Junos® OS

Security Services Administration Guide for Routing Devices

Modified: 2017-02-08

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

Junos® OS Security Services Administration Guide for Routing Devices

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

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- M Series
- MX Series
- T Series
- T4000

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

   ```
   commit {
     file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

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

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

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

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

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

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/feedback/.
- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

SSH and SSL

CHAPTER 1

Configuring SSH and SSL for Secure Access to the Router

Configuring SSH Host Keys for Secure Copying of Data

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

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

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

1. Configuring SSH Known Hosts on page 3
2. Configuring Support for SCP File Transfer on page 4
3. Updating SSH Host Key Information on page 4

Configuring SSH Known Hosts

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

```
[edit security ssh-known-hosts]
host corporate-archive-server, ip-address {
```

```
    dsa-key key;
}
host archive-server-url {
    rsa-key key;
}
host server-with-ssh-version-1, ip-address {
    rsa1-key key;
}
```

Host keys are one of the following:

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

Configuring Support for SCP File Transfer

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

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

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

Setting the **archive-sites** statement to point to an SCP URL triggers automatic host key retrieval. At this point, Junos OS connects to the SCP host to fetch the SSH public key, displays the host key message digest or fingerprint as output to the console, and terminates the connection to the server.

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

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

Updating SSH Host Key Information

Typically, SSH host key information is automatically retrieved when you set a URL attribute for SCP using the **archival configuration archive-sites** statement at the **[edit system]**

hierarchy level. However, if you need to manually update the host key database, use one of the following methods.

1. Retrieving Host Key Information Manually on page 5
2. Importing Host Key Information from a File on page 5

Retrieving Host Key Information Manually

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

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

Importing Host Key Information from a File

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

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

Importing SSL Certificates for Junos XML Protocol Support

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

A Junos XML protocol client application can use one of four protocols to connect to the Junos XML protocol server on a router or switch: clear-text (a Junos XML protocol-specific protocol for sending unencrypted text over a TCP connection), SSH, SSL, or Telnet. For clients to use the SSL protocol, you must copy an X.509 authentication certificate onto the router or switch, as described in this topic. You must also include the **xnm-ssl** statement at the **[edit system services]** hierarchy level.

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

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

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

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

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

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

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

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

Related Documentation

- Configuring SSH Host Keys for Secure Copying of Data on page 3
- *Configuring clear-text or SSL Service for Junos XML Protocol Client Applications*

PART 2

Digital Certificates

CHAPTER 2

Understanding How Digital Certificates Can Be Used to Authenticate Users

Digital Certificates Overview

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

A certificate includes the following information:

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

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

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

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

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

Related Documentation

- Configuration Statements for Configuring Digital Certificates for an ES PIC on page 11
- Obtaining a Certificate from a Certificate Authority for an ES PIC on page 12
- Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 13
- Generating a Private and Public Key Pair for Digital Certificates for an ES PIC on page 13
- Configuring Digital Certificates for an ES PIC on page 15
- Configuring an IKE Policy for Digital Certificates for an ES PIC on page 19
- Associating the Configured Security Association with a Logical Interface on page 21

CHAPTER 3

Configuring Digital Certificates

Configuration Statements for Setting Up Digital Certificates for an ES PIC

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

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

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

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

For information about how to configure the **description** and **mode** statements, see "Configuring the Description for an IKE Policy" on page 196. For information about how to configure the IKE proposal, see "Associating Proposals with an IKE Policy" on page 197

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

Related Documentation

- Digital Certificates Overview on page 9

Obtaining a Certificate from a Certificate Authority for an ES PIC

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

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

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

Related Documentation

- Digital Certificates Overview on page 9

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

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

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

Related Documentation

- Example: Requesting a CA Digital Certificate on page 13
- Digital Certificates Overview on page 9

Example: Requesting a CA Digital Certificate

Specify a URL to the SCEP server and the name of the certification authority whose certificate you want: **mycompany.com**. **filename 1** is name of the file that stores the result. The output, "Received CA certificate:" provides the signature for the certificate, which allows you to verify (offline) that the certificate is genuine.

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

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

Related Documentation

- Requesting a CA Digital Certificate for an ES PIC on an M Series or T Series Router on page 13

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

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

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

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

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

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

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

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

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

Related Documentation

- Digital Certificates Overview on page 9

Obtaining a Signed Certificate from the CA for an ES PIC

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

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

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

The following example shows how to obtain a CA signed certificate by referencing the configured **certification-authority** statement **local** . This statement is referenced by the **request security certificate enroll filename *filename* subject *subject* alternative-subject *alternative-subject* certification-authority *certification-authority*** command.

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

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

```
user@host> request security certificate enroll filename I subject c=uk,o=london
  alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv
  domain-name host.xyzcompany.com
CA name: xyz.company.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.com
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To see the certificate enrollment status, check the key
  management process (kmd) log file at /var/log/kmd. <--------------
```

For information about how to use the operational mode commands to obtain a signed certificate, see the CLI Explorer.

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

```
user@host> request security certificate enroll filename m subject c=us ,o=x
  alternative-subject 192.0.2.1 certification-authority local key-file y domain-name
  abc.company.com
```

Related Documentation

- Digital Certificates Overview on page 9

Configuring Digital Certificates for an ES PIC

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

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

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

Tasks to configure digital certificates for ES PICs are:

- Configuring the Certificate Authority Properties for an ES PIC on page 16
- Configuring the Cache Size on page 18
- Configuring the Negative Cache on page 18
- Configuring the Number of Enrollment Retries on page 18

- Configuring the Maximum Number of Peer Certificates on page 19
- Configuring the Path Length for the Certificate Hierarchy on page 19

Configuring the Certificate Authority Properties for an ES PIC

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

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

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

ca-profile-name is the CA profile name.

Tasks for configuring the CA properties are:

1. Specifying the Certificate Authority Name on page 16
2. Configuring the Certificate Revocation List on page 16
3. Configuring the Type of Encoding Your CA Supports on page 17
4. Specifying an Enrollment URL on page 17
5. Specifying a File to Read the Digital Certificate on page 17
6. Specifying an LDAP URL on page 17

Specifying the Certificate Authority Name

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

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

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

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

Configuring the Certificate Revocation List

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

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

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

Configuring the Type of Encoding Your CA Supports

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

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

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

Specifying an Enrollment URL

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

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

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

Specifying a File to Read the Digital Certificate

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

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

Specifying an LDAP URL

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

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

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

Configuring the Cache Size

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

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

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

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

Configuring the Negative Cache

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

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

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

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

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

Configuring the Number of Enrollment Retries

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

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

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

Configuring the Maximum Number of Peer Certificates

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

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

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

Configuring the Path Length for the Certificate Hierarchy

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

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

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

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

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

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

Configuring an IKE Policy for Digital Certificates for an ES PIC

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

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

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

Tasks for configuring an IKE policy for digital certificates are:

1. Configuring the Type of Encoding Your CA Supports on page 20
2. Configuring the Identity to Define the Remote Certificate Name on page 20
3. Specifying the Certificate Filename on page 20
4. Specifying the Private and Public Key File on page 20

Configuring the Type of Encoding Your CA Supports

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

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

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

Configuring the Identity to Define the Remote Certificate Name

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

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

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

Specifying the Certificate Filename

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

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

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

Specifying the Private and Public Key File

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

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

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

Associating the Configured Security Association with a Logical Interface

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

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

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

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

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

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

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

Related Documentation

- Configuring Security Associations for IPsec on an ES PIC on page 181

Configuring Digital Certificates for Adaptive Services Interfaces

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

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

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

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

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

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

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

1. Configuring the Certificate Authority Properties on page 23
2. Configuring the Certificate Revocation List on page 24
3. Managing Digital Certificates on page 25
4. Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27

Configuring the Certificate Authority Properties

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

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

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

Tasks for configuring the Certificate Authority properties are:

1. Specifying the CA Profile Name on page 23
2. Specifying an Enrollment URL on page 23
3. Specifying the Enrollment Properties on page 24

Specifying the CA Profile Name

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

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

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

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

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

Specifying an Enrollment URL

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

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

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

Specifying the Enrollment Properties

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

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

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

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

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

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

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

Configuring the Certificate Revocation List

Tasks to configure the certificate revocation list are:

1. Specifying an LDAP URL on page 24
2. Configuring the Interval Between CRL Updates on page 25
3. Overriding Certificate Verification if CRL Download Fails on page 25

Specifying an LDAP URL

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

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

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

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

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

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

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

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

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

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

Configuring the Interval Between CRL Updates

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

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

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

Overriding Certificate Verification if CRL Download Fails

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

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

Managing Digital Certificates

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

Tasks to manage digital certificates are:

1. Requesting a CA Digital Certificate for AS and Multiservices PICs installed on M Series and T Series Routers on page 26
2. Generating a Public/Private Key Pair on page 26
3. Generating and Enrolling a Local Digital Certificate on page 26

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

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

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

For information about how to configure a CA profile, see "Configuring the Certificate Authority Properties" on page 23.

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

