related
Documentation**

- [Configuration Statements for Configuring Digital Certificates for an ES PIC on page 41](#)
- [Obtaining a Certificate from a Certificate Authority for an ES PIC on page 42](#)
- [Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 43](#)
- [Generating a Private and Public Key Pair for Digital Certificates for an ES PIC on page 43](#)
- [Configuring Digital Certificates for an ES PIC on page 45](#)
- [Configuring an IKE Policy for Digital Certificates for an ES PIC on page 49](#)
- [Associating the Configured Security Association with a Logical Interface on page 51](#)

PART 2

Configuration

- [Configuring IPsec for an ES PIC on page 13](#)
- [Configuring Digital Certificates for ES and AS PICs on page 41](#)
- [Configuring Traffic Filters and Tracing Operations on page 63](#)
- [Configuring Authentication Key Updates on page 71](#)

CHAPTER 4

Configuring IPsec for an ES PIC

- [Configuring Minimum Manual Security Associations for IPsec on an ES PIC on page 13](#)
- [Configuring Minimum IKE Requirements for IPsec on an ES PIC on page 14](#)
- [Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC on page 14](#)
- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)
- [Configuring Manual IPsec Security Associations for an ES PIC on page 22](#)
- [Configuring Dynamic IPsec Security Associations on page 26](#)
- [Configuring an IKE Proposal for Dynamic SAs on page 26](#)
- [Example: Configuring an IKE Proposal on page 29](#)
- [Configuring an IKE Policy for Preshared Keys on page 29](#)
- [Example: Configuring an IKE Policy on page 31](#)
- [Configuring an IPsec Proposal for an ES PIC on page 32](#)
- [Configuring the IPsec Policy for an ES PIC on page 34](#)
- [Example: Configuring an IPsec Policy on page 35](#)
- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 36](#)
- [Example: Configuring Internal IPsec on page 39](#)

Configuring Minimum Manual Security Associations for IPsec on an ES PIC

To define a manual security association (SA) configuration for an ES PIC, include at least the following statements at the **[edit security ipsec]** hierarchy level:

```
[edit security ipsec]
security-association sa-name {
  manual {
    direction (inbound | outbound | bidirectional) {
      authentication {
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
    }
  }
}
```

```
        protocol (ah | esp | bundle);
        spi spi-value;
    }
}
```

Related Documentation • [IPsec Configuration for an ES PIC Overview on page 4](#)

Configuring Minimum IKE Requirements for IPsec on an ES PIC

To define an IKE configuration for an ES PIC, include at least the following statements at the **[edit security]** hierarchy level:

```
[edit security ike]
proposal ike-proposal-name {
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbd | des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);
}
policy ike-peer-address {
    proposals [ ike-proposal-names ];
    pre-shared-key (ascii-text key | hexadecimal key);
}
```

Related Documentation • [IPsec Configuration for an ES PIC Overview on page 4](#)

Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC

To define a digital certificate configuration for IKE for an encryption interface on M Series and T Series routers, include at least the following statements at the **[edit security certificates]** and **[edit security ike]** hierarchy levels:

```
[edit security]
certificates {
    certification-authority ca-profile-name {
        ca-name ca-identity;
        crl filename;
        enrollment-url url-name;
        file certificate-filename;
        ldap-url url-name;
    }
}
ike {
    policy ike-peer-address {
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        proposal [ ike-proposal-names ];
    }
    proposal ike-proposal-name {
        authentication-method rsa-signatures;
    }
}
```

- Related Documentation**
- [IPsec Configuration for an ES PIC Overview on page 4](#)

Configuring Security Associations for IPsec on an ES PIC

To use IPsec security services, you create an SA between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. You can configure two types of SAs:

- **Manual**—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see [“Configuring Manual IPsec Security Associations for an ES PIC” on page 17](#).
- **Dynamic**—Specify proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more **proposal** statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see [“Associating the Configured Security Association with a Logical Interface” on page 51](#).



NOTE: The Junos OS does not perform a commit check when an SA name referenced in the Border Gateway Protocol (BGP) protocol section is not configured at the `[edit security ipsec]` hierarchy level.

We recommend that you configure no more than 512 dynamic security associations per ES Physical Interface Card (PIC).

To configure an SA for IPsec for an ES PIC, include the **security-association** statement at the `[edit security ipsec]` hierarchy level:

```
[edit security ipsec]
security-associationsa-name;
```



NOTE: You configure a dynamic SA for the AS and MultiServices PICs at the `[edit services ipsec-vpn rule rule-name term term-name then dynamic]`, `[edit services ipsec-vpn ike]`, and `[edit services ipsec-vpn ipsec]` hierarchy levels.

For more information, see the “IPsec Services Configuration Guidelines” chapter of the *Junos OS Services Interfaces Library for Routing Devices*.

Tasks to configure SAs for IPsec for an ES PIC are:

1. [Configuring the Description for an SA on page 16](#)
2. [Configuring IPsec Transport Mode on page 16](#)
3. [Configuring IPsec Tunnel Mode on page 16](#)
4. [Configuring Manual IPsec Security Associations for an ES PIC on page 17](#)

- 5. [Configuring Dynamic IPsec Security Associations on page 21](#)
- 6. [Enabling Dynamic IPsec Security Associations on page 21](#)

Configuring the Description for an SA

To specify a description for an IPsec SA, include the **description** statement at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
descriptiondescription;
```

Configuring IPsec Transport Mode

In transport mode, the data portion of the IP packet is encrypted, but the IP header is not. Transport mode can be used only when the communication endpoint and cryptographic endpoint are the same. Virtual private network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications. You configure manual SAs, and you must configure static values on both ends of the SA.



NOTE: When you use transport mode, the Junos OS supports both BGP and OSPFv3 for manual SAs.

To configure IPsec security for transport mode, include the **mode** statement with the **transport** option at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
mode transport;
```

To apply tunnel mode, you configure manual SAs in transport mode and then reference the SA by name at the **[edit protocols bgp]** hierarchy level to protect a session with a given peer.



NOTE: You can configure BGP to establish a peer relationship over encrypted tunnels.

Configuring IPsec Tunnel Mode

You use tunnel mode when you use preshared keys with IKE to authenticate peers, or digital certificates with IKE to authenticate peers.

When you use preshared keys, you manually configure a preshared key, which must match that of its peer. With digital certificates, each router is dynamically or manually enrolled with a certificate authority (CA). When a tunnel is established, the public keys used for IPsec are dynamically obtained through IKE and validated against the CA certificate. This avoids the manual configuration of keys on routers within the topology. Adding a new router to the topology does not require any security configuration changes to existing routers.

To configure the IPsec in tunnel mode, include the **mode** statement with the **tunnel** option at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
mode tunnel;
```



NOTE: The Junos OS supports both both BGP and OSPFv3 in transport mode.

To enable tunnel mode, follow the steps in these sections:

- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)
- [Configuring an IKE Proposal for Dynamic SAs on page 26](#)
- [Associating the Configured Security Association with a Logical Interface on page 51](#)
- [IPsec Tunnel Traffic Configuration Overview on page 4](#)

Configuring Manual IPsec Security Associations for an ES PIC

To use IPsec security services, you create security associations (SAs) between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. There are two types of SAs: manual and dynamic.

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, peers can communicate only when they all share the same configured options.

To configure the manual IPsec SA for an ES PIC, include the **manual** statement at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
manual {
  direction (inbound | outbound | bi-directional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
```

Tasks to configure a manual SA are:

1. [Configuring the Processing Direction on page 18](#)
2. [Configuring the Protocol for a Manual SA on page 19](#)
3. [Configuring the Security Parameter Index on page 19](#)

4. [Configuring the Auxiliary Security Parameter Index on page 19](#)
5. [Configuring the Authentication Algorithm and Key on page 20](#)
6. [Configuring the Encryption Algorithm and Key on page 20](#)

Configuring the Processing Direction

The **direction** statement sets inbound and outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each direction, you configure the **inbound** and **outbound** options. If you want the same attributes in both directions, use the **bidirectional** option.

To configure the direction of IPsec processing, include the **direction** statement and specify the direction at the **[edit security ipsec security-association sa-name manual]** hierarchy level:

```
[edit security ipsec security-association sa-name manual]
direction (inbound | outbound | bidirectional);
```

The following example shows how to define different algorithms, keys, and security parameter index values for inbound and outbound processing directions:

```
[edit security ipsec security-association sa-name]
manual {
  direction inbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 23456789012345678901234;
    }
    protocol esp;
    spi 16384;
  }
  direction outbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
    protocol esp;
    spi 24576;
  }
}
```

The following example shows how to define the same algorithms, keys, and security parameter index values for bidirectional processing:

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
  authentication {
    algorithm hmac-md5-96;
    key ascii-text 123456789012abcd;
  }
  protocol ah;
  spi 20001;
}
```

Configuring the Protocol for a Manual SA

IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). For transport mode SAs, both ESP and AH are supported. The AH protocol is used for strong authentication. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.



NOTE: The AH protocol is supported only on M Series routers.

To configure the IPsec protocol on an ES PIC, include the **protocol** statement at the **edit security ipsec security-association sa-name manual direction (inbound | outbound | bidirectional)]** hierarchy level and specify the **ah**, **bundle**, or **esp** option:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bi-directional)]
protocol (ah | bundle | esp);
```

Configuring the Security Parameter Index

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.



NOTE: Each manual SA must have a unique SPI and protocol combination.

Use the auxiliary SPI when you configure the protocol statement to use the **bundle** option.

To configure the SPI on an ES PIC, include the **spi** statement and specify a value (256 through 16,639) at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
spi spi-value;
```

Configuring the Auxiliary Security Parameter Index

When you configure the **protocol** statement to use the **bundle** option, the Junos OS uses the auxiliary SPI for the ESP and the SPI for the AH.



NOTE: Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the **auxiliary-spi** statement at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level and set the value to an integer between 256 and 16,639:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
auxiliary-spi auxiliary-spi-value;
```

Configuring the Authentication Algorithm and Key

To configure an authentication algorithm and key, include the **authentication** statement at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
bidirectional)]
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text key**—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal key**—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

Configuring the Encryption Algorithm and Key

To configure IPsec encryption, include the **encryption** statement and specify an algorithm and key at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
bi-directional)]
encryption {
  algorithm (des-cbc | 3des-cbc);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.



NOTE: For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409. For **3des-cbc**, we recommend that the first 8 bytes not be the same as the second 8 bytes, and that the second 8 bytes be the same as the third 8 bytes.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.



NOTE: You cannot configure encryption when you use the AH protocol.

Configuring Dynamic IPsec Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To configure a dynamic SA, include the **dynamic** statement at the **[edit security ipsec security-association sa-name]** hierarchy level. Specify an IPsec policy name, and optionally, a 32-packet or 64-packet replay window size.

```
[edit security ipsec security-association sa-name]
dynamic {
  ipsec-policy policy-name;
  replay-window-size (32 | 64);
}
```

Enabling Dynamic IPsec Security Associations

To enable a dynamic SA, follow these steps:

1. Configure IKE proposals and IKE policies associated with these proposals.
2. Configure IPsec proposals and an IPsec policy associated with these proposals.
3. Associate an SA with an IPsec policy.



NOTE: Dynamic tunnel SAs require an ES PIC. If you want to establish a dynamic SA, the attributes in at least one configured IPsec and IKE proposal must match those of its peer.

The replay window is not used with manual SAs.

Configuring Manual IPsec Security Associations for an ES PIC

To use IPsec security services, you create security associations (SAs) between hosts. An SA is a simplex connection that allows two hosts to communicate with each other securely by means of IPsec. There are two types of SAs: manual and dynamic.

Manual SAs require no negotiation; all values, including the keys, are static and specified in the configuration. As a result, peers can communicate only when they all share the same configured options.

To configure the manual IPsec SA for an ES PIC, include the **manual** statement at the **edit security ipsec security-association sa-name** hierarchy level:

```
[edit security ipsec security-association sa-name]
manual {
  direction (inbound | outbound | bi-directional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi-value;
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
```

Tasks to configure a manual SA are:

1. [Configuring the Processing Direction on page 22](#)
2. [Configuring the Protocol for a Manual SA on page 23](#)
3. [Configuring the Security Parameter Index on page 24](#)
4. [Configuring the Auxiliary Security Parameter Index on page 24](#)
5. [Configuring the Authentication Algorithm and Key on page 25](#)
6. [Configuring the Encryption Algorithm and Key on page 25](#)

Configuring the Processing Direction

The **direction** statement sets inbound and outbound IPsec processing. If you want to define different algorithms, keys, or security parameter index (SPI) values for each

direction, you configure the **inbound** and **outbound** options. If you want the same attributes in both directions, use the **bidirectional** option.

To configure the direction of IPsec processing, include the **direction** statement and specify the direction at the **[edit security ipsec security-association sa-name manual]** hierarchy level:

```
[edit security ipsec security-association sa-name manual]
direction (inbound | outbound | bidirectional);
```

The following example shows how to define different algorithms, keys, and security parameter index values for inbound and outbound processing directions:

```
[edit security ipsec security-association sa-name]
manual {
  direction inbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 23456789012345678901234;
    }
    protocol esp;
    spi 16384;
  }
  direction outbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 12345678901234567890abcd;
    }
    protocol esp;
    spi 24576;
  }
}
```

The following example shows how to define the same algorithms, keys, and security parameter index values for bidirectional processing:

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
  authentication {
    algorithm hmac-md5-96;
    key ascii-text 123456789012abcd;
  }
  protocol ah;
  spi 20001;
}
```

Configuring the Protocol for a Manual SA

IPsec uses two protocols to protect IP traffic: Encapsulating Security Payload (ESP) and authentication header (AH). For transport mode SAs, both ESP and AH are supported. The AH protocol is used for strong authentication. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.



NOTE: The AH protocol is supported only on M Series routers.

To configure the IPsec protocol on an ES PIC, include the **protocol** statement at the **edit security ipsec security-association sa-name manual direction (inbound | outbound | bidirectional)]** hierarchy level and specify the **ah**, **bundle**, or **esp** option:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bi-directional)]
protocol (ah | bundle | esp);
```

Configuring the Security Parameter Index

An SPI is an arbitrary value that uniquely identifies which SA to use at the receiving host. The sending host uses the SPI to identify and select which SA to use to secure every packet. The receiving host uses the SPI to identify and select the encryption algorithm and key used to decrypt packets.



NOTE: Each manual SA must have a unique SPI and protocol combination.

Use the auxiliary SPI when you configure the protocol statement to use the **bundle** option.

To configure the SPI on an ES PIC, include the **spi** statement and specify a value (256 through 16,639) at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
spi spi-value;
```

Configuring the Auxiliary Security Parameter Index

When you configure the **protocol statement to use the bundle** option, the Junos OS uses the auxiliary SPI for the ESP and the SPI for the AH.



NOTE: Each manual SA must have a unique SPI and protocol combination.

To configure the auxiliary SPI, include the **auxiliary-spi** statement at the **[edit security ipsec security-association sa-name manual direction (inbound | outbound | bi-directional)]** hierarchy level and set the value to an integer between 256 and 16,639:

```
[edit security ipsec security-association sa-name manual direction (inbound |
outbound | bidirectional)]
auxiliary-spi auxiliary-spi-value;
```

Configuring the Authentication Algorithm and Key

To configure an authentication algorithm and key, include the **authentication** statement at the **[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
  bidirectional)]
authentication {
  algorithm (hmac-md5-96 | hmac-sha1-96);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit authenticator value and 96-bit digest.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit authenticator value and a 96-bit digest.

The key can be one of the following:

- **ascii-text *key***—ASCII text key. With the **hmac-md5-96** option, the key contains 16 ASCII characters. With the **hmac-sha1-96** option, the key contains 20 ASCII characters.
- **hexadecimal *key***—Hexadecimal key. With the **hmac-md5-96** option, the key contains 32 hexadecimal characters. With the **hmac-sha1-96** option, the key contains 40 hexadecimal characters.

Configuring the Encryption Algorithm and Key

To configure IPsec encryption, include the **encryption** statement and specify an algorithm and key at the **[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]** hierarchy level:

```
[edit security ipsec security-association sa-name manual direction (inbound | outbound |
  bi-directional)]
encryption {
  algorithm (des-cbc | 3des-cbc);
  key (ascii-text key | hexadecimal key);
}
```

The algorithm can be one of the following:

- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 64 bits long.
- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.



NOTE: For a list of Data Encryption Standard (DES) encryption algorithm weak and semiweak keys, see RFC 2409. For **3des-cbc**, we recommend that the first 8 bytes not be the same as the second 8 bytes, and that the second 8 bytes be the same as the third 8 bytes.

The key can be one of the following:

- **ascii-text**—ASCII text key. With the **des-cbc** option, the key contains 8 ASCII characters. With the **3des-cbc** option, the key contains 24 ASCII characters.
- **hexadecimal**—Hexadecimal key. With the **des-cbc** option, the key contains 16 hexadecimal characters. With the **3des-cbc** option, the key contains 48 hexadecimal characters.



NOTE: You cannot configure encryption when you use the AH protocol.

Configuring Dynamic IPsec Security Associations

You configure dynamic SAs with a set of proposals that are negotiated by the security gateways. The keys are generated as part of the negotiation and do not need to be specified in the configuration. The dynamic SA includes one or more proposals, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer.

To configure a dynamic SA, include the **dynamic** statement at the **[edit security ipsec security-association sa-name]** hierarchy level. Specify an IPsec policy name, and optionally, a 32-packet or 64-packet replay window size.

```
[edit security ipsec security-association sa-name]
dynamic {
  ipsec-policy policy-name;
  replay-window-size (32 | 64);
}
```

Related Documentation

- [Configuring Manual IPsec Security Associations for an ES PIC on page 17](#)

Configuring an IKE Proposal for Dynamic SAs

Dynamic Security Associations (SAs) require IKE configuration. The IKE configuration defines the algorithms and keys used to establish the secure IKE connection with the peer security gateway.

You can configure one or more IKE proposals. Each proposal is a list of IKE attributes to protect the IKE connection between the IKE host and its peer.

To configure an IKE proposal and define its properties, include the following statements at the **[edit security ike]** hierarchy level:

```
[edit security ike]
proposal ike-proposal-name {
  authentication-algorithm (md5 | sha1);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group2);
  encryption-algorithm (3des-cbc | des-cbc | ase-128-cbc | ase-192-cbc | ase-256-cbc);
  lifetime-seconds seconds;
}
```

For information about associating an IKE proposal with an IKE policy, see [“Configuring an IKE Policy for Preshared Keys” on page 29](#).

Tasks for configuring the IKE proposal are:

1. [Configuring the Authentication Algorithm for an IKE Proposal on page 27](#)
2. [Configuring the Authentication Method for an IKE Proposal on page 27](#)
3. [Configuring the Description for an IKE Proposal on page 28](#)
4. [Configuring the Diffie-Hellman Group for an IKE Proposal on page 28](#)
5. [Configuring the Encryption Algorithm for an IKE Proposal on page 28](#)
6. [Configuring the Lifetime for an IKE SA on page 29](#)

Configuring the Authentication Algorithm for an IKE Proposal

To configure an IKE authentication algorithm, include the **authentication-algorithm** statement at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name]
authentication-algorithm (md5 | sha1);
```

The authentication algorithm can be one of the following:

- **md5**—Produces a 128-bit digest.
- **sha1**—Produces a 160-bit digest.

Configuring the Authentication Method for an IKE Proposal

To configure an IKE authentication method, include the **authentication-method** statement at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name]
authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
```

The authentication method can be one of the following:

- **dsa-signatures**—Digital Signature Algorithm (DSA)
- **pre-shared-keys**—Preshared keys; a key derived from an out-of-band mechanism is used to authenticate an exchange
- **rsa-signatures**—Public key algorithm that supports encryption and digital signatures

Configuring the Description for an IKE Proposal

To specify a description for an IKE proposal, include the **description** statement at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name]  
  description description;
```

Configuring the Diffie-Hellman Group for an IKE Proposal

The Diffie-Hellman key exchange is a public-key cryptography scheme that allows two parties to establish a shared secret over an insecure communications channel. It is also used within IKE to establish session keys.

To configure an IKE Diffie-Hellman group, include the **dh-group** statement at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name ]  
  dh-group (group1 | group2);
```

The group can be one of the following:

- **group1**—Specify that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specify that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security but requires more processing time.

Configuring the Encryption Algorithm for an IKE Proposal

To configure an IKE encryption algorithm, include the **encryption-algorithm** statement at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name ]  
  encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a key size of 8 bytes; its key size is 56 bits long.
- **aes-128-cbc**—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.
- **aes-192-cbc**—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.
- **aes-256-cbc**—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.

Configuring the Lifetime for an IKE SA

The IKE lifetime sets the lifetime of an IKE SA. When the IKE SA expires, it is replaced by a new SA (and SPI) or is terminated. The default value IKE lifetime is 3600 seconds.

To configure the IKE lifetime, include the **lifetime-seconds** statement and specify the number of seconds (180 through 86,400) at the **[edit security ike proposal *ike-proposal-name*]** hierarchy level:

```
[edit security ike proposal ike-proposal-name ]
lifetime-seconds seconds;
```

Example: Configuring an IKE Proposal

The following example shows how to configure an IKE proposal:

```
[edit security ike]
proposal ike-proposal {
  authentication-method pre-shared-keys;
  dh-group group;
  authentication-algorithm sha1;
  encryption-algorithm 3des-cbc;
}
```

Related Documentation

- [Configuring an IKE Proposal for Dynamic SAs on page 26](#)

Configuring an IKE Policy for Preshared Keys

An IKE policy defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address, the preshared key for the given peer, and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used. The configured preshared key must also match its peer.

You can create multiple, prioritized proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IKE proposals; then you associate these proposals with an IKE policy. You can also prioritize a list of proposals used by IKE in the **policy** statement by listing the proposals you want to use, from first to last.

To configure an IKE policy, include the **policy** statement at the **[edit security ike]** hierarchy level and specify a peer address:

```
[edit security ike]
policy ike-peer-address;
```



NOTE: The IKE policy peer address must be an IPsec tunnel destination address.

Tasks for configuring an IKE policy are:

1. [Configuring the Description for an IKE Policy on page 30](#)
2. [Configuring the Mode for an IKE Policy on page 30](#)
3. [Configuring the Preshared Key for an IKE Policy on page 30](#)
4. [Associating Proposals with an IKE Policy on page 31](#)

Configuring the Description for an IKE Policy

To specify a description for an IKE policy, include the **description** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]  
description description;
```

Configuring the Mode for an IKE Policy

IKE policy has two modes: aggressive and main. By default, main mode is enabled. Main mode uses six messages, in three exchanges, to establish the IKE SA. (These three steps are IKE SA negotiation, a Diffie-Hellman key exchange, and authentication of the peer.) Main mode also allows a peer to hide its identity.

