

# Encryption Properties



---

Published: 2012-02-28

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

#### *Encryption Properties*

Copyright © 2012, 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 . . . . .	ix
	Documentation and Release Notes . . . . .	ix
	Supported Platforms . . . . .	ix
	Using the Examples in This Manual . . . . .	ix
	Merging a Full Example . . . . .	x
	Merging a Snippet . . . . .	x
	Documentation Conventions . . . . .	xi
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiii
	Opening a Case with JTAC . . . . .	xiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Encryption Services . . . . .</b>	<b>3</b>
	Encryption Overview . . . . .	3
	Configuring an ES Tunnel Interface for a Layer 3 VPN . . . . .	3
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 2</b>	<b>Configuration Tasks . . . . .</b>	<b>7</b>
	Configuring Encryption Interfaces . . . . .	7
	Specifying the Security Association Name for Encryption Interfaces . . . . .	8
	Configuring the MTU for Encryption Interfaces . . . . .	8
	Example: Configuring an Encryption Interface . . . . .	8
	Configuring Filters for Traffic Transiting the ES PIC . . . . .	8
	Traffic Overview . . . . .	9
	Configuring the Security Association . . . . .	10
	Configuring an Outbound Traffic Filter . . . . .	10
	Example: Configuring an Outbound Traffic Filter . . . . .	11
	Applying the Outbound Traffic Filter . . . . .	11
	Example: Applying the Outbound Traffic Filter . . . . .	11
	Configuring an Inbound Traffic Filter . . . . .	12
	Example: Configuring an Inbound Traffic Filter . . . . .	12
	Applying the Inbound Traffic Filter to the Encryption Interface . . . . .	13
	Example: Applying the Inbound Traffic Filter to the Encryption Interface . . . . .	13
	Configuring ES PIC Redundancy . . . . .	14
	Example: Configuring ES PIC Redundancy . . . . .	14
	Configuring IPsec Tunnel Redundancy . . . . .	15

<b>Chapter 3</b>	<b>Configuration Statements</b> . . . . .	<b>17</b>
	address . . . . .	17
	backup-destination . . . . .	18
	backup-interface . . . . .	18
	destination . . . . .	19
	es-options . . . . .	19
	family . . . . .	20
	filter . . . . .	21
	interfaces . . . . .	21
	ipsec-sa . . . . .	22
	source . . . . .	22
	tunnel . . . . .	23
	unit . . . . .	24
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>IP Security Operational Mode Commands</b> . . . . .	<b>27</b>
	clear ike security-associations . . . . .	28
	clear ipsec security-associations . . . . .	29
	request security certificate (signed) . . . . .	31
	request security certificate (unsigned) . . . . .	32
	request security key-pair . . . . .	33
	request ipsec switch . . . . .	34
	request system certificate add . . . . .	35
	show ike security-associations . . . . .	36
	show ipsec certificates . . . . .	40
	show ipsec redundancy . . . . .	43
	show ipsec security-associations . . . . .	45
	show system certificate . . . . .	48
<b>Chapter 5</b>	<b>Encryption Interface Operational Mode Commands</b> . . . . .	<b>51</b>
	show interfaces (Encryption) . . . . .	52
<b>Part 4</b>	<b>Index</b>	
	Index . . . . .	61

# List of Figures

Part 2	Configuration	
Chapter 2	Configuration Tasks .....	7
	Figure 1: Example: IPsec Tunnel Connecting Security Gateways .....	9
	Figure 2: IPsec Tunnel Redundancy .....	15



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>ix</b>
	Table 1: Notice Icons . . . . .	xi
	Table 2: Text and Syntax Conventions . . . . .	xi
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 4</b>	<b>IP Security Operational Mode Commands . . . . .</b>	<b>27</b>
	Table 3: show ike security-associations Output Fields . . . . .	36
	Table 4: show ipsec certificates Output Fields . . . . .	40
	Table 5: show ipsec redundancy Output Fields . . . . .	43
	Table 6: show ipsec security-associations Output Fields . . . . .	45
	Table 7: show system certificate Output Fields . . . . .	48
<b>Chapter 5</b>	<b>Encryption Interface Operational Mode Commands . . . . .</b>	<b>51</b>
	Table 8: Encryption show interfaces Output Fields . . . . .	52





# About the Documentation

- [Documentation and Release Notes on page ix](#)
- [Supported Platforms on page ix](#)
- [Using the Examples in This Manual on page ix](#)
- [Documentation Conventions on page xi](#)
- [Documentation Feedback on page xiii](#)
- [Requesting Technical Support on page xiii](#)

## 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](#)
- [T Series](#)
- [J Series](#)
- [MX Series](#)

## Using the Examples in This Manual

---

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

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

## Merging a Full Example

To merge a full example, follow these steps:

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

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

```
system {
  scripts {
    commit {
      file ex-script.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 [Junos OS CLI User Guide](#).

## Documentation Conventions

Table 1 on page xi 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.

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b> No alarms currently active

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

Convention	Description	Examples
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<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@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(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.	<b>broadcast   multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [</b> <i>community-ids</i> <b>]</b>
Indentation and braces ( { } )	Identify 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.	
<b>J-Web GUI Conventions</b>		
<b>Bold text like this</b>	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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 JNASC 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: <https://www.juniper.net/alerts/>

- 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

- [Encryption Services on page 3](#)





## CHAPTER 1

# Encryption Services

- [Encryption Overview on page 3](#)
- [Configuring an ES Tunnel Interface for a Layer 3 VPN on page 3](#)

## Encryption Overview

---

The IP Security (IPsec) architecture provides a security suite for the IP version 4 (IPv4) and IP version 6 (IPv6) network layers. The suite provides functionality such as authentication of origin, data integrity, confidentiality, replay protection, and nonrepudiation of source. It also defines mechanisms for key generation and exchange, management of security associations, and support for digital certificates.

IPsec defines a security association (SA) 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. For more information, see the [Junos OS System Basics Configuration Guide](#). The standards are defined in the following RFCs:

- RFC 2401, *Security Architecture for the Internet Protocol*
- RFC 2406, *IP Encapsulating Security Payload (ESP)*

## Configuring an ES Tunnel Interface 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. For more information about configuring an ES tunnel for a Layer 3 VPN, see the [Junos OS VPNs Configuration Guide](#).



## PART 2

# Configuration

- [Configuration Tasks on page 7](#)
- [Configuration Statements on page 17](#)



## CHAPTER 2

# Configuration Tasks

- [Configuring Encryption Interfaces on page 7](#)
- [Configuring Filters for Traffic Transiting the ES PIC on page 8](#)
- [Configuring ES PIC Redundancy on page 14](#)
- [Configuring IPsec Tunnel Redundancy on page 15](#)

## Configuring Encryption Interfaces

---

When you configure the encryption interface, you associate the configured SA with a logical interface. This configuration defines the tunnel, including the logical unit, tunnel addresses, maximum transmission unit (MTU), optional interface addresses, and the name of the IPsec SA to apply to traffic. To configure an encryption interface, include the following statements at the `[edit interfaces es-fpc/pic/port unit logical-unit-number]` hierarchy level:

```
family inet {
  ipsec-sa ipsec-sa; # name of security association to apply to packet
  address address; # local interface address inside local VPN
  destination address; # destination address inside remote VPN
}
tunnel {
  source source-address;
  destination destination-address;
}
```

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



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

The ES Physical Interface Card (PIC) is supported on M Series and T Series routers.

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.

## Specifying the Security Association Name for Encryption Interfaces

The security association is the set of properties that defines the protocols for encrypting Internet traffic. To configure encryption interfaces, you specify the SA name associated with the interface by including the **ipsec-sa** statement at the **[edit interfaces es-fpc/pic/port unit logical-unit-number family inet]** hierarchy level:

```
ipsec-sa sa-name;
```

For information about configuring the security association, see [“Configuring Filters for Traffic Transiting the ES PIC” on page 8](#).

## Configuring the MTU for Encryption Interfaces

The protocol MTU value for encryption interfaces must always be less than the default interface MTU value of 3900 bytes; the configuration fails to commit if you select a greater value. To set the MTU value, include the **mtu** statement at the **[edit interfaces interface-name unit logical-unit-number family inet]** hierarchy level:

```
mtu bytes;
```

For more information, see the [Junos OS Network Interfaces Configuration Guide](#).

## Example: Configuring an Encryption Interface

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 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      ipsec-sa manual-sa1; # name of security association to apply to packet
      mtu 3800;
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
    }
  }
}
```