```
user@host> request security pki ca-certificate enroll ca-profile entrust
Received following certificates:
Certificate: C=us, O=juniper
 Fingerprint:00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Certificate: C=us, O=juniper, CN=First Officer
 Fingerprint:bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
Certificate: C=us, O=juniper, CN=First Officer
 Fingerprint:46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

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

Generating a Public/Private Key Pair

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

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

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

Generating and Enrolling a Local Digital Certificate

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

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

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

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

Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8oOXyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH4O6gQ3G
3iHOZfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ7OfO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tasks to configure automatic reenrollment of certificates are:

1. Specify the Certificate ID on page 29
2. Specify the CA Profile on page 29
3. Specify the Challenge Password on page 29
4. Specify the Reenroll Trigger Time on page 29
5. Specify the Regenerate Key Pair on page 29
6. Specify the Validity Period on page 30

Specify the Certificate ID

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

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

Specify the CA Profile

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

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

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

Specify the Challenge Password

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

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

Specify the Reenroll Trigger Time

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

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

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

Specify the Regenerate Key Pair

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

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

Specify the Validity Period

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

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

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

Related Documentation

- Digital Certificates Overview on page 9
- Configuring Digital Certificates for an ES PIC on page 15

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

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

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

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

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

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

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

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

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

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

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

Tasks to configure automatic reenrollment of certificates are:

1. Specify the Certificate ID on page 31
2. Specify the CA Profile on page 31
3. Specify the Challenge Password on page 32
4. Specify the Reenroll Trigger Time on page 32
5. Specify the Regenerate Key Pair on page 32
6. Specify the Validity Period on page 32

Specify the Certificate ID

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

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

Specify the CA Profile

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

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

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

Specify the Challenge Password

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

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

Specify the Reenroll Trigger Time

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

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

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

Specify the Regenerate Key Pair

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

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

Specify the Validity Period

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

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

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

PART 3

Distributed Denial-of-Service (DDoS) Protection

CHAPTER 4

DDoS Overview

Distributed Denial-of-Service (DDoS) Protection Overview

A denial-of-service attack is any attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service attacks involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the router's control plane. This results in an excessive processing load that disrupts normal network operations.

Junos OS DDoS protection enables the router to continue functioning while under an attack. It identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. A single point of DDoS protection management enables network administrators to customize profiles for their network control traffic. Protection and monitoring persists across graceful Routing Engine switchover (GRES) and unified in-service-software-upgrade (ISSU) switchovers. Protection is not diminished as the number of subscribers increases.

To protect against DDoS attacks, you can configure policers for host-bound exception traffic. The policers specify rate limits for individual types of protocol control packets or for all control packet types for a protocol. You can monitor policer actions for packet types and protocol groups at the level of the router, Routing Engine, and line cards. You can also control logging of policer events.

The first line of protection is the policer on the Packet Forwarding Engine.Control traffic is dropped when it exceeds any configured policer values or, for unconfigured policers, the default policer values. Each violation immediately generates a notification to alert operators about a possible attack. The violation is counted, the time that the violation starts is noted, and the time of the last observed violation is noted. When the traffic rate drops below the bandwidth violation threshold, a recovery timer determines when the traffic flow is considered to have returned to normal. If no further violation occurs before the timer expires, the violation state is cleared and a notification is generated.

Policer states and statistics from each line card are relayed to the Routing Engine and aggregated. The policer states are maintained during a switchover. Although line card

statistics and violation counts are preserved during a switchover, Routing Engine policer statistics are not.

Platform Support

Starting in Junos OS Release 14.2, DDoS protection is supported on only specific platforms. Verify that your installation includes any of the following:

- EX9200 switches
- MX Series routers that have only MPCs installed: MX240, MX480, MX960, MX2010, and MX2020.
- MX Series routers with a built-in MPC: MX5, MX10, MX40, MX80, and MX104.

NOTE: **For simplicity, where the text refers to line cards or line card policers, for these routers that means the built-in MPC.**

Because these routers do not have FPC slots, information displayed in FPC fields by show commands actually refers to TFEB.

- T4000 routers that have only Type 5 FPCs installed.

If the router platforms have other line cards in addition to MPCs (MX Series) or Type 5 FPCs (T4000), the CLI accepts the configuration but the other line cards are not protected and so the router is not protected.

Policer Types and Packet Priorities

DDoS protection includes two types of policers:

- An *aggregate policer* is applied to the complete set of packet types that belong to a protocol group. For example, you can configure an aggregate policer that applies to all PPPoE control packet types or to all DHCPv4 control packet types. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for aggregate policers. An aggregate policer is available for all protocol groups. Aggregate policers are supported by all protocol groups.
- An *individual policer*, also referred to as a *packet-type policer*, is allocated for each control packet type within a protocol group. For example, you can configure a policer for one or more types of PPPoE control packets. You can specify bandwidth and burst limits, scale the bandwidth and burst limits, and set a traffic priority for packet-type policers. Individual policers are not available for all protocol groups. See **protocols** for a list of protocol groups that have individual policers.

A control packet is policed first by its individual policer (if supported) and then by its aggregate policer. A packet dropped by the individual policer never reaches the aggregate policer. A packet that passes the individual policer can subsequently be dropped by the aggregate policer.

Each packet type within a protocol group has a default, configurable priority: low, medium, or high. Each control packet competes with other packets for the bandwidth within the

limit imposed by its aggregate policer based on the priority configured for each packet type in the protocol group.

The priority mechanism is absolute. High-priority traffic gets bandwidth in preference to medium- and low-priority traffic. Medium-priority traffic gets bandwidth in preference to low-priority traffic. Low-priority traffic can use only the bandwidth left by high- and medium-priority traffic. If higher-priority traffic takes all of the bandwidth, then all the lower-priority traffic is dropped.

Example of Policer Priority Behavior

For example, consider how you might configure packet types within the PPPoE protocol group. Ignoring other PPPoE packet types for this example, suppose you configure individual policers for PADI and PADT packets, as well as a PPPoE aggregate policer for all those packets. PADT packets are more important than PADI packets, because PADT packets enable the PPPoE application to release resources to accept new connections. Therefore, you might assign high priority to the PADT packets and low priority to the PADI packets.

The aggregate policer imposes a total bandwidth limit for the protocol group. PADT packets passed by their individual policer have access to that bandwidth before PADI packets passed by their individual policer, because the PADT packets have a higher priority. If so many PADT packets are passed that they use all the available bandwidth, then all the PADI packets are dropped, because there is no bandwidth remaining at the aggregate policer.

Policer Hierarchy

DDoS policers are organized to match the hierarchical flow of protocol control traffic. Control traffic arriving from all ports of a line card converges on the Packet Forwarding Engine. Control traffic from all line cards on the router converges on the Routing Engine. Similarly, the DDoS policers are placed hierarchically along the control paths so that excess packets are dropped as early as possible on the path. This design preserves system resources by removing excess, malicious traffic so that the Routing Engine receives only the amount of traffic that it can process. To implement this design, typically five DDoS policers are present: One on the Packet Forwarding Engine (the chipset), two at the line card, and two at the Routing Engine. An aggregate policer is also present on the Packet Forwarding Engine for some protocol groups, for a total of six policers; for simplicity, the text follows the general case. Figure 1 on page 38 shows the policer process for PPPoE traffic. Figure 2 on page 38 shows the policer process for DHCPv4 traffic. (The same process applies to DHCPv6 traffic.)