Aggressive mode also establishes an authenticated IKE SA and keys. However, aggressive mode uses half the number of messages, has less negotiation power, and does not provide identity protection. The peer can use the aggressive or main mode to start IKE negotiation; the remote peer accepts the mode sent by the peer.

To configure IKE policy mode, include the **mode** statement and specify **aggressive** or **main** at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address ]  
mode (aggressive | main);
```

Configuring the Preshared Key for an IKE Policy

IKE policy preshared keys authenticate peers. You must manually configure a preshared key, which must match that of its peer. The preshared key can be an ASCII text (alphanumeric) key or a hexadecimal key.

A local certificate is an alternative to the preshared key. A commit operation fails if either a preshared key or a local certificate is not configured.

To configure an IKE policy preshared key, include the **pre-shared-key** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]  
pre-shared-key (ascii-text key | hexadecimal key);
```

Associating Proposals with an IKE Policy

The IKE policy proposal is a list of one or more proposals associated with an IKE policy.

To configure an IKE policy proposal, include the **proposals** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level and specify one or more proposal names:

```
[edit security ike policy ike-peer-address]  
proposals [ proposal-names ];
```

Related Documentation

- [Example: Configuring an IKE Policy on page 31](#)

Example: Configuring an IKE Policy

Define two IKE policies: policy 10.1.1.2 and policy 10.1.1.1. Each policy is associated with **proposal-1** and **proposal-2**.

```
[edit security]  
ike {  
  proposal proposal-1 {  
    authentication-method pre-shared-keys;  
    dh-group group1;  
    authentication-algorithm sha1;  
    encryption-algorithm 3des-cbc;  
    lifetime-seconds 1000;  
  }  
  proposal proposal-2 {  
    authentication-method pre-shared-keys;  
    dh-group group2;  
    authentication-algorithm md5;  
    encryption-algorithm des-cbc;  
    lifetime-seconds 10000;  
  }  
  proposal proposal-3 {  
    authentication-method rsa-signatures;  
    dh-group group2;  
    authentication-algorithm md5;  
    encryption-algorithm des-cbc;  
    lifetime-seconds 10000;  
  }  
  policy 10.1.1.2 {  
    mode main;  
    proposals [ proposal-1 proposal-2 ];  
    pre-shared-key ascii-text example-pre-shared-key;  
  }  
  policy 10.1.1.1 {  
    local-certificate certificate-filename;  
    local-key-pair private-public-key-file;  
    mode aggressive;  
    proposals [ proposal-2 proposal-3 ]  
    pre-shared-key hexadecimal 0102030abbcd;  
  }  
}
```



NOTE: Updates to the current IKE proposal and policy configuration are not applied to the current IKE SA; updates are applied to new IKE SAs.

If you want the new updates to take immediate effect, you must clear the existing IKE security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IKE security association, see the [CLI Explorer](#).

Related Documentation

- [Configuring an IKE Policy for Preshared Keys on page 29](#)

Configuring an IPsec Proposal for an ES PIC

An IPsec proposal lists protocols and algorithms (security services) to be negotiated with the remote IPsec peer.

To configure an IPsec proposal and define its properties, include the following statements at the `[edit security ipsec]` hierarchy level:

```
[edit security ipsec]
proposal ipsec-proposal-name {
  authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
  description description ;
  encryption-algorithm (3des-cbc | des-cbc);
  lifetime-seconds seconds;
  protocol (ah | esp | bundle);
}
```

Tasks to configure an IPsec proposal for an ES PIC include:

- [Configuring the Authentication Algorithm for an IPsec Proposal on page 32](#)
- [Configuring the Description for an IPsec Proposal on page 33](#)
- [Configuring the Encryption Algorithm for an IPsec Proposal on page 33](#)
- [Configuring the Lifetime for an IPsec SA on page 33](#)
- [Configuring the Protocol for a Dynamic IPsec SA on page 34](#)

Configuring the Authentication Algorithm for an IPsec Proposal

To configure an IPsec authentication algorithm, include the **authentication-algorithm** statement at the `[edit security ipsec proposal ipsec-proposal-name]` hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]
authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
```

The authentication algorithm can be one of the following:

- **hmac-md5-96**—Hash algorithm that authenticates packet data. It produces a 128-bit digest. Only 96 bits are used for authentication.
- **hmac-sha1-96**—Hash algorithm that authenticates packet data. It produces a 160-bit digest. Only 96 bits are used for authentication.

Configuring the Description for an IPsec Proposal

To specify a description for an IPsec proposal, include the **description** statement at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ike policy ipsec-proposal-name]  
description description;
```

Configuring the Encryption Algorithm for an IPsec Proposal

To configure the IPsec encryption algorithm, include the **encryption-algorithm** statement at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name ]  
encryption-algorithm (3des-cbc | des-cbc);
```

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a block size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a block size of 8 bytes; its key size is 48 bits long.



NOTE: We recommend that you use the triple DES cipher block chaining (3DES-CBC) encryption algorithm.

Configuring the Lifetime for an IPsec SA

The IPsec lifetime option sets the lifetime of an IPsec SA. When the IPsec SA expires, it is replaced by a new SA (and SPI) or is terminated. A new SA has new authentication and encryption keys, and SPI; however, the algorithms may remain the same if the proposal is not changed. If you do not configure a lifetime and a lifetime is not sent by a responder, the lifetime is 28,800 seconds.

To configure the IPsec lifetime, include the **lifetime-seconds** statement and specify the number of seconds (180 through 86,400) at the **[edit security ipsec proposal *ipsec-proposal-name*]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name]  
lifetime-seconds seconds;
```



NOTE: When a dynamic SA is created, two types of lifetimes are used: hard and soft. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. When you specify the lifetime, you specify a hard lifetime.

Configuring the Protocol for a Dynamic IPsec SA

The **protocol** statement sets the protocol for a dynamic SA. The ESP protocol can support authentication, encryption, or both. The AH protocol is used for strong authentication. AH also authenticates the IP packet. The **bundle** option uses AH authentication and ESP encryption; it does not use ESP authentication because AH provides stronger authentication of IP packets.

To configure the protocol for a dynamic SA, include the **protocol** statement at the **[edit security ipsec proposal ipsec-proposal-name]** hierarchy level:

```
[edit security ipsec proposal ipsec-proposal-name ] protocol ( ah | esp | bundle );
```

Configuring the IPsec Policy for an ES PIC

An IPsec policy defines a combination of security parameters (IPsec proposals) used during IPsec negotiation. It defines Perfect Forward Secrecy (PFS) and the proposals needed for the connection. During the IPsec negotiation, IPsec looks for an IPsec proposal that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

A match is made when both policies from the two peers have a proposal that contains the same configured attributes. If the lifetimes are not identical, the shorter lifetime between the two policies (from the host and peer) is used.

You can create multiple, prioritized IPsec proposals at each peer to ensure that at least one proposal will match a remote peer's proposal.

First, you configure one or more IPsec proposals; then you associate these proposals with an IPsec policy. You can prioritize the proposals in the list by listing them in the order in which the IPsec policy uses them (first to last).

To configure an IPsec policy, include the **policy** statement at the **[edit security ipsec]** hierarchy level, specifying the policy name and one or more proposals you want to associate with this policy:

```
[edit security ipsec]
policy ipsec-policy-name {
  proposals [ proposal-names ];
}
```

Configuring Perfect Forward Secrecy

PFS provides additional security by means of a Diffie-Hellman key exchange shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys. This statement is optional.

To configure PFS, include the **perfect-forward-secrecy** statement and specify a Diffie-Hellman group at the **[edit security ipsec policy ipsec-policy-name]** hierarchy level:

```
[edit security ipsec policy ipsec-policy-name]
perfect-forward-secrecy {
  keys (group1 | group2);
}
```

```
}

```

The key can be one of the following:

- **group1**—Specify that IKE use the 768-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.
- **group2**—Specify that IKE use the 1024-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

group2 provides more security than **group1**, but requires more processing time.

**Related
Documentation**

- [Example: Configuring an IPsec Policy on page 35](#)
- [IPsec Configuration for an ES PIC Overview on page 4](#)

Example: Configuring an IPsec Policy

The following example shows how to configure an IPsec policy:

```
[edit security ipsec]
proposal dynamic-1 {
  protocol esp;
  authentication-algorithm hmac-md5-96;
  encryption-algorithm 3des-cbc;
  lifetime-seconds 6000;
}
proposal dynamic-2 {
  protocol esp;
  authentication-algorithm hmac-sha1-96;
  encryption-algorithm 3des-cbc;
  lifetime-seconds 6000;
}
policy dynamic-policy-1 {
  perfect-forward-secrecy {
    keys group1;
  }
  proposals [ dynamic-1 dynamic-2 ];
}
security-association dynamic-sa1 {
  dynamic {
    replay-window-size 64;
    ipsec-policy dynamic-policy-1;
  }
}
```



NOTE: Updates to the current IPsec proposal and policy configuration are not applied to the current IPsec SA; updates are applied to new IPsec SAs.

If you want the new updates to take immediate effect, you must clear the existing IPsec security associations so that they will be reestablished with the changed configuration. For information about how to clear the current IPsec security association, see the [CLI Explorer](#).

- Related Documentation**
- [Configuring the IPsec Policy for an ES PIC on page 34](#)
 - [IPsec Configuration for an ES PIC Overview on page 4](#)

Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode

In a Junos OS in FIPS mode environment, routers with two Routing Engines must use IPsec for internal communication between the Routing Engines. You configure internal IPsec after you install the Junos OS in FIPS mode. You must be a Crypto Officer to configure internal IPsec.



NOTE: You cannot configure DES-based IPsec SAs in Junos OS in FIPS mode. The internal IPsec SAs use HMAC-SHA1-96 authentication and 3DES-CBC encryption.

Manual SAs require no negotiation. All values, including the keys, are static and specified in the configuration. Manual SAs statically define the SPI values, algorithms, and keys to be used, and require matching configurations on both ends of the tunnel. Each peer must have the same configured options for communication to take place.



NOTE: When the switch is in FIPS mode, you cannot use the `commit synchronize` command until you have established an IPsec SA on each Routing Engine.

As Crypto Officer, you configure an internal IPsec SA for communication between Routing Engines by creating an SA on each Routing Engine with the following statements at the `[edit security]` hierarchy level:

To configure internal IPsec, include the `security-association` statement at the `[edit security]` hierarchy level. You can configure parameters, such as the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          encryption {
            algorithm (hmac-sha1-96 | hmac-sha2-256);
            key (ascii-text ascii-text-string | hexadecimal hexadecimal-number);
          }
        }
      }
    }
  }
}
```



```

    }
  }
}

```

Tasks for configuring internal IPsec for Junos-FIPS are the following. You can configure the direction in which the manual IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

1. [Configuring the SA Direction on page 37](#)
2. [Configuring the IPsec SPI on page 38](#)
3. [Configuring the IPsec Key on page 38](#)

Configuring the SA Direction

To configure the IPsec SA direction in which manual SAs of the IPsec tunnels must be applied, include the **direction** statement at the **[edit security ipsec internal security-association manual]** hierarchy level:

direction (bidirectional | inbound | outbound);

The value can be one of the following:

- **bidirectional**—Apply the same SA values in both directions between Routing Engines.
- **inbound**—Apply these SA properties only to the inbound IPsec tunnel.
- **outbound**—Apply these SA properties only to the outbound IPsec tunnel.

If you do not configure the SA to be bidirectional, you must configure SA parameters for IPsec tunnels in both the inbound and outbound directions. The following example uses an inbound and outbound IPsec tunnel:



NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

```

[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction inbound {
          protocol esp;
          spi 512;
          encryption {
            algorithm 3des-cbc;
            key hexadecimal 309fc4be20f04e53e011b00744642d3fe66c2c7c;
          }
        }
        direction outbound {
          protocol esp;

```

```

spi 513;
encryption {
    algorithm 3des-cbc;
    key hexadecimal b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7;
}
}
}
}
}
}

```

Configuring the IPsec SPI

A security parameter index (SPI) is a 32-bit index that identifies a security context between a pair of Routing Engines. To configure the IPsec SPI value, include the **spi** statement at the **[edit security ipsec internal security-association manual direction]** hierarchy level:

spi *value*;

The value must be from 256 through 16,639.

Configuring the IPsec Key



NOTE: We recommend that you do not use the IPsec keys as ASCII keys for Junos OS in FIPS mode. Instead, you must use the IPsec keys as hexadecimal keys for maximum key strength.

The distribution and management of keys are critical to using VPNs successfully. You must configure the ASCII text key values for authentication and encryption. To configure the ASCII text key, include the **key** statement at the **[edit security ipsec internal security-association manual direction encryption]** hierarchy level:

key (*ascii-text ascii-text-string* | *hexadecimal hexadecimal-string*);

For this type of SA, both keys must be preshared hexadecimal values, and each requires a specific cryptographic algorithm:

- Authentication algorithm
 - HMAC-SHA1-96 (40 characters)
 - HMAC-SHA2-256 (64 characters)
- Encryption algorithm
 - 3DES-CBC (48 characters)

You must enter the key hexadecimal value twice and the strings entered must match, or the key will not be set. The hexadecimal key is never displayed in plain text. We recommend that you use the IPsec keys as hexadecimal keys for maximum key strength and not as ASCII keys for Junos OS in FIPS mode.

Related Documentation

- [Example: Configuring Internal IPsec on page 39](#)

Example: Configuring Internal IPsec

Configure a bidirectional IPsec SA with an SPI value of 512 and a key value conforming to the FIPS 140-2 rules:

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction bidirectional {
          protocol esp;
          spi 512;
          encryption {
            algorithm 3des-cbc;
            key ascii-text "$ABC123";
          }
        }
      }
    }
  }
}
```

Related Documentation

- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 36](#)

CHAPTER 5

Configuring Digital Certificates for ES and AS PICs

- Configuration Statements for Setting Up Digital Certificates for an ES PIC on page 41
- Obtaining a Certificate from a Certificate Authority for an ES PIC on page 42
- Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 43
- Example: Requesting a CA Digital Certificate on page 43
- Generating a Private and Public Key Pair for Digital Certificates for an ES PIC on page 43
- Obtaining a Signed Certificate from the CA for an ES PIC on page 44
- Configuring Digital Certificates for an ES PIC on page 45
- Configuring an IKE Policy for Digital Certificates for an ES PIC on page 49
- Associating the Configured Security Association with a Logical Interface on page 51
- Configuring Digital Certificates for Adaptive Services Interfaces on page 51
- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 60

Configuration Statements for Setting Up Digital Certificates for an ES PIC

To define the digital certificate configuration for an encryption service interface, include the following statements at the **[edit security certificates]** and **[edit security ike]** hierarchy levels:

```
[edit security]
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
```

```
local certificate-filename {  
    certificate-key-string;  
    load-key-file URL key-file-name;  
}  
maximum-certificates number;  
path-length certificate-path-length;  
}  
ike {  
    policy ike-peer-address {  
        description policy;  
        encoding (binary | pem);  
        identity identity-name;  
        local-certificate certificate-filename;  
        local-key-pair private-public-key-file;  
        mode (aggressive | main);  
        pre-shared-key (ascii-text key | hexadecimal key);  
        proposals [ proposal-names ];  
    }  
}
```

The statements for configuring digital certificates differ for the AS and MultiServices PICs and the ES PIC.

For information about how to configure the **description** and **mode** statements, see [“Configuring the Description for an IKE Policy” on page 30](#). For information about how to configure the IKE proposal, see [“Associating Proposals with an IKE Policy” on page 31](#).



NOTE: For digital certificates, the Junos OS supports only VeriSign CAs for the ES PIC.

**Related
Documentation**

- [Digital Certificates Overview on page 9](#)

Obtaining a Certificate from a Certificate Authority for an ES PIC

Certificate authorities (CAs) manage certificate requests and issue certificates to participating IPsec network devices. When you create a certificate request, you need to provide the information about the owner of the certificate. The required information and its format vary across certificate authorities.

Certificates use names in the X.500 format, a directory access protocol that provides both read and update access. The entire name is called a DN (distinguished name). It consists of a set of components, which often includes a CN (common name), an organization (O), an organization unit (OU), a country (C), a locality (L), and so on.



NOTE: For the dynamic registration of digital certificates, the Junos OS supports only the Simple Certificate Enrollment Protocol (SCEP).

- Related Documentation
- [Digital Certificates Overview on page 9](#)

Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router

For an encryption interface on an M Series or T Series router, issue the following command to obtain a public key certificate from a CA. The results are saved in the specified file in the `/var/etc/ikecert` directory. The CA public key verifies certificates from remote peers.

```
user@host> request security certificate enroll filename filename ca-name ca-name
parameters parameters
```

- Related Documentation
- [Example: Requesting a CA Digital Certificate on page 43](#)
 - [Digital Certificates Overview on page 9](#)

Example: Requesting a CA Digital Certificate

Specify a URL to the SCEP server and the name of the certification authority whose certificate you want: **mycompany.com**. **filename1** is name of the file that stores the result. The output, "Received CA certificate:" provides the signature for the certificate, which allows you to verify (offline) that the certificate is genuine.

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
xyzcompany url
http://hostname/path/filename
URL: http://hostname/path/filename name: example.com CA file: verisign Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the key
management process (kmd) log file at /var/log/kmd. <-----
```



NOTE: Each router is initially manually enrolled with a certificate authority.

- Related Documentation
- [Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 43](#)

Generating a Private and Public Key Pair for Digital Certificates for an ES PIC

To generate a private and public key, issue the following command:

```
user@host> request security key-pair name size key-size type ( rsa | dsa )
```

name specifies the filename in which to store the public and private keys.

key-size can be 512, 1024, 1596, or 2048 bytes. The default key size is 1024 bytes.

type can be **rsa** or **dsa**. The default is RSA.



NOTE: When you use SCEP, the Junos OS only supports RSA.

The following example shows how to generate a private and public key pair:

```
user@host> request security key-pair batt
Generated key pair, key size 1024, file batt Algorithm RSA
```

Related Documentation

- [Digital Certificates Overview on page 9](#)

Obtaining a Signed Certificate from the CA for an ES PIC

To obtain a signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename filename subject c=us,o=x
alternative-subject certificate-ip-address certification-authority certificate-authority
key-file key-file-name domain-name domain-name
```

The results are saved in a specified file to the `/var/etc/ikecert` directory.

The following example shows how to obtain a CA signed certificate by referencing the configured `certification-authority` statement `local`. This statement is referenced by the `request security certificate enroll filename m subject c=us,O=x alternative subject 1.1.1.1 certification-authority` command.

```
[edit]
security {
  certificates {
    certification-authority local {
      ca-name xyz.company.com;
      file l;
      enrollment-url "http://www.xyzcompany.com";
    }
  }
}
```

To obtain a signed certificate from the CA, issue the following command:

```
user@host> request security certificate enroll filename l subject c=uk,o=london
alternative-subject 10.50.1.4 certification-authority verisign key-file host-l.prv
domain-name host.xyzcompany.com
CA name: xyz.company.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.net
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the key
management process (kmd) log file at /var/log/kmd. <-----
```

For information about how to use the operational mode commands to obtain a signed certificate, see the [CLI Explorer](#).

Another way to obtain a signed certificate from the CA is to reference the configured statements such as the URL, CA name, and CA certificate file by means of the `certification-authority` statement:

```
user@host> request security certificate enroll filename m subject c=us,o=x
alternative-subject 1.1.1.1 certification-authority local key-file y domain-name
abc.company.com
```


Related Documentation

- [Digital Certificates Overview on page 9](#)

Configuring Digital Certificates for an ES PIC

Digital certificates provide a way of authenticating users through a trusted third party called a certificate authority (CA). The CA validates the identity of a certificate holder and “signs” the certificate to attest that it has not been forged or altered.

To define the digital certificate configuration for an encryption service interface, include the following statements at the **[edit security certificates]** and **[edit security ike]** hierarchy levels:

```
[edit security]
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl filename;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-filename {
    certificate-key-string;
    load-key-file URL key-file-name;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
ike {
  policy ike-peer-address {
    description policy;
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
  }
}
```

Tasks to configure digital certificates for ES PICs are:

- [Configuring the Certificate Authority Properties for an ES PIC on page 46](#)
- [Configuring the Cache Size on page 48](#)
- [Configuring the Negative Cache on page 48](#)
- [Configuring the Number of Enrollment Retries on page 48](#)

- [Configuring the Maximum Number of Peer Certificates on page 49](#)
- [Configuring the Path Length for the Certificate Hierarchy on page 49](#)

Configuring the Certificate Authority Properties for an ES PIC

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for an ES PIC, include the following statements at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
certification-authority ca-profile-name {
  ca-name ca-identity;
  crl filename;
  encoding (binary | pem);
  enrollment-url url-name;
  file certificate-filename;
  ldap-url url-name;
}
```

ca-profile-name is the CA profile name.

Tasks for configuring the CA properties are:

1. [Specifying the Certificate Authority Name on page 46](#)
2. [Configuring the Certificate Revocation List on page 46](#)
3. [Configuring the Type of Encoding Your CA Supports on page 47](#)
4. [Specifying an Enrollment URL on page 47](#)
5. [Specifying a File to Read the Digital Certificate on page 47](#)
6. [Specifying an LDAP URL on page 47](#)

Specifying the Certificate Authority Name

If you are enrolling with a CA using simple certificate enrollment protocols (SCEP), you need to specify the CA name (CA identity) that is used in the certificate request, in addition to the URL for the SCEP server.

To specify the name of the CA identity, include the **ca-name** statement at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]
ca-name ca-identity;
```

ca-identity specifies the CA identity to use in the certificate request. It is typically the CA domain name.

Configuring the Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

To configure the CA certificate revocation list, include the **crl** statement and specify the file from which to read the CRL at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  crl filename;
```

Configuring the Type of Encoding Your CA Supports

By default, encoding is set to binary. Encoding specifies the file format used for the **local-certificate** and **local-key-pair** statements. By default, the binary (distinguished encoding rules) format is enabled. Privacy-enhanced mail (PEM) is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the **encoding** statement and specify a binary or PEM format at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  encoding (binary | pem);
```

Specifying an Enrollment URL

You specify the CA location where your router or switch sends SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the **enrollment-url** statement at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  enrollment-url url-name;
```

url-name is the CA location. The format is **http://*ca-name***, where ***ca-name*** is the CA host DNS name or IP address.

Specifying a File to Read the Digital Certificate

To specify the file from which to read the digital certificate, include the **file** statement and specify the certificate filename at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  file certificate-filename;
```

Specifying an LDAP URL

If your CA stores its current CRL at its Lightweight Directory Access Protocol (LDAP) server, you can optionally check your CA CRL list before using a digital certificate. If the digital certificate appears on the CA CRL, your router or switch cannot use it. To access your CA CRL, include the **ldap-url** statement at the **[edit security certificates certification-authority *ca-profile-name*]** hierarchy level:

```
[edit security certificates certification-authority ca-profile-name]  
  ldap-url url-name;
```

url-name is the certification authority LDAP server name. The format is **ldap://server-name**, where **server-name** is the CA host DNS name or IP address.