---

## Configuring Filters for Traffic Transiting the ES PIC

This section contains the following topics:

- [Traffic Overview on page 9](#)
- [Configuring the Security Association on page 10](#)

- [Configuring an Outbound Traffic Filter on page 10](#)
- [Applying the Outbound Traffic Filter on page 11](#)
- [Configuring an Inbound Traffic Filter on page 12](#)
- [Applying the Inbound Traffic Filter to the Encryption Interface on page 13](#)

## Traffic Overview

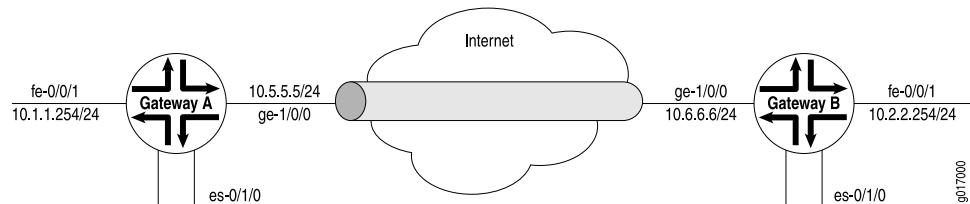
Traffic configuration defines the traffic that must flow through the tunnel. You configure outbound and inbound firewall filters, which identify and direct traffic to be encrypted and confirm that decrypted traffic parameters match those defined for the given tunnel. The outbound filter is applied to the LAN or WAN interface for the incoming traffic you want to encrypt. 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.



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

In [Figure 1 on page 9](#), 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. For more information about firewalls, see the [Junos OS Policy Framework Configuration Guide](#).

**Figure 1: Example: IPsec Tunnel Connecting Security Gateways**



The SA and ES interface for security 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 10.2.2.254;  
    }  
  }  
}
```

## Configuring the Security Association

To configure the SA, include the **security-association** statement at the **[edit security]** hierarchy level:

```
security-association name {  
  mode (tunnel | transport);  
  manual {  
    direction (inbound | outbound | bi-directional) {  
      auxiliary-spi auxiliary-spi-value;  
      spi spi-value;  
      protocol (ah | esp | bundle);  
      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);  
      }  
    }  
    dynamic {  
      replay-window-size (32 | 64);  
      ipsec-policy policy-name;  
    }  
  }  
}
```

For more information about configuring an SA, see the [Junos OS System Basics Configuration Guide](#). For information about applying the SA to an interface, see “[Specifying the Security Association Name for Encryption Interfaces](#)” on page 8.

## Configuring an Outbound Traffic Filter

To configure the outbound traffic filter, include the **filter** statement at the **[edit firewall]** hierarchy level:

```
filter filter-name {  
  term term-name {  
    from {  
      match-conditions;  
    }  
    then {
```



```

        action;
        action-modifiers;
    }
}

```

For more information, see the [Junos OS Policy Framework Configuration Guide](#).

### 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 9](#)). 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 virtual private network (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.

### Applying the Outbound Traffic Filter

After you have configured the outbound firewall filter, you apply it by including the **filter** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level:

```

filter {
  input filter-name;
}

```

### Example: Applying the Outbound Traffic Filter

Apply the outbound traffic filter. 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. So, 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 end point; add a static route if necessary.

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

## Configuring an Inbound Traffic Filter

To configure an inbound traffic filter, include the **filter** statement at the **[edit firewall]** hierarchy level:

```
filter filter-name {
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
  }
}
```

For more information, see the *Junos OS Policy Framework Configuration Guide*.

---

### Example: Configuring an Inbound Traffic Filter

Configure an inbound firewall filter. This filter performs the final IPsec policy check and is created on security gateway A. The policy check ensures that only packets that match the traffic configured for this tunnel are accepted.

```
[edit firewall]
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;

## Applying the Inbound Traffic Filter to the Encryption Interface

After you create the inbound firewall filter, you can apply it to the ES PIC. To apply the filter to the ES PIC, include the **filter** statement at the **[edit interfaces es-fpc/pic/port unit logical-unit-number family inet filter]** hierarchy level:

```
filter {
  input filter;
}
```

The input filter is the name of the filter applied to received traffic. For a configuration example, see “[Example: Configuring an Inbound Traffic Filter](#)” on page 12. For more information about firewall filters, see the *Junos OS Policy Framework Configuration Guide*.

### Example: Applying the Inbound Traffic Filter to the Encryption Interface

Apply the inbound firewall filter (**ipsec-decrypt-policy-filter**) to 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.

The Packet Forwarding Engine directs IPsec packets to the ES PIC. It uses the packet's security parameter index (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. For information about **term1**, see “[Example: Configuring an Inbound Traffic Filter](#)” on page 12.



**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.

```
[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
      }
    }
  }
}
```

```
    }  
  }  
}
```

## Configuring ES PIC Redundancy

---

You can configure ES PIC redundancy on M Series and T Series routers that have multiple ES PICs. With ES PIC redundancy, one ES PIC is active and another ES PIC is on standby. When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and SAs, and acts as the new next hop for IPsec traffic. Reestablishment of tunnels on the backup ES PIC does not require new Internet Key Exchange (IKE) negotiations. If the primary ES PIC comes online, it remains in standby and does not preempt the backup. To determine which PIC is currently active, use the **show ipsec redundancy** command.



**NOTE:** ES PIC redundancy is supported on M Series and T Series routers.

To configure an ES PIC as the backup, include the **backup-interface** statement at the **[edit interfaces fpc/pic/port es-options]** hierarchy level:

```
backup-interface es-fpc/pic/port;
```

## Example: Configuring ES PIC Redundancy

After you create the inbound firewall filter, apply it to the master 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. This example does not show SA and filter configuration. For information about SA and filter configuration, see the [Junos OS System Basics Configuration Guide](#), the [Junos OS Policy Framework Configuration Guide](#), and “Example: Configuring an Inbound Traffic Filter” on page 12.

```
[edit interfaces]  
es-1/2/0 {  
  es-options {  
    backup-interface es-1/0/0;  
  }  
  unit 0 {  
    tunnel {  
      source 10.5.5.5;  
      destination 10.6.6.6;  
    }  
    family inet {  
      ipsec-sa manual-sa1;  
      filter {  
        input ipsec-decrypt-policy-filter;  
      }  
      address 10.1.1.8/32 {  
        destination 10.2.2.254;  
      }  
    }  
  }  
}
```

```

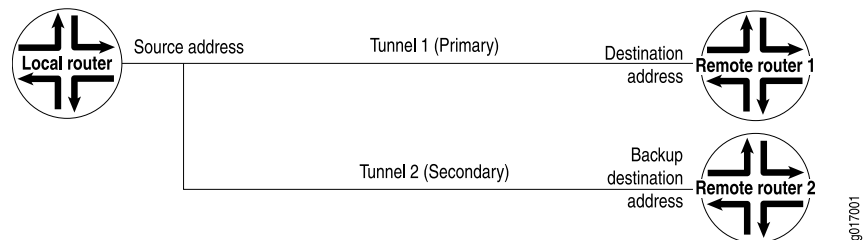
    }
  }
}

```

## Configuring IPsec Tunnel Redundancy

You can configure IPsec tunnel redundancy by specifying a backup destination address. The local router sends keepalives to determine the remote site's reachability. When the peer is no longer reachable, a new tunnel is established. For up to 60 seconds during failover, traffic is dropped without notification being sent. [Figure 2 on page 15](#) shows IPsec primary and backup tunnels.

**Figure 2: IPsec Tunnel Redundancy**



To configure IPsec tunnel redundancy, include the **backup-destination** statement at the **[edit interfaces unit *logical-unit-number* tunnel]** hierarchy level:

```

backup-destination address;
destination address;
source address;

```



**NOTE:** Tunnel redundancy is supported on M Series and T Series routers.

The primary and backup destinations must be on different routers.

The tunnels must be distinct from each other and policies must match.

For more information about tunnels, see Tunnel Properties.



## CHAPTER 3

# Configuration Statements

### address

---

<b>Syntax</b>	<code>address <i>address</i> {     <i>destination address</i>; }</code>
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> <a href="#">unit</a> <i>logical-unit-number</i> <a href="#">family</a> <i>family</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure the interface address.
<b>Options</b>	<b><i>address</i></b> —Address of the interface.  The remaining statement is explained separately.
<b>Usage Guidelines</b>	See <a href="#">“Configuring Encryption Interfaces” on page 7</a> .
<b>Required Privilege Level</b>	<b>interface</b> —To view this statement in the configuration. <b>interface-control</b> —To add this statement to the configuration.