Figure 1: Policer Hierarchy for PPPoE Packets

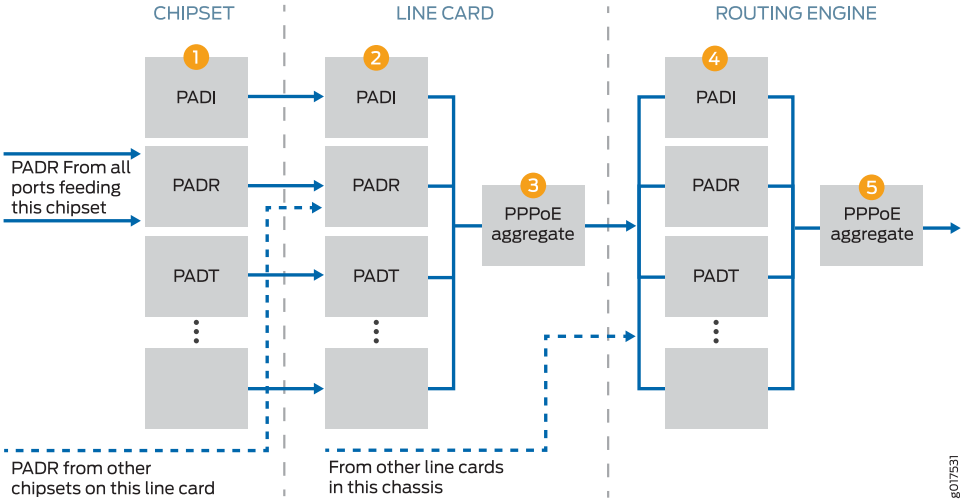
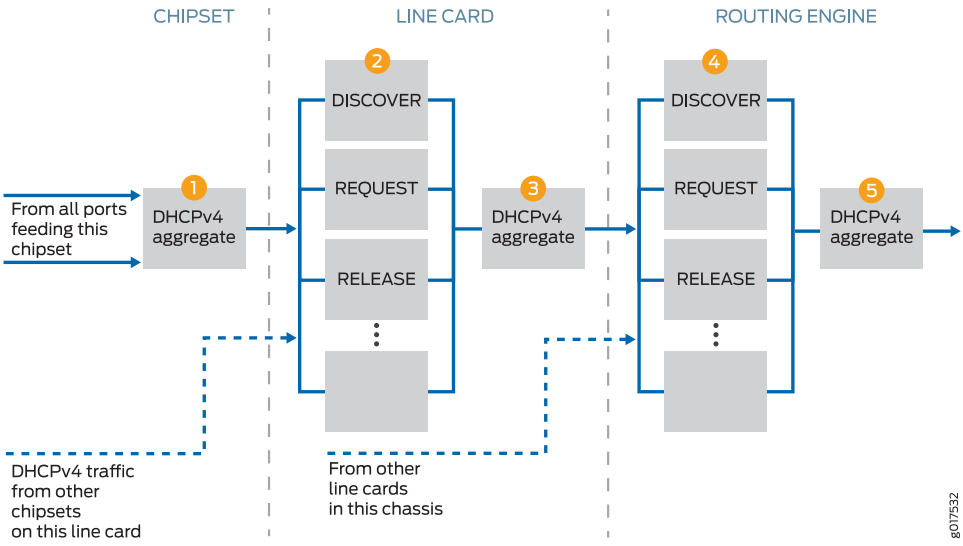


Figure 2: Policer Hierarchy for DHCPv4 Packets



Control packets arrive at the Packet Forwarding Engine for processing and forwarding. The first policer (1) is either an individual policer (Figure 1 on page 38) or an aggregate policer (Figure 2 on page 38).

- The first policer is an individual policer for protocol groups that support individual policers, with two exceptions. For DHCPv4 and DHCPv6 traffic, the first policer is an aggregate policer.
- The first policer is an aggregate policer for protocol groups that support only aggregate policers.

Traffic that passes the first policer is monitored by one or both of the line card policers. If the card has more than one Packet Forwarding Engine, traffic from all Packet Forwarding Engines converges on the line card policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the line card individual policer (2) and then the line card aggregate policer (3). Traffic that passes the individual policer can be dropped by the aggregate policer. Although DHCPv4 and DHCPv6 traffic was monitored by an aggregate policer at the Packet Forwarding Engine, at the line card it is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the line card aggregate policer monitors the traffic.

Traffic that passes the line card policers is monitored by one or both of the Routing Engine policers. Traffic from all the line cards converges on the Routing Engine policers.

- When the traffic belongs to a protocol group that supports individual policers, it passes through the Routing Engine individual policer (4) and then the Routing Engine aggregate policer (5). Traffic that passes the individual policer can be dropped by the aggregate policer. As it was at the line card level, DHCPv4 and DHCPv6 traffic at the Routing Engine is handled like other protocols that support individual policers.
- When the traffic belongs to a protocol group that supports only aggregate policers, only the aggregate policer monitors the traffic.

The result of this design is that traffic for protocol groups that support only aggregate policers is evaluated by three policers. Among other groups, this includes ANCP, dynamic VLAN, FTP, and IGMP traffic. Traffic for protocol groups that support both aggregate and individual policers is evaluated by all five policers. Among other groups, this includes DHCPv4, MLP, PPP, PPPoE, and virtual chassis traffic.

Figure 1 on page 38 shows how DDoS protection polices PPPoE control packets:

1. PADR packets, for example, are evaluated at the first policer on the Packet Forwarding Engine to determine whether they are within the bandwidth limits. PADR packets that exceed the limit are dropped.
2. All PADR packets that pass the policer on all Packet Forwarding Engines on the line card are next evaluated by the line card individual policer. PADR packets that exceed the limit are dropped.
3. All PADR packets that pass the line card individual policer proceed to the line card aggregate policer. PADR packets that exceed the limit are dropped.
4. All PADR packets that are passed by the line card aggregate policers on all line cards on the router proceed to the Routing Engine individual policer. PADR packets that exceed the limit are dropped.
5. Finally, all PADR packets that are passed by the Routing Engine individual policer proceed to the Routing Engine aggregate policer. PADR packets that exceed the limit are dropped. PADR packets that are not dropped here are passed along as safe, normal traffic.

By default, all three individual policers (Packet Forwarding Engine, line card, and Routing Engine) have the same bandwidth limit for a given packet type. This design enables all the control traffic from a Packet Forwarding Engine and line card to reach the Routing Engine, as long as there is no competing traffic of the same type from other Packet Forwarding Engines or line cards. When competing traffic is present, excess packets are dropped at the convergence points. That is, they are dropped at the line card for all competing Packet Forwarding Engines and at the Routing Engine for all competing line cards.

Example of Policer Bandwidth Limit Behavior

For example, suppose you set the policer bandwidth for PADI packets to 1000 packets per second. This value applies to the individual PADI policers at the Packet Forwarding Engine, the line card, and the Routing Engine. If only the card in slot 5 is receiving PADI packets, then up to 1000 PADI pps can reach the Routing Engine (if the PPPoE aggregate policer is not exceeded). However, suppose the card in slot 9 is also receiving PADI packets at 1000 pps and that its PPPoE aggregate policer is not exceeded. The traffic passes the individual and aggregate policers at both line cards and proceeds to the Routing Engine. At the Routing Engine, the combined bandwidth is 2000 pps. Because the PADI policer at the Routing Engine allows only 1000 PADI pps to pass, it drops the excess 1000 packets. It continues to drop the excess packets for as long as the bandwidth is exceeded.

You can apply a scaling factor for both the bandwidth limit and the burst limit at the line card. This enables you to fine-tune the traffic limits for each slot. For example, suppose the individual policer sets the PADI packet bandwidth to 1000 pps and the burst size to 50,000 packets. You can reduce the traffic limit for PADI packets on any line card by specifying the slot number and scaling factor. A bandwidth scaling factor of 20 for slot 5 reduces the traffic in this example to 20 percent of 1000 pps, or 200 pps for the line card in that slot. Similarly, a burst scaling factor of 50 for that slot reduces the burst size by 50 percent to 25,000 packets. By default, scaling factors are set to 100 so traffic can pass through at 100 percent of the rate limit.

DDoS Protection Compared to Subscriber Login Packet Overload Protection

In addition to the DDoS protection capability, MX Series routers also have a built-in subscriber login overload protection mechanism. The login overload protection mechanism (also called a load-throttling mechanism) monitors the incoming subscriber login packets and admits only what the system is capable of handling in accordance with the prevailing load on the system. Packets in excess of what the system can handle are discarded. By shedding this excess load, the system is able to maintain optimal performance and prevent any degradation of login-completion rate under overload conditions. This mechanism uses minimal resources and is enabled by default; no user configuration is required.

The protection provided by this mechanism is secondary to what DDoS protection provides as a first level of defense against high rates of incoming packets. DDoS protection operates on the Packet Forwarding Engine and protects against all packet types of all protocols. In contrast, the login overload protection mechanism is located on the Routing Engine and specifically operates only on incoming connection-initiation packets such as DHCPv4 DHCPDISCOVER, DHCPv6 SOLICIT, and PPPoE PADI packets.

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, DDoS protection is supported on only specific platforms.

Related Documentation

- Configuring Protection Against DDoS Attacks on page 43
- DDoS Protection Flow Detection Overview on page 66

Understanding Distributed Denial-of-Service Protection with IPv6 Neighbor Discovery Protocol

Starting with Junos OS Release 16.1R1, you can address the IPv6 Neighbor Discovery Protocol denial-of-service issue at the Routing Engine. A denial-of-service (DoS) attack is any attempt to deny valid user access to network or server resources by using up all the resources of the network element or server. Distributed denial-of-service attacks (DDoS) involve an attack from multiple sources, enabling a much greater amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the router or switch control plane. This results in an excessive processing load that disrupts normal network operations.

In IPv4, subnets are generally small, made just large enough to cover the actual number of machines on the subnet. In contrast, the default IPv6 subnet size is /64, a number so large it covers billions of addresses, the overwhelming majority of which will be unassigned. The large address space of IPv6 allows attackers to trigger huge numbers of resolves that exhaust the router resources. Consequently, simplistic implementations of neighbor discovery might fail to perform as desired when they carry out address resolution of large numbers of unassigned addresses. Such failures can be triggered either intentionally by an attacker launching a denial-of-service attack (DoS) to exploit this vulnerability, or unintentionally due to the use of legitimate operational tools that scan networks for inventory and other purposes.

The Neighbor Discovery Protocol DDoS policer uses an aggregate policer to throttle the packets rate of following message types to mitigate the problem:

- Router advertisement (RA)—Messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
- Router solicitation (RS)—Messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- Neighbor solicitation (NS)—Messages used for duplicate address detection and to test reachability of neighbors.