Configuring the Cache Size

By default, the cache size is 2 megabytes (MB). To configure total cache size for digital certificates, include the **cache-size** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
cache-size bytes;
```

bytes is the cache size for digital certificates. The range can be from 64 through 4,294,967,295 bytes.



NOTE: We recommend that you limit your cache size to 4 MB.

Configuring the Negative Cache

Negative caching stores negative results and reduces the response time for negative answers. It also reduces the number of messages that are sent to the remote server. Maintaining a negative cache state allows the system to quickly return a failure condition when a lookup attempt is retried. Without a negative cache state, a retry would require waiting for the remote server to fail to respond, even though the system already “knows” that remote server is not responding.

By default, the negative cache is 20 seconds. To configure the negative cache, include the **cache-timeout-negative** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
cache-timeout-negative seconds;
```

seconds is the amount of time for which a failed CA or router certificate is present in the negative cache. While searching for certificates with a matching CA identity (domain name for certificates or CA domain name and serial for CRLs), the negative cache is searched first. If an entry is found in the negative cache, the search fails immediately.



NOTE: Configuring a large negative cache value can make you susceptible to a denial-of-service (DoS) attack.

Configuring the Number of Enrollment Retries

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router or switch will resend a certificate request, include the **enrollment-retry** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
enrollment-retry attempts;
```

attempts is the number of enrollment retries (0 through 100).

Configuring the Maximum Number of Peer Certificates

By default, the maximum number of peer certificates to be cached is 1024. To configure the maximum number of peer certificates to be cached, include the **maximum-certificates** statement at the **[edit security certificates]** hierarchy statement level:

```
[edit security certificates]
maximum-certificates number;
```

number is the maximum number of peer certificates to be cached. The range is from 64 through 4,294,967,295 peer certificates.

Configuring the Path Length for the Certificate Hierarchy

Certification authorities can issue certificates to other CAs. This creates a tree-like certification hierarchy. The highest trusted CA in the hierarchy is called the *trust anchor*. Sometimes the trust anchor is the root CA, which is usually signed by itself. In the hierarchy, every certificate is signed by the CA immediately above it. An exception is the root CA certificate, which is usually signed by the root CA itself. In general, a chain of multiple certificates may be needed, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs. Such chains, called certification paths, are required because a public key user is only initialized with a limited number of assured CA public keys.

Path length refers to a path of certificates from one certificate to another certificate, based on the relationship of a CA and its “children.” When you configure the **path-length** statement, you specify the maximum depth of the hierarchy to validate a certificate from the trusted root CA certificate to the certificate in question. For more information about the certificate hierarchy, see RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

By default, the maximum certificate path length is set to 15. The root anchor is 1.

To configure path length, include the **path-length** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
path-length certificate-path-length;
```

certificate-path-length is the maximum number certificates for the certificate path length. The range is from 2 through 15 certificates.

Configuring an IKE Policy for Digital Certificates for an ES PIC

An IKE policy for digital certificates defines a combination of security parameters (IKE proposals) to be used during IKE negotiation. It defines a peer address and the proposals needed for that connection. During the IKE negotiation, IKE looks for an IKE policy that is the same on both peers. The peer that initiates the negotiation sends all its policies to the remote peer, and the remote peer tries to find a match.

To configure an IKE policy for digital certificates for an ES PIC, include the following statements at the **[edit security ike policy ike-peer-address]** hierarchy level:

```
[edit security ike]
policy ike-peer-address{
  encoding (binary | pem);
  identity identity-name;
  local-certificate certificate-filename;
  local-key-pair private-public-key-file;
}
```

Tasks for configuring an IKE policy for digital certificates are:

1. [Configuring the Type of Encoding Your CA Supports on page 50](#)
2. [Configuring the Identity to Define the Remote Certificate Name on page 50](#)
3. [Specifying the Certificate Filename on page 50](#)
4. [Specifying the Private and Public Key File on page 50](#)

Configuring the Type of Encoding Your CA Supports

By default, the encoding is set to binary. Encoding specifies the file format used for the **local-certificate** and **local-key-pair** statements. By default, the binary (distinguished encoding rules) format is enabled. PEM is an ASCII base 64 encoded format. Check with your CA to determine which file formats it supports.

To configure the file format that your CA supports, include the **encoding** statement and specify a binary or PEM format at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address ]
encoding (binary | pem);
```

Configuring the Identity to Define the Remote Certificate Name

To define the remote certificate name, include the **identity** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]
identity identity-name;
```

identity-name defines the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).

Specifying the Certificate Filename

To configure the certificate filename from which to read the local certificate, include the **local-certificate** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address]
local-certificate certificate-filename;
```

certificate-filename specifies the file from which to read the local certificate.

Specifying the Private and Public Key File

To specify the filename from which to read the public and private key, include the **local-key-pair** statement at the **[edit security ike policy *ike-peer-address*]** hierarchy level:

```
[edit security ike policy ike-peer-address ]
local-key-pair private-public-key-file;
```

private-public-key-file specifies the file from which to read the pair key.

Associating the Configured Security Association with a Logical Interface

Configuring the ES PIC associates the configured SA with a logical interface. This configuration defines the tunnel itself (logical subunit, tunnel addresses, maximum transmission unit [MTU], optional interface addresses, and the name of the SA to apply to traffic).

The addresses configured as the tunnel source and destination are the addresses in the outer IP header of the tunnel.



NOTE: The tunnel source address must be configured locally on the router, and the tunnel destination address must be a valid address for the security gateway terminating the tunnel.

The M5, M10, M20, and M40 routers support the ES PIC.

The SA must be a valid tunnel-mode SA. The interface address and destination address listed are optional. The destination address allows the user to configure a static route to encrypt traffic. If a static route uses that destination address as the next hop, traffic is forwarded through the portion of the tunnel in which encryption occurs.

The following example shows how to configure an IPsec tunnel as a logical interface on the ES PIC. The logical interface specifies the tunnel through which the encrypted traffic travels. The **ipsec-sa** statement associates the security profile with the interface.

```
[edit interfaces]
es-0/0/0 {
  unit 0 {
    tunnel {
      source tunnel 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      ipsec-sa ipsec-sa; # name of security association to apply to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

**Related
Documentation**

- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)

Configuring Digital Certificates for Adaptive Services Interfaces

A digital certificate implementation uses the public key infrastructure (PKI), which requires that you generate a key pair consisting of a public key and a private key. The keys are

created with a random number generator and are used to encrypt and decrypt data. In networks that do not use digital certificates, an IPsec-enabled device encrypts data with the private key and IPsec peers decrypt the data with the public key.

With digital certificates, the key sharing process requires an additional level of complexity. First, you and your IPsec peers request that a certificate authority (CA) send you a CA certificate that contains the public key of the CA. Next you request the CA to assign you a local digital certificate that contains the public key and some additional information. When the CA processes your request, it signs your local certificate with the private key of the CA. Then you install the CA certificate and the local certificate in your router and load the CA in remote devices before you can establish IPsec tunnels with your peers.



NOTE: For digital certificates, the Junos OS supports VeriSign, Entrust, Cisco Systems, and Microsoft Windows CAs for the Adaptive Services (AS) and Multiservices PICs.

To define digital certificates configuration for J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security]
pki {
  ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
      url-name;
      retry number-of-enrollment-attempts;
      retry-interval seconds;
    }
    revocation-check {
      disable;
      crl {
        disable on-download-failure;
        refresh-interval number-of-hours;
        url {
          url-name;
          password;
        }
      }
    }
  }
}
```

The following tasks enable you to implement digital certificates on J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers:

1. [Configuring the Certificate Authority Properties on page 53](#)
2. [Configuring the Certificate Revocation List on page 54](#)
3. [Managing Digital Certificates on page 55](#)
4. [Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57](#)

Configuring the Certificate Authority Properties

A CA is a trusted third-party organization that creates, enrolls, validates, and revokes digital certificates.

To configure a certificate authority and its properties for the AS and Multiservices PICs, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security pki]
ca-profile ca-profile-name {
  ca-identity ca-identity;
  enrollment {
    url url-name;
    retry number-of-attempts;
    retry-interval seconds;
  }
}
```

Tasks for configuring the Certificate Authority properties are:

1. [Specifying the CA Profile Name on page 53](#)
2. [Specifying an Enrollment URL on page 53](#)
3. [Specifying the Enrollment Properties on page 54](#)

Specifying the CA Profile Name

The CA profile contains the name and URL of the CA or RA, as well as some retry-timer settings. CA certificates issued by Entrust, VeriSign, Cisco Systems, and Microsoft are compatible with the J Series Services Routers and AS and Multiservices PICs installed in the M Series and T Series routers.

To specify the CA profile name, include the **ca-profile statement** at the **[edit security pki]** security level:

```
[edit security pki]
ca-profile ca-profile-name;
```

You also need to specify the name of the CA identity used in the certificate request. This name is typically the domain name. To specify the name of the CA identity, include the **ca-identity statement** at the **[edit security pki ca-profile ca-profile-name]** level:

```
[edit security pki ca-profile ca-profile-name]
ca-identity ca-identity;
```

Specifying an Enrollment URL

You specify the CA location where your router should send the SCEP-based certificate enrollment requests. To specify the CA location by naming the CA URL, include the **url statement** at the **[edit security pki enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
url url-name;
```

url-name is the CA location. The format is **http://CA_name**, where **CA_name** is the CA host DNS name or IP address.

Specifying the Enrollment Properties

You can specify the number of times a router will resend a certificate request and the amount of time, in seconds, the router should wait between enrollment attempts.

By default, the number of enrollment retries is set to 0, an infinite number of retries. To specify how many times a router will resend a certificate request, include the **retry number-of-attempts** statement at the **[edit security pki ca-profile ca-profile-name enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
  retry number-of-attempts;
```

The range for **number-of-attempts** is from 0 through 100.

To specify the amount of time, in seconds, that a router should wait between enrollment attempts, include the **retry-interval seconds** statement at the **[edit security pki ca-profile ca-profile-name enrollment]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name enrollment]
  retry-interval seconds;
```

The range for **seconds** is from 0 through 3600.

Configuring the Certificate Revocation List

Tasks to configure the certificate revocation list are:

1. [Specifying an LDAP URL on page 54](#)
2. [Configuring the Interval Between CRL Updates on page 55](#)
3. [Overriding Certificate Verification if CRL Download Fails on page 55](#)

Specifying an LDAP URL

You can specify the URL for the Lightweight Directory Access Protocol (LDAP) server where your CA stores its current CRL. If the CA includes the Certificate Distribution Point (CDP) in the digital certificate, you do not need to specify a URL for the LDAP server. The CDP is a field within the certificate that contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically.

Configure an LDAP URL if you want to use a different CDP from the one specified in the certificate. Any LDAP URL you configure takes precedence over the CDP included in the certificate.

You can configure up to three URLs for each CA profile.

If the LDAP server requires a password to access the CRL, you need to include the **password** statement.

To configure the router to retrieve the CRL from the LDAP server, include the **url** statement and specify the URL name at the **[edit security pki ca-profile ca-profile-name revocation-check crl]** hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
url {
  url-name;
}
```

url-name is the certificate authority LDAP server name. The format is `ldap://server-name`, where **server-name** is the CA host DNS name or IP address.

To specify to use a password to access the CRL, include the **password** statement at the `[edit security pki ca-profile ca-profile-name revocation-check crl url]` hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl url]
password password;
```

password is the secret password that the LDAP server requires for access.

Configuring the Interval Between CRL Updates

By default, the time interval between CRL updates is 24 hours. To configure the amount of time between CRL updates, include the **refresh-interval** statement at the `[edit security pki ca-profile ca-profile-name revocation-check crl]` hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
refresh-interval number-of-hours;
```

The range for number of hours is from 0 through 8784.

Overriding Certificate Verification if CRL Download Fails

By default, if the router either cannot access the LDAP URL or retrieve a valid certificate revocation list, certificate verification fails and the IPsec tunnel is not established. To override this behavior and permit the authentication of the IPsec peer when the CRL is not downloaded, include the **disable on-download-failure** statement at the `[edit security pki ca-profile ca-profile-name revocation-check crl]` hierarchy level:

```
[edit security pki ca-profile ca-profile-name revocation-check crl]
disable on-download-failure;
```

Managing Digital Certificates

After you configure the CA profile, you can request a CA certificate from the trusted CA. Next, you must generate a public/private key pair. When the key pair is available, you can generate a local certificate either online or manually.

Tasks to manage digital certificates are:

1. [Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers on page 56](#)
2. [Generating a Public/Private Key Pair on page 56](#)
3. [Generating and Enrolling a Local Digital Certificate on page 56](#)

Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers

For J Series Services Routers and AS and Multiservices PICs installed on M Series and T Series routers, issue the following command to obtain a digital certificate from a CA. Specify a configured **ca-profile-name** to request a CA certificate from the trusted CA.

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

For information about how to configure a CA profile, see [“Configuring the Certificate Authority Properties” on page 53](#).

In this example, the certificate is enrolled online and installed into the router automatically.

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

Received following certificates:

Certificate: C=us, O=juniper

Fingerprint:00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10

Certificate: C=us, O=juniper, CN=First Officer

Fingerprint:bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17

Certificate: C=us, O=juniper, CN=First Officer

Fingerprint:46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f

Do you want to load the above CA certificate ? [yes,no] (no) yes



NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or Web site download), you can install it with the **request security pki ca-certificate load** command. For more information, see the [CLI Explorer](#).

Generating a Public/Private Key Pair

After obtaining a certificate for an AS PIC or Multiservices PIC, you must generate a public-private key before you can generate a local certificate. The public key is included in the local digital certificate and the private key is used to decrypt data received from peers. To generate a public-private key pair, issue the **request security pki generate-key-pair certificate-id certificate-id-name** command.

The following example shows how to generate a public-private key for an AS PIC or Multiservices PIC:

```
user@host>request security pki generate-key-pair certificate-id local-entrust2
Generated key pair local-entrust2, key size 1024 bits
```

Generating and Enrolling a Local Digital Certificate

You can generate and enroll local digital certificates either online or manually. To generate and enroll a local certificate online by using the Simple Certificate Enrollment Protocol (SCEP) for an AS PIC or Multiservices PIC, issue the **request security pki local-certificate enroll** command. To generate a local certificate request manually in the PKCS-10 format, issue the **request security pki generate-certificate-request** command.

If you create the local certificate request manually, you must also load the certificate manually. To manually install a certificate in your router, issue the **request security pki local-certificate load** command.

The following example shows how to generate a local certificate request manually and send it to the CA for processing:

```
user@host> request security pki generate-certificate-request certificate-id local-entrust2
domain-name router2.example.net filename entrust-req2
subject cn=router2.example.net

Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHxLmp1bm1wZXIubmV0MIGfMAOGCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8E1wTJ1kmIt2cB3yi fB6zePd+6WYpf57Crwre7YqPkIXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDFVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AA0BgQ8c2rq1v5S0QXH7LCb/FdqAL8ZM6GoaNs5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bVL4P5nvEZLND
EIMUHwteo1ZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

The trusted CA digitally signs the local certificate and returns it to you. Copy the certificate file into the router and load the certificate:

```
user@host> request security pki local-certificate load filename /tmp/router2-cert
certificate-id local-entrust2
Local certificate local-entrust2 loaded successfully
```



NOTE: The name of the file sent to you by the CA might not match the name of the certificate identifier. However, the **certificate-id** name must always match the name of the key pair you generated for the router.

After the local and CA certificates have been loaded, you can reference them in your IPsec configuration. Using default values in the AS and Multiservices PICs, you do not need to configure an IPsec proposal or an IPsec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the IKE proposal and locate the certificate in an IKE policy, and apply the CA profile to the service set.

Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA

Use the **auto-re-enrollment** statement to configure automatic reenrollment of a specified existing router certificate before its existing expiration date. This function automatically reenrolls the router certificate. The reenrollment process requests the certificate authority (CA) to issue a new router certificate with a new expiration date. The date of auto-reenrollment is determined by the following parameters:

- **re-enroll-trigger-time**—The percentage of the difference between the router certificate start date/time (when the certificate was generated) and the validity period; used to specify how long auto-reenrollment should be initiated before expiration.
- **validity-period**—The number of days after issuance when the router certificate will expire, as set when a certificate is generated.



NOTE: By default, this feature is not enabled unless configured explicitly. This means that a certificate that does not have auto-reenrollment configured will expire on its normal expiration date.

The **ca-profile** statement specifies which CA will be contacted to reenroll the expiring certificate. This is the CA that issued the original router certificate.

The **challenge-password** statement provides the issuing CA with the router certificate's password, as set by the administrator and normally obtained from the SCEP enrollment Web page of the CA. The password is 16 characters in length.

Optionally, the router certificate key pair can be regenerated by using the **re-generate-keypair** statement.

To configure automatic reenrollment properties, include the following statements at the **[edit security pki]** hierarchy level:

```
[edit security pki]
auto-re-enrollment {
  certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
  }
}
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

days is the number of days for the validity period. The range can be from 1 through 4095.

Tasks to configure automatic reenrollment of certificates are:

1. [Specify the Certificate ID on page 59](#)
2. [Specify the CA Profile on page 59](#)
3. [Specify the Challenge Password on page 59](#)
4. [Specify the Reenroll Trigger Time on page 59](#)
5. [Specify the Regenerate Key Pair on page 59](#)
6. [Specify the Validity Period on page 60](#)

Specify the Certificate ID

Use the **certificate-id** statement to specify the name of the router certificate to configure for auto-reenrollment. To specify the certificate ID, include the statement at the **[edit security pki auto-re-enrollment]** hierarchy level:

```
[edit security pki auto-re-enrollment]
certificate-id certificate-name;
```

Specify the CA Profile

Use the **ca-profile** statement to specify the name of the CA profile from the router certificate previously specified by certificate ID. To specify the CA profile, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
ca-profile ca-profile-name;
```



NOTE: The referenced **ca-profile** must have an enrollment URL configured at the **[edit security pki ca-profile *ca-profile-name* enrollment url]** hierarchy level.

Specify the Challenge Password

The challenge password is used by the CA specified by the PKI certificate ID for reenrollment and revocation. To specify the challenge password, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
challenge-password password;
```

Specify the Reenroll Trigger Time

Use the **re-enroll-trigger-time** statement to set the percentage of the validity period before expiration at which reenrollment occurs. To specify the reenroll trigger time, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
re-enroll-trigger-time percentage;
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

Specify the Regenerate Key Pair

When a regenerate key pair is configured, a new key pair is generated during reenrollment. On successful reenrollment, a new key pair and new certificate replace the old certificate and key pair. To generate a new key pair, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-generate-keypair;
```

Specify the Validity Period

The **validity-period** statement specifies the router certificate validity period, in number of days, that the specified router certificate remains valid. To specify the validity period, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
validity-period days;
```

days is the number of days for the validity period. The range can be from 1 through 4095.

- Related Documentation**
- [Digital Certificates Overview on page 9](#)
 - [Configuring Digital Certificates for an ES PIC on page 45](#)

Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA

Use the **auto-re-enrollment** statement to configure automatic reenrollment of a specified existing router certificate before its existing expiration date. This function automatically reenrolls the router certificate. The reenrollment process requests the certificate authority (CA) to issue a new router certificate with a new expiration date. The date of auto-reenrollment is determined by the following parameters:

- **re-enroll-trigger-time**—The percentage of the difference between the router certificate start date/time (when the certificate was generated) and the validity period; used to specify how long auto-reenrollment should be initiated before expiration.
- **validity-period**—The number of days after issuance when the router certificate will expire, as set when a certificate is generated.



NOTE: By default, this feature is not enabled unless configured explicitly. This means that a certificate that does not have auto-reenrollment configured will expire on its normal expiration date.

The **ca-profile** statement specifies which CA will be contacted to reenroll the expiring certificate. This is the CA that issued the original router certificate.

The **challenge-password** statement provides the issuing CA with the router certificate's password, as set by the administrator and normally obtained from the SCEP enrollment Web page of the CA. The password is 16 characters in length.

Optionally, the router certificate key pair can be regenerated by using the **re-generate-keypair** statement.

To configure automatic reenrollment properties, include the following statements at the **[edit security pki]** hierarchy level:


```
[edit security pki]
auto-re-enrollment {
  certificate-id {
    ca-profile ca-profile-name;
    challenge-password password;
    re-enroll-trigger-time-percentage percentage;
    re-generate-keypair;
    validity-period days;
  }
}
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

days is the number of days for the validity period. The range can be from 1 through 4095.

Tasks to configure automatic reenrollment of certificates are:

1. [Specify the Certificate ID on page 61](#)
2. [Specify the CA Profile on page 61](#)
3. [Specify the Challenge Password on page 62](#)
4. [Specify the Reenroll Trigger Time on page 62](#)
5. [Specify the Regenerate Key Pair on page 62](#)
6. [Specify the Validity Period on page 62](#)

Specify the Certificate ID

Use the **certificate-id** statement to specify the name of the router certificate to configure for auto-reenrollment. To specify the certificate ID, include the statement at the **[edit security pki auto-re-enrollment]** hierarchy level:

```
[edit security pki auto-re-enrollment]
certificate-id certificate-name;
```

Specify the CA Profile

Use the **ca-profile** statement to specify the name of the CA profile from the router certificate previously specified by certificate ID. To specify the CA profile, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]
ca-profile ca-profile-name;
```



NOTE: The referenced *ca-profile* must have an enrollment URL configured at the **[edit security pki ca-profile *ca-profile-name* enrollment url]** hierarchy level.

Specify the Challenge Password

The challenge password is used by the CA specified by the PKI certificate ID for reenrollment and revocation. To specify the challenge password, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
challenge-password password;
```

Specify the Reenroll Trigger Time

Use the **re-enroll-trigger-time** statement to set the percentage of the validity period before expiration at which reenrollment occurs. To specify the reenroll trigger time, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-enroll-trigger-time percentage;
```

percentage is the percentage for the reenroll trigger time. The range can be from 1 through 99 percent.