## backup-destination

---

<b>Syntax</b>	<code>backup-destination <i>destination-address</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">unit logical-unit-number tunnel</a> ],[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For tunnel interfaces, specify the remote address of the backup tunnel.
<b>Options</b>	<i>destination-address</i> —Address of the remote side of the connection.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring IPsec Tunnel Redundancy</a> ” on page 15.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">destination on page 19</a></li><li>• destination (Tunnel Remote End)</li></ul>

## backup-interface

---

<b>Syntax</b>	<code>backup-interface <i>interface-name</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <a href="#">es-options</a> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure a backup ES Physical Interface Card (PIC). When the primary ES PIC has a servicing failure, the backup becomes active, inherits all the tunnels and security associations (SAs), and acts as the new next hop for IPsec traffic.
<b>Options</b>	<i>interface-name</i> —Name of ES interface to serve as the backup.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring ES PIC Redundancy</a> ” on page 14.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.



## destination

---

<b>Syntax</b>	<code>destination <i>destination-address</i>;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>address</b> <i>address</i> ], [edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For tunnel and encryption interfaces, specify the remote address.
<b>Options</b>	<b><i>destination-address</i></b> —Address of the remote side of the connection.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Encryption Interfaces</a> ” on page 7, Configuring Traffic Sampling, and Configuring Flow Monitoring.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## es-options

---

<b>Syntax</b>	<code>es-options {     <b>backup-interface</b> <i>interface-name</i>; }</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	On ES interfaces, configure ES interface-specific interface properties.  The <b>backup-interface</b> statement is explained separately.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring ES PIC Redundancy</a> ” on page 14.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## family

---

Syntax	<pre>family inet {     ipsec-sa sa-name; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure protocol family information for the logical interface.
Options	<p><b>family</b>—Protocol family:</p> <ul style="list-style-type: none"><li>• <b>ccc</b>—Circuit cross-connect protocol suite</li><li>• <b>inet</b>—IP version 4 suite</li><li>• <b>inet6</b>—IP version 6 suite</li><li>• <b>iso</b>—Open Systems Interconnection (OSI) International Organization for Standardization (ISO) protocol suite</li><li>• <b>mlfr-end-to-end</b>—Multilink Frame Relay FRF.15</li><li>• <b>mlfr-uni-nni</b>—Multilink Frame Relay FRF.16</li><li>• <b>multilink-ppp</b>—Multilink Point-to-Point Protocol</li><li>• <b>mpls</b>—MPLS</li><li>• <b>tcc</b>—Translational cross-connect protocol suite</li><li>• <b>tnp</b>—Trivial Network Protocol</li><li>• <b>vpls</b>—Virtual private LAN service</li></ul> <p>The remaining statements are explained separately.</p>
Usage Guidelines	See “ <a href="#">Configuring Encryption Interfaces</a> ” on page 7; for a general discussion of <b>family</b> statement options, see the <a href="#">Junos OS Network Interfaces Configuration Guide</a> .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• <a href="#">Junos OS Network Interfaces Configuration Guide</a> for other statements that do not affect services interfaces.

## filter

---

<b>Syntax</b>	filter { input <i>filter-name</i> ; output <i>filter-name</i> ; }
<b>Hierarchy Level</b>	[edit <a href="#">interfaces</a> <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Define the filters to be applied on an interface.
<b>Options</b>	<b>input <i>filter-name</i></b> —Identifier for the input filter.  <b>output <i>filter-name</i></b> —Identifier for the output filter.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Filters for Traffic Transiting the ES PIC</a> ” on page 8.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## interfaces

---

<b>Syntax</b>	interfaces { ... }
<b>Hierarchy Level</b>	[edit]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Configure interfaces on the router.
<b>Default</b>	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
<b>Usage Guidelines</b>	See the <a href="#">Junos OS Network Interfaces Configuration Guide</a> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## ipsec-sa

---

<b>Syntax</b>	<code>ipsec-sa sa-name;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>es-fpc/pic/port</i> <b>unit</b> <i>logical-unit-number</i> family inet]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	Specify the IP Security (IPsec) SA name associated with the interface.
<b>Options</b>	<b>sa-name</b> —IPsec SA name.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Encryption Interfaces</a> ” on page 7.
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Junos OS System Basics Configuration Guide</a></li></ul>

## source

---

<b>Syntax</b>	<code>source source-address;</code>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> <b>family</b> inet <b>address</b> <i>address</i> ], [edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> tunnel]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	For tunnel and encryption interfaces, specify the source address.
<b>Options</b>	<b>source-address</b> —Address of the source side of the connection.
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Encryption Interfaces</a> ” on page 7, <a href="#">Configuring Traffic Sampling</a> , and <a href="#">Configuring Flow Monitoring</a> .
<b>Required Privilege Level</b>	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

## tunnel

---

<b>Syntax</b>	<pre> tunnel {   backup-destination destination-address;   destination destination-address;   routing-instance {     destination routing-instance-name;   }   source source-address;   ttl number; } </pre>
<b>Hierarchy Level</b>	[edit interfaces <i>interface-name</i> <b>unit</b> <i>logical-unit-number</i> ]
<b>Release Information</b>	Statement introduced before Junos OS Release 7.4.
<b>Description</b>	<p>Configure a tunnel. You can use the tunnel for unicast and multicast traffic or just for multicast traffic. You can also use tunnels for encrypted traffic or virtual private networks (VPNs).</p> <p>The statements are explained separately.</p>
<b>Usage Guidelines</b>	See “ <a href="#">Configuring Encryption Interfaces</a> ” on page 7 and Tunnel Properties.
<b>Required Privilege Level</b>	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">Junos OS VPNs Configuration Guide</a></li> </ul>

## unit

---

**Syntax**    `unit logical-unit-number {  
              family inet {  
                  ipsec-sa sa-name;  
              }  
              tunnel {  
                  backup-destination destination-address;  
                  destination destination-address;  
                  routing-instance {  
                      destination routing-instance-name;  
                  }  
                  source source-address;  
                  ttl number;  
              }  
          }`

**Hierarchy Level**    [edit [interfaces](#) *interface-name*]

**Release Information**    Statement introduced before Junos OS Release 7.4.

**Description**    Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

**Options**    *logical-unit-number*—Number of the logical unit.

**Range:** 0 through 16,384

The remaining statements are explained separately.

**Usage Guidelines**    See “[Configuring Encryption Interfaces](#)” on page 7; for a general discussion of logical interface properties, see the [Junos OS Network Interfaces Configuration Guide](#).

**Required Privilege**    interface—To view this statement in the configuration.

**Level**    interface-control—To add this statement to the configuration.

**Related Documentation**

- [Junos OS Network Interfaces Configuration Guide](#) for other statements that do not affect services interfaces.

## PART 3

# Administration

- [IP Security Operational Mode Commands on page 27](#)
- [Encryption Interface Operational Mode Commands on page 51](#)





## CHAPTER 4

# IP Security Operational Mode Commands

## clear ike security-associations

---

<b>Syntax</b>	clear ike security-associations <destination-ip-address>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(Encryption interface on M Series and T Series routers only) Clear information about the current Internet Key Exchange (IKE) security association. This command is valid for dynamic security associations only.
<b>Options</b>	<b>none</b> —Clear all IKE security associations.  <b>destination-ip-address</b> —(Optional) Clear the IKE security association at the specified destination address.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show ike security-associations on page 36</a></li></ul>
<b>List of Sample Output</b>	<a href="#">clear ike security-associations on page 28</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

clear ike security-associations	user@host> clear ike security-associations
---------------------------------	--

## clear ipsec security-associations

<b>Syntax</b>	<code>clear ipsec security-associations</code> <code>&lt;sa-name&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(Encryption interface on M Series and T Series routers only) Clear information about the current IP Security (IPsec) security association. This command is valid for dynamic security associations only. When this command is issued, a new security association is created.
<b>Options</b>	<b>none</b> —Clear all IPsec security associations.  <b>sa-name</b> —(Optional) Clear the specified security association.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">show ipsec security-associations on page 45</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">clear ipsec security-associations on page 29</a>
<b>Output Fields</b>	See the <a href="#">show ipsec security-associations</a> for an explanation of output fields.