A host can verify that its address is unique by sending a neighbor solicitation message destined to the new address. If the host receives a neighbor advertisement in reply, the address is a duplicate.

- Neighbor advertisement (NA)—Messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.

NOTE: You can disabled or deactivate the DDoS policer. However, the overall bandwidth will then be restricted to 8360 packets per second (PPS). When the incoming IPv6 NDP packet rate rises above PPS, RS and NS types, IPv6 NDP packets will be prioritized over other NDP packets and other NDP packets will be discarded.

Release History Table

Release	Description
16.1	Starting with Junos OS Release 16.1R1, you can address the IPv6 Neighbor Discovery Protocol denial-of-service issue at the Routing Engine.

Related Documentation

-

CHAPTER 5

Configuring DDoS Protection

Configuring Protection Against DDoS Attacks

DDoS protection is enabled by default for all supported protocol groups and packet types. Default values are present for bandwidth, bandwidth scale, burst, burst scale, priority, and recover time. You can change the DDoS configuration for individual packet types within a protocol group or for the aggregate policer for the protocol group. DDoS logging is enabled by default, but you can disable it globally for all DDoS events or for individual packet types within a protocol group. You can also fine-tune monitoring of DDoS events by configuring tracing operations.

You can disable DDoS protection at the Routing Engine and for all line cards either globally or for individual packet types within a protocol group.

NOTE: DDoS protection is supported only on MX Series routers that have only MPCs installed, T4000 routers that have only FPC5s installed, EX9200 switches, QFX5200 switches, and QFX10000 switches. If the router platforms have other line cards in addition to MPCs (MX Series) or FPC5s (T4000), the CLI accepts the configuration but the other line cards are not protected and so the router is not protected. Neither QFX10002 switches nor QFX5200 switches support policers at the Routing Engine.

To configure DDoS protection:

1. (Optional) Configure global DDoS settings.

   See "Disabling DDoS Protection Policers and Logging Globally" on page 57.

2. (Optional) Configure DDoS settings for individual packet types.

   For MX Series routers, T4000 routers, or EX9200 switches, see "Configuring DDoS Protection Policers for Individual Packet Types" on page 54. For QFX10000 switches, see *Configuring DDoS Protection Policers on QFX Series Switches*.

3. (Optional) Configure tracing for DDoS operations.

   See "Tracing DDoS Protection Operations" on page 58.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 35
- *Understanding Distributed Denial-of-Service Protection on QFX Series Switches*
- Example: Configuring DDoS Protection on page 44
- *Example: Configuring DDoS Protection on QFX Series Switches*

Example: Configuring DDoS Protection

This example shows how to configure DDoS protection that enables the router to quickly identify an attack and prevent a flood of malicious control packets from exhausting system resources.

Requirements

DDoS protection requires the following hardware and software:

- MX Series routers that have only MPCs installed, T4000 Core Routers that have only FPC5s installed, EX9200 switches.

NOTE: If a router has other cards in addition to MPCs or FPC5s, the CLI accepts the configuration but the other cards are not protected and therefore the router is not protected.

- Junos OS Release 11.2 or later

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Distributed denial-of-service attacks use multiple sources to flood a network or router with protocol control packets. This malicious traffic triggers a large number of exceptions in the network and attempts exhaust the system resources to deny valid users access to the network or server.

This example describes how to configure rate-limiting policers that identify excess control traffic and drop the packets before the router is adversely affected. Sample tasks include configuring policers for particular control packet types within a protocol group, configuring an aggregate policer for a protocol group and bypassing that policer for a particular control packet type, and specifying trace options for DDoS operations.

This example does not show all possible configuration choices.

Configuration

CLI Quick Configuration

To quickly configure DDoS protection for protocol groups and particular control packet types, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit system
set ddos-protection protocols dhcpv4 aggregate bandwidth 669
set ddos-protection protocols dhcpv4 aggregate burst 6000
set ddos-protection protocols dhcpv4 discover bandwidth 100
set ddos-protection protocols dhcpv4 discover recover-time 200
set ddos-protection protocols dhcpv4 discover burst 300
set ddos-protection protocols dhcpv4 offer priority medium
set ddos-protection protocols dhcpv4 offer bypass-aggregate
set ddos-protection protocols dhcpv4 offer fpc 1 bandwidth-scale 80
set ddos-protection protocols dhcpv4 offer fpc 1 burst-scale 75
set ddos-protection protocols pppoe aggregate bandwidth 800
set ddos-protection traceoptions file ddos-trace size 10m
set ddos-protection traceoptions flag all
top
```

Step-by-Step Procedure

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

To configure DDoS protection:

1. Specify a protocol group.

   ```
   [edit system ddos-protection protocols]
   user@host# edit dhcpv4
   ```

2. Configure the maximum traffic rate for the DHCPv4 aggregate policer; that is, for the combination of all DHCPv4 packets.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set aggregate bandwidth 669
   ```

3. Configure the maximum burst rate for the DHCPv4 aggregate policer.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set aggregate burst 6000
   ```

4. Configure the maximum traffic rate for the DHCPv4 policer for discover packets.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set discover bandwidth 100
   ```

5. Decrease the recover time for violations of the DHCPv4 discover policer.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set discover recover-time 200
   ```

6. Configure the maximum burst rate for the DHCPv4 discover policer.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set discover burst 300
   ```

7. Increase the priority for DHCPv4 offer packets.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set offer priority medium
   ```

8. Prevent offer packets from being included in the aggregate bandwidth; that is, offer packets do not contribute towards the combined DHCPv4 traffic to determine whether the aggregate bandwidth is exceeded. However, the offer packets are still included in traffic rate statistics.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set offer bypass-aggregate
   ```

9. Reduce the bandwidth and burst size allowed before violation is declared for the DHCPv4 offer policer on the MPC or FPC5 in slot 1.

   ```
   [edit system ddos-protection protocols dhcpv4]
   user@host# set offer fpc 1 bandwidth-scale 80
   user@host# set offer fpc 1 burst-scale 75
   ```

10. Configure the maximum traffic rate for the PPPoE aggregate policer, that is, for the combination of all PPPoE packets.

    ```
    [edit system ddos-protection protocols dhcpv4]
    user@host# up
    ```

```
[edit system ddos-protection protocols]
user@host# set pppoe aggregate bandwidth 800
```

11. Configure tracing for all DDoS protocol processing events.

```
[edit system ddos-protection traceoptions]
user@host# set file ddos-log
user@host# set file size 10m
user@host# set flag all
```

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

```
[edit system]
user@host# show ddos-protection
traceoptions {
  file ddos-trace size 10m;
  flag all;
}
  protocols {
    pppoe {
      aggregate {
        bandwidth 800;
      }
    }
    dhcpv4 {
      aggregate {
        bandwidth 669;
        burst 6000;
      }
      discover {
        bandwidth 100;
        burst 300;
        recover-time 200;
      }
      offer {
        priority medium;
        fpc 1 {
          bandwidth-scale 80;
          burst-scale 75;
        }
        bypass-aggregate;
      }
    }
  }
```

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

Verification

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

- Verifying the DHCPv4 DDoS Protection Configuration and Operation on page 48
- Verifying the PPPoE DDoS Configuration on page 51

Verifying the DHCPv4 DDoS Protection Configuration and Operation

Purpose Verify that the DHCPv4 aggregate and protocol policer values have changed from the default. With DHCPv4 and PPPoE traffic flowing, verify that the policers are working correctly. You can enter commands to display the individual policers you are interested in, as shown here, or you can enter the **show ddos-protection protocols dhcpv4** command to display this information for all DHCPv4 packet types.

Action From operational mode, enter the **show ddos-protection protocols dhcpv4 aggregate** command.

```
user@host> show ddos-protection protocols dhcpv4 aggregate
Protocol Group: DHCPv4

  Packet type: aggregate (aggregate for all DHCPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:        669 pps
      Burst:            6000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
    System-wide information:
      Aggregate bandwidth is no longer being violated
        No. of FPCs currently receiving excess traffic: 0
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-03-10 06:27:47 PST
        Violation last seen at:      2011-03-10 06:28:57 PST
        Duration of violation: 00:01:10 Number of violations: 1
      Received:  71064              Arrival rate:     0 pps
      Dropped:   23115              Max arrival rate: 1000 pps
    Routing Engine information:
      Bandwidth: 669 pps, Burst: 6000 packets, enabled
      Aggregate policer is never violated
      Received:  36130              Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 671 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled
      Aggregate policer is no longer being violated
        Violation first detected at: 2011-03-10 06:27:48 PST
        Violation last seen at:      2011-03-10 06:28:58 PST
        Duration of violation: 00:01:10 Number of violations: 1
      Received:  71064              Arrival rate:     0 pps
      Dropped:   34934              Max arrival rate: 1000 pps
        Dropped by individual policers: 11819
        Dropped by aggregate policer: 23115
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 discover** command.