Specify the Regenerate Key Pair

When a regenerate key pair is configured, a new key pair is generated during reenrollment. On successful reenrollment, a new key pair and new certificate replace the old certificate and key pair. To generate a new key pair, include the following statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
re-generate-keypair;
```

Specify the Validity Period

The **validity-period** statement specifies the router certificate validity period, in number of days, that the specified router certificate remains valid. To specify the validity period, include the statement at the **[edit security pki auto-re-enrollment certificate-id *certificate-name*]** hierarchy level:

```
[edit security pki auto-re-enrollment certificate-id certificate-name]  
validity-period days;
```

days is the number of days for the validity period. The range can be from 1 through 4095.

CHAPTER 6

Configuring Traffic Filters and Tracing Operations

- [Example: Configuring an Outbound Traffic Filter on page 63](#)
- [Example: Applying an Outbound Traffic Filter on page 64](#)
- [Example: Configuring an Inbound Traffic Filter for a Policy Check on page 64](#)
- [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check on page 66](#)
- [Configuring Tracing Operations for Security Services on page 67](#)
- [Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 68](#)

Example: Configuring an Outbound Traffic Filter

Firewall filters for outbound traffic direct the traffic through the desired IPsec tunnel and ensure that the tunneled traffic goes out the appropriate interface (see [Figure 1 on page 5](#)). Here, an outbound firewall filter is created on security Gateway A; it identifies the traffic to be encrypted and adds it to the input side of the interface that carries the internal VPN traffic:

```
[edit firewall]
filter ipsec-encrypt-policy-filter {
  term term1 {
    from {
      source-address { # local network
        10.1.1.0/24;
      }
      destination-address { # remote network
        10.2.2.0/24;
      }
    }
  }
  then ipsec-sa manual-sa1; # apply SA name to packet
  term default {
    then accept;
  }
}
```



NOTE: The source address, port, and protocol on the outbound traffic filter must match the destination address, port, and protocol on the inbound traffic filter. The destination address, port, and protocol on the outbound traffic filter must match the source address, port, and protocol on the inbound traffic filter.

- Related Documentation**
- [Example: Applying an Outbound Traffic Filter on page 64](#)
 - [IPsec Tunnel Traffic Configuration Overview on page 4](#)

Example: Applying an Outbound Traffic Filter

After you have configured the outbound firewall filter, you apply it:

```
[edit interfaces]
fe-0/0/1 {
  unit 0 {
    family inet {
      filter {
        input ipsec-encrypt-policy-filter;
      }
      address 10.1.1.254/24;
    }
  }
}
```

The outbound filter is applied on the Fast Ethernet interface at the **[edit interfaces fe-0/0/1 unit 0 family inet]** hierarchy level. Any packet matching the IPsec action term (**term 1**) on the input filter (**ipsec-encrypt-policy-filter**), configured on the Fast Ethernet interface, is directed to the ES PIC interface at the **[edit interfaces es-0/1/0 unit 0 family inet]** hierarchy level. If a packet arrives from the source address 10.1.1.0/24 and goes to the destination address 10.2.2.0/24, the Packet Forwarding Engine directs the packet to the ES PIC interface, which is configured with the **manual-sa1** SA. The ES PIC receives the packet, applies the **manual-sa1** SA, and sends the packet through the tunnel.

The router must have a route to the tunnel endpoint; add a static route if necessary.

- Related Documentation**
- [IPsec Tunnel Traffic Configuration Overview on page 4](#)

Example: Configuring an Inbound Traffic Filter for a Policy Check

- [Requirements on page 65](#)
- [Overview on page 65](#)
- [Configuration on page 65](#)

Requirements

No special configuration beyond device initialization is required before configuring this example.

Overview

Here, an inbound firewall filter, which performs the final IPsec policy check, is created on security Gateway A. This check ensures that only packets that match the traffic configured for this tunnel are accepted. This filter is configured via the CLI interface at the **[edit firewall family inet]** hierarchy level.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For information about navigating the CLI, see *Using the CLI Editor in Configuration Mode*.

To configure this example, perform the following tasks:

- [Configuring the firewall filter on page 65](#)

CLI Quick Configuration

To quickly configure this example, copy the following configuration commands into a text file, remove any line breaks, and then paste the commands into the CLI at the **[edit]** hierarchy level.

```
[edit]
set firewall family inet filter ipsec-decrypt-policy-filter term term1 from source-address 10.2.2.0/24
set firewall family inet filter ipsec-decrypt-policy-filter term term1 from destination-address 10.1.1.0/24
set firewall family inet filter ipsec-decrypt-policy-filter term term1 then accept
commit
```

Configuring the firewall filter

Step-by-Step Procedure

To configure the firewall filter, **ipsec-decrypt-policy-filter** that catches traffic from the remote 10.2.2.0/24 network that is destined for the local 10.1.1.0/24 network:

1. Create the firewall filter:


```
[edit]
user@host# edit firewall family inet filter ipsec-decrypt-policy-filter
```
2. Configure matching for source and destination addresses:


```
[edit firewall family inet filter ipsec-decrypt-policy-filter]
user@host# set term term1 from source-address 10.2.2.0/24
user@host# set term term1 from destination-address 10.1.1.0/24
```
3. Configure the filter to accept the matched traffic:


```
[edit firewall family inet filter ipsec-decrypt-policy-filter]
user@host# set term term1 then accept
```



NOTE: The accept statement within the term *term1* is for this filter only. Traffic that does not match this filter term will be dropped by the default firewall action.

4. Confirm your candidate firewall configuration by issuing the **show** configuration command at the **[edit firewall family inet]** hierarchy level

```
[edit firewall family inet]
user@host# show
filter ipsec-decrypt-policy-filter {
  term term1 { # perform policy check
    from {
      source-address { # remote network
        10.2.2.0/24;
      }
      destination-address { # local network
        10.1.1.0/24;
      }
    }
    then accept;
  }
}
```

If the command output does not display the intended configuration, repeat the instructions in this example to correct the configuration.

5. If you are done configuring the device, commit your candidate configuration.

```
[edit]
user@host# commit
```

To implement this filter, you apply it as an input filter to the **es-0/1/0** logical interface of Gateway A. See [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check](#) for details.

Related Documentation

- [IPsec Tunnel Traffic Configuration Overview on page 4](#)
- [Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check on page 66](#)

Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check

After you create the inbound firewall filter, apply it to the ES PIC. Here, the inbound firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and decrypts the incoming packet.

```
[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5; # tunnel source address
```

```

        destination 10.6.6.6; # tunnel destination address
    }
    family inet {
        filter {
            input ipsec-decrypt-policy-filter;
        }
        ipsec-sa manual-sa1; # SA name applied to packet
        address 10.1.1.8/32 { # local interface address inside local VPN
            destination 10.2.2.254; # destination address inside remote VPN
        }
    }
}

```

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's SPI, protocol, and destination address to look up the SA configured on one of the ES interfaces. The IPsec **manual-sa1** SA is referenced at the **[edit interfaces es-1/2/0 unit 0 family inet]** hierarchy level and is used to decrypt the incoming packet. When the packets are processed (decrypted, authenticated, or both), the input firewall filter (**ipsec-decrypt-policy-filter**) is applied on the decrypted packet to perform the final policy check. Term1 defines the decrypted (and verified) traffic and performs the required policy check.



NOTE: The inbound traffic filter is applied after the ES PIC has processed the packet, so the decrypted traffic is defined as any traffic that the remote gateway is encrypting and sending to this router. IKE uses this filter to determine the policy required for a tunnel. This policy is used during the negotiation with the remote gateway to find the matching SA configuration.

Related Documentation

- [IPsec Tunnel Traffic Configuration Overview on page 4](#)

Configuring Tracing Operations for Security Services

To configure trace options for security services, specify flags using the **traceoptions** statement:

```

[edit security]
traceoptions {
    file filename <files number> <size size>;
    flag all;
    flag database;
    flag general;
    flag ike;
    flag parse;
    flag policy-manager;
    flag routing-socket;
    flag timer;
}

```

You can include these statements at the following hierarchy levels:

- **[edit security]**

- **[edit services ipsec-vpn]**

You can specify one or more of the following security tracing flags:

- **all**—Trace all security events
- **database**—Trace database events
- **general**—Trace general events
- **ike**—Trace IKE module processing
- **parse**—Trace configuration processing
- **policy-manager**—Trace policy manager processing
- **routing-socket**—Trace routing socket messages
- **timer**—Trace internal timer events

**Related
Documentation**

- [Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 68](#)
- [IPsec Security Associations on page 7](#)

Configuring Tracing Operations for IPsec Events for Adaptive Services PICs

To configure trace options to trace IPsec events for Adaptive Services PICs, include the following statements at the **[edit services ipsec-vpn]** hierarchy level:

```
[edit services ipsec-vpn]
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}
```

Trace option output is recorded in the `/var/log/kmd` file.

You can specify one or more of the following security tracing flags:

- **all**—Trace all security events
- **database**—Trace database events
- **general**—Trace general events
- **ike**—Trace IKE module processing
- **parse**—Trace configuration processing
- **policy-manager**—Trace policy manager processing

- **routing-socket**—Trace routing socket messages
- **timer**—Trace internal timer events

**Related
Documentation**

- [Configuring Tracing Operations for Security Services on page 67](#)

CHAPTER 7

Configuring Authentication Key Updates

- [Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols on page 71](#)

Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols

You can configure an authentication key update mechanism for the Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) routing protocols. This mechanism allows you to update authentication keys without interrupting associated routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

To configure this feature, include the **authentication-key-chains** statement at the **[edit security]** level, and include the **authentication-key-chain** statement for the BGP or LDP routing protocols at the **[edit protocols]** level.

The following topics provide more details about configuring authentication key updates for BGP and LDP Routing Protocols:

1. [Configuring Authentication Key Updates on page 71](#)
2. [Configuring BGP and LDP for Authentication Key Updates on page 72](#)

Configuring Authentication Key Updates

To configure the authentication key update mechanism, include the **key-chain** statement at the **[edit security authentication-key-chains]** hierarchy level, and specify the **key** option to create a keychain consisting of several authentication keys.

```
[edit security authentication-key-chains]
key-chain key-chain-name {
  key key {
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
}
```

key-chain—Assigns a name to the keychain mechanism. This name is also configured at the **[edit protocols bgp]** or the **[edit protocols ldp]** hierarchy levels to associate unique **authentication key-chain** attributes as specified using the following options:

- **key**—Each key within a keychain is identified by a unique integer value. The range is from 0 through 63.
- **secret**—Each key must specify a secret in encrypted text or plain text format. Even if you enter the secret data in plain-text format, the secret always appears in encrypted format.
- **start-time**—Start times for authentication key updates are specified in UTC (Coordinated Universal Time), and must be unique within the keychain.

Configuring BGP and LDP for Authentication Key Updates

To configure the authentication key update mechanism for the BGP and LDP routing protocols, include the **authentication-key-chain** statement at the **[edit protocols (bgp | ldp)]** hierarchy level to associate each routing protocol with the **[edit security authentication-key-chains]** authentication keys.

```
[edit protocols (bgp | ldp)]
group group-name {
  neighbor address {
    authentication-key-chain key-chain-name;
  }
}
```



NOTE: When configuring the authentication key update mechanism for BGP, you cannot commit the 0.0.0.0/allow statement with authentication keys or key chains. The CLI issues a warning and fails to commit such configurations.

For information about the BGP protocol, see the *Junos OS Routing Protocols Library for Routing Devices*.

Related Documentation

- *Example: Configuring the BGP and IS-IS Routing Protocols*

CHAPTER 8

Configuring Keys for SSH and SSL

- [Configuring SSH Host Keys for Secure Copying of Data on page 73](#)
- [Importing SSL Certificates for Junos XML Protocol Support on page 75](#)
- [global \(DDoS\) on page 77](#)
- [logical-interface \(DDoS Flow Detection\) on page 78](#)
- [no-flow-logging \(DDoS Flow Detection\) on page 79](#)
- [physical-interface \(DDoS Flow Detection\) on page 80](#)
- [priority \(DDoS\) on page 81](#)
- [protocols \(DDoS\) on page 82](#)
- [recover-time \(DDoS\) on page 91](#)
- [subscriber \(DDoS Flow Detection\) on page 92](#)
- [timeout-active-flows \(DDoS Flow Detection\) on page 93](#)
- [traceoptions \(DDoS\) on page 94](#)
- [violation-report-rate \(DDoS Flow Detection\) on page 96](#)

Configuring SSH Host Keys for Secure Copying of Data

Secure Shell (SSH) uses encryption algorithms to generate a host, server, and session key system that ensures secure data transfer. You can configure SSH host keys to support secure copy (SCP) as an alternative to FTP for the background transfer of data such as configuration archives and event logs. To configure SSH support for SCP, you must complete the following tasks:

- Specify SSH known hosts by including hostnames and host key information in the Routing Engine configuration hierarchy.
- Set an SCP URL to specify the host from which to receive data. Setting this attribute automatically retrieves SSH host key information from the SCP server.
- Verify that the host key is authentic.
- Accept the secure connection. Accepting this connection automatically stores host key information in the local host key database. Storing host key information in the

configuration hierarchy automates the secure handshake and allows background data transfer using SCP.

Tasks to configure SSH host keys for secure copying of data are:

1. [Configuring SSH Known Hosts on page 74](#)
2. [Configuring Support for SCP File Transfer on page 74](#)
3. [Updating SSH Host Key Information on page 75](#)

Configuring SSH Known Hosts

To configure SSH known hosts, include the **host** statement, and specify hostname and host key options for trusted servers at the **[edit security ssh-known-hosts]** hierarchy level:

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
    dsa-key key;
}
host archive-server-url {
    rsa-key key;
}
host server-with-ssh-version-1, ip-address {
    rsa1-key key;
}
```

Host keys are one of the following:

- **dsa-key**—Base64 encoded Digital Signature Algorithm (DSA) key.
- **rsa-key**—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures.
- **rsa1-key**—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1 and SSH version 2.

Configuring Support for SCP File Transfer

To configure a known host to support background SCP file transfers, include the **archive-sites** statement at the **[edit system archival configuration]** hierarchy level.

```
[edit system archival configuration]
archive-sites {
    scp://username<:password>@host<:port>/url-path;
}
```



NOTE: When specifying a URL in a Junos OS statement using an IPv6 host address, you must enclose the entire URL in quotation marks (" ") and enclose the IPv6 host address in brackets ([]). For example, "scp://username<:password>@[host]<:port>/url-path";

Setting the **archive-sites** statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key,

displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

```
user@host# set system archival configuration archive-sites "<scp-url-path>"
The authenticity of host <my-archive-server (<server-ip-address>)> can't be established.
RSA key fingerprint is <ascii-text key>. Are you sure you want to continue connecting
(yes/no)?
```

To verify that the host key is authentic, compare this fingerprint with a fingerprint that you obtain from the same host using a trusted source. If the fingerprints are identical, accept the host key by entering **yes** at the prompt. The host key information is then stored in the Routing Engine configuration and supports background data transfers using SCP.

Updating SSH Host Key Information

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the **archival configuration archive-sites** statement at the **[edit system]** hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

1. [Retrieving Host Key Information Manually on page 75](#)
2. [Importing Host Key Information from a File on page 75](#)

Retrieving Host Key Information Manually

To manually retrieve SSH public host key information, use the **fetch-from-server** option with the **set security ssh-known-hosts** command. You must include a hostname attribute with the **set security ssh-known-hosts fetch-from-server** command to specify the host from which to retrieve the SSH public key.

```
user@host# set security ssh-known-hosts fetch-from-server <hostname>
```

Importing Host Key Information from a File

To manually import SSH host key information from the known-hosts file located at **/var/tmp/known-hosts** on the server, include the **load-key-file** option with the **set security ssh-known-hosts** command. You must include the path to the **known-hosts** file with the **set security ssh-known-hosts load-key-file** command to specify the location from which to import host key information.

```
user@host# set security ssh-known-hosts load-key-file /var/tmp/known-hosts
```

Importing SSL Certificates for Junos XML Protocol Support



NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router or switch: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For

clients to use the SSL protocol, you must copy an X.509 authentication certificate onto the router or switch, as described in this topic. You must also include the **xnm-ssl** statement at the **[edit system services]** hierarchy level.



NOTE: The **xnm-ssl** statement does not apply to standard IPsec services.

After obtaining an X.509 authentication certificate and private key, copy it to the router or switch by including the **local** statement at the **[edit security certificates]** hierarchy level:

```
[edit security certificates]
local certificate-name {
  load-key-file (filename | url);
}
```

certificate-name is a name you choose to identify the certificate uniquely (for example, **Junos XML protocol-ssl-client-hostname**, where **hostname** is the computer where the client application runs).

filename is the pathname of the file on the local disk that contains the paired certificate and private key (assuming you have already used another method to copy them to the router's or switch's local disk).

url is the URL to the file that contains a paired certificate and private key (for instance, on the computer where the Junos XML protocol client application runs).




NOTE: The CLI expects the private key in the **URL-or-path** file to be unencrypted. If the key is encrypted, the CLI prompts you for the passphrase associated with it, decrypts it, and stores the unencrypted version.

The **load-key-file** statement acts as a directive that copies the contents of the certificate file into the configuration. When you view the configuration, the CLI displays the string of characters that constitute the private key and certificate, marking them as **SECRET-DATA**. The **load-key-file** keyword is not recorded in the configuration.

**Related
Documentation**

- [Configuring SSH Host Keys for Secure Copying of Data on page 73](#)
- [Configuring clear-text or SSL Service for Junos XML Protocol Client Applications](#)

global (DDoS)

Syntax	<pre>global { disable-fpc; disable-logging; disable-routing-engine; flow-detection; flow-report-rate; violation-report-rate; }</pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Modify DDoS policers, event logging, and flow detection globally for all protocols.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The following statements are not supported on QFX5200 and QFX10000 switches: <code>disable-routing-engine</code>, <code>flow-detection</code>, <code>flow-report-rate</code>, and <code>violation-report-rate</code>.</p> </div> </div>	
<p>The remaining statements are explained separately.</p>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Disabling DDoS Protection Policers and Logging Globally</i>

logical-interface (DDoS Flow Detection)

Syntax	<code>logical-interface (<i>flow-bandwidth</i> <i>flow-control-mode</i> <i>flow-detection-mode</i>)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode for flow detection at the logical interface flow aggregation level for the packet type.
Options	<p><i>flow-bandwidth</i>—Bandwidth for the flow at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 200 packets per second</p> <p>Range: 1 through 30,000 packets per second</p> <p><i>flow-control-mode</i>—Mode for how traffic in the detected flow is controlled at the logical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p> <ul style="list-style-type: none">• drop—Drop all traffic in flow.• keep—Keep all traffic in flow.• police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p><i>flow-detection-mode</i>—Mode for how flow detection operates at the logical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p> <ul style="list-style-type: none">• automatic—Search flows at the logical interface level only when a DDoS policer is being violated and only when the flow causing the policer violation is not discovered at the finer flow aggregation level, subscriber. When the suspicious flow is not found at this level, then the search moves to a coarser level of flow aggregation (physical interface). Flows at the logical interface level are subsequently not searched again until the policer is no longer violated at the coarser level, and a subsequent violation occurs that cannot be found at the subscriber level.• off—Disable flow detection at the logical interface level so that flows are never searched at this level.• on—Search flows at the logical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level*
- *Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level*
- *Configuring How Flow Detection Operates at Each Flow Aggregation Level*
- *Configuring Flow Detection for DDoS Protection*

no-flow-logging (DDoS Flow Detection)

Syntax no-flow-logging;

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type*]

Release Information Statement introduced in Junos OS Release 12.3.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Disable automatic logging of flow detection culprit flow events (flow reports) for the packet type.



NOTE: You can disable logging of suspicious flow events (violation reports) with the `disable-logging` statement at the [edit system ddos-protection global hierarchy level].

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Disabling Automatic Logging of Culprit Flow Events for a Packet Type*
- *Configuring Flow Detection for DDoS Protection*

physical-interface (DDoS Flow Detection)

Syntax	<code>physical-interface (<i>flow-bandwidth</i> <i>flow-control-mode</i> <i>flow-detection-mode</i>)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the physical interface flow aggregation level for the packet type.
Options	<p><i>flow-bandwidth</i>—Bandwidth for the flow at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 20,000 packets per second</p> <p>Range: 1 through 50,000 packets per second</p> <p><i>flow-control-mode</i>—Mode for how traffic in the detected flow is controlled at the physical interface level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p> <ul style="list-style-type: none">• drop—Drop all traffic in flow.• keep—Keep all traffic in flow.• police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p><i>flow-detection-mode</i>—Mode for how flow detection operates at the physical interface level when a policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p> <ul style="list-style-type: none">• automatic—Search flows at the physical interface level only when a DDoS policer is being violated and only when the policer violation is not discovered at the finer aggregation levels, logical interface or subscriber. Flows at the physical interface level are subsequently not searched again until a subsequent violation occurs that cannot be found at the subscriber or logical interface levels.• off—Disable flow detection at the physical interface level so that flows are never searched at this level.• on—Search flows at the physical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level</i> • <i>Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level</i> • <i>Configuring How Flow Detection Operates at Each Flow Aggregation Level</i> • <i>Configuring Flow Detection for DDoS Protection</i>

priority (DDoS)

Syntax	<code>priority level;</code>
Hierarchy Level	<ul style="list-style-type: none"> • For MX Series routers, T4000 routers, and EX9200 switches: [edit system ddos-protection protocols <i>protocol-group packet-type</i>] • For QFX10000 and QFX5200 switches: [edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth.
Options	<i>level</i> —Priority of the packet type, low, medium, or high.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring DDoS Protection Policers for Individual Packet Types</i> • <i>Configuring DDoS Protection Policers on QFX Series Switches</i>

protocols (DDoS)

Syntax `protocols protocol-group (aggregate | packet-type) {`
 `bandwidth packets-per-second;`
 `burst size;`
 `bypass-aggregate;`
 `disable-fpc;`
 `disable-logging;`
 `disable-routing-engine;`
 `flow-detection-mode (automatic | off | on);`
 `flow-detect-time seconds;`
 `flow-level-bandwidth {`
 `logical-interface flow-bandwidth;`
 `physical-interface flow-bandwidth;`
 `subscriber flow-bandwidth;`
 `}`
 `flow-level-control {`
 `logical-interface flow-control-mode;`
 `physical-interface flow-control-mode;`
 `subscriber flow-control-mode;`
 `}`
 `flow-level-detection {`
 `logical-interface flow-operation-mode;`
 `physical-interface flow-operation-mode;`
 `subscriber flow-operation-mode;`
 `}`
 `flow-recover-time seconds;`
 `flow-timeout-time seconds;`
 `fpc slot-number {`
 `bandwidth-scale percentage;`
 `burst-scale percentage;`
 `disable-fpc;`
 `}`
 `no-flow-logging`
 `priority level;`
 `recover-time seconds;`
 `timeout-active-flows;`
}

Hierarchy Level [edit system ddos-protection]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure DDoS policers for all packet types within a protocol group or for a particular packet type within a protocol group.