## Sample Output

**clear ipsec security-associations** The following output from the **show ipsec security-associations detail** command is displayed before and after the **clear ipsec security-associations** command is issued:

```
user@host> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up

Direction: inbound, SPI: 242379418, State: Installed
Mode: tunnel, Type: dynamic
Protocol: ESP, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expires in 22979 seconds
Hard lifetime: Expires in 28739 seconds

Direction: outbound, SPI: 368592771, State: Installed
Mode: tunnel, Type: dynamic
Protocol: ESP, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expires in 22979 seconds
Hard lifetime: Expires in 28739 seconds

user@host> clear ipsec security-associations

user@host> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up

Direction: inbound, SPI: 1031597683, State: Installed
Mode: tunnel, Type: dynamic
Protocol: ESP, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expires in 23037 seconds
```

Hard lifetime: Expires in 28797 seconds

Direction: outbound, SPI: 1618419878, State: Installed

Mode: tunnel, Type: dynamic

Protocol: ESP, Authentication: hmac-md5-96, Encryption: None

Soft lifetime: Expires in 23037 seconds

Hard lifetime: Expires in 28797 seconds

## request security certificate (signed)

<b>Syntax</b>	<code>request security certificate enroll filename <i>filename</i> subject <i>subject</i> alternative-subject <i>alternative-subject</i> certification-authority <i>certification-authority</i> encoding (binary   pem) key-file <i>key-file</i> domain-name <i>domain-name</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
<b>Options</b>	<p><b>filename <i>filename</i></b>—File that stores the certificate.</p> <p><b>subject <i>subject</i></b>—Distinguished name (<b>dn</b>), which consists of a set of components—for example, an organization (<b>o</b>), an organization unit (<b>ou</b>), a country (<b>c</b>), and a locality (<b>l</b>).</p> <p><b>alternative-subject <i>alternative-subject</i></b>—Tunnel source address.</p> <p><b>certification-authority <i>certification-authority</i></b>—Name of the certificate authority profile in the configuration.</p> <p><b>encoding (binary   pem)</b>—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.</p> <p><b>key-file <i>key-file</i></b>—File containing a local private key.</p> <p><b>domain-name <i>domain-name</i></b>—Fully qualified domain name.</p>
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request security certificate (signed) on page 31</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

```

request security certificate (signed) user@host> request security certificate enroll filename host.crt subject c=uk,o=london
alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name
host.juniper.net
CA name: juniper.net CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.juniper.net
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
the key management process (kmd) log file at /var/log/kmd. <-----

```

## request security certificate (unsigned)

---

<b>Syntax</b>	<code>request security certificate enroll filename <i>filename</i> ca-file <i>ca-file</i> ca-name <i>ca-name</i> encoding (binary   perm) url <i>url</i></code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
<b>Options</b>	<b>filename <i>filename</i></b> —File that stores the public key certificate.  <b>ca-file <i>ca-file</i></b> —Name of the certificate authority profile in the configuration.  <b>ca-name <i>ca-name</i></b> —Name of the certificate authority.  <b>encoding (binary   pem)</b> —File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is <b>binary</b> .  <b>url <i>url</i></b> —Certificate authority URL.
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request security certificate (unsigned) on page 32</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

<b>request security certificate (unsigned)</b>	<pre>user@host&gt; request security certificate enroll filename ca_verisign ca-file verisign ca-name juniper.net urlxyzcompany URL http://&lt;verisign ca-name xyzcompany url&gt;/cgi-bin/pkiclient.exe CA name: juniper.net CA file: verisign Encoding: binary Certificate enrollment has started. To view the status of your enrollment, check the key management process (kmd) log file at /var/log/kmd. &lt;-----</pre>
--	---

## request security key-pair

---

<b>Syntax</b>	<code>request security key-pair <i>filename</i></code> <code>&lt;size <i>key-size</i>&gt;</code> <code>&lt;type (rsa   dsa)&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	(Encryption interface on M Series and T Series routers and EX Series switches only) Generate a public and private key pair for a digital certificate.
<b>Options</b>	<p><b><i>filename</i></b>—Name of a file in which to store the key pair.</p> <p><b><i>size key-size</i></b>—(Optional) Key size, in bits. The key size can be <b>512</b>, <b>1024</b>, or <b>2048</b>. The default value is <b>1024</b>.</p> <p><b><i>type</i></b>—(Optional) Algorithm used to encrypt the key:</p> <ul style="list-style-type: none"> <li>• <b>rsa</b>—RSA algorithm. This is the default.</li> <li>• <b>dsa</b>—Digital signature algorithm with Secure Hash Algorithm (SHA).</li> </ul>
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request security key-pair on page 33</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

```
request security user@host> request security key-pair security-key-file
key-pair
```

## request ipsec switch

---

<b>Syntax</b>	<code>request ipsec switch (interface &lt;es-fpc/pic/port&gt;   security-associations &lt;sa-name&gt;)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
<b>Description</b>	(Encryption interface on M Series and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.
<b>Options</b>	<code>interface &lt;es-fpc/pic/port&gt;</code> —Switch to the backup encryption interface. <code>security-associations &lt;sa-name&gt;</code> —Switch to the backup tunnel.
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">show ipsec redundancy on page 43</a></li></ul>
<b>List of Sample Output</b>	<a href="#">request ipsec switch on page 34</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

## Sample Output

**request ipsec switch**     user@host> request ipsec switch security-associations sa-private



## request system certificate add

---

<b>Syntax</b>	<code>request system certificate add (<i>filename</i>   terminal)</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	(Encryption interface on M Series, T Series routers and QFX Series switches only) Add a certificate provided by the Juniper Networks certificate authority (CA).
<b>Options</b>	<b><i>filename</i></b> —Filename (URL, local, or remote). <b>terminal</b> —Use login terminal.
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">request system certificate add on page 35</a>
<b>Output Fields</b>	When you enter this command, you are provided feedback on the status of your request.

### Sample Output

<code>request system certificate add</code>	<code>user@host&gt; request system certificate add terminal</code>
---	--

## show ike security-associations

<b>Syntax</b>	show ike security-associations <brief   detail> <peer-address>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(Encryption interface on M Series and T Series routers only) Display information about Internet Key Exchange (IKE) security associations.
<b>Options</b>	<p><b>none</b>—Display standard information about all IKE security associations.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>peer-address</b>—(Optional) Display IKE security associations for the specified peer address.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <a href="#">clear ike security-associations on page 28</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show ike security-associations on page 39</a> <a href="#">show ike security-associations detail on page 39</a>
<b>Output Fields</b>	<p><a href="#">Table 3 on page 36</a> lists the output fields for the <b>show ike security-associations</b> command. Output fields are listed in the approximate order in which they appear.</p>

**Table 3: show ike security-associations Output Fields**

Field Name	Field Description	Level of Output
<b>IKE peer</b>	Remote end of the IKE negotiation.	<b>detail</b>
<b>Role</b>	Part played in the IKE session. The router triggering the IKE negotiation is the initiator, and the router accepting the first IKE exchange packets is the responder.	<b>detail</b>
<b>Remote Address</b>	Responder's address.	none specified
<b>State</b>	State of the IKE security association: <ul style="list-style-type: none"> <li>• <b>Matured</b>—The IKE security association is established.</li> <li>• <b>Not matured</b>—The IKE security association is in the process of negotiation.</li> </ul>	none specified
<b>Initiator cookie</b>	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels

Table 3: show ike security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Responder cookie</b>	<p>The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received.</p> <p>Of the numerous security services available, protection against denial of service (DoS) is one of the most difficult to address. A “cookie” or anticlogging token (ACT) is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine the cookie's authenticity. An exchange prior to CPU-intensive public key operations can thwart some DoS attempts (such as simple flooding with invalid IP source addresses).</p>	All levels
<b>Exchange type</b>	<p>Specifies the number of messages in an IKE exchange, and the payload types that are contained in each message. Each exchange type provides a particular set of security services, such as anonymity of the participants, perfect forward secrecy of the keying material, and authentication of the participants. Junos OS supports two types of exchanges:</p> <ul style="list-style-type: none"> <li>• <b>Main</b>—The exchange is done with six messages. <b>Main</b> encrypts the payload, protecting the identity of the neighbor.</li> <li>• <b>Aggressive</b>—The exchange is done with three messages. <b>Aggressive</b> does not encrypt the payload, leaving the identity of the neighbor unprotected.</li> </ul>	All Levels
<b>Authentication method</b>	Type of authentication determines which payloads are exchanged and when they are exchanged. The Junos OS supports only <b>pre-shared keys</b> .	<b>detail</b>
<b>Local</b>	Prefix and port number of the local end.	<b>detail</b>
<b>Remote</b>	Prefix and port number of the remote end.	<b>detail</b>
<b>Lifetime</b>	Number of seconds remaining until the IKE security association expires.	<b>detail</b>
<b>Algorithms</b>	<p>Header for the IKE algorithms output.</p> <ul style="list-style-type: none"> <li>• <b>Authentication</b>—Type of authentication algorithm used: <b>md5</b> or <b>sha1</b>.</li> <li>• <b>Encryption</b>—Type of encryption algorithm used: <b>des-cbc</b>, <b>3des-cbc</b>, or <b>None</b>.</li> <li>• <b>Pseudo random function</b>—Function that generates highly unpredictable random numbers: <b>hmac-md5</b> or <b>hmac-sha1</b>.</li> </ul>	<b>detail</b>
<b>Traffic statistics</b>	<p>Number of bytes and packets received and transmitted on the IKE security association.</p> <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the IKE security association.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the IKE security association.</li> </ul>	<b>detail</b>