```
user@host> show ddos-protection protocols dhcpv4 discover
Protocol Group: DHCPv4

  Packet type: discover (DHCPv4 DHCPDISCOVER)
    Individual policer configuration:
      Bandwidth:        100 pps
      Burst:            300 packets
      Priority:         low
      Recover time:     200 seconds
      Enabled:          Yes
      Bypass aggregate: No
    System-wide information:
      Bandwidth is no longer being violated
        No. of FPCs currently receiving excess traffic: 0
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-03-10 06:28:34 PST
        Violation last seen at:      2011-03-10 06:28:55 PST
        Duration of violation: 00:00:21 Number of violations: 1
      Received:  47949              Arrival rate:     0 pps
      Dropped:   11819              Max arrival rate: 671 pps
    Routing Engine information:
      Bandwidth: 100 pps, Burst: 300 packets, enabled
      Policer is never violated
      Received:  36130              Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (100 pps), Burst: 100% (300 packets), enabled
      Policer is no longer being violated
        Violation first detected at: 2011-03-10 06:28:35 PST
        Violation last seen at:      2011-03-10 06:28:55 PST
        Duration of violation: 00:00:20 Number of violations: 1
      Received:  47949              Arrival rate:     0 pps
      Dropped:   11819              Max arrival rate: 671 pps
        Dropped by this policer: 11819
        Dropped by aggregate policer: 0
```

From operational mode, enter the **show ddos-protection protocols dhcpv4 offer** command.

```
user@host> show ddos-protection protocols dhcpv4 offer
Protocol Group: DHCPv4

  Packet type: offer (DHCPv4 DHCPOFFER)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: Yes
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
```

```
    Dropped by aggregate policer: 0
FPC slot 1 information:
  Bandwidth: 80% (800 pps), Burst: 75% (750 packets), enabled
  Policer is never violated
  Received:  0                  Arrival rate:     0 pps
  Dropped:   0                  Max arrival rate: 0 pps
    Dropped by aggregate policer: 0
```

Meaning The output of these commands lists the policer configuration and traffic statistics for the DHCPv4 aggregate, discover, and offer policers respectively.

The **Aggregate policer configuration** section in the first output example and **Individual policer configuration** sections in the second and third output examples list the configured values for bandwidth, burst, priority, recover time, and bypass-aggregate.

The **System-wide information** section shows the total of all DHCPv4 traffic statistics and violations for the policer recorded across all line cards and at the Routing Engine. The **Routing engine information** section shows the traffic statistics and violations for the policer recorded at the Routing Engine. The **FPC slot 1 information** section shows the traffic statistics and violations for the policer recorded only at the line card in slot 1.

The output for the aggregate policer in this example shows the following information:

- The **System-wide information** section shows that 71,064 DHCPv4 packets of all types were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 23,115 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 71,064 DHCPv4 packets, but its aggregate policer experienced a violation and dropped the 23,115 packets shown in the other section. The line card individual policers dropped an additional 11,819 packets.
- The **Routing Engine information** section shows that the remaining 36,130 packets all reached the Routing Engine and that its aggregate policer dropped no additional packets.

  The difference between the number of DHCPv4 packets received and dropped at the line card [71,064 - (23,115 + 11,819)] matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1received any DHCPv4 packets.

The output for the DHCPv4 discover packet policer in this example shows the following information:

- The **System-wide information** section shows that 47,949 DHCPv4 discover packets were received across all line cards and the Routing Engine. The section shows a single violation with a time stamp and that the aggregate policer at a line card dropped 11,819 of these packets.
- The **FPC slot 1 information** section shows that this line card received all 47,949 DHCPv4 discover packets, but its individual policer experienced a violation and dropped the 11,819 packets shown in the other section.

- The **Routing Engine information** section shows that only 36,130 DHCPv4 discover packets reached the Routing Engine and that it dropped no additional packets.

  The difference between the number of DHCPv4 discover packets received and dropped at the line card (47,949 - 11,819) matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1received any DHCPv4 discover packets.

The output for the DHCPv4 offer packet policer in this example shows the following information:

- This individual policer has never been violated at any location.
- No DHCPv4 offer packets have been received at any location.

Verifying the PPPoE DDoS Configuration

Purpose Verify that the PPPoE policer values have changed from the default.

Action From operational mode, enter the **show ddos-protection protocols pppoe parameters brief** command.

```
user@host> show ddos-protection protocols pppoe parameters brief
Number of policers modified: 1
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
pppoe       aggregate   800*      2000   medium   300       yes     --     no
pppoe       padi        500       500    low      300       yes     no     no
pppoe       pado        0         0      low      300       yes     no     no
pppoe       padr        500       500    medium   300       yes     no     no
pppoe       pads        0         0      low      300       yes     no     no
pppoe       padt        1000      1000   high     300       yes     no     no
pppoe       padm        0         0      low      300       yes     no     no
pppoe       padn        0         0      low      300       yes     no     no
```

From operational mode, enter the **show ddos-protection protocols pppoe padi** command, and enter the command for **padr** as well.

```
user@host> show ddos-protection protocols pppoe padi
Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    System-wide information:
      Bandwidth for this packet type is being violated!
        Number of slots currently receiving excess traffic: 1
        Number of slots that have received excess traffic:  1
        Violation first detected at: 2011-03-09 11:26:33 PST
        Violation last seen at:      2011-03-10 12:03:44 PST
        Duration of violation: 1d 00:37 Number of violations: 1
      Received:  704832908          Arrival rate:     8000 pps
```

```
    Dropped:   660788548           Max arrival rate: 8008 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  39950330            Arrival rate:     298 pps
    Dropped:   0                   Max arrival rate: 503 pps
      Dropped by aggregate policer: 0
  FPC slot 3 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Policer is currently being violated!
      Violation first detected at: 2011-03-09 11:26:35 PST
      Violation last seen at:      2011-03-10 12:03:44 PST
      Duration of violation: 1d 00:37 Number of violations: 1
    Received:  704832908           Arrival rate:     8000 pps
    Dropped:   664882578           Max arrival rate: 8008 pps
      Dropped by this policer: 660788548
      Dropped by aggregate policer: 4094030

user@host> show ddos-protection protocols pppoe padr
Protocol Group: PPPoE

  Packet type: padr (PPPoE PADR)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    System-wide information:
      Bandwidth for this packet type is being violated!
        Number of slots currently receiving excess traffic: 1
        Number of slots that have received excess traffic:  1
        Violation first detected at: 2011-03-10 06:21:17 PST
        Violation last seen at:      2011-03-10 12:04:14 PST
        Duration of violation: 05:42:57 Number of violations: 1
      Received:  494663595           Arrival rate:     24038 pps
      Dropped:   484375900           Max arrival rate: 24062 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  10287695            Arrival rate:     500 pps
      Dropped:   0                   Max arrival rate: 502 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is currently being violated!
        Violation first detected at: 2011-03-10 06:21:18 PST
        Violation last seen at:      2011-03-10 12:04:14 PST
        Duration of violation: 05:42:56 Number of violations: 1
      Received:  494663595           Arrival rate:     24038 pps
      Dropped:   484375900           Max arrival rate: 24062 pps
        Dropped by this policer: 484375900
        Dropped by aggregate policer: 0
```

Meaning The output from the **show ddos-protection protocols pppoe parameters brief** command lists the current configuration for each of the individual PPPoE packet policers and the PPPoE aggregate policer. A change from a default value is indicated by an asterisk next to the modified value. The only change made to PPPoE policers in the configuration steps was to the aggregate policer bandwidth; this change is confirmed in the output. Besides

the configuration values, the command output also reports whether a policer has been disabled, whether it bypasses the aggregate policer (meaning that the traffic for that packet type is not included for evaluation by the aggregate policer), and whether the policer has been modified for one or more line cards.

The output of the **show ddos-protection protocols pppoe padi** command in this example shows the following information:

- The **System-wide information** section shows that 704,832,908 PPPoE PADI packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the aggregate policer at the line card dropped 660,788,548 of the PADI packets.
- The **FPC slot 3 information** section shows that this line card received all 704,832,908 PADI packets. Its individual policer dropped 660,788,548 of those packets and its aggregate policer dropped the other 4,094,030 packets. The violation is ongoing and has lasted more than a day.
- The **Routing Engine information** section shows that only 39,950,330 PADI packets reached the Routing Engine and that it dropped no additional packets.

  The difference between the number of PADI packets received and dropped at the line card [704,832,908 - (660,788,548 + 4,094030)] matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 3 received any PADI packets.

The output of the **show ddos-protection protocols pppoe padr** command in this example shows the following information:

- The **System-wide information** section shows that 494,663,595 PPPoE PADR packets were received across all line cards and the Routing Engine. The section shows a single violation on a line card that is still in progress, and that the policer at the line card dropped 484,375,900 of the PADR packets.
- The **FPC slot 1 information** section shows that this line card received all 494,663,595 PADR packets. Its individual policer dropped 484,375,900 of those packets. The violation is ongoing and has lasted more than five hours.
- The **Routing Engine information** section shows that only 10,287,695 PADR packets reached the Routing Engine and that it dropped no additional packets.

  The difference between the number of PADR packets received and dropped at the line card (494,663,595 - 484,375,900) matches the number received at the Routing Engine. That might not always be the case, because packets can be received and dropped at more than one line card. In this example, only the line card in slot 1 received any PADR packets.

NOTE: This scenario is unrealistic in showing all PADI packets received on one line card and all PADR packets on a different line card. The intent of the scenario is to illustrate how policer violations are reported for individual line cards.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 35
- Configuring Protection Against DDoS Attacks on page 43

Configuring DDoS Protection Policers for Individual Packet Types

DDoS policers are applied to control packet traffic. You configure the maximum allowed traffic rate, maximum burst size, traffic priority, and how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack. You can also scale the bandwidth and burst values for individual line cards so that the policers at this level trigger at lower thresholds than the overall protocol or packet thresholds.

You can configure an aggregate policer for any protocol group. The aggregate policer applies to the combination of all types of control packet traffic for that group. When you configure an aggregate policer for certain protocol groups, you can optionally bypass that policer for one or more particular packet types in that group. For those same groups, you can configure policers for individual packet types instead of configuring an aggregate policer.

DDoS protection is enabled by default. Although all policers have default parameter values, these values might not accurately reflect the control traffic pattern of your network.

BEST PRACTICE: We recommend that you model your network to determine the best values for your situation. Before you configure policers for your network, you can quickly view the default values for all packet types from operational mode by issuing the show ddos-protection protocols parameters brief command. You can also use the command to specify a single protocol group of interest; for example, issue the show ddos-protection protocols dhcpv4 parameters brief command.

You can disable a packet type's policer at either the Routing Engine, at a specified line card, or for all line cards. You can also disable logging of all DDoS events for individual packet types within a protocol group.

To configure individual, packet-level DDoS settings:

1. Specify the protocol group.

   ```
   [edit system ddos-protection protocols]
   user@host# edit protocol-group
   ```

   For example, to specify the DHCPv4 protocol group:

   ```
   [edit system ddos-protection protocols]
   user@host# edit dhcpv4
   ```

2. Specify the packet type or the combination of all packet types in the group.

   ```
   [edit system ddos-protection protocols protocol-group]
   user@host# set packet-type
   ```

   or