Options **aggregate**—Configure the policer to monitor all control packets within the protocol group. You can configure an aggregate policer for any protocol group.

packet-type—(Optional) Name of the control packet type to be policed. You can configure a specific policer for only the following packet types and protocol groups:

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:
 - **ack**—DHCPACK packets.
 - **bad-packets**—DHCPv4 packets with bad formats.
 - **bootp**—DHCPBOOTP packets.
 - **decline**—DHCPDECLINE packets.
 - **discover**—DHCPDISCOVER packets.
 - **force-renew**—DHCPFORCERENEW packets.
 - **inform**—DHCPINFORM packets.
 - **lease-active**—DHCPLEASEACTIVE packets.
 - **lease-query**—DHCPLEASEQUERY packets.
 - **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
 - **lease-unknown**—DHCPLEASEUNKNOWN packets.
 - **nak**—DHCPNAK packets.
 - **no-message-type**—DHCP packets that are missing the message type.
 - **offer**—DHCPOFFER packets.
 - **release**—DHCPRELEASE packets.
 - **renew**—DHCPRENEW packets.
 - **request**—DHCPREQUEST packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
 - **advertise**—ADVERTISE packets.
 - **confirm**—CONFIRM packets.
 - **decline**—DECLINE packets.
 - **information-request**—INFORMATION-REQUEST packets.
 - **leasequery**—LEASEQUERY packets.
 - **leasequery-data**—LEASEQUERY-DATA packets.
 - **leasequery-done**—LEASEQUERY-DONE packets.
 - **leasequery-reply**—LEASEQUERY-REPLY packets.
 - **rebind**—REBIND packets.
 - **reconfigure**—RECONFIGURE packets.
 - **relay-forward**—RELAY-FORWARD packets.

- **relay-reply**—RELAY-REPLY packets.
- **release**—RELEASE packets.
- **renew**—RENEW packets.
- **reply**—REPLY packets.
- **request**—REQUEST packets.
- **solicit**—SOLICIT packets.
- **unclassified**—All unclassified packets in the protocol group.
- **filter-action**—The following packet types are available for unclassified firewall filter action packets, sent to the host because of reject terms in firewall filters:
 - **filter-v4**—Unclassified IPv4 filter action packets.
 - **filter-v6**—Unclassified IPv6 filter action packets.
 - **other**—All other unclassified filter action packets that are not IPv4 or IPv6.
- **frame-relay**—The following packet types are available for Frame Relay traffic:
 - **frf15**—Multilink frame relay FRF.15 packets.
 - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
 - **first-fragment**—First IP fragment.
 - **trail-fragment**—Last IP fragment.
- **ip-options**—The following packet types are available for IP option traffic:
 - **non-v4v6**—Options packets other than IPv4/v6.
 - **router-alert**—Router alert options packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **l2tp**—The following packet types are available for L2TP traffic:
 - **cdn**—Call-Disconnect-Notify message packets.
 - **hello**—Hello message packets.
 - **iccn**—Incoming-Call-Connected message packets.
 - **icrq**—Incoming-Call-Request message packets.
 - **scccn**—Start-Control-Connection-Connected message packets.
 - **sccrq**—Start-Control-Connection-Request message packets.
 - **stopccn**—Stop-Control-Connection-Notification message packets.
 - **unclassified**—All unclassified packets in the protocol group.

- **mcast-snoop**—Control traffic for multicast snooping.
 - **igmp**—Snooped IGMP traffic.
 - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
 - **add**—Add requests; internal MAC address learning request packets sent to the host.
 - **delete**—Delete requests; internal MAC address learning request packets sent to the host.
 - **lookup**—Lookup requests; internal MAC address learning request packets sent to the host.
 - **unclassified**—All unclassified packets in the protocol group.
- **ppp**—The following PPP packet types are available:
 - **authentication**—PPP authentication protocol packets.
 - **echo-rep**
 - **echo-req**—LCP echo request packets.
 - **ipcp**—IP Control Protocol packets.
 - **ipv6cp**—IPv6 Control Protocol packets.
 - **isis**—IS-IS packets.
 - **lcp**—Link Control Protocol packets.
 - **mlppp-lcp**—MLPPP LCP packets.
 - **mplscp**—MPLS Control Protocol packets.
 - **unclassified**—All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
 - **padi**—PADI packets.
 - **padm**—PADM packets.
 - **padn**—PADN packets.
 - **pado**—PADO packets.
 - **padr**—PADR packets.
 - **pads**—PADS packets.
 - **padt**—PADT packets.

- **radius**—The following RADIUS packet types are available:
 - **accounting**—RADIUS accounting packets.
 - **authorization**—RADIUS authorization packets.
 - **server**—RADIUS server traffic.
 - **unclassified**—All unclassified packets in the protocol group.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect:
 - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
 - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
 - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
 - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
 - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
 - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
 - **host**—Host packets.
 - **pfe**—Packet Forwarding Engine packets.
 - **syslog**—System log message packets.
 - **tap**—TAP packets.
- **tcp-flags**—The following TCP-flagged packet types are available:
 - **established**—TCP ACK and RST connection packets.
 - **initial**—TCP SYN and NAK packets.

- **unclassified**—The following unclassified packet types are available:
 - **control-layer2**—Unclassified layer 2 control packets.
 - **control-v4**—Unclassified IPv4 control packets.
 - **control-v6**—Unclassified IPv6 control packets.
 - **fw-host**—Unclassified send-to-host firewall packets.
 - **host-route-v4**—Unclassified IPv4 routing protocol and host packets in traffic sent to the router local interface address for broadcast and multicast.
 - **host-route-v6**—Unclassified IPv6 routing protocol and host packets in traffic sent to the router local interface address for broadcast and multicast.
 - **other**—All unclassified packets that do not belong to another type.
- **virtual-chassis**—The following packet types are available for virtual chassis packets:
 - **control-low**—Low-priority control packets.
 - **control-high**—High-priority control packets.
 - **unclassified**—All unclassified packets in the protocol group.
 - **vc-packets**—All exception packets on the virtual chassis link.
 - **vc-ttl-errors**—Virtual chassis TTL error packets.

protocol-group—Name of the protocol group for which traffic is policed. You can configure a policer for any of the following protocol groups:

- **amtv4**—IPv4 AMT traffic.
- **amtv6**—IPv6 AMT traffic.
- **ancp**—ANCP traffic.
- **ancpv6**—ANCPv6 traffic.
- **arp**—ARP traffic.
- **atm**—ATM traffic.
- **bfd**—BFD traffic.
- **bfdv6**—BFDv6 traffic.
- **bgp**—BGP traffic.
- **bgpv6**—BGPv6 traffic.
- **control**—Control traffic.
- **demux-autosense**—Demux autosensing traffic.
- **dhcpv4**—DHCPv4 traffic.
- **dhcpv6**—DHCPv6 traffic.
- **diameter**—Diameter and Gx-Plus traffic.
- **dns**—DNS traffic.
- **dtcp**—DTCP traffic.
- **dynamic-vlan**—Dynamic VLAN exception traffic.
- **egpv6**—EGPv6 traffic.
- **eoam**—EOAM traffic.
- **esmc**—ESMC traffic.
- **fab-probe**—Fab out probe packets.
- **filter-action**—IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters
- **frame-relay**—Frame relay traffic.
- **ftp**—FTP traffic.
- **ftpv6**—FTPv6 traffic.
- **gre**—GRE traffic.
- **icmp**—ICMP traffic.
- **igmp**—IGMP traffic
- **igmpv4v6**—IGMP v4/v6 traffic.
- **igmpv6**—IGMPv6 traffic.

- **inline-ka**—Inline service interfaces keepalive traffic.
- **inline-svcs**—Inline services traffic.
- **ip-fragments**—IP fragments traffic.
- **ip-options**—IP traffic with IP packet header options.
- **isis**—IS-IS traffic.
- **jfm**—JFM traffic.
- **l2pt**—Layer 2 protocol tunneling traffic.
- **lACP**—LACP traffic.
- **ldp**—LDP traffic.
- **ldpv6**—LDPv6 traffic.
- **lldp**—LLDP traffic.
- **lmp**—LMP traffic.
- **lmpv6**—LMPv6 traffic.
- **mac-host**—Layer 2 MAC send-to-host traffic.
- **mcast-snoop**—Control traffic for multicast snooping.
- **mlp**—MLP traffic.
- **msdp**—MSDP traffic.
- **msdpv6**—MSDPv6 traffic.
- **multicast-copy**—Host copy traffic due to multicast routing.
- **mvrp**—MVRP traffic.
- **ndpv6**—NDPv6 traffic.
- **ntp**—NTP traffic.
- **oam-lfm**—OAM-LFM traffic.
- **ospf**—OSPF traffic.
- **ospfv3v6**—OSPFv3/IPv6 traffic.
- **pfe-alive**—Packet Forwarding Engine keepalive traffic.
- **pim**—PIM traffic.
- **pimv6**—PIMv6 traffic.
- **pmvrp**—PMVRP traffic.
- **pos**—POS traffic.
- **ppp**—PPP traffic.
- **pppoe**—PPPoE traffic.
- **ptp**—PTP traffic.

- **pvstp**—PVSTP traffic.
- **radius**—RADIUS traffic.
- **re-services**—Captive portal content delivery traffic for Routing Engine HTTP redirect.
- **redirect**—Traffic that triggers ICMP redirects.
- **reject**—Packets rejected by a next-hop forwarding decision.
- **rejectv6**—V6 packets rejected by a next-hop forwarding decision.
- **resolve**—Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action.
- **rip**—RIP traffic.
- **ripv6**—RIPv6 traffic.
- **rsvp**—RSVP traffic.
- **rsvpv6**—RSVPv6 traffic.
- **services**—Service traffic.
- **snmp**—SNMP traffic.
- **snmpv6**—SNMPv6 traffic.
- **ssh**—SSH traffic.
- **sshv6**—SSHv6 traffic.
- **stp**—STP traffic.
- **syslog**—System log messages UDP traffic on port 6333 for the Routing Engine syslog server.
- **tacacs**—TACACS traffic.
- **tcp-flags**—Traffic with TCP flags.
- **telnet**—TELNET traffic.
- **telnetv6**—TELNETv6 traffic.
- **ttl**—TTL traffic.
- **tunnel-fragment**—Tunnel fragments traffic.
- **tunnel-ka**—Tunnel keepalive traffic.
- **unclassified**—Unclassified traffic.
- **virtual-chassis**—Virtual chassis traffic.
- **vrrp**—VRRP traffic.
- **vrrpv6**—VRRPv6 traffic.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • *Configuring DDoS Protection Policers for Individual Packet Types*

recover-time (DDoS)

Syntax recover-time *seconds*;

Hierarchy Level [edit system ddos-protection [protocols](#) *protocol-group* (aggregate | *packet-type*)]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass since the last detected DDoS violation before the traffic is considered to have recovered from the attack and returned to normal.

Options *seconds*—Period required for the traffic to recover.

Range: 1 through 3600 seconds

Default: 300

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation • *Configuring DDoS Protection Policers for Individual Packet Types*

subscriber (DDoS Flow Detection)

Syntax	<code>subscriber (<i>flow-bandwidth</i> <i>flow-control-mode</i> <i>flow-detection-mode</i>)</code>
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control], [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the subscriber flow aggregation level for the packet type.
Options	<p><i>flow-bandwidth</i>—Specify the bandwidth for the flow at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-bandwidth] hierarchy level.</p> <p>Default: 100 packets per second</p> <p>Range: 1 through 10,000 packets per second</p> <p><i>flow-control-mode</i>—Specify how traffic in the detected flow is controlled at the subscriber level. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-control] hierarchy level.</p> <ul style="list-style-type: none">• drop—Drop all traffic in flow.• keep—Keep all traffic in flow.• police—Police the traffic to within its allowed bandwidth. <p>Default: drop</p> <p><i>flow-detection-mode</i>—Specify how flow detection operates at the subscriber level when a DDoS protection policer has been violated. Available only at the [edit system ddos-protection protocols <i>protocol-group packet-type</i> flow-level-detection] hierarchy level.</p> <ul style="list-style-type: none">• automatic—Search flows at the subscriber level only when a DDoS policer is being violated and only until it is established that the flow causing the violation is not at this level. When the suspicious flow is not at this level, then the search moves to a coarser level of flow aggregation (logical interface). Flows at the subscriber level are subsequently not searched again until the policer is no longer violated at the coarser level.• off—Disable flow detection at the subscriber level so that flows are never searched at this level.• on—Search flows at the subscriber level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level</i> • <i>Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level</i> • <i>Configuring How Flow Detection Operates at Each Flow Aggregation Level</i> • <i>Configuring Flow Detection for DDoS Protection</i>

timeout-active-flows (DDoS Flow Detection)

Syntax	timeout-active-flows;
Hierarchy Level	[edit system ddos-protection protocols <i>protocol-group packet-type</i>]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Enable culprit flows for the packet type to time out according to the timeout period. The culprit flow is suppressed for the duration of the timeout period. When the period expires, the flow times out and is released from suppression.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Timeout Period for a Culprit Flow</i> • <i>Configuring Flow Detection for DDoS Protection</i>

traceoptions (DDoS)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system ddos-protection]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.</p> <p>Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.</p> <p>Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.</p>
Description	(MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Define tracing operations for DDoS protection processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <i>/var/log</i>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• all—Trace all operations.• config—Trace processing of the DDoS configuration at an extensive level.• events—Trace jddosd event processing; currently only exit events are traced.• gres—Trace messages exchanged with the kernel and jddosd process that could affect graceful Routing Engine switchover (GRES).• init—Trace jddosd initialization.• ipc—Trace interface interprocess communication (IPC) messages.• memory—Trace memory management code. This flag is not currently supported.• protocol—Trace DDoS protocol state processing. Only the violation state is currently traced.• rtsock—Trace messages exchanged with the kernel and jddosd process.

- **signal**—Trace system signals that are passed to jddosd, such as SIGTERM.
- **socket**—Trace socket messages that are passed to jddosd from the Packet Forwarding Engine.
- **state**—Trace state machine events. This flag is not currently supported.
- **timer**—Trace jddosd timer events.
- **ui**—Trace user interface processing. This flag is not currently supported.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10,240 through 1,073,741,824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	<p>trace—To view this statement in the configuration.</p> <p>trace-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Tracing DDoS Protection Operations</i>

violation-report-rate (DDoS Flow Detection)

Syntax	<code>violation-report-rate <i>report-rate</i>;</code>
Hierarchy Level	[edit system ddos-protection global]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Description	(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Limit the rate at which bandwidth violations (violation reports) are reported from an FPC to the Routing Engine, for all protocol groups and packet types on all line cards.
Options	<i>report-rate</i> —Number of violations per second. Range: 1 through 50,000 Default: 100
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types</i>• <i>Configuring Flow Detection for DDoS Protection</i>

CHAPTER 9

Configuration Statements

- [\[edit security\] Hierarchy Level](#) on page 99
- [algorithm \(Authentication Keychain\)](#) on page 102
- [algorithm \(Junos FIPS\)](#) on page 103
- [authentication \(Security IPsec\)](#) on page 104
- [authentication-algorithm \(Security IKE\)](#) on page 105
- [authentication-algorithm \(Security IPsec\)](#) on page 106
- [authentication-key-chains](#) on page 108
- [authentication-method](#) on page 109
- [auto-re-enrollment](#) on page 110
- [auxiliary-spi \(Security IPsec\)](#) on page 111
- [ca-identity](#) on page 111
- [ca-name](#) on page 112
- [ca-profile](#) on page 113
- [cache-size](#) on page 114
- [cache-timeout-negative](#) on page 115
- [certificate-id](#) on page 116
- [certificates](#) on page 117
- [certification-authority](#) on page 118
- [challenge-password](#) on page 119
- [crl \(Adaptive Services Interface\)](#) on page 120
- [crl \(Encryption Interface\)](#) on page 121
- [description \(Authentication Keychain\)](#) on page 121
- [description \(IKE policy\)](#) on page 122
- [dh-group](#) on page 122
- [direction \(Junos OS\)](#) on page 123
- [direction \(Junos-FIPS Software\)](#) on page 124
- [dynamic](#) on page 125
- [encoding](#) on page 126

- [encryption \(Junos OS\) on page 127](#)
- [encryption \(Junos-FIPS Software\) on page 128](#)
- [encryption-algorithm \(Security\) on page 129](#)
- [enrollment on page 130](#)
- [enrollment-retry on page 131](#)
- [enrollment-url on page 131](#)
- [file on page 132](#)
- [identity on page 132](#)
- [ike \(Security\) on page 133](#)
- [internal on page 134](#)
- [ipsec \(Security\) on page 135](#)
- [key \(Authentication Keychain\) on page 137](#)
- [key \(Junos FIPS\) on page 138](#)
- [key-chain \(Security\) on page 139](#)
- [ldap-url on page 140](#)
- [lifetime-seconds \(Security\) on page 140](#)
- [local on page 141](#)
- [local-certificate \(Security\) on page 142](#)
- [local-key-pair on page 142](#)
- [manual \(Junos OS\) on page 143](#)
- [manual \(Junos FIPS\) on page 144](#)
- [maximum-certificates on page 145](#)
- [mode \(IKE\) on page 146](#)
- [mode \(IPsec\) on page 147](#)
- [options \(Security\) on page 148](#)
- [path-length on page 149](#)
- [perfect-forward-secrecy \(Security\) on page 149](#)
- [pki on page 150](#)
- [policy \(Security IKE\) on page 151](#)
- [policy \(Security IPsec\) on page 152](#)
- [pre-shared-key \(Security\) on page 152](#)
- [proposal \(Security IKE\) on page 153](#)
- [proposal \(Security IPsec\) on page 153](#)
- [proposals on page 154](#)
- [protocol \(Junos OS\) on page 155](#)
- [protocol \(Junos-FIPS Software\) on page 156](#)
- [re-enroll-trigger-time-percentage on page 156](#)

- [re-generate-keypair](#) on page 157
- [refresh-interval](#) on page 157
- [retry](#) (Adaptive Services Interface) on page 158
- [retry-interval](#) on page 158
- [revocation-check](#) on page 159
- [secret](#) on page 160
- [security-association](#) (Junos OS) on page 161
- [security-association](#) (Junos-FIPS Software) on page 162
- [spi](#) (Junos OS) on page 163
- [spi](#) (Junos-FIPS Software) on page 163
- [ssh-known-hosts](#) on page 164
- [start-time](#) (Authentication Key Transmission) on page 165
- [tolerance](#) on page 166
- [traceoptions](#) on page 167
- [url](#) (Security) on page 169
- [validity-period](#) on page 169
- [Security Services Configuration Statements](#) on page 170

[edit security] Hierarchy Level

To configure security services, you can include the following configuration statements at the **[edit security]** hierarchy level:

```
[edit security]
authentication-key-chains {
  key-chain key-chain-name {
    key key {
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
  }
}
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-filename {
    certificate-key-string;
    load-key-file URL key-filename;
  }
}
```

```

    }
    maximum-certificates number;
    path-length certificate-path-length;
  }
  ike {
    proposal ike-proposal-name {
      authentication-algorithm (md5 | sha1);
      authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
      description description;
      dh-group (group1 | group2);
      encryption-algorithm (3des-cbc | des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);
      lifetime-seconds seconds;
    }
    policy ike-peer-address {
      description description;
      encoding (binary | pem);
      identity identity-name;
      local-certificate certificate-filename;
      local-key-pair private-public-key-file;
      mode (aggressive | main);
      pre-shared-key (ascii-text key | hexadecimal key);
      proposals [ proposal-names ];
    }
  }
  ipsec {
    security-association {
      manual {
        direction (bidirectional | inbound | outbound) {
          protocol esp;
          spi spi-value;
          encryption {
            algorithm 3des-cbc;
            key ascii-text ascii-text-string;
          }
        }
      }
    }
    proposal ipsec-proposal-name {
      authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
      description description;
      encryption-algorithm (3des-cbc | des-cbc);
      lifetime-seconds seconds;
      protocol (ah | esp | bundle);
    }
    policy ipsec-policy-name {
      description description;
      perfect-forward-secrecy {
        keys (group1 | group2);
      }
      proposals [ proposal-names ];
    }
    security-association sa-name {
      description description;
      dynamic {
        ipsec-policy policy-name;
        replay-window-size (32 | 64);
      }
    }
  }

```



```

}
manual {
  direction (inbound | outbound | bidirectional) {
    authentication {
      algorithm (hmac-md5-96 | hmac-sha1-96);
      key (ascii-text key | hexadecimal key);
    }
    auxiliary-spi auxiliary-spi;
    encryption {
      algorithm (des-cbc | 3des-cbc);
      key (ascii-text key | hexadecimal key);
    }
    protocol (ah | esp | bundle);
    spi spi-value;
  }
}
mode (tunnel | transport);
}
}
pki {
  auto-re-enrollment {
    certificate-id {
      ca-profile ca-profile-name;
      challenge-password password;
      re-enroll-trigger-time-percentage percentage;
      re-generate-keypair;
      validity-period days;
    }
  }
  ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
      url url-name;
      retry number-of-attempts;
      retry-interval seconds;
    }
    revocation-check {
      disable;
      crl {
        disable on-download-failure;
        refresh-interval number-of-hours;
        url {
          url-name;
          password;
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
ssh-known-hosts {
  host {

```

```

    dsa-key key;
    rsa-key key;
    rsa1-key key;
  }
}
traceoptions {
  file filename <files number> < size size>;
  flag all;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
}

```



NOTE: Most of the configuration statements do not have default values. If you do not specify an identifier for a statement that does not have a default value, you cannot commit the configuration.

For information about IP Security (IPsec) monitoring and troubleshooting, see the [CLI Explorer](#).

- Related Documentation**
- [Security Services Configuration Statements on page 170](#)

algorithm (Authentication Keychain)

Syntax	algorithm (hmac-sha-1 md5);
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	Configure the authentication algorithm for IS-IS.
Options	hmac-sha-1 —96-bit hash-based message authentication code (SHA-1). md5 —Message digest 5. Default: md5
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Hitless Authentication Key Rollover for IS-IS • Understanding Hitless Authentication Key Rollover for IS-IS

algorithm (Junos FIPS)

Syntax	algorithm 3des-cbc;
Hierarchy Level	[edit security ipsec internal security-association manual direction encryption]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Select the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	Only 3des-cbc is supported.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.

authentication (Security IPsec)

Syntax	<pre>authentication { algorithm (hmac-sha1-96 hmac-sha2-256); key (ascii-text <i>key</i> hexadecimal <i>key</i>); }</pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure IP Security (IPsec) authentication parameters for manual security association (SA).



NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Options	<p>algorithm—Hash algorithm that authenticates packet data. It can be one of the following:</p> <ul style="list-style-type: none">• hmac-md5-96—Produces a 128-bit digest.• hmac-sha1-96—Produces a 160-bit digest. <p>key—Type of authentication key. It can be one of the following:</p> <ul style="list-style-type: none">• ascii-text <i>key</i>—ASCII text key. For hmac-md5-96, the key is 16 ASCII characters; for hmac-sha1-96, the key is 20 ASCII characters.• hexadecimal <i>key</i>—Hexadecimal key. For hmac-md5-96, the key is 32 hexadecimal characters; for hmac-sha1-96, the key is 40 hexadecimal characters.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Manual IPsec Security Associations for an ES PIC on page 17

authentication-algorithm (Security IKE)

Syntax	authentication-algorithm (md5 sha1);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the Internet Key Exchange (IKE) authentication algorithm.
Options	authentication-algorithm —Hash algorithm that authenticates packet data. It can be one of two algorithms: <ul style="list-style-type: none">• md5—Produces a 128-bit digest.• sha1—Produces a 160-bit digest.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Authentication Algorithm for an IKE Proposal on page 27

authentication-algorithm (Security IPsec)

Syntax	authentication-algorithm (hmac-md5-96 hmac-sha1-96);
Hierarchy Level	[edit security ipsec proposal <i>ipsec-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IPsec authentication algorithm.