Table 3: show ike security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Flags</b>	Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> <li>• <b>caller notification sent</b>—Caller program notified about the completion of the IKE negotiation.</li> <li>• <b>waiting for done</b>—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.</li> <li>• <b>waiting for remove</b>—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.</li> <li>• <b>waiting for policy manager</b>—Negotiation is waiting for a response from the policy manager.</li> </ul>	<b>detail</b>
<b>IPsec security associates</b>	Number of IPsec security associations created and deleted with this IKE security association.	<b>detail</b>
<b>Phase 2 negotiations in progress</b>	Number of phase 2 IKE negotiations in progress and status information: <ul style="list-style-type: none"> <li>• <b>Negotiation type</b>—Type of phase 2 negotiation. The Junos OS currently supports <b>quick mode</b>.</li> <li>• <b>Message ID</b>—Unique identifier for a phase 2 negotiation.</li> <li>• <b>Local identity</b>—Identity of the local phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[O..id-data-len] = iddata-presentation)</i></li> <li>• <b>Remote identity</b>—Identity of the remote phase 2 negotiation. The format is <i>id-type-name (proto-name:port-number,[O..id-data-len] = iddata-presentation)</i></li> <li>• <b>Flags</b>—Notification to the key management process of the status of the IKE negotiation: <ul style="list-style-type: none"> <li>• <b>caller notification sent</b>—Caller program notified about the completion of the IKE negotiation.</li> <li>• <b>waiting for done</b>—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.</li> <li>• <b>waiting for remove</b>—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.</li> <li>• <b>waiting for policy manager</b>—Negotiation is waiting for a response from the policy manager.</li> </ul> </li> </ul>	<b>detail</b>

## Sample Output

```

show ike          user@host> show ike security-associations
security-associations
Remote Address  State      Initiator cookie  Responder cookie  Exchange type
4.4.4.4        Matured    93870456fa000011  723a20713700003e  Main

show ike          user@host> show ike security-associations detail
security-associations
detail            IKE peer 4.4.4.4
                    Role: Initiator, State: Matured
                    Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
                    Exchange type: Main, Authentication method: Pre-shared-keys
                    Local: 4.4.4.5:500, Remote: 4.4.4.4:500
                    Lifetime: Expires in 187 seconds
                    Algorithms:
                    Authentication      : md5
                    Encryption          : 3des-cbc
                    Pseudo random function: hmac-md5
                    Traffic statistics:
                    Input  bytes   :          1000
                    Output bytes   :          1280
                    Input  packets:           5
                    Output packets:           9
                    Flags: Caller notification sent
                    IPsec security associations: 2 created, 0 deleted
                    Phase 2 negotiations in progress: 1

                    Negotiation type: Quick mode, Role: Initiator, Message ID: 3582889153
                    Local: 4.4.4.5:500, Remote: 4.4.4.4:500
                    Local identity: ipv4_subnet(tcp:80,[0..7]=10.1.1.0/24)
                    Remote identity: ipv4_subnet(tcp:100,[0..7]=10.1.2.0/24)
                    Flags: Caller notification sent, Waiting for done

```

## show ipsec certificates

<b>Syntax</b>	show ipsec certificates <brief   detail> <crl <i>crl-name</i>   <i>serial-number</i> >
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(Encryption interface on M Series and T Series routers only) Display information about the IPsec certificate database.
<b>Options</b>	<p><b>none</b>—Display standard information about all of the entries in the IPsec certificate database.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>crl <i>crl-name</i>   <i>serial-number</i></b>—(Optional) Display information about the entries on the certificate revocation list (CRL) or for the specified serial number. A CRL is a timestamped list identifying revoked certificates. The CRL is signed by a certificate authority (CA) or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">clear ipsec security-associations on page 29</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show ipsec certificates detail on page 41</a>
<b>Output Fields</b>	<a href="#">Table 4 on page 40</a> lists the output fields for the <b>show ipsec certificates</b> command. Output fields are listed in the approximate order in which they appear.

Table 4: show ipsec certificates Output Fields

Field Name	Field Description	Level of Output
<b>Database</b>	Display information about the IPsec certificate database. <ul style="list-style-type: none"> <li><b>Total entries</b>—Number of database entries, including entries that are not trusted or that are in the process of being deleted.</li> <li><b>Active entries</b>—Number of database entries, excluding entries that are marked as deleted.</li> <li><b>Locked entries</b>—Number of statically configured database entries that cannot expire, such as CA certificates that are root or trusted.</li> </ul>	All levels
<b>Subject</b>	Distinguished name for the certificate for <b>C, O, CN</b> , as described in RFC 3280, <i>Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile</i> .	All levels
<b>ID</b>	Identification number of the database entry. <b>ID</b> is generated by the internal certificate database.	All levels

Table 4: show ipsec certificates Output Fields (*continued*)

Field Name	Field Description	Level of Output
References	Reference number the certificate manager has for the particular entry.	detail
Serial	Unique serial number assigned to each certificate by the CA.	All levels
Flags	State of the certificate. <ul style="list-style-type: none"> <li>• <b>Trusted</b>—Passed validity checks.</li> <li>• <b>Not trusted</b>—Failed validity checks.</li> <li>• <b>Root</b>—Entry is locked and may have been learned through IKE or a locally configured CA certificate.</li> <li>• <b>Non-root</b>—Entry is not locked.</li> <li>• <b>Crl-issuer</b>—Entity issues CRLs.</li> <li>• <b>Non-crl-issuer</b>—Entity does not issue CRLs.</li> </ul>	detail
Validity period starts	Start time that the certificate is valid, in the format <i>yyyy mon dd, hh:mm:ss GMT</i> .	detail
Validity period ends	End time that the certificate is valid, in the format <i>yyyy mon dd, hh:mm:ss GMT</i> .	detail
Alternative name information	Auxiliary identity for the certificate: <i>dns-name</i> , <i>email-address</i> , <i>ip-address</i> , or <i>uri</i> (uniform resource identifier).	detail
Issuer	Information about the entity that has signed and issued the CRL as described in RFC 2459, <i>Internet X.509 Public Key Infrastructure Certificate and CRL Profile</i> .	detail

## Sample Output

```

show ipsec certificates user@host> show ipsec certificates detail
detail Database: Total entries: 3 Active entries: 4 Locked entries: 1
Subject: C=us, O=x
ID: 5, References: 0, Serial: 22314868
Flags: Trusted Non-root Crl-issuer
Validity period starts: 2003 Mar 1st, 01:20:42 GMT
Validity period ends: 2003 Mar 31st, 01:50:42 GMT
Alternative name information:
IP address: 10.20.210.1
Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2

Subject: C=us, O=x
ID: 4, References: 0, Serial: 22315496
Flags: Trusted Non-root Crl-issuer
Validity period starts: 2003 Mar 1st, 01:21:45 GMT
Validity period ends: 2003 Mar 31st, 01:51:45 GMT
Alternative name information:
IP address: 10.20.210.20
Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2

Subject: C=FI, O=SSH Company-ABC, CN=Company ABC class 2
ID: 1, References: 1, Serial: 1538512
Flags: Trusted Root Non-crl-issuer
Validity period starts: 2001 Aug 1st, 07:08:32 GMT

```

Validity period ends: 2004 Aug 1st, 07:08:32 GMT  
Alternative name information:  
Email address: certifier-support@ssh.com  
Issuer: C=FI, O=Company-ABC, CN=Company ABC class 2



## show ipsec redundancy

<b>Syntax</b>	show ipsec redundancy (interface <es-fpc/pic/port>   security association <sa-name>)
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(Encryption interface on M Series and T Series routers only) Display information about IPsec redundancy.
<b>Options</b>	<p><b>interface &lt;es-fpc/pic/port&gt;</b>—Display information about all encryption interfaces, or optionally, about a particular encryption interface.</p> <p><b>security association &lt;sa-name&gt;</b>—Display information about all remote tunnels, or optionally, about a particular remote tunnel.</p>
<b>Required Privilege Level</b>	view
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li><a href="#">request ipsec switch on page 34</a></li> </ul>
<b>List of Sample Output</b>	<a href="#">show ipsec redundancy interface on page 44</a> <a href="#">show ipsec redundancy security-associations on page 44</a>
<b>Output Fields</b>	<a href="#">Table 5 on page 43</a> lists the output fields for the <b>show ipsec redundancy</b> command. Output fields are listed in the approximate order in which they appear.