```
[edit system ddos-protection protocols protocol-group]
user@host# set aggregate
```

For example, to specify the DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4]
user@host# edit release
```

3. (Optional) Configure the maximum traffic rate the policer allows for the packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bandwidth packets-per-second
```

For example, to set a bandwidth of 600 packets per second for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set bandwidth 600
```

4. (Optional) Configure the maximum number of packets of the packet type that the policer allows in a burst of traffic.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set burst size
```

For example, to set a maximum of 5000 DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set burst 5000
```

5. (Optional) Set the traffic priority.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set priority level
```

For example, to specify a medium priority for DHCPv4 release packets:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set priority medium
```

6. (Optional) Configure how much time must pass since the last violation before the traffic flow is considered to have recovered from the attack.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set recover-time seconds
```

For example, to specify that 600 seconds must have passed since the last violation of the DHCPv4 release packet policer:

```
[edit system ddos-protection protocols dhcpv4 release]
user@host# set recover-time 600
```

7. (Optional) Bypass the aggregate policer configuration. This is relevant only when an aggregate policer is configured for the protocol group.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set bypass-aggregate
```

For example, to bypass the aggregate policer for DHCPv4 renew packets:

```
[edit system ddos-protection protocols dhcpv4 renew]
user@host# set bypass-aggregate
```

8. (Optional) Disable line card policers for the packet type on all line cards.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-fpc
```

NOTE: When you disable line card policers globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the line card policer for DHCPv4 bootp packets:

```
[edit system ddos-protection protocols dhcpv4 bootp]
user@host# set disable-fpc
```

9. (Optional) Disable DDoS event logging for only this packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-logging
```

NOTE: Events disabled for the packet are associated with policer violations; logging of flow detection culprit flow events is not affected by this statement.

NOTE: When you disable DDoS event logging globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable DDoS event logging line card policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set disable-logging
```

10. (Optional) Disable the Routing Engine policer for only this packet type.

```
[edit system ddos-protection protocols protocol-group packet-type]
user@host# set disable-routing-engine
```

NOTE: When you disable the Routing Engine policer globally at the **[edit system ddos-protection global]** hierarchy level, the global setting overrides the per-packet type setting shown in this step. If you subsequently remove the global configuration, then the per-packet type configuration takes effect.

For example, to disable the Routing Engine policer for DHCPv4 discover packets:

```
[edit system ddos-protection protocols dhcpv4 discover]
```

```
user@host# set disable-routing-engine
```

11. (Optional) Configure packet-level settings for the packet type on a single line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type]
    user@host# edit fpc slot-number
    ```

    For example, to access DHCPv4 discover packet settings on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover]
    user@host# edit fpc 3
    ```

12. (Optional) Scale the policer bandwidth for the packet type on the line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set bandwidth-scale percentage
    ```

    For example, to scale the bandwidth to 80 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit bandwidth-scale 80
    ```

13. (Optional) Scale the policer burst size for the packet type on the line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set burst-scale percentage
    ```

    For example, to scale the maximum bandwidth to 75 percent of the all-line-card setting configured for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit burst-scale 75
    ```

14. (Optional) Disable the line card policer for the packet type on a particular line card.

    ```
    [edit system ddos-protection protocols protocol-group packet-type fpc slot-number]
    user@host# set disable-fpc
    ```

    For example, to disable the line card policer for DHCPv4 discover packets on the line card in slot 3:

    ```
    [edit system ddos-protection protocols dhcpv4 discover fpc 3]
    user@host# edit disable-fpc
    ```

Related Documentation

- Configuring Protection Against DDoS Attacks on page 43
- For a list of supported protocol groups and packet types, see protocols on page 277.
- Example: Configuring DDoS Protection on page 44

Disabling DDoS Protection Policers and Logging Globally

DDoS policers are enabled by default for all supported protocol groups and packet types.

On MX Series routers, T4000 routers, and EX9200 switches, policers are established at the level of the individual line card and the Routing Engine. You can disable the line card policers globally for all MPCs or FPC5s. You can also disable the Routing Engine policer. When you disable either of these policers, the policers at that level for all protocol groups and packet types are disabled.

On both QFX10002 switches and QFX5200 switches, policers are established at the level of individual line cards only. If you disable line-card policers globally, DDoS protection is disabled on the switch.

DDoS logging is also enabled by default. You can disable all DDoS event logging (including flow detection event logging) for all protocol groups and packet types across the router or switch.

NOTE: **The global configuration for disabling policers and logging overrides any local configuration for packet types.**

To configure global DDoS settings:

1. (Optional) Disable line card policers.

   ```
   [edit system ddos-protection global]
   user@host# set disable-fpc
   ```

2. (Optional) Disable Routing Engine policers (not supported on QFX10002 switches).

   ```
   [edit system ddos-protection global]
   user@host# set disable-routing-engine
   ```

3. (Optional) Disable event logging.

   ```
   [edit system ddos-protection global]
   user@host# set disable-logging
   ```

Related Documentation

- Configuring Protection Against DDoS Attacks on page 43
- Configuring DDoS Protection Policers for Individual Packet Types on page 54 (MX Series routers, T4000 routers, or EX9200 switches)
- *Configuring DDoS Protection Policers on QFX Series Switches* (QFX10000 switches)

Tracing DDoS Protection Operations

The Junos OS trace feature tracks DDoS protection operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **jddosd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename*.0.gz**. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until

the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the System Log Explorer.)

By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure all aspects of DDoS tracing operations:

1. (Optional) Configure a trace log filename.

   See "Configuring the DDoS Protection Trace Log Filename" on page 59.

2. (Optional) Configure the number and size of trace logs.

   See "Configuring the Number and Size of DDoS Protection Log Files" on page 60.

3. (Optional) Configure user access to trace logs.

   See "Configuring Access to the DDoS Protection Log File" on page 60.

4. (Optional) Configure a regular expression to filter the information to be included in the trace log.

   See "Configuring a Regular Expression for DDoS Protection Messages to Be Logged" on page 61.

5. (Optional) Configure flags to specify which events are logged.

   See "Configuring the DDoS Protection Tracing Flags" on page 61.

6. (Optional) Configure a severity level for messages to specify which event messages are logged.

   See "Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged" on page 61.

Related Documentation

- Example: Configuring DDoS Protection on page 44

Configuring the DDoS Protection Trace Log Filename

By default, the name of the file that records trace output for DDoS protection is **jddosd**. You can specify a different name with the **file** option.

To configure the filename for subscriber management database tracing operations:

- Specify the name of the file used for the trace output.