NOTE: Keep the following points in mind when you configure the authentication algorithm in an IPsec proposal:

- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, an error occurs and the tunnel is not established in this scenario. For example, if one end of the tunnel contains router 1 configured with the authentication algorithm as hmac-sha-256-128 and the other end of the tunnel contains router 2 configured with the authentication algorithm as hmac-md5-96, the VPN tunnel is not established.
- When both ends of an IPsec VPN tunnel contain the same IKE proposal but different IPsec proposals, and when one end of the tunnel contains two IPsec proposals to check whether a less secure algorithm is selected or not, an error occurs and the tunnel is not established. For example, if you configure two authentication algorithms for an IPsec proposal as hmac-sha-256-128 and hmac-md5-96 on one end of the tunnel, router 1, and if you configure the algorithm for an IPsec proposal as hmac-md5-96 on the other end of the tunnel, router 2, the tunnel is not established and the number of proposals mismatch.
- When you configure two IPsec proposals at both ends of a tunnel, such as the authentication-algorithm hmac-sha-256-128 and authentication-algorithm hmac-md5-96 statements at the [edit services ipsec-vpn ipsec proposal *proposal-name*] hierarchy level on one of the tunnel, router 1 (with the algorithms in two successive statements to specify the order), and the authentication-algorithm hmac-md5-96 and authentication-algorithm hmac-sha-256-128 statements at the [edit services ipsec-vpn ipsec proposal *proposal-name*] hierarchy level on one of the tunnel, router 2 (with the algorithms in two successive statements to specify the order, which is the reverse order of router 1), the tunnel is established in this combination as expected because the number of proposals is the same on both ends and they contain the same set of algorithms. However, the authentication algorithm selected is hmac-md5-96 and not the stronger algorithm of hmac-sha-256-128. This method of selection of the algorithm occurs because the first matching proposal is selected. Also, for a default proposal, regardless of whether the router supports the Advanced Encryption Standard (AES) encryption algorithm, the 3des-cbc algorithm is chosen and not the aes-cfb algorithm, which is because of the first algorithm in

the default proposal being selected. In the sample scenario described here, on router 2, if you reverse the order of the algorithm configuration in the proposal so that it is the same order as the one specified on router 1, hmac-sha-256-128 is selected as the authentication method.

- You must be aware of the order of proposals in an IPsec policy at the time of configuration if you want the matching of proposals to happen in a certain order of preference, such as the strongest algorithm to be considered first when a match is made when both policies from the two peers have a proposal.

Options	authentication-algorithm —Hash algorithm that authenticates packet data. It can be one of two algorithms: <ul style="list-style-type: none">• hmac-md5-96—Produces a 128-bit digest.• hmac-sha1-96—Produces a 160-bit digest.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Authentication Algorithm for an IPsec Proposal on page 32

authentication-key-chains

Syntax	<pre>authentication-key-chains { key-chain key-chain-name { description text-string; key key { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); secret secret-data; start-time yyyy-mm-dd.hh:mm:ss; } tolerance seconds; } }</pre>
Hierarchy Level	[edit security]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in JUNOS OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the authentication-key-chains statement is configured at the [edit security] hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the [edit protocols] hierarchy level or with the BFD protocol using the bfd-liveness-detection statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication Key Updates on page 71• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

authentication-method

Syntax	authentication-method (dsa-signatures pre-shared-keys rsa-signatures);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IKE authentication method.
Options	<p>dsa-signatures—Digital Signature Algorithm (DSA)</p> <p>rsa-signatures—A public key algorithm, which supports encryption and digital signatures</p> <p>pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Manual IPsec Security Associations for an ES PIC on page 17

auto-re-enrollment

Syntax	<pre>auto-re-enrollment { certificate-id { ca-profile <i>ca-profile-name</i>; challenge-password <i>password</i>; re-enroll-trigger-time-percentage <i>percentage</i>; re-generate-keypair; validity-period <i>days</i>; } }</pre>
Hierarchy Level	[edit security pki]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify auto-reenrollment parameters for a certificate authority (CA) issued router certificate. Auto-reenrollment requests that the issuing CA replace a router certificate before its specified expiration date.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57• Configuring Digital Certificates for Adaptive Services Interfaces on page 51

auxiliary-spi (Security IPsec)

Syntax	<code>auxiliary-spi <i>auxiliary-spi-value</i>;</code>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the protocol statement to use the bundle option.
Options	<p><i>auxiliary-spi-value</i>—Arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).</p> <p>Range: 256 through 16,639</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Manual IPsec Security Associations for an ES PIC on page 17 • spi on page 163

ca-identity

Syntax	<code>ca-identity <i>ca-identity</i>;</code>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	Specify the certificate authority (CA) identity to use in requesting digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.
Options	<i>ca-identity</i> —The name of the CA identity. This name is typically the domain name of the CA.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Specifying the CA Profile Name on page 53

ca-name

Syntax	<code>ca-name <i>ca-identity</i>;</code>
Hierarchy Level	[edit security certificates certification-authority]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.
Options	<i>ca-identity</i> —CA identity to use in the certificate request.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Certificate Authority Name on page 46

ca-profile

Syntax	<pre> ca-profile <i>ca-profile-name</i> { <i>ca-identity</i> <i>ca-identity</i>; enrollment { url <i>url-name</i>; retry <i>number-of-enrollment-attempts</i>; retry-interval <i>seconds</i>; } revocation-check { disable: <i>crl</i> { disable on-download-failure; refresh-interval <i>number-of-hours</i>; url { url-name; password; } } } } </pre>
Hierarchy Level	[edit security pki]
Release Information	<p>Statement introduced in Junos OS Release 7.5.</p> <p>revocation-check and crl statements added in Junos OS Release 8.1.</p>
Description	<p>Specify the name of the certificate authority (CA) profile for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M Series and T Series routers.</p> <p>The remaining statements are explained separately.</p>
Options	ca-profile-name —Name of the trusted CA.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Specifying the CA Profile Name on page 53

cache-size

Syntax	cache-size <i>bytes</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.
Options	bytes —Cache size for digital certificates. Range: 64 through 4,294,967,295 Default: 2 megabytes (MB)



NOTE: We recommend that you limit your cache size to 4 MB.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none">• Configuring the Cache Size on page 48

cache-timeout-negative

Syntax	cache-timeout-negative <i>seconds</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.
Options	seconds —Negative time to cache digital certificates, in seconds. Range: 10 through 4,294,967,295 Default: 20



CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none"> • Configuring the Negative Cache on page 48

certificate-id

Syntax	<pre>certificate-id { <i>ca-profile</i> <i>ca-profile-name</i>; <i>challenge-password</i> <i>password</i>; <i>re-enroll-trigger-time-percentage</i> <i>percentage</i>; <i>re-generate-keypair</i>; <i>validity-period</i> <i>days</i>; }</pre>
Hierarchy Level	[edit security auto-re-enrollment]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify a router certificate for auto-reenrollment. The ID is the same as that used to get the end entity's certificate from the issuing certificate authority.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57• auto-re-enrollment on page 110

certificates

Syntax	<pre> certificates { cache-size <i>bytes</i>; cache-timeout-negative <i>seconds</i>; certification-authority <i>ca-profile-name</i> { ca-name <i>ca-identity</i>; crt <i>file-name</i>; encoding (binary pem); enrollment-url <i>url-name</i>; file <i>certificate-filename</i>; ldap-url <i>url-name</i>; } enrollment-retry <i>attempts</i>; local <i>certificate-name</i> { certificate-key-string; load-key-file <i>URL filename</i>; } maximum-certificates <i>number</i>; path-length <i>certificate-path-length</i>; } </pre>
Hierarchy Level	[edit security]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure the digital certificates for IPsec.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Digital Certificates for an ES PIC on page 45

certification-authority

Syntax	<pre>certification-authority <i>ca-profile-name</i> { <i>ca-name</i> <i>ca-identity</i>; <i>crl</i> <i>file-name</i>; <i>encoding</i> (binary pem); <i>enrollment-url</i> <i>url-name</i>; <i>file</i> <i>certificate-filename</i>; <i>ldap-url</i> <i>url-name</i>; }</pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced before Junos OS Release 12.1 for the SRX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure a certificate authority profile name.</p> <p>Configure certification authority (CA) for X.509 certificate.</p>
Options	<ul style="list-style-type: none">• <i>profile-name</i>—Name of this CA configuration.• <i>ca-name</i> <i>name</i>—Name of the CA.• <i>crl</i> <i>filename</i>—Certificate revocation list (CRL) filename.• <i>encoding</i>—Certificate encoding, either binary or pem (privacy-enhanced mail).• <i>enrollment-url</i> <i>url</i>—Enrollment URL.• <i>file</i> <i>filename</i>—Certificate filename.• <i>ldap-url</i> <i>url</i>—Lightweight Directory Access Protocol (LDAP) URL.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Certificate Authority Properties for an ES PIC on page 46• Network Monitoring and Troubleshooting Guide for Security Devices• Security Basics• Configuring the Certificate Authority Properties for an ES PIC on page 46

challenge-password

Syntax	<code>challenge-password <i>password</i>;</code>
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Specify the challenge password used by the certificate authority (CA) for router certificate enrollment and revocation. This challenge password must be the same used when the router certificate was originally configured.
Options	<i>password</i> —The password required by the CA.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57• auto-re-enrollment on page 110

crl (Adaptive Services Interface)

Syntax	<pre>crl { disable on-download-failure; refresh-interval <i>number-of-hours</i>; url { url-name; password; } }</pre>
Hierarchy Level	[edit security pki <i>ca-profile</i> <i>ca-profile-name</i> revocation-check]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
Options	<p>disable on-download-failure—Permit the authentication of the IPsec peer when the CRL is not downloaded.</p> <p>password—Password to access the URLs.</p> <p>refresh-interval <i>number-of-hours</i>—Time interval, in hours, between CRL updates. Range: 0 through 8784 Default: 24</p> <p>url <i>url-name</i>—Location from which to retrieve the CRL through the Lightweight Directory Access Protocol (LDAP). You can configure as many as three URLs for each configured CA profile.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Certificate Revocation List on page 54

crl (Encryption Interface)

Syntax	<code>crl <i>file-name</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
Options	<i>file-name</i> —Specify the file from which to read the CRL.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none"> • Configuring the Certificate Authority Properties for an ES PIC on page 46

description (Authentication Keychain)

Syntax	<code>description <i>text-string</i>;</code>
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i>]
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the BFD protocol introduced in Junos OS Release 9.6. Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches. Support for IS-IS introduced in JUNOS OS Release 11.2.
Description	Configure a description for an authentication key-chain.
Options	<i>text-string</i> —A text string describing the authentication-key-chain . Put the text string in quotes ("text description").
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication Key Updates on page 71 • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

description (IKE policy)

Syntax	<code>description <i>description</i>;</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec policy <i>ipsec-policy-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>], [edit security ipsec security-association <i>sa-name</i>]
Description	Specify a text description for an IKE proposal or policy, or an IPsec proposal, policy, or SA.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Security Associations for IPsec on an ES PIC on page 15• Configuring the Description for an IKE Proposal on page 28• Configuring the Description for an IKE Policy on page 30• Configuring an IPsec Proposal for an ES PIC on page 32• Configuring the IPsec Policy for an ES PIC on page 34

dh-group

Syntax	<code>dh-group (group1 group2 group5 group14);</code>
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IKE Diffie-Hellman group.
Options	dh-group —Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. It can be one of the following: <ul style="list-style-type: none">• group1—768-bit.• group2—1024-bit.• group5—1536-bit.• group14—2048-bit.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Diffie-Hellman Group for an IKE Proposal on page 28

direction (Junos OS)

Syntax	<pre> direction (inbound outbound bidirectional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text key hexadecimal key); } auxiliary-spi auxiliary-spi-value; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text key hexadecimal key); } protocol (ah esp bundle); spi spi-value; } </pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the direction of IPsec processing.
Options	<p>inbound—Inbound SA—Define algorithms, keys, or security parameter index (SPI) values to decrypt and authenticate incoming traffic coming from the peer.</p> <p>outbound—Outbound SA—Define algorithms, keys, or SPI values to decrypt and authenticate outbound traffic to the peer.</p> <p>bidirectional—Bidirectional SA—Decrypt and authenticate the incoming and outgoing traffic using the same algorithm, keys, or SPI in both directions, unlike inbound and outbound SAs that use different attributes in both directions.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Manual IPsec Security Associations for an ES PIC on page 17 • <i>Example: Using IPsec to Protect BGP Traffic</i>

direction (Junos-FIPS Software)

Syntax	<pre>direction (bidirectional inbound outbound) { protocol esp; spi spi-value; encryption { algorithm 3des-cbc; key ascii-text <i>ascii-text-string</i>; } }</pre>
Hierarchy Level	[edit security ipsec internal security-association manual], [edit security trusted-channel ipsec security-association manual]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Establish a manual security association (SA) for internal Routing-Engine-to-Routing-Engine communication.
Options	<p>bidirectional—Apply the same SA values in both directions between Routing Engines.</p> <p>inbound—Apply these SA properties only to the inbound IPsec tunnel.</p> <p>outbound—Apply these SA properties only to the outbound IPsec tunnel.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	Crypto Officer—To view and add this statement in the configuration.



dynamic

Syntax	<pre>dynamic { ipsec-policy <i>ipsec-policy-name</i>; replay-window-size (32 64); }</pre>
Hierarchy Level	[edit security ipsec security-association name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define a dynamic IPsec SA.
Options	<p>ipsec-policy <i>ipsec-policy-name</i>—Name of the IPsec policy.</p> <p>replay-window-size—(Optional) Antireplay window size. It can be one of the following values:</p> <ul style="list-style-type: none">• 32—32-packet window size.• 64—64-packet window size.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Dynamic IPsec Security Associations on page 21• Associating the Configured Security Association with a Logical Interface on page 51

encoding

Syntax	encoding (binary pem);
Hierarchy Level	[edit security ike policy ike-peer-address], [edit security certificates certification-authority ca-profile-name]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the local-certificate and local-key-pair statements.
Options	binary —Binary file format. pem —Privacy-enhanced mail (PEM), an ASCII base 64 encoded format. Default: binary
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Type of Encoding Your CA Supports on page 47• Configuring the Type of Encoding Your CA Supports on page 50

encryption (Junos OS)

Syntax	<pre> encryption { algorithm (des-cbc 3des-cbc aes-128-cbc aes-192-cbc aes-256-cbc); key (ascii-text key hexadecimal key); } </pre>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bidirectional)]
Release Information	Statement introduced before Junos OS Release 7.4. aes-128-cbc , aes-192-cbc , and aes-256-cbc algorithm options added in Junos OS Release 15.1.
Description	Configure an encryption algorithm and key for a manual Security Association.
Options	<p>algorithm—Type of encryption algorithm. It can be one of the following:</p> <ul style="list-style-type: none"> 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. <p> 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.</p> <ul style="list-style-type: none"> aes-128-cbc—Has a block size of 128 bits; its key size is 128 bits long. aes-192-cbc—Has a block size of 128 bits; its key size is 192 bits long. aes-256-cbc—Has a block size of 128 bits; its key size is 256 bits long. <p> NOTE: The aes-*-cbc algorithms support both IKE and IPsec configurations at the [security] hierarchy level.</p> <p>key—Type of encryption key. It can be one of the following:</p> <ul style="list-style-type: none"> ascii-text—ASCII text key. For the des-cbc option, the key contains 8 ASCII characters; for 3des-cbc, the key contains 24 ASCII characters. hexadecimal—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	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Example: Using IPsec to Protect BGP Traffic](#)
 - [Configuring Manual IPsec Security Associations for an ES PIC on page 17](#)

encryption (Junos-FIPS Software)

Syntax

```
encryption {  
  algorithm 3des-cbc;  
  key ascii-text ascii-text-string;  
}
```

Hierarchy Level [edit security ipsec internal security-association manual direction]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the encryption parameters for internal Routing-Engine-to-Routing-Engine communication. The remaining statements are explained separately.



NOTE: The hexadecimal format must be used for the encryption key to be FIPS compliant. The hexadecimal keys provide maximum key strength.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

encryption-algorithm (Security)

Syntax	encryption-algorithm (3des-cbc des-cbc aes-128-cbc aes-192-cbc aes-256-cbc);
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure an IKE or IPsec encryption algorithm.
Options	<p>3des-cbc—Encryption algorithm with key size of 24 bytes; its key size is 192 bits long.</p> <p>des-cbc—Encryption algorithm with key size of 8 bytes; its key size is 48 bits long.</p> <p>aes-128-cbc—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.</p> <p>aes-192-cbc—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.</p> <p>aes-256-cbc—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Proposal for Dynamic SAs on page 26 • Configuring an IPsec Proposal for an ES PIC on page 32

enrollment

Syntax	<pre>enrollment { url <i>url-name</i>; retry <i>number-of-enrollment-attempts</i>; retry-interval <i>seconds</i>; }</pre>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	Specify the URL and enrollment parameters of the certificate authority (CA) for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M Series and T Series routers.
Options	<p>url <i>url-name</i>—Location of the CA to which the router sends the Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests for the configured CA profile. Use the CA host DNS name or IP address.</p> <p>retry <i>number-of-enrollment-attempts</i>—Number of enrollment retries. Range: 0 through 100 Default: 0</p> <p>retry-interval <i>seconds</i>—Length of time, in seconds, that a router should wait between enrollment attempts. Range: 0 through 3600 Default: 0</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Specifying an Enrollment URL on page 53• Specifying the Enrollment Properties on page 54

enrollment-retry

Syntax	<code>enrollment-retry <i>attempts</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.
Options	<i>attempts</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Number of Enrollment Retries on page 48

enrollment-url

Syntax	<code>enrollment-url <i>url-name</i>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).
Options	<i>url-name</i> —Certificate authority URL.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying an Enrollment URL on page 47

file

Syntax	<code>file <i>certificate-filename</i>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.
Options	<i>certificate-filename</i> —File from which to read the digital certificate.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying a File to Read the Digital Certificate on page 47

identity

Syntax	<code>identity <i>identity-name</i>;</code>
Hierarchy Level	[edit security ike]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the identity of the remote certificate name if the identity cannot be learned through IKE (ID payload or IP address).
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Identity to Define the Remote Certificate Name on page 50

ike (Security)

Syntax	<pre> ike { policy <i>ike-peer-address</i> { description <i>policy-description</i>; encoding (binary pem); identity <i>identity-name</i>; local-certificate <i>certificate-filename</i>; local-key-pair <i>private-public-key-file</i>; mode (aggressive main); pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); proposals [<i>proposal-names</i>]; } proposal <i>ike-proposal-name</i> { authentication-algorithm (md5 sha1); authentication-method (dsa-signatures pre-shared-keys rsa-signatures); dh-group (group1 group2); encryption-algorithm (3des-cbc des-cbc); lifetime-seconds <i>seconds</i>; } } </pre>
Hierarchy Level	[edit security]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	(Encryption interface on M Series and T Series routers only) Configure IKE.
Options	The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Proposal for Dynamic SAs on page 26 • Configuring an IKE Policy for Preshared Keys on page 29

internal

Syntax

```
internal {  
  security-association {  
    manual {  
      direction (bidirectional | inbound | outbound) {  
        protocol esp;  
        spi spi-value;  
        encryption {  
          algorithm 3des-cbc;  
          key ascii-text ascii-text-string;  
        }  
      }  
    }  
  }  
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Junos-FIPS only) Define an internal security association (SA) for internal Routing-Engine-to-Routing-Engine communication.

Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

Related Documentation

- [Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 36](#)
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

ipsec (Security)

```

Syntax  ipsec {
        security-association {
            manual {
                direction (bidirectional | inbound | outbound) {
                    protocol esp;
                    spi spi-value;
                    encryption {
                        algorithm 3des-cbc;
                        key (ascii-text ascii-text-string | hexadecimal hexadecimal-string);
                    }
                }
            }
        }
        policy ipsec-policy-name {
            perfect-forward-secrecy {
                keys (group1 | group2);
            }
            proposals [ proposal-names ];
        }
        proposal ipsec-proposal-name {
            authentication-algorithm (hmac-sha1-96 | hmac-sha2-256);
            encryption-algorithm (3des-cbc | des-cbc);
            lifetime-seconds seconds;
            protocol (ah | esp | bundle);
        }
        security-association name {
            dynamic {
                ipsec-policy policy-name;
                replay-window-size (32 | 64);
            }
            manual {
                direction (inbound | outbound | bi-directional) {
                    authentication {
                        algorithm (hmac-sha1-96 | hmac-sha2-256);
                        key (ascii-text key | hexadecimal key);
                    }
                    auxiliary-spi auxiliary-spi-value;
                    encryption {
                        algorithm (des-cbc | 3des-cbc);
                        key (ascii-text key | hexadecimal key);
                    }
                    protocol (ah | esp | bundle);
                    spi spi-value;
                }
            }
            mode (tunnel | transport);
        }
        traceoptions {
            file <files number> < size size>;
            flag all;
            flag database;
            flag general;
        }
    }

```

```
    flag ike;  
    flag parse;  
    flag policy-manager;  
    flag routing-socket;  
    flag timer;  
  }  
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IPsec on encryption interfaces.



NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Options The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)

key (Authentication Keychain)

Syntax	<pre>key key { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); secret secret-data; start-time yyyy-mm-dd.hh:mm:ss; }</pre>
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i>]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the authentication element.
Options	<p>key—Each key within a keychain is identified by a unique integer value.</p> <p>Range: 0 through 63</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication Key Updates on page 71 • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

key (Junos FIPS)

Syntax	<code>key (ascii-text <i>key</i> hexadecimal <i>key</i>);</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction encryption]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The key used for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	<i>ascii-text-key</i> —The encrypted ASCII text key. <i>hexadecimal key</i> —The encrypted hexadecimal key.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.

key-chain (Security)

Syntax	<pre>keychain <i>key-chain-name</i> { description <i>text-string</i>; key <i>key</i> { algorithm (md5 hmac-sha-1); options (basic isis-enhanced); secret <i>secret-data</i>; start-time <i>yyyy-mm-dd.hh:mm:ss</i>; } tolerance <i>seconds</i>; }</pre>
Hierarchy Level	[edit security authentication-key-chains]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.
Options	<p>key-chain-name—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (" ").</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • authentication-key-chains on page 108 • Configuring Authentication Key Updates on page 71 • <i>Example: Configuring BFD Authentication for Securing Static Routes</i> • <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>


ldap-url

Syntax	<ldap-url <i>url-name</i> >;
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.
Options	<i>url-name</i> —Name of the LDAP URL.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an LDAP URL on page 47

lifetime-seconds (Security)

Syntax	<lifetime-seconds <i>seconds</i> >;
Hierarchy Level	[edit security ike proposal <i>ike-proposal-name</i>], [edit security ipsec proposal <i>ipsec-proposal-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	(Optional) Configure the lifetime of IKE or IPsec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.
Options	<i>seconds</i> —Lifetime, in seconds. Range: 180 through 86,400
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Lifetime for an IKE SA on page 29• Configuring the Lifetime for an IPsec SA on page 33

local

Syntax	<pre>local <i>certificate-name</i> { <i>certificate-key-string</i>; load-key-file <i>URL filename</i>; }</pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.
<div>  <p>NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.</p> </div>	
Options	<p><i>certificate-key-string</i>—String of alphanumeric characters that constitute the private key and certificate.</p> <p><i>certificate-name</i>—Name that uniquely identifies the certificate.</p> <p><i>load-key-file URL filename</i>—File that contains the private key and certificate. It can be one of two types of values:</p> <ul style="list-style-type: none"> • Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk) • URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Importing SSL Certificates for Junos XML Protocol Support on page 75

local-certificate (Security)

Syntax	<code>local-certificate <i>certificate-filename</i>;</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the certificate filename from which to read the local certificate.
Options	<i>certificate-filename</i> —File from which to read the local certificate.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Certificate Filename on page 50

local-key-pair

Syntax	<code>local-key-pair <i>private-public-key-file</i>;</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Release Information	Statement introduced before Junos 7.4.
Description	Specify private and public keys.
Options	<i>private-public-key-file</i> —Specify the file from which to read the private and public key pair.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Private and Public Key File on page 50

manual (Junos OS)

Syntax	<pre> manual { direction (inbound outbound bi-directional) { authentication { algorithm (hmac-md5-96 hmac-sha1-96); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } auxiliary-spi <i>auxiliary-spi-value</i>; encryption { algorithm (des-cbc 3des-cbc); key (ascii-text <i>key</i> hexadecimal <i>key</i>); } protocol (ah esp bundle); spi <i>spi-value</i>; } } </pre>
Hierarchy Level	[edit security ipsec security-association]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define a manual IPsec SA.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Manual IPsec Security Associations for an ES PIC on page 17

manual (Junos FIPS)

Syntax manual {
 direction (bidirectional | inbound | outbound) {
 protocol esp;
 spi *spi-value*;
 encryption {
 algorithm 3des-cbc;
 key ascii-text *ascii-text-string*;
 }
 auxiliary-spi *auxiliary-spi-value*;
 encryption {
 algorithm 3des-cbc;
 key (ascii-text *key* | hexadecimal *key*);
 }
 protocol (esp | bundle);
 spi *spi-value*;
 }
 }

Hierarchy Level [edit security ipsec internal security-association]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual security association (SA) for internal Routing Engine-to-Routing Engine communication.


Options The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.


maximum-certificates

Syntax	<code>maximum-certificates <i>number</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.
Options	<i>number</i> —Maximum number of peer digital certificates to be cached. Range: 64 through 4,294,967,295 peer certificates Default: 1024 peer certificates
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Number of Peer Certificates on page 49

mode (IKE)

Syntax	mode (aggressive main);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the IKE policy mode.
<div> NOTE: IKEv2 protocol does not negotiate using mode configuration.</div>	
Default	main
Options	<p>aggressive—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection.</p> <p>main—Use six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Mode for an IKE Policy on page 30

mode (IPsec)

Syntax	mode (transport tunnel);
Hierarchy Level	[edit security ipsec security-association name]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the mode for the IPsec security association.
Default	tunnel
Options	<p>transport—Protect traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. Virtual Private Network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications.</p> <p>tunnel—Protect traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.</p>
<div>  <p>NOTE: The Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.</p> <p>In transport mode, the Junos OS does not support authentication header (AH) and ESP header bundles.</p> <p>In transport mode, the Junos OS supports only Border Gateway Protocol (BGP).</p> </div>	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Using IPsec to Protect BGP Traffic • Configuring IPsec Tunnel Mode on page 16

options (Security)

Syntax	options (basic isis-enhanced);
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 11.3 for the QFX Series.
Description	<p>For IS-IS only, configure the protocol transmission encoding format for encoding the message authentication code in routing protocol packets.</p> <p>Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.</p>
Options	<p>basic—RFC 5304 based encoding. Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.</p> <p>isis-enhanced—RFC 5310 based encoding. Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.</p> <p>Default: basic</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>• <i>Understanding Hitless Authentication Key Rollover for IS-IS</i>

path-length

Syntax	<code>path-length <i>certificate-path-length</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.
Options	<i>certificate-path-length</i> —Digital certificate path length. Range: 2 through 15 certificates Default: 15 certificates
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Path Length for the Certificate Hierarchy on page 49

perfect-forward-secrecy (Security)

Syntax	<code>perfect-forward-secrecy { keys (group1 group2); }</code>
Hierarchy Level	[edit security ipsec policy <i>ipsec-policy-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the Perfect Forward Secrecy (PFS) protocol. Create single-use keys.
Options	keys —Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange. The key can be one of the following: <ul style="list-style-type: none"> • group1—768-bit. • group2—1024-bit.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Perfect Forward Secrecy on page 34

pki

Syntax	<pre> pki { auto-re-enrollment { certificate-id { ca-profile <i>ca-profile-name</i>; challenge-password <i>password</i>; re-enroll-trigger-time-percentage <i>percentage</i>; re-generate-keypair; validity-period <i>days</i>; } } ca-profile <i>ca-profile-name</i> { ca-identity <i>ca-identity</i>; enrollment { url <i>url-name</i>; retry <i>number-of-enrollment-attempts</i>; retry-interval <i>seconds</i>; } revocation-check { disable; crl { disable on-download-failure; refresh-interval <i>hours</i>; url { url-name; password; } } } } traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } } </pre>
Hierarchy Level	[edit security]
Release Information	Statement introduced in Junos OS Release 7.5. revocation-check and crl statements added in Junos OS Release 8.1.
Description	Configure an IPsec profile to request digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> Configuring Digital Certificates for Adaptive Services Interfaces on page 51

- [Junos OS, Release 15.1](#)
- [CLI Explorer](#)

policy (Security IKE)

Syntax	<pre> policy <i>ike-peer-address</i> { description <i>policy-description</i>; encoding (binary pem); identity <i>identity-name</i>; local-certificate <i>certificate-filename</i>; local-key-pair <i>private-public-key-file</i>; mode (aggressive main); pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>); proposals [<i>proposal-names</i>]; } </pre>
Hierarchy Level	[edit security ike]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IKE policy.
Options	<p><i>ike-peer-address</i>—A tunnel address configured at the [edit interfaces es] hierarchy level.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Policy for Preshared Keys on page 29 • Configuring an IKE Policy for Digital Certificates for an ES PIC on page 49

policy (Security IPsec)

Syntax	<pre>policy <i>ipsec-policy-name</i> { description <i>description</i>; perfect-forward-secrecy { keys (group1 group 14 group2 group 5); } proposals [<i>proposal-names</i>]; }</pre>
Hierarchy Level	[edit security ipsec]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IPsec policy.
Options	<p><i>ipsec-policy-name</i>—Specify an IPsec policy name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the IPsec Policy for an ES PIC on page 34

pre-shared-key (Security)

Syntax	<pre>pre-shared-key (ascii-text <i>key</i> hexadecimal <i>key</i>);</pre>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.
Options	<p><i>ascii-text key</i>—Authentication key in ASCII format.</p> <p><i>hexadecimal key</i>—Authentication key in hexadecimal format.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Preshared Key for an IKE Policy on page 30

proposal (Security IKE)

Syntax	<pre>proposal <i>ike-proposal-name</i> { authentication-algorithm (md5 sha1 sha-256); authentication-method (dsa-signatures pre-shared-keys rsa-signatures); description <i>description</i>; dh-group (group1 group2 group 5 group14); encryption-algorithm <i>algorithm</i>; lifetime-seconds <i>seconds</i>; }</pre>
Hierarchy Level	[edit security ike]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IKE proposal for a dynamic SA.
Options	<p><i>ike-proposal-name</i>—Specify an IKE proposal name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IKE Proposal for Dynamic SAs on page 26

proposal (Security IPsec)

Syntax	<pre>proposal <i>ipsec-proposal-name</i> { authentication-algorithm (hmac-md5-96 hmac-sha1-96); encryption-algorithm <i>algorithm</i>; lifetime-seconds <i>seconds</i>; protocol (ah bundle esp); }</pre>
Hierarchy Level	[edit security ipsec]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define an IPsec proposal for a dynamic SA.
Options	<p><i>ipsec-proposal-name</i>—Specify an IPsec proposal name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>security—To view this statement in the configuration.</p> <p>security-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring an IPsec Proposal for an ES PIC on page 32

proposals

Syntax	<code>proposals [<i>proposal-names</i>];</code>
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security ipsec policy <i>ipsec-policy-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Associate one or more proposals with an IKE or IPsec policy.
Options	<i>proposal-names</i> —Name of one or more proposals.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Associating Proposals with an IKE Policy on page 31• Configuring the IPsec Policy for an ES PIC on page 34

protocol (Junos OS)

Syntax	protocol (esp bundle);
Hierarchy Level	[edit security ipsec proposal <i>ipsec-proposal-name</i>], [edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bidirectional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Define the IPsec protocol for a manual or dynamic SA.



NOTE: The Junos OS supports only encapsulating security payload (ESP) when you use tunnel mode.

In transport mode, the Junos OS does not support authentication header (AH) and ESP header bundles.

In transport mode, the Junos OS supports only Border Gateway Protocol (BGP).

Options	<p>ah—Authentication Header protocol</p> <p>bundle—AH and ESP protocols</p> <p>esp—ESP protocol (the tunnel statement must be included at the [edit security ipsec security-association <i>sa-name</i> mode hierarchy level])</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Using IPsec to Protect BGP Traffic • Configuring Manual IPsec Security Associations for an ES PIC on page 17 • Configuring the Protocol for a Dynamic IPsec SA on page 34

protocol (Junos-FIPS Software)

Syntax	protocol esp;
Hierarchy Level	[edit security ipsec internal security-association manual direction]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The protocol used for the internal Routing-Engine-to-Routing-Engine IPsec security association (SA) configuration.
Options	Only esp is supported.
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 36• <i>Secure Configuration Guide for Common Criteria and Junos-FIPS</i>

re-enroll-trigger-time-percentage

Syntax	re-enroll-trigger-time-percentage <i>percentage</i> ;
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Percentage of the router certificate validity-period statement value, in days, when auto-reenrollment should start before expiration.
Options	percentage —Percentage for the reenroll trigger time. Range: 1 through 99
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57• auto-re-enrollment on page 110

re-generate-keypair

Syntax	<re-generate-keypair>;
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(Optional) Automatically generate a new key pair when auto-reenrolling a router certificate. If this statement is not configured, the current key pair is used.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57 • auto-re-enrollment on page 110

refresh-interval

Syntax	refresh-interval <i>number-of-hours</i> ;
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> revocation-check crl]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	(Adaptive services interfaces only) Specify the amount of time between certificate revocation list (CRL) updates.
Options	<i>number-of-hours</i> —Time interval, in hours, between CRL updates. Range: 0 through 8784 Default: 24
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Certificate Revocation List on page 54 • crl on page 120

retry (Adaptive Services Interface)

Syntax	<code>retry number-of-attempts;</code>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> enrollment]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Specify how many times a router can resend a digital certificate request.
Options	<i>number-of-attempts</i> —Number of enrollment retries. Range: 0 through 100 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Enrollment Properties on page 54• enrollment on page 130

retry-interval

Syntax	<code>retry-interval seconds;</code>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> enrollment]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Specify the amount of time the router should wait between enrollment retries.
Options	<i>seconds</i> —Time interval, in seconds, between enrollment retries. Range: 0 through 3600 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Enrollment Properties on page 54• enrollment on page 130

revocation-check

Syntax	<pre> revocation-check { disable; crl { refresh-interval <i>number-of-hours</i>; url { <i>url-name</i>; } } } </pre>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.1.
Description	Specify the method to verify revocation status of digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.
Options	<p>disable—Disable verification of status of digital certificates.</p> <p>crl—Only certificate revocation list (CRL) is supported. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis. By default, crl is enabled.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Certificate Revocation List on page 54

secret

Syntax	<code>secret <i>secret-data</i>;</code>
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in JUNOS OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for QFX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.
Options	<i>secret-data</i> —Password to use; it can include spaces if the character string is enclosed in quotation marks.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication Key Updates on page 71• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

security-association (Junos OS)

```
Syntax  security-association sa-name {
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bi-directional) {
                authentication {
                    algorithm (hmac-sha1-96 | hmac-sha2-256);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi-value;
                encryption {
                    algorithm (des-cbc | 3des-cbc);
                    key (ascii-text key | hexadecimal key);
                }
                protocol ( ah | esp | bundle);
                spi spi-value;
            }
            mode (tunnel | transport);
        }
    }
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.



NOTE: You must configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Security Associations for IPsec on an ES PIC on page 15](#)

security-association (Junos-FIPS Software)

```
Syntax  security-association sa-name {
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        manual {
            direction (inbound | outbound | bi-directional) {
                authentication {
                    algorithm (hmac-sha1-96 | hmac-sha2-256);
                    key (ascii-text key | hexadecimal key);
                }
                auxiliary-spi auxiliary-spi-value;
                encryption {
                    algorithm 3des-cbc;
                    key (ascii-text key | hexadecimal key);
                }
                protocol ( ah | esp | bundle);
                spi spi-value;
            }
            mode (tunnel | transport);
        }
    }
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.



NOTE: We recommend that you configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately.

Required Privilege Level Crypto Officer—To view and add this statement in the configuration.

spi (Junos OS)

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec security-association <i>sa-name</i> manual direction (inbound outbound bi-directional)]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the security parameter index (SPI) for a security association (SA).
Options	<p>spi-value—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).</p> <p>Range: 256 through 16,639</p>



NOTE: Use the auxiliary SPI when you configure the protocol statement to use the bundle option.

Required Privilege	system—To view this statement in the configuration.
Level	system-control—To add this statement to the configuration.

spi (Junos-FIPS Software)

Syntax	<code>spi spi-value;</code>
Hierarchy Level	[edit security ipsec internal security-association manual direction]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	The security parameter index (SPI) value used for the internal Routing Engine-to-Routing Engine IPsec security association (SA) configuration.
Options	<p>spi-value—Integer to use for this SPI.</p> <p>Range: 256 through 16,639</p>
Required Privilege Level	Crypto Officer—To add and view this statement in the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 36 • <i>Secure Configuration Guide for Common Criteria and Junos-FIPS</i>

ssh-known-hosts

Syntax	<pre>ssh-known-hosts { host <i>host-name</i> { dsa-key <i>key</i>; fetch-from-server <i>host-name</i>; load-key-file <i>URL filename</i>; rsa-key <i>key</i>; rsa1-key <i>key</i>; } }</pre>
Hierarchy Level	[edit security ssh-known-hosts]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	Configure SSH support for known hosts and for administering SSH host key updates.
Options	<p>host <i>host-name</i>—Hostname of the SSH known host entry. This option has the following suboptions:</p> <ul style="list-style-type: none">• dsa-key <i>key</i>—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.• fetch-from-server <i>host-name</i>—Retrieve SSH public host key information from a specified server.• load-key-file <i>filename</i>—Import SSH host key information from the <code>/var/tmp/ssh-known-hosts</code> file.• rsa-key <i>key</i>—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.• rsa1-key <i>key</i>—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring SSH Host Keys for Secure Copying of Data on page 73

start-time (Authentication Key Transmission)


Syntax	<code>start-time (now yyyy-mm-dd.hh:mm:ss);</code>
Hierarchy Level	[edit security authentication-key-chains key-chain <i>key-chain-name</i> key <i>key</i>]
Release Information	<p>Statement introduced in Junos OS Release 7.6.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6.</p> <p>Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.</p> <p>Support for IS-IS introduced in JUNOS OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 11.3 for QFX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.</p>
Options	<p>now—Start time as the current year, month, day, hour, minute, and second.</p> <p>daydays—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure start-time 2day, the start time will be on the 14th, exactly two days after the configuration is entered.</p> <p>hourhours—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure start-time 3hour, the start time will be in 12:00, exactly three hours after the configuration is entered.</p> <p>minuteminutes—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure start-time 5min, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.</p> <p>monthmonths—Start time as the specified number of months after the current month. For example, if the current month is March and you configure start-time 4month, the start time will be in July, exactly four months after the configuration is entered.</p> <p>secondseconds—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure start-time 10seconds, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.</p> <p>yearyears—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure start-time 1year, the start time will be in 2012, exactly one year after the configuration is entered.</p> <p>yyyy-mm-dd.hh:mm:ss—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Configuring Authentication Key Updates on page 71](#)
 - *Example: Configuring BFD Authentication for Securing Static Routes*
 - *Example: Configuring BFD Authentication for Securing Static Routes*
 - *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

tolerance

Syntax	<code>tolerance seconds;</code>
Hierarchy Level	<code>[edit security authentication-key-chains key-chain <i>key-chain-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 7.6. Statement introduced in Junos OS Release 9.0 for EX Series switches. Support for the BFD protocol introduced in Junos OS Release 9.6. Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches. Support for IS-IS introduced in Junos OS Release 11.2.
Description	Configure the clock-skew tolerance for accepting keys for a key chain.
Options	<i>seconds</i> —Number of seconds to accept for clock-skew. Default: 0 seconds Range: 0 through 999,999,999
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication Key Updates on page 71• <i>Example: Configuring BFD Authentication for Securing Static Routes</i>• <i>Example: Configuring Hitless Authentication Key Rollover for IS-IS</i>

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>>; flag all; flag certificates; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; level no-remote-trace } </pre>
Hierarchy Level	<p>[edit security], [edit services ipsec-vpn]</p> <p>Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure security trace options.</p> <p>To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the <code>/var/log/kmd</code> file.</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The <code>traceoptions</code> statement is not supported on QFabric systems.</p> </div> </div>	
Options	<p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file (for example, <code>kmd</code>) reaches its maximum size, it is renamed <code>kmd.0</code>, then <code>kmd.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files</p> <p>Default: 0 files</p> <p>size <i>size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, <code>kmd</code>) reaches this size, it is renamed, <code>kmd.0</code>, then <code>kmd.1</code> and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>Default: 1024 KB</p>

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

Required Privilege	admin—To view the configuration.
Level	admin-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring Tracing Operations for Security Services on page 67
------------------------------	---

url (Security)

Syntax	<code>url <i>url-name</i>;</code>
Hierarchy Level	[edit security pki ca-profile <i>ca-profile-name</i> enrollment], [edit security pki ca-profile <i>ca-profile-name</i> revocation-check <i>crl</i>]
Release Information	Statement introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Specify the certificate authority (CA) URL to use in requesting digital certificates or the URL for the Lightweight Access Directory Protocol (LDAP) location from which retrieve the certificate revocation list (CRL).
Options	<i>url-name</i> —URL of CA or URL of LDAP location of CRL.
Required Privilege Level	admin—To view the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying an Enrollment URL on page 53 • Specifying an LDAP URL on page 54 • crl on page 120 • enrollment on page 130

validity-period

Syntax	<code>validity-period <i>days</i>;</code>
Hierarchy Level	[edit security pki auto-re-enrollment certificate-id]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	Certificate validity period, in days, from the enrollment start date. If not specified, the issuing certificate authority (CA) sets this time as per its own policy. The start time is when auto-reenrollment is initiated.
Options	<i>days</i> —Number of days that the certificate is valid. Range: 1 through 4095 days Default: Per CA policy
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 57 • auto-re-enrollment on page 110

Security Services Configuration Statements

The following table lists the security services configuration statements available at the **[edit security]** hierarchy level:

Table 3: Security Services Configuration Statements

A-C	D-G	H-M	N-R	S-Z
algorithm (Authentication Keychain)	description (Authentication Keychain)	identity	options (Security)	secret
algorithm (FIPS)	description (IKE policy)	ike	path-length	security-association (Junos OS)
authentication (Security IPsec)	dh-group	internal	perfect-forward-secrecy (Security)	security-association (Junos-FIPS Software)
authentication-algorithm (Security IKE)	direction (Junos OS)	ipsec (Security)	pki	spi (Junos OS)
authentication-algorithm (Security IPsec)	direction (FIPS)	key (Authentication Keychain)	policy (Security IKE)	spi (Junos-FIPS Software)
authentication-key-chains	dynamic	key (Junos FIPS)	policy (Security IPsec)	ssh-known-hosts
authentication-method	encoding	key-chain (Security)	pre-shared-key (Security)	start-time (Authentication Key Transmission)
auto-re-enrollment	encryption (Junos OS)	ldap-url	proposal (Security IKE)	tolerance
auxiliary-spi	encryption (FIPS)	lifetime-seconds (Security)	proposal (Security IPsec)	traceoptions
ca-identity	encryption-algorithm	local	proposals	url
ca-name	enrollment	local-certificate (Security)	protocol (Junos OS)	validity-period
ca-profile	enrollment-retry	local-key-pair	protocol (Junos-FIPS Software)	
cache-size	enrollment-url	manual (Junos OS)	re-enroll-trigger-time-percentage	
cache-timeout-negative	file	manual (Junos-FIPS Software)	re-generate-keypair	
certificate-id		maximum-certificates	refresh-interval	
certificates		mode (IKE)	retry (Adaptive Services Interface)	

Table 3: Security Services Configuration Statements *(continued)*

A-C	D-G	H-M	N-R	S-Z
certification-authority		mode (IPsec)	retry-interval	
challenge-password			revocation-check	
crl (Adaptive Services Interface)				
crl (Encryption Interface)				

Related Documentation • [\[edit security\] Hierarchy Level on page 99](#)

PART 3

Administration

- [IPsec Administrative Commands on page 175](#)
- [IPsec Monitoring Commands on page 187](#)