**Table 5: show ipsec redundancy Output Fields**

Field Name	Field Description
<b>Failure counter</b>	Number of times a PIC switched between primary and backup interfaces, or the number of times the tunnel switched between the primary and remote peers since the software has been activated.
<b>Primary interface '</b>	Name of the interface configured to be the primary interface.
<b>Backup interface</b>	Name of the interface configured to be the backup interface.
<b>State</b>	State of the primary or backup interface can be <b>Active</b> , <b>Offline</b> , or <b>Standby</b> . Both ES PICs are initialized to <b>Offline</b> . For primary and remote peers, <b>State</b> can be <b>Active</b> or <b>Standby</b> . Both peers are in a state of <b>Standby</b> by default (there is not yet a connection between the two peers).
<b>Security association</b>	Name of the security association.
<b>Local IP</b>	Local IP address.
<b>Primary remote IP</b>	IP address of the configured primary remote peer.
<b>Backup remote IP</b>	IP address of the configured backup remote peer.

## Sample Output

```
show ipsec redundancy interface  user@host> show ipsec redundancy interface
                                Failure counter: 0
                                Primary interface: es-1/3/0, State: Active
                                Backup interface : es-1/1/0, State: Standby

show ipsec redundancy security-associations  user@host> show ipsec redundancy security-associations sa-dynamic
security-associations           Security association: sa-dynamic, Failure counter: 0
                                Local IP: 4.4.4.4
                                Primary remote IP: 4.4.4.5, State: Standby
                                Backup remote IP : 3.3.3.3, State: Standby
```

## show ipsec security-associations

<b>Syntax</b>	show ipsec security-associations <brief   detail> <sa-name>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	Display information about the IPsec security associations applied to the local or transit traffic stream.
<b>Options</b>	<p><b>none</b>—Display standard information about all IPsec security associations.</p> <p><b>brief   detail</b>—(Optional) Display the specified level of output.</p> <p><b>sa-name</b>—(Optional) Display the specified IPsec security association.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show ipsec security-associations sa-name on page 47</a> <a href="#">show ipsec security-associations sa-name detail on page 47</a>
<b>Output Fields</b>	Table 6 on page 45 lists the output fields for the <b>show ipsec security-associations</b> command. Output fields are listed in the approximate order in which they appear.

Table 6: show ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
<b>Security association</b>	Name of the security association.	All levels
<b>Interface family</b>	<p>Status of the interface family of the security association. If the interface family field is absent, it is a transport mode security association. The interface family can have one of three options:</p> <ul style="list-style-type: none"> <li>• <b>Up</b>—The security association is referenced in the interface family and the interface family is up.</li> <li>• <b>Down</b>—The security association is referenced in the interface family and the interface family is down.</li> <li>• <b>No reference</b>—The security association is not referenced in the interface family.</li> </ul>	All levels
<b>Local gateway</b>	Gateway address of the local system.	All levels
<b>Remote gateway</b>	Gateway address of the remote system.	All levels
<b>Local identity</b>	Prefix and port number of the local end	All levels
<b>Remote identity</b>	Prefix and port number of the remote end.	All levels
<b>Direction</b>	Direction of the security association: <b>inbound</b> or <b>outbound</b> .	All levels
<b>SPI</b>	Value of the security parameter index.	All levels

Table 6: show ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>AUX-SPI</b>	Value of the auxiliary security parameter index. <ul style="list-style-type: none"> <li>When the value is <b>AH</b> or <b>ESP</b>, <b>AUX-SPI</b> is always <b>0</b>.</li> <li>When the value is <b>AH+ESP</b>, <b>AUX-SPI</b> is always a positive integer.</li> </ul>	All levels
<b>State</b>	Status of the security association: <ul style="list-style-type: none"> <li><b>Installed</b>—The security association is installed in the security association database. (For transport mode security associations, the value of <b>State</b> must always be <b>Installed</b>.)</li> <li><b>Not installed</b>—The security association is not installed in the security association database.</li> </ul>	detail
<b>Mode</b>	Mode of the security association: <ul style="list-style-type: none"> <li><b>transport</b>—Protects single host-to-host protections.</li> <li><b>tunnel</b>—Protects connections between security gateways.</li> </ul>	All levels
<b>Type</b>	Type of security association: <ul style="list-style-type: none"> <li><b>manual</b>—Security parameters require no negotiation. They are static, and are configured by the user.</li> <li><b>dynamic</b>—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode.</li> </ul>	All levels
<b>Protocol</b>	Protocol supported: <ul style="list-style-type: none"> <li><b>transport mode</b>—Supports Encapsulation Security Protocol (<b>ESP</b>) or Authentication Header (<b>AH</b>).</li> <li><b>tunnel mode</b>—Supports <b>ESP</b> or <b>AH+ESP</b>.</li> </ul>	All levels
<b>Authentication</b>	Type of authentication used: <b>hmac-md5-96</b> , <b>hmac-sha1-96</b> , or <b>None</b> .	detail
<b>Encryption</b>	Type of encryption used: <b>des-cbc</b> , <b>3des-csc</b> , or <b>None</b> .	detail
<b>Soft lifetime</b> <b>Hard lifetime</b>	(dynamic output only) Each lifetime of a security association has two display options, hard and soft, one of which must be present for a dynamic security association. The <b>hard lifetime</b> specifies the lifetime of the SA. The <b>soft lifetime</b> , 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. <ul style="list-style-type: none"> <li><b>Expires in seconds seconds</b>—Number of seconds left until the security association expires.</li> <li><b>Expires in kilobytes kilobytes</b>—Number of kilobytes left until the security association expires.</li> </ul>	detail
<b>Anti-replay service</b>	State of the service that prevents packets from being replayed: <b>Enabled</b> or <b>Disabled</b> .	detail

Table 6: show ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
Replay window size	Configured size, in packets, of the antireplay service window: <b>32</b> or <b>64</b> . The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is <b>0</b> , the antireplay service is disabled.	detail

## Sample Output

```

show ipsec security-associations sa-name
user@host> show ipsec security-associations sa-cosmic brief
Security association: sa-cosmic, Interface family: Up
Local gateway: 21.21.1.1, Remote gateway: 21.21.2.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction SPI      AUX-SPI      Mode      Type      Protocol
inbound  2908734119  0          tunnel    dynamic   AH
outbound  3494029335  0          tunnel    dynamic   AH

show ipsec security-associations sa-name detail
user@host> show ipsec security-associations sa-cosmic detail
Security association: sa-cosmic, Interface family: Up

Local gateway: 21.21.1.1, Remote gateway: 21.21.2.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 2908734119, AUX-SPI: 0, State: Installed
Mode: tunnel, Type: dynamic
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expired
Hard lifetime: Expires in 120 seconds
Anti-replay service: Disabled

Direction: outbound, SPI: 3494029335, AUX-SPI: 0, State: Installed
Mode: tunnel, Type: dynamic
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expired
Hard lifetime: Expires in 120 seconds
Anti-replay service: Disabled

```

## show system certificate

<b>Syntax</b>	<code>show system certificate</code> <code>&lt;certificate-id&gt;</code>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 11.1 for the QFX Series.
<b>Description</b>	(Encryption interface on M Series, T Series routers, and QFX Series switches only) Display installed certificates signed by the Juniper Networks certificate authority.
<b>Options</b>	<b>none</b> —Display all installed certificates signed by the Juniper Networks certificate authority. <b>certificate-id</b> —(Optional) Display the details of a particular certificate.
<b>Required Privilege Level</b>	maintenance
<b>List of Sample Output</b>	<a href="#">show system certificate on page 49</a> <a href="#">show system certificate (QFX Series) on page 49</a>
<b>Output Fields</b>	<a href="#">Table 7 on page 48</a> lists the output fields for the <b>show system certificate</b> command. Output fields are listed in the approximate order in which they appear.