  ```
  [edit system ddos-protection traceoptions]
  user@host# set file ddos_logfile_1
  ```

Related Documentation

- Tracing DDoS Protection Operations on page 58

Configuring the Number and Size of DDoS Protection Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format ***.number*.gz**. The newest archived file is **.0.gz** and the oldest archived file is ***.(maximum number)-1*.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, ***filename***, reaches 2 MB, ***filename*** is compressed and renamed ***filename*.0.gz**, and a new file called ***filename*** is created. When the new ***filename*** reaches 2 MB, ***filename*.0.gz** is renamed ***filename*.1.gz** and ***filename*** is compressed and renamed ***filename*.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, ***filename*.19.gz**, is simply overwritten when the next oldest file, ***filename*.18.gz** is compressed and renamed to ***filename*.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

  [edit system ddos-protection traceoptions]
  user@host# set file ddos_1_logfile_1 files 20 size 2097152

Related Documentation

- Tracing DDoS Protection Operations on page 58

Configuring Access to the DDoS Protection Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable.

  [edit system ddos-protection traceoptions]
  user@host# set file ddos_1 _logfile_1 world-readable

To explicitly set the default behavior, only the user who configured tracing can read the log file:

- Configure the log file to be no-world-readable.

  [edit system ddos-protection traceoptions]
  user@host# set file ddos_1 _logfile_1 no-world-readable

Related Documentation
- Tracing DDoS Protection Operations on page 58

Configuring a Regular Expression for DDoS Protection Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events.

You can refine the output by including regular expressions to be matched.

To configure regular expressions to be matched:

- Configure the regular expression.

  [edit system ddos-protection traceoptions]
  user@host# **set file ddos_1 _logfile_1 match *regex***

Related Documentation
- Tracing DDoS Protection Operations on page 58

Configuring the DDoS Protection Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

  [edit system ddos-protection traceoptions]
  user@host# **set flag *flag***

Related Documentation
- Tracing DDoS Protection Operations on page 58

Configuring the Severity Level to Filter Which DDoS Protection Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages . By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

  [edit system ddos-protection traceoptions]
  user@host# **set level *severity***

Related Documentation

- Tracing DDoS Protection Operations on page 58

Verifying and Managing DDoS Protection

Purpose View or clear information about DDoS configurations, states, and statistics.

Action

- To display the DDoS policer configuration, violation state, and statistics for all packet types in all protocol groups:

  user@host> show ddos-protection protocols

  If you issue the command before you make any configuration changes, the default policer values are displayed.

- To display the DDoS policer configuration, violation state, and statistics for a particular packet type in a particular protocol group:

  user@host> show ddos-protection protocols ***protocol-group packet-type***

- To display only the number of DDoS policer violations for all protocol groups:

  user@host> show ddos-protection protocols **violations**

- To display a table of the DDoS configuration for all packet types in all protocol groups:

  user@host> show ddos-protection protocols **parameters brief**

- To display a complete list of packet statistics and DDoS violation statistics for all packet types in all protocol groups:

  user@host> show ddos-protection protocols **statistics detail**

- To display global DDoS violation statistics:

  user@host> show ddos-protection statistics

- To display the DDoS version number:

  user@host> show ddos-protection version

- To clear DDoS statistics for all packet types in all protocol groups:

  user@host> clear ddos-protection protocols **statistics**

- To clear DDoS statistics for all packet types in a particular protocol group:

  user@host> clear ddos-protection protocols ***protocol-group*** **statistics**

- To clear DDoS statistics for a particular packet type in a particular protocol group:

  user@host> clear ddos-protection protocols ***protocol-group*** **statistics*packet-type***

- To clear DDoS violation states for all packet types in all protocol groups:

  user@host> clear ddos-protection protocols **states**

- To clear DDoS violation states for all packet types in a particular protocol group:

  user@host> clear ddos-protection protocols ***protocol-group*** **states**

- To clear DDoS violation states for a particular packet type in a particular protocol group:

user@host> clear ddos-protection protocols *protocol-group* states*packet-type*

Related Documentation

- Verifying and Managing Flow Detection on page 80

CHAPTER 6

Configuring Flow Detection for DDoS Protection

DDoS Protection Flow Detection Overview

Flow detection is an enhancement to DDoS protection that supplements the DDoS policer hierarchies; it is part of a complete DDoS protection solution. Flow detection uses a limited amount of hardware resources to monitor the arrival rate of host-bound flows of control traffic. Flow detection is much more scalable than a solution based on filter policers. Filter policers track all flows, which consumes a considerable amount of resources. In contrast, flow detection only tracks flows it identifies as suspicious, using far fewer resources to do so.

The flow detection application has two interrelated components, detection and tracking. Detection is the process where flows suspected of being improper are identified and subsequently controlled. Tracking is the process where flows are tracked to determine whether they are truly hostile and when these flows recover to within acceptable limits.

Flow Detection and Control

Flow detection is disabled by default. When you enable it at the **[edit system ddos-protection global]** hierarchy level, the application begins monitoring control traffic flows when a DDoS protection policer is violated for almost all protocol groups and packet types. In addition to enabling flow detection globally, you can configure its operation mode—that is, whether it is automatically triggered by the violation of a DDoS protection policer (the default) or is always on—for almost all protocol groups and packet types. You can override the global configuration settings for individual protocol groups and packet types. Other than event report rates, all other characteristics of flow detection are configurable only at the level of individual packet types.

NOTE: You cannot enable flow detection globally for the following groups and packet type because they do not have typical Ethernet, IP, or IPv6 headers:

- Protocol groups: **fab-probe**, **frame-relay**, **inline-ka**, **isis**, **jfm**, **mlp**, **pfe-alive**, **pos**, and **services**.
- Packet type: **unclassified** in the **ip-options** protocol group.

Control flows are aggregated at three levels. The *subscriber level* is the finest grained of the three and consists of flows for individual subscriber sessions. The *logical interface level* aggregates multiple subscriber flows, so it is coarser grained and does not provide discrimination into individual subscriber flows. The *physical interface level* aggregates multiple logical interface flows, so it provides the coarsest view of traffic flows.

You can turn flow detection off or on at any of these levels. You can also configure whether it is automatically triggered by the violation of a DDoS protection policer or is always

on—meaning that it always monitors flows, even when no policer is being violated. Flow detection begins at the finest-grained level that has detection configured to **on** or **automatic**.

When a flow arrives, flow detection checks whether the flow is already listed in a table of *suspicious* flows. A suspicious flow is one that exceeds the bandwidth allowed by default or configuration. If the flow is not in the table and the aggregation level flow detection mode is **on**, then flow detection lists the flow in the table. If the flow is not in the table and the flow detection mode is **automatic**, flow detection checks whether this flow is suspicious.

If the flow is suspicious, then it goes in the flow table. If the flow is not suspicious, then it is processed the same way at the next coarser aggregation level that has flow detection set to **on**. If none of the higher levels have detection on, then the flow continues to the DDoS protection packet policer for action, where it can be passed or dropped.

When the initial check finds the flow in the table, then the flow is dropped, policed, or kept, depending on the control mode setting for that aggregation level. All packets in dropped flows are dropped. In policed flows, packets are dropped until the flow is within the acceptable bandwidth for the aggregation level. Kept flows are passed along to the next aggregation level for processing.

Flow Tracking

The flow detection application tracks flows that have been listed in the suspicious flow table. It periodically checks each entry in the table to determine whether the listed flow is still suspicious (violating the bandwidth). If a suspicious flow has continuously violated the bandwidth since it was inserted in the table for a period greater than the configurable flow detection period, then it is considered to be a *culprit* flow rather than merely suspicious. However, if the bandwidth has been violated for less than the detection period, the violation is treated as a false positive. Flow detection considers the flow to be safe and stops tracking it (deletes it from the table).

You can enable a timeout feature that suppresses culprit flows for a configurable timeout period, during which the flow is kept in the flow table. (Suppression is the default behavior, but the flow detection action can be changed by the flow level control configuration.) If the check of listed flows finds one for which the timeout is enabled and the timeout period has expired, then the flow has timed out and it is removed from the flow table.

If the timeout has not yet expired or if the timeout feature is not enabled, then the application performs a recovery check. If the time since the flow last violated the bandwidth is longer than the configurable recovery period, the flow has recovered and is removed from the flow table. If the time since last violation is less than the recovery period, the flow is kept in the flow table.

Notifications

By default, flow detection automatically generates system logs for a variety of events that occur during flow detection. The logs are referred to as *reports* in the flow detection CLI. All protocol groups and packet types are covered by default, but you can disable

automatic logging for individual packet types. You can also configure the rate at which reports are sent, but this applies globally to all packet types.

Each report belongs to one of the following two types:

- Flow reports—These reports are generated by events associated with the identification and tracking of culprit flows. Each report includes identifying information for the flow that experienced the event. This information is used to accurately maintain the flow table; flows are deleted or retained in the table based on the information in the report. Table 3 on page 68 describes the event that triggers each flow report.

Table 3: Triggering Event for Flow Detection Reports

Name	Description
DDOS_SCFD_FLOW_FOUND	A suspicious flow is detected.
DDOS_SCFD_FLOW_TIMEOUT	The timeout period expires for a culprit flow. Flow detection stops suppressing (or monitoring) the flow.
DDOS_SCFD_FLOW_RETURN_NORMAL	A culprit flow returns to within the bandwidth limit.
DDOS_SCFD_FLOW_CLEARED	A culprit flow is cleared manually with a **clear** command or automatically as the result of suspicious flow monitoring shifting to a different aggregation level.
DDOS_SCFD_FLOW_AGGREGATED	Control flows are aggregated to a coarser level. This event happens when the flow table nears capacity or when the flow cannot be found at a particular flow level and the next coarser level has to be searched.
DDOS_SCFD_FLOW_DEAGGREGATED	Control flows are deaggregated to a finer level. This event happens when the flow table is not very full or when flow control is effective and the total arrival rate for the flow at the policer for the packet type is below its bandwidth for a fixed, internal period.

- Bandwidth violation reports—These reports are generated by events associated with the discovery of suspicious flows. Each report includes identifying information for the flow that experienced the event. This information is used to track the suspicious flow and identify flows that are placed in the flow table. Table 4 on page 68 describes the event that triggers each violation report.

Table 4: Triggering Event for Bandwidth Violation Reports

Name	Description
DDOS_PROTOCOL_VIOLATION_SET	The incoming traffic for a violated control protocol returned to normal.
DDOS_PROTOCOL_VIOLATION_CLEAR	The incoming traffic for a control protocol exceeded the configured bandwidth.

A report is sent only when triggered by an event; that is, there are no null or empty reports. Because the reports are made periodically, the only events of interest are ones that occur during the interval since the last report.

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring Flow Detection for DDoS Protection

Flow detection monitors the flows of control traffic for violation of the bandwidth allowed for each flow and manages traffic identified as a culprit flow. Suppression of the traffic is the default management option. Flow detection is typically implemented as part of an overall DDoS protection strategy, but it is also useful for troubleshooting and understanding traffic flow in new configurations. Flow detection is disabled by default.

Before you begin, ensure you have configured DDoS protection appropriately for you network. See "Configuring Protection Against DDoS Attacks" on page 43 for detailed information about DDoS protection.

To configure flow detection:

1. Enable flow detection globally for all protocol groups and packet types.

   See "Enabling Flow Detection for All Protocol Groups and Packet Types" on page 70.

2. (Optional) Set the rate at which culprit flow events are reported for all line cards, protocol groups, and packet types.

   See "Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types" on page 71.

3. Set the rate at which bandwidth violations are reported for all line cards, protocol groups, and packet types.

   See "Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types" on page 71.

4. (Optional) Configure how long a suspicious flow must be in violation of flow bandwidth before being declared a culprit flow.

   See "Configuring the Detection Period for Suspicious Flows" on page 71.

5. (Optional) Configure how long a culprit flow must drop to within its allowed bandwidth before being declared normal.

   See "Configuring the Recovery Period for a Culprit Flow" on page 72.

6. (Optional) Enable and configure how long a culprit flow is suppressed or monitored.

   See "Configuring the Timeout Period for a Culprit Flow" on page 73.

7. (Optional) Configure the global flow detection operation mode for all protocol groups and packet types.

   See "Configuring How Flow Detection Operates Globally" on page 73.

8. (Optional) Override the global flow detection operation mode for protocol groups or packet types.

   See "Configuring How Flow Detection Operates for Individual Protocol Groups or Packets" on page 74.

9. (Optional) Override the global, protocol group, or packet type flow detection operation mode for one or more flow aggregation levels (subscriber, logical interface, and physical interface).

   See "Configuring How Flow Detection Operates at Each Flow Aggregation Level" on page 75.

10. Configure the maximum bandwidth for packet flows at each flow aggregation level (subscriber, logical interface, and physical interface).

    See "Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level" on page 76.

11. (Optional) Configure how traffic is controlled at each flow aggregation level (subscriber, logical interface, and physical interface) for flows that violate their bandwidth.

    See "Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level" on page 78.

12. (Optional) Disable automatic logging of suspicious flows.

    See "Disabling Automatic Logging of Culprit Flow Events for a Packet Type" on page 79.

Related Documentation

- Distributed Denial-of-Service (DDoS) Protection Overview on page 35
- DDoS Protection Flow Detection Overview on page 66

Enabling Flow Detection for All Protocol Groups and Packet Types

By default, flow detection is disabled for all protocol groups and packet types. You must enable flow detection globally by including the **flow-detection** statement. If you subsequently disable flow detection for individual packet types, you cannot use this global statement to override all such individual configurations; you must re-enable detection at the packet configuration level.

To enable flow detection globally:

- Set flow detection.