CHAPTER 10

IPsec Administrative Commands

- request security pki ca-certificate enroll
- request security pki ca-certificate load
- request security pki ca-certificate verify
- request security pki crl load
- request security pki generate-certificate-request
- request security pki local-certificate generate-self-signed
- request security pki local-certificate enroll
- request security pki local-certificate verify

request security pki ca-certificate enroll

Syntax	<code>request security pki ca-certificate enroll ca-profile <i>ca-profile-name</i></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Request a digital certificate from a certificate authority (CA) online by using the Simple Certificate Enrollment Protocol (SCEP).
Options	<code>ca-profile <i>ca-profile-name</i></code> —CA profile name.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• clear security pki ca-certificate on page 188• show security pki ca-certificate
List of Sample Output	request security pki ca-certificate enroll on page 176
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate enroll

```
user@host> request security pki ca-certificate enroll ca-profile entrust
Received following certificates:
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Certificate: C=us, O=juniper, CN=First Officer
Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper
Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

request security pki ca-certificate load

Syntax	<code>request security pki ca-certificate load ca-profile <i>ca-profile-name</i> filename <i>path/filename</i></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Manually load a certificate authority (CA) digital certificate from a specified location.
Options	<p>ca-profile <i>ca-profile-name</i>—Load the specified CA profile.</p> <p>filename <i>path/filename</i>—Directory location and filename of the CA digital certificate.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • clear security pki ca-certificate on page 188 • show security pki ca-certificate
List of Sample Output	request security pki ca-certificate load on page 177
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate load

```
user@host> request security pki ca-certificate load ca-profile ca-private filename pki-file
```

request security pki ca-certificate verify

Syntax	<code>request security pki ca-certificate verify ca-profile <i>ca-profile-name</i></code>
Release Information	Command introduced in Junos OS Release 8.5.
Description	Verify the digital certificate installed for the specified certificate authority (CA).
Options	ca-profile <i>ca-profile-name</i> —Name of the local digital certificate identifier.
Required Privilege Level	maintenance
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)
user@host> request security pki ca-certificate verify ca-profile ca1
```

```
CA certificate ca1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

request security pki crt load

Syntax	<code>request security pki crt load ca-profile <i>ca-profile-name</i> filename <i>path/filename</i></code>
Release Information	Command introduced in Junos OS Release 8.1.
Description	Manually install a certificate revocation list (CRL) on the router from a specified location.
Options	<code>ca-profile <i>ca-profile-name</i></code> —Load the specified certificate authority (CA) profile. <code>filename <i>path/filename</i></code> —Directory location and filename of the CRL.
Required Privilege Level	maintenance
List of Sample Output	request security pki crt load on page 179
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki crt load

```
user@host> request security pki crt load ca-profile ca-private filename pki-file
```

request security pki generate-certificate-request

Syntax	<code>request security pki generate-certificate-request certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> subject <i>subject-distinguished-name</i> <email <i>email-address</i>> <filename (<i>path</i> <i>terminal</i>)> <ip-address <i>ip-address</i>></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country <p>email <i>email-address</i>—(Optional) E-mail address of the certificate holder.</p> <p>filename (<i>path</i> <i>terminal</i>)—(Optional) Location where the local digital certificate request should be placed or the login terminal.</p> <p>ip-address <i>ip-address</i>—(Optional) IP address of the router.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• clear security pki certificate-request on page 189• show security pki certificate-request
List of Sample Output	request security pki generate-certificate-request on page 181
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-certificate-request

```
user@host> request security pki generate-certificate-request certificate-id local-entrust2
domain-name router2.example.net filename entrust-req2 subject cn=router2.example.net
```

Generated certificate request

-----BEGIN CERTIFICATE REQUEST-----

```
MIIBOTCCAQoCAQAwGjEYMBYGA1UEAxMPdHxLmp1bm1wZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFk1Qws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8E1wTJ1kmIt2cB3yi fB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8o0Xyqog8ACDFVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjA0BGNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5S0QXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH406gQ3G
3iH0Zfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteo1ZCiZ70f09Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
```

-----END CERTIFICATE REQUEST-----

Fingerprint:

```
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

request security pki local-certificate generate-self-signed

Syntax	<code>request security pki local-certificate generate-self-signed certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> ip-address <i>ip-address</i> email <i>email-address</i> subject <i>subject-distinguished-name</i></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Manually generate a self-signed certificate for the given distinguished name.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>email <i>email-address</i>—E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—IP address of the router.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country
Required Privilege Level	<p>maintenance</p> <p>security</p>
Related Documentation	<ul style="list-style-type: none">• show security pki local-certificate (View)
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert  
subject cn=abc domain-name example.net email user1@example.net  
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate enroll

Syntax	request security pki local-certificate enroll <i>ca-profile ca-profile-name</i> <i>certificate-id certificate-id-name</i> challenge-password <i>password</i> domain-name <i>domain-name</i> subject <i>subject-distinguished-name</i> <email <i>email-address</i> > <ip-address <i>ip-address</i> >
Release Information	Command introduced in Junos OS Release 7.5.
Description	Request that a certificate authority (CA) enroll and install a local digital certificate online by using the Simple Certificate Enrollment Protocol (SCEP).
Options	<p>ca-profile <i>ca-profile-name</i>—CA profile name.</p> <p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>challenge-password <i>password</i>—Password set by the administrator and normally obtained from the SCEP enrollment webpage of the CA. The password is 16 characters in length.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none"> • CN—Common name • OU—Organizational unit name • O—Organization name • ST—State • C—Country <p>email <i>email-address</i>—(Optional) E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—(Optional) IP address of the router.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • <i>show security pki local-certificate</i>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate enroll certificate-id r3-entrust-scep ca-profile  
entrust domain-name router3.example.net subject "CN=router3,OU=Engineering,O=juniper,C=US"  
challenge-password 123
```

Certificate enrollment has started. To view the status of your enrollment, check the public key infrastructure log (pkid) log file at /var/log/pkid. Please save the challenge-password for revoking this certificate in future. Note that this password is not stored on the router.

request security pki local-certificate verify

Syntax	<code>request security pki local-certificate verify certificate-id <i>certificate-id-name</i></code>
Release Information	Command introduced in Junos OS Release 8.5.
Description	Verify the validity of the local digital certificate identifier.
Options	<code>certificate-id <i>certificate-id-name</i></code> —Display the specified certificate identifier name.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> <code>show security pki local-certificate</code>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate-id bme1 (not downloaded)
user@host> request security pki local-certificate verify certificate-id bme1
```

```
Local certificate bme1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

You receive the following response after the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate bme1 (downloaded)
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1 verification success
```


CHAPTER 11

IPsec Monitoring Commands

- `clear security pki ca-certificate`
- `clear security pki certificate-request`
- `clear security pki crl`
- `clear security pki key-pair`
- `clear security pki local-certificate`
- `clear services ipsec-vpn certificates`
- `clear services ipsec-vpn ipsec statistics`
- `clear services ipsec-vpn ike security-associations`
- `clear services ipsec-vpn ipsec security-associations`

clear security pki ca-certificate

Syntax	clear security pki ca-certificate (all ca-profile <i>ca-profile-name</i>)
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete certificate authority (CA) digital certificates from the router.
Options	all —Delete all CA digital certificates from the router. ca-profile <i>ca-profile-name</i> —Delete the specified CA profile.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• request security pki ca-certificate enroll on page 176• request security pki ca-certificate load on page 177• show security pki ca-certificate
List of Sample Output	clear security pki ca-certificate all on page 188
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki ca-certificate all

```
user@host> clear security pki ca-certificate all
```


clear security pki certificate-request

Syntax	clear security pki certificate-request (all certificate-id <i>certificate-id-name</i>)
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete manually generated local digital certificate requests from the router.
Options	<p>all—Delete all local digital certificate requests from the router.</p> <p>certificate-id <i>certificate-id-name</i>—Delete the specified local digital certificate and corresponding public/private key pair.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show security pki certificate-request
List of Sample Output	clear security pki certificate-request all on page 189
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki certificate-request all

```
user@host> clear security pki certificate-request all
```

clear security pki crt

Syntax	clear security pki crt (all ca-profile <i>ca-profile-name</i>)
Release Information	Command introduced in Junos 8.1
Description	Delete certificate revocation lists (CRLs) from the router.
Options	all —Delete all CRLs from the router. ca-profile <i>ca-profile-name</i> —Delete CRLs associated with the specified CA profile.
Required Privilege Level	clear
List of Sample Output	clear security pki crt ca-profile all on page 190
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki crt ca-profile all

```
user@host> clear security pki crt ca-profile all
```

clear security pki key-pair

Syntax	clear security pki key-pair (all certificate-id <i>certificate-id-name</i>)
Release Information	Command introduced in Junos OS Release 8.5.
Description	Clear public key infrastructure (PKI) key pair information for local digital certificates from the router.
Options	<p>all—Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.</p> <p>certificate-id <i>certificate-id-name</i>—Delete the specified local digital certificate and corresponding public/private key pair.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • request security pki local-certificate enroll on page 183 • <i>show security pki local-certificate</i>
Output Fields	This command produces no output.

Sample Output

```
user@host> clear security pki key pair
```

clear security pki local-certificate

Syntax	clear security pki local-certificate <all certificate-id <i>certificate-id-name</i> system-generated>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the router.
Options	<p>all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.</p> <p>certificate-id <i>certificate-id-name</i>—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.</p> <p>system-generated—(Optional) Auto-generated self-signed certificate.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• request security pki local-certificate enroll on page 183• show security pki local-certificate
List of Sample Output	clear security pki local-certificate all on page 192
Output Fields	This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

clear services ipsec-vpn certificates

Syntax	clear services ipsec-vpn certificates (all service-set <i>service-set</i>) <certificate-cache-entry <i>number</i> >
Release Information	Command introduced in Junos OS Release 7.5.
Description	(Adaptive services interfaces only) Delete digital certificates from the IPsec configuration memory cache. Issuing this command also clears the certificate revocation list (CRL) from the cache along with the certificates.
Options	all —Delete digital certificates for all service sets. service-set <i>service-set</i> —Delete digital certificates for the specified service set.
Required Privilege Level	clear
List of Sample Output	clear services ipsec-vpn certificates all on page 193
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn certificates all

```
user@host> clear services ipsec-vpn certificates all
```

clear services ipsec-vpn ipsec statistics

Syntax	<code>clear services ipsec-vpn ipsec statistics</code> <code><remote-gateway address></code> <code><service-set service-set-name></code>
Release Information	Command introduced in Junos OS Release 8.1.
Description	(Adaptive services interface only) Clear IP Security (IPsec) statistics.
Options	remote-gateway address —(Optional) Clear statistics for the specified remote system. service-set service-set-name —(Optional) Clear statistics for the specified service set.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>show services ipsec-vpn ipsec statistics</i>
List of Sample Output	clear services ipsec-vpn ipsec statistics on page 194
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec statistics

```
user@host> clear services ipsec-vpn ipsec statistics
```

clear services ipsec-vpn ike security-associations

Syntax	clear services ipsec-vpn ike security-associations <peer-address-name> <service-set service-set-name>
Release Information	Command introduced before Junos OS Release 7.4. service-set option added in Junos OS Release 8.5.
Description	(Adaptive services interfaces only) Clear Internet Key Exchange (IKE) security associations.
Options	<p>peer-address-name—(Optional) Clear only the security association specified by the peer address.</p> <p>service-set service-set-name—(Optional) Clear only the security association specified by the service-set name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>show services ipsec-vpn ike security-associations</i>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ike security-associations

```
user@host> clear services ipsec-vpn ike security-associations
```

clear services ipsec-vpn ipsec security-associations

Syntax	<code>clear services ipsec-vpn security-associations</code> <code><peer-address-name></code> <code><remote-gateway remote-gateway-address></code> <code><service-set-name></code> <code><tunnel-index tunnel-index-number></code>
Release Information	Command introduced before Junos OS Release 7.4. remote-gateway , service-set-name , and tunnel-index options added in Junos OS Release 8.4.
Description	(Adaptive services interfaces only) Clear IP Security (IPsec) security associations. You can combine the options for greater specificity.
Options	<p>peer-address-name—(Optional) Clear only the security association specified by the peer address.</p> <p>remote-gateway remote-gateway-address—(Optional) Clear only the security association specified by the remote gateway address.</p> <p>service-set-name—(Optional) Clear only the security association specified by the service-set name.</p> <p>tunnel-index tunnel-index-number—(Optional) Clear only the security association specified by the tunnel index number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"><code>show services ipsec-vpn ipsec security-associations</code>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec security-associations

```
user@host> clear services ipsec-vpn ipsec security-associations
```


PART 3

Index

- [Index on page 199](#)

Index

Symbols

#, comments in configuration statements.....	xviii
(), in syntax descriptions.....	xviii
< >, in syntax descriptions.....	xviii
[], in configuration statements.....	xviii
{ }, in configuration statements.....	xviii
(pipe), in syntax descriptions.....	xviii

A

algorithm statement.....	102
IPsec.....	104
Junos-FIPS software.....	103
usage guidelines.....	36
associations, clearing.....	196
authentication key update mechanism.....	71
authentication statement	
IPsec.....	104
usage guidelines.....	20, 25
authentication-algorithm statement	
IKE.....	105
usage guidelines.....	27
IPsec.....	106
usage guidelines.....	32
authentication-key-chains statement.....	108
authentication-method statement	
IKE.....	109
usage guidelines.....	27
auto-re-enrollment statement.....	110
auxiliary-spi statement.....	111
usage guidelines.....	19, 24

B

braces, in configuration statements.....	xviii
brackets	
angle, in syntax descriptions.....	xviii
square, in configuration statements.....	xviii

C

ca-identity statement.....	111
usage guidelines.....	53

ca-name statement.....	112
usage guidelines.....	46
ca-profile statement.....	113
usage guidelines.....	53
cache-size statement.....	114
usage guidelines.....	48
cache-timeout-negative statement.....	115
usage guidelines.....	48
certificate-id statement.....	116
certificates	
PKI	
CA certificates, clearing.....	188
CA certificates, loading manually.....	177
certificate revocation lists, clearing.....	190
certificate revocation lists, loading	
manually.....	179
local certificates, clearing.....	191, 192
local certificates, requesting	
manually.....	180, 182
local certificates, requesting online.....	176
local certificates, requesting that CA	
install.....	183
local certificates, requests, clearing.....	189
certificates statement.....	117
usage guidelines.....	75
certification-authority statement.....	118
usage guidelines.....	46
challenge-password statement.....	119
clear security pki ca-certificate command.....	188
clear security pki certificate-request	
command.....	189
clear security pki crl command.....	190
clear security pki key-pair.....	191
clear security pki local-certificate command.....	192
clear services ipsec-vpn certificates	
command.....	193
clear services ipsec-vpn ike security-associations	
command.....	195
clear services ipsec-vpn ipsec security-associations	
command.....	196
clear services ipsec-vpn ipsec statistics	
command.....	194
comments, in configuration statements.....	xviii
conventions	
text and syntax.....	xvii
crl statement	
AS and MultiServices PICs.....	120
ES PIC.....	121

usage guidelines (AS and Multiservices PICs).....	54
usage guidelines (ES PIC).....	46
curly braces, in configuration statements.....	xviii
customer support.....	xix
contacting JTAC.....	xix

D

DDoS protection statements	
global.....	77
logical-interface.....	78
no-flow-logging.....	79
physical-interface.....	80
priority.....	81
protocols.....	82
recover-time.....	91
subscriber.....	92
timeout-active-flows.....	93
traceoptions.....	94
violation-report-rate.....	96
description statement.....	121
IKE policy.....	122
usage guidelines.....	30
IKE proposal.....	122
usage guidelines.....	28
IPsec policy.....	122
usage guidelines.....	34
IPsec proposal.....	122
usage guidelines.....	33
IPsec SA.....	122
usage guidelines.....	16
usage guidelines.....	16, 28, 33
dh-group statement.....	122
usage guidelines.....	28
direction statement	
Junos OS.....	123
Junos-FIPS software.....	124
usage guidelines.....	18, 22, 37
direction, IPsec.....	37
documentation	
comments on.....	xix
dynamic security associations.....	26
dynamic security associations (IPsec).....	21, 26
dynamic statement.....	125
usage guidelines.....	21, 26

E

enable-timeout-active statement	
DDoS protection flow detection.....	93

encoding statement.....	126
usage guidelines	
certificate authority.....	47
IKE policy.....	50
encryption statement	
Junos OS.....	127
Junos-FIPS software.....	128
usage guidelines.....	20, 25, 36
encryption-algorithm statement.....	129
usage guidelines	
IKE.....	28
IPsec.....	33
encryption-algorithm statement (IKE)	
usage guidelines.....	28
enrollment statement.....	130
usage guidelines.....	53
enrollment-retry statement.....	131
usage guidelines.....	48
enrollment-url statement.....	131
usage guidelines.....	47
ES PIC.....	51

F

file statement	
security	
usage guidelines.....	47
security certificate.....	132
flow detection, DDoS protection statements	
logical-interface.....	78
no-flow-logging.....	79
physical-interface.....	80
subscriber.....	92
timeout-active-flows.....	93
violation-report-rate.....	96
font conventions.....	xvii

G

global statement	
DDoS protection.....	77

I

identity statement.....	132
usage guidelines.....	50
IKE.....	8, 26
adaptive services interfaces	
security associations, clearing.....	195
statistics, clearing.....	194
authentication algorithm.....	27
authentication method.....	27

Diffie-Hellman group.....	28	minimum configurations	
dynamic SAs.....	26	dynamic SA	14
encryption algorithm.....	28	manual SA	13
encryption-algorithm statement		overview.....	3
usage guidelines.....	28	Perfect Forward Secrecy.....	34
lifetime statement		policy.....	34
usage guidelines.....	29	proposal.....	32
policy configuration, example.....	31	proposal description.....	33
policy description.....	30	SA description.....	16
policy mode.....	30	security associations.....	7
policy statement		security parameter index.....	19, 24
usage guidelines.....	29	SPI.....	38
preshared key.....	30	IPsec services	
proposal description.....	28	adaptive services interfaces	
proposals associated with policy.....	31	IKE security associations, clearing.....	195
SA lifetime.....	29	IPSec security associations, clearing.....	196
ike statement.....	133	IPSec statistics, clearing.....	194
usage guidelines	26	ipsec statement.....	135
internal statement.....	134	usage guidelines.....	15
usage guidelines.....	36	ipsec-policy statement.....	125
IPsec		usage guidelines.....	21, 26
algorithm.....	104		
authentication.....	20, 25	J	
authentication algorithm.....	32	Junos XML protocol xnm-ssl service.....	75
auxiliary security parameter index.....	19, 24	Junos-FIPS	
configuring internal.....	36	IPsec requirements.....	3
digital certificates, configuring (AS and			
Multiservices PICs).....	51	K	
digital certificates, configuring (ES PIC).....	45	key statement.....	137, 138
direction.....	18, 22, 36	usage guidelines.....	38
direction of processing.....	18, 22	key, IPsec.....	38
dynamic security associations.....	21, 26	key-chain statement.....	139
encryption.....	20, 25, 36, 128		
encryption algorithm.....	33, 36	L	
ES PIC.....	51	ldap-url statement.....	140
example.....	39	usage guidelines.....	47
inbound traffic filter, applying.....	66	lifetime-seconds statement.....	140
inbound traffic filter, configuring.....	64	usage guidelines	
outbound traffic filter, applying.....	64	IKE.....	29
outbound traffic filter, configuring.....	63	IPsec.....	33
example configuration		local statement.....	141
outbound traffic.....	63	usage guidelines.....	75
IKE.....	8	local-certificate statement.....	142
internal.....	36	usage guidelines.....	50
key.....	38	local-key-pair statement.....	142
lifetime of SA.....	33	usage guidelines.....	50
manual.....	17, 22, 36	logical-interface statement	
		DDoS protection flow detection.....	78

M

manual security association.....	17, 22
manual statement	
Junos OS.....	143
Junos-FIPS software.....	144
usage guidelines.....	17, 22, 36
manuals	
comments on.....	xix
maximum-certificates statement.....	145
usage guidelines.....	49
mode statement	
IKE.....	146
usage guidelines.....	30
IPsec.....	147

N

no-flow-logging statement	
DDoS protection flow detection.....	79

O

options statement.....	148
------------------------	-----

P

parentheses, in syntax descriptions.....	xviii
path-length statement.....	149
usage guidelines.....	49
perfect-forward-secrecy statement.....	149
usage guidelines.....	34
physical-interface statement	
DDoS protection flow detection.....	80
PKI See certificates, PKI	
pki statement.....	150
policy statement	
IKE.....	151
usage guidelines, digital certificates (ES	
PIC).....	49
usage guidelines, preshared keys.....	29
IPsec.....	152
usage guidelines.....	34
pre-shared-key statement.....	152
usage guidelines.....	30
priority statement	
DDoS protection.....	81
proposal statement	
IKE.....	153
usage guidelines.....	26
IPsec.....	153
usage guidelines.....	32

proposals statement.....	154
usage guidelines	
IKE.....	31
IPsec.....	34
protocol	
for dynamic SA.....	34
for internal SA.....	36, 156
for manual SA.....	19, 23
protocol statement	
Junos OS.....	155
Junos-FIPS software.....	156
usage guidelines	
dynamic SA.....	34
internal SA.....	36
manual SA.....	19, 23
protocols statement	
DDoS protection.....	82

R

re-enroll-trigger-time-percentage statement.....	156
re-generate-keypair statement.....	157
recover-time statement	
DDoS protection.....	91
refresh-interval statement.....	157
usage guidelines.....	55
replay-window-size statement.....	125
usage guidelines.....	21, 26
request security certificate command.....	43
usage guidelines.....	43
request security key-pair	
usage guidelines.....	43
request security pki ca-certificate enroll	
command.....	176
request security pki ca-certificate load	
command.....	177
request security pki ca-certificate verify	
command.....	178
request security pki crl load command.....	179
request security pki generate-certificate-request	
command.....	180
request security pki local-certificate enroll	
command.....	183
request security pki local-certificate	
generate-self-signed command.....	182
request security pki local-certificate verify	
command.....	185
retry statement.....	158
usage guidelines.....	54

retry-interval statement.....	158
usage guidelines.....	54
revocation-check statement.....	159

S

SCP.....	73
secret statement.....	160
secure copy See SCP	
security	
tracing operations.....	67
security association statement	
usage guidelines.....	36
security services configuration guidelines.....	99
security-association statement	
Junos OS.....	161
Junos-FIPS software.....	162
usage guidelines.....	15
SPI	
IPsec.....	38
spi statement	
Junos OS.....	163
Junos-FIPS software.....	163
usage guidelines	19, 24, 38
ssh-known-hosts statement.....	164
usage guidelines.....	73
start-time statement.....	165
subscriber statement	
DDoS protection flow detection.....	92
support, technical See technical support	
syntax conventions.....	xvii

T

technical support	
contacting JTAC.....	xix
tolerance statement.....	166
traceoptions statement	
DDoS protection.....	94
security.....	167
usage guidelines.....	67
tracing operations	
security.....	67
traffic	
inbound (application of filter).....	66
inbound (decryption).....	64
outbound (application of filter).....	64
outbound (encryption).....	63

U

url statement.....	169
--------------------	-----

V

validity-period statement.....	169
violation-report-rate statement	
DDoS protection flow detection.....	96