**Table 7: show system certificate Output Fields**

Field Name	Field Description
<b>Certificate identifier</b>	Unique identifier associated with a certificate. The certificate identifier is the common name of the subject.
<b>Issuer</b> <b>Subject</b>	Information about the certificate issuer and the distinguished name (DN) of the issuer, respectively: <ul style="list-style-type: none"> <li>• <b>Organization</b>—Name of the owner's organization.</li> <li>• <b>Organizational unit</b>—Name of the owner's department.</li> <li>• <b>Country</b>—Two-character country code in which the owner's system is located.</li> <li>• <b>State</b>—State in the USA in which the owner is using the certificate.</li> <li>• <b>Locality</b>—City in which the owner's system is located.</li> <li>• <b>Common name</b>—Name of the owner of the certificate.</li> <li>• <b>E-mail address</b>—E-mail address of the owner of the certificate.</li> </ul>
<b>Validity</b>	When a certificate is valid.
<b>Signature algorithm</b>	Encryption algorithm applied to the installed certificate.
<b>Public key algorithm</b>	Encryption algorithm applied to the public key.

## Sample Output

```
show system certificate user@host> show system certificate
Certificate identifier: Dallas-v3
  Issuer:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas CA,
    E-mail address:ca@juniper.net
  Subject:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
    E-mail address:ca@juniper.net
  Validity:
    Not before: Mar 13 03:23:25 2004 GMT
    Not after: Mar 24 03:23:25 2014 GMT
  Signature algorithm: sha1WithRSAEncryption
  Public key algorithm: dsaEncryption

show system certificate (QFX user@host> show system certificate
Series) Certificate identifier: Dallas-v3
  Issuer:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas CA,
    E-mail address:ca@juniper.net
  Subject:
    Organization: Juniper Networks, Organizational unit: Juniper CA,
    Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
    E-mail address:ca@juniper.net
  Validity:
    Not before: Mar 13 03:23:25 2004 GMT
    Not after: Mar 24 03:23:25 2014 GMT
  Signature algorithm: sha1WithRSAEncryption
  Public key algorithm: dsaEncryption
```





## CHAPTER 5

# Encryption Interface Operational Mode Commands

## show interfaces (Encryption)

<b>Syntax</b>	<pre>show interfaces es-fpc/pic/port:channel &lt;brief   detail   extensive   terse&gt; &lt;descriptions&gt; &lt;media&gt; &lt;snmp-index <i>snmp-index</i>&gt; &lt;statistics&gt;</pre>
<b>Release Information</b>	Command introduced before Junos OS Release 7.4.
<b>Description</b>	(M Series and T Series routers only) Display status information about the specified encryption interface.
<b>Options</b>	<p><b>es-fpc/pic/port:channel</b>—Display standard status information about the specified encryption interface.</p> <p><b>brief   detail   extensive   terse</b>—(Optional) Display the specified level of output.</p> <p><b>descriptions</b>—(Optional) Display interface description strings.</p> <p><b>media</b>—(Optional) Display media-specific information about network interfaces.</p> <p><b>snmp-index <i>snmp-index</i></b>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><b>statistics</b>—(Optional) Display static interface statistics.</p>
<b>Required Privilege Level</b>	view
<b>List of Sample Output</b>	<a href="#">show interfaces (Encryption) on page 55</a> <a href="#">show interfaces brief (Encryption) on page 55</a> <a href="#">show interfaces detail (Encryption) on page 55</a> <a href="#">show interfaces extensive (Encryption) on page 56</a>
<b>Output Fields</b>	<a href="#">Table 8 on page 52</a> lists the output fields for the <b>show interfaces</b> (ES) command. Output fields are listed in the approximate order in which they appear.

**Table 8: Encryption show interfaces Output Fields**

Field Name	Field Description	Level of Output
<b>Physical Interface</b>		
<b>Physical interface</b>	Name of the physical interface.	All levels
<b>Enabled</b>	State of the interface. Possible values are described in the “Enabled Field” section under Common Output Fields Description.	All levels
<b>Interface index</b>	Physical interface's index number, which reflects its initialization sequence.	<b>detail extensive none</b>
<b>SNMP ifIndex</b>	SNMP index number for the physical interface.	<b>detail extensive none</b>

Table 8: Encryption show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Type</b>	Encapsulation being used on the interface.	All levels
<b>Link-level type</b>	Encapsulation being used on the physical interface.	All levels
<b>MTU</b>	MTU size on the physical interface.	All levels
<b>Speed</b>	Speed at which the interface is running.	All levels
<b>Device flags</b>	Information about the physical device. Possible values are described in the "Link Flags" section under Common Output Fields Description.	All levels
<b>Interface flags</b>	Information about the interface. Possible values are described in the "Interface Flags" section under Common Output Fields Description.	All levels
<b>Input rate</b>	Input rate in bits per second (bps) and packets per second (pps).	None specified
<b>Output rate</b>	Output rate in bps and pps.	None specified
<b>Hold-times</b>	Current interface hold-time up and hold-time down, in milliseconds.	<b>detail extensive</b>
<b>Statistics last cleared</b>	Time when the statistics for the interface were last set to zero.	<b>detail extensive</b>
<b>Traffic statistics</b>	Number and rate of bytes and packets received and transmitted on the physical interface. <ul style="list-style-type: none"> <li>• <b>Input bytes, Output bytes</b>—Number of bytes received and transmitted on the interface.</li> <li>• <b>Input packets, Output packets</b>—Number of packets received and transmitted on the interface.</li> <li>• <b>Anti-replay failures</b>—Total number of antireplay failures seen on all tunnels configured on the ES PIC.</li> <li>• <b>Authentication</b>—Total number of authentication failures seen on all tunnels configured on the ES PIC.</li> </ul>	<b>detail extensive</b>
<b>Egress queues</b>	Total number of egress queues supported on the specified interface.	<b>detail extensive</b>
<b>Queue counters</b>	CoS queue number and its associated user-configured forwarding class name. <ul style="list-style-type: none"> <li>• <b>Queued packets</b>—Number of queued packets.</li> <li>• <b>Transmitted packets</b>—Number of transmitted packets.</li> <li>• <b>Dropped packets</b>—Number of packets dropped by the ASIC's RED mechanism.</li> </ul>	<b>detail extensive</b>
<b>Logical Interface</b>		
<b>Logical interface</b>	Name of the logical interface.	All levels
<b>Index</b>	Logical interface index number, which reflects its initialization sequence.	<b>detail extensive none</b>

Table 8: Encryption show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
<b>SNMP ifIndex</b>	Logical interface SNMP interface index number.	<b>detail extensive none</b>
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Flags</b>	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under Common Output Fields Description.	All levels
<b>IP-Header</b>	IP header of the logical interface.	All levels
<b>Encapsulation</b>	Encapsulation on the logical interface.	All levels
<b><i>protocol-family</i></b>	Protocol family configured on the logical interface. If the protocol is <b>inet</b> , the IP address of the interface is also displayed.	<b>brief</b>
<b>Input packets</b>	Number of packets received on the logical interface.	None specified
<b>Output packets</b>	Number of packets transmitted on the logical interface.	None specified
<b>Traffic statistics</b>	Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	<b>detail extensive</b>
<b>Local statistics</b>	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	<b>detail extensive</b>
<b>Transit statistics</b>	Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	<b>detail extensive</b>
<b>Protocol</b>	Protocol family configured on the logical interface, such as <b>iso</b> , <b>inet6</b> , <b>mpls</b> .	<b>detail extensive none</b>
<b>MTU</b>	MTU size on the logical interface.	<b>detail extensive none</b>
<b>Generation</b>	Unique number for use by Juniper Networks technical support only.	<b>detail extensive</b>
<b>Route table</b>	Routing table in which the logical interface address is located. For example, <b>0</b> refers to the routing table <b>inet.0</b> .	<b>detail extensive</b>
<b>Flags</b>	Information about the protocol family flags. Possible values are described in the “Family Flags” section under Common Output Fields Description.	<b>detail extensive none</b>
<b>Addresses, Flags</b>	Information about the address flags. Possible values are described in the “Addresses Flags” section under Common Output Fields Description.Address	<b>detail extensive none</b>
<b>Destination</b>	IP address of the remote side of the connection.	<b>detail extensive none</b>