```
[edit system ddos-protection global]
user@host# set flow-detection
```

NOTE: You cannot enable flow detection globally for the following groups and packet type because they do not have typical Ethernet, IP, or IPv6 headers:

- Protocol groups: **fab-probe**, **frame-relay**, **inline-ka**, **isis**, **jfm**, **mlp**, **pfe-alive**, **pos**, and **services**.
- Packet type: **unclassified** in the **ip-options** protocol group.

Related Documentation
- Configuring Flow Detection for DDoS Protection on page 69
- Configuring Protection Against DDoS Attacks on page 43

Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types

When flow detection confirms that a suspicious flow it is tracking on a line card is indeed a culprit flow, it sends a report to the Routing Engine. Flow detection also reports each culprit flow that subsequently recovers to within the allowed bandwidth or is cleared. You can include the **flow-report-rate** statement to limit how many flows per second on each line card can be reported. Culprit flow events are reported for all protocol groups and packet types by default. When too many flows are reported, congestion can occur on the host path to the Routing Engine flow.

To globally configure the maximum report rate for culprit flows:

- Set the reporting rate.

```
[edit system ddos-protection global]
user@host# set flow-report-rate rate
```

Related Documentation
- Configuring Flow Detection for DDoS Protection on page 69
- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 79

Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types

By default, flow detection reports to the Routing Engine all violations of bandwidth at the FPC for all protocol groups and packet types. You can include the **violation-report-rate** statement to limit how many violations per second flow detection reports from the line cards, thus reducing the load on the router. We recommend that you configure a report rate that is suitable for your network rather than rely on the default value.

To globally configure the maximum bandwidth violation reporting rate:

- Set the reporting rate.

```
[edit system ddos-protection global]
user@host# set violation-report-rate rate
```

Related Documentation
- Configuring Flow Detection for DDoS Protection on page 69

Configuring the Detection Period for Suspicious Flows

DDoS protection flow detection considers a monitored flow to be a suspicious flow whenever the flow exceeds its allowed bandwidth, based on a crude test that eliminates obviously good flows from consideration. A closer examination of a suspicious flow requires the flow to remain in violation of the bandwidth for a period of time before flow detection considers it to be a culprit flow against which it must take action. You can

include the **flow-detect-time** statement to configure the duration of this detection period or you can rely on the default period of three seconds.

BEST PRACTICE: We recommend that you use the default value for the detection period.

To specify how long a flow must be in violation before flow detection declares it to be a culprit flow:

- Set the detection period.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# set flow-detect-time ***seconds***

  For example, include the following statement to require the DHCPv4 discover packet flow to be in violation of its allowed bandwidth for 30 seconds before it is considered to be a culprit flow:

  [edit system ddos-protection protocols dhcpv4 discover]
  user@host# set flow-detect-time 30

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring the Recovery Period for a Culprit Flow

After DDoS protection flow detection has identified a suspicious flow as a culprit flow, it has to determine when that flow no longer represents a threat to the router. When the traffic flow rate drops back to within the allowed bandwidth, the rate must remain within the bandwidth for a recovery period. Only then does flow detection consider the flow to be normal and stop the traffic handling action enacted against the culprit flow. You can include the **flow-recover-time** statement to configure the duration of this recovery period or you can rely on the default period of 60 seconds.

To specify how long a flow must be within its allowed bandwidth after a violation before flow detection declares it to be a normal flow:

- Set the recovery period.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# set flow-recover-time ***seconds***

  For example, include the following statement to require the DHCPv4 discover packet flow to be in recovery for five minutes (300 seconds):

  [edit system ddos-protection protocols dhcpv4 discover]
  user@host# set flow-recover-time 300

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring the Timeout Period for a Culprit Flow

When DDoS protection flow detection identifies a suspicious flow as a culprit flow, by default it suppresses traffic for that flow for as long as the traffic flow exceeds the bandwidth limit. Suppression stops and the flow is removed from the flow table when the time since the last violation by the flow is greater than the recovery period.

Alternatively, you can include the **timeout-active-flows** statement to enable flow detection to suppress a culprit flow for a configurable timeout period. When the timeout period expires, suppression stops and the flow is removed from the flow table. You can either include the **flow-timeout-time** statement to configure the duration of the timeout period or rely on the default timeout of 300 seconds.

To enable flow detection to suppress a culprit flow for a timeout period:

1. Enable the timeout.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# **set** timeout-active-flows

2. Specify the timeout period.

   [edit system ddos-protection protocols *protocol-group packet-type*]
   user@host# **set**flow-timeout-time ***seconds***

For example, include the following statements to suppress the DHCPv4 discover packet flow for 10 minutes (600 seconds):

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set timeout-active-flows
user@host# setflow-timeout-time 600
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring How Flow Detection Operates Globally

Flow detection is disabled globally for all protocol groups and packet types by default. After you have turned on flow