Table 8: Encryption show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

## Sample Output

```

show interfaces (Encryption) user@host> show interfaces es-0/3/0
Physical interface: es-0/3/0, Enabled, Physical link is Up
Interface index: 138, SNMP ifIndex: 71
Type: IPSEC, Link-level type: IPSEC-over-IP, MTU: 3900, Speed: 800mbps
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)

Logical interface es-0/3/0.0 (Index 70) (SNMP ifIndex 45)
Flags: Hardware-Down Point-To-Point SNMP-Traps
IP-Header 10.0.10.2:10.0.10.1::df:64:00000000 Encapsulation: IPSEC
Input packets : 0
Output packets: 0
Protocol inet, MTU: 3800
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
Destination: 10.10.0.2, Local: 10.10.0.1

show interfaces brief (Encryption) user@host> show interfaces es-0/3/0 brief
Physical interface: es-0/3/0, Enabled, Physical link is Up
Type: IPSEC, Link-level type: IPSEC-over-IP, MTU: 3900, Speed: 800mbps
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps

Logical interface es-0/3/0.0
Flags: Hardware-Down Point-To-Point SNMP-Traps
IP-Header 10.0.10.2:10.0.10.1::df:64:00000000 Encapsulation: IPSEC
inet 10.10.0.1 --> 10.10.0.2s

show interfaces detail (Encryption) user@host> show interfaces es-0/3/0 detail
Physical interface: es-0/3/0, Enabled, Physical link is Up
Interface index: 138, SNMP ifIndex: 71, Generation: 21
Type: IPSEC, Link-level type: IPSEC-over-IP, MTU: 3900, Speed: 800mbps
Hold-times : Up 0 ms, Down 0 ms
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Anti-replay failures : 0
Authentication failures : 0

```

```

Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort              0              0              0
  1 expedited-fo             0              0              0
  2 assured-forw             0              0              0
  3 network-cont             0              0              0

```

```

Logical interface es-0/3/0.0 (Index 70) (SNMP ifIndex 45) (Generation 9)
Flags: Hardware-Down Point-To-Point SNMP-Traps
IP-Header 10.0.10.2:10.0.10.1::df:64:00000000 Encapsulation: IPSEC
Traffic statistics:
  Input bytes :              0
  Output bytes :              0
  Input packets:              0
  Output packets:            0
Local statistics:
  Input bytes :              0
  Output bytes :              0
  Input packets:              0
  Output packets:            0
Transit statistics:
  Input bytes :              0              0 bps
  Output bytes :              0              0 bps
  Input packets:              0              0 pps
  Output packets:            0              0 pps
Protocol inet, MTU: 3800, Generation: 22, Route table: 0
Flags: None
Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
  Destination: 10.10.0.2, Local: 10.10.0.1, Broadcast: Unspecified,
  Generation: 26

```

```

show interfaces extensive (Encryption) user@host> show interfaces es-0/3/0 extensive
Physical interface: es-0/3/0, Enabled, Physical link is Up
Interface index: 138, SNMP ifIndex: 71, Generation: 21
Type: IPSEC, Link-level type: IPSEC-over-IP, MTU: 3900, Speed: 800mbps
Hold-times      : Up 0 ms, Down 0 ms
Device flags    : Present Running
Interface flags: Point-To-Point SNMP-Traps
Statistics last cleared: Never
Traffic statistics:
  Input bytes :              0              0 bps
  Output bytes :              0              0 bps
  Input packets:              0              0 pps
  Output packets:            0              0 pps
  Anti-replay failures      : 0
  Authentication failures   : 0
Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort              0              0              0
  1 expedited-fo             0              0              0
  2 assured-forw             0              0              0
  3 network-cont             0              0              0

```

```
Logical interface es-0/3/0.0 (Index 70) (SNMP ifIndex 45) (Generation 9)
  Flags: Hardware-Down Point-To-Point SNMP-Traps
  IP-Header 10.0.10.2:10.0.10.1::df:64:00000000 Encapsulation: IPSEC
  Traffic statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Local statistics:
    Input bytes : 0
    Output bytes : 0
    Input packets: 0
    Output packets: 0
  Transit statistics:
    Input bytes : 0 0 bps
    Output bytes : 0 0 bps
    Input packets: 0 0 pps
    Output packets: 0 0 pps
  Protocol inet, MTU: 3800, Generation: 22, Route table: 0
    Flags: None
    Addresses, Flags: Dest-route-down Is-Preferred Is-Primary
      Destination: 10.10.0.2, Local: 10.10.0.1, Broadcast: Unspecified,
      Generation: 26
```





## PART 4

# Index

- [Index on page 61](#)



# Index

## Symbols

#, comments in configuration statements.....	xii
( ), in syntax descriptions.....	xii
< >, in syntax descriptions.....	xii
[ ], in configuration statements.....	xii
{ }, in configuration statements.....	xii
(pipe), in syntax descriptions.....	xii

## A

address statement	
encryption.....	17
usage guidelines.....	7

## B

backup-destination statement.....	18
usage guidelines.....	15
backup-interface statement.....	18
usage guidelines.....	14
braces, in configuration statements.....	xii
brackets	
angle, in syntax descriptions.....	xii
square, in configuration statements.....	xii

## C

certificates	
installed, displaying.....	48
key pairs, generating.....	33
provided by Juniper Networks, adding.....	35
signed certificate, obtaining.....	31
unsigned certificate, obtaining.....	32
clear ike security-associations command.....	28
clear ipsec security-associations command.....	29
comments, in configuration statements.....	xii
conventions	
text and syntax.....	xi
curly braces, in configuration statements.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

## D

destination statement	
encryption.....	19
usage guidelines.....	7, 15
digital certificates See certificates	
documentation	
comments on.....	xiii

## E

encryption interface.....	7
applying inbound filter.....	13
example configuration.....	13
applying outbound filter.....	11
example configuration.....	11
configuring inbound filter.....	12
example configuration.....	12
configuring MTU.....	8
encryption interfaces	
status information, displaying.....	52
ES interfaces	
example configuration.....	8
ES PIC	
apply inbound filter.....	13
PIC redundancy.....	14
redundancy	
example configuration.....	14
tunnel redundancy.....	15
es-options statement.....	19
usage guidelines.....	14

## F

family statement	
encryption.....	20
usage guidelines.....	7
filter statement	
encryption.....	21
usage guidelines.....	13
font conventions.....	xi

## I

IKE	
encryption services interfaces	
security associations, clearing.....	28
security associations, displaying.....	36
interface statement	
encryption	
usage guidelines.....	7

interfaces statement		show ipsec certificates command.....	40
encryption.....	21	show ipsec redundancy command.....	43
usage guidelines.....	7	show ipsec security-associations command.....	45
Internet Key Exchange See IKE		show system certificate command.....	48
IPsec		show system statistics command.....	35
ES PIC.....	7	source statement	
example configuration		encryption.....	22
inbound traffic.....	12	usage guidelines.....	15
outbound traffic.....	11	support, technical See technical support	
traffic.....	8	syntax conventions.....	xi
IPsec services		<b>T</b>	
encryption services interfaces		technical support	
backup and primary, switching		contacting JTAC.....	xiii
interfaces.....	34	traffic.....	8
backup and primary, switching		inbound (decryption).....	12
services.....	34	IPsec, configuring.....	9
certificate database, displaying.....	40	outbound (encryption).....	10
IKE security associations, clearing.....	28	tunnel statement	
IKE security associations, displaying.....	36	encryption.....	23
IPSec security associations, clearing.....	29	usage guidelines.....	7
IPSec security associations,		redundancy	
displaying.....	45	usage guidelines.....	15
redundancy information, displaying.....	43	<b>U</b>	
ipsec-sa statement		unit statement	
encryption.....	22	encryption.....	24
usage guidelines.....	7	usage guidelines.....	7
<b>K</b>			
key pair for digital certificate, generating.....	33		
<b>M</b>			
manuals			
comments on.....	xiii		
<b>P</b>			
parentheses, in syntax descriptions.....	xii		
<b>R</b>			
request ipsec switch command.....	34		
request security certificate (signed) command.....	31		
request security certificate (unsigned)			
command.....	32		
request security key-pair command.....	33		
request system certificate add command.....	35		
<b>S</b>			
security certificate See certificates			
show ike security-associations command.....	36		
show interfaces (Encryption) command.....	52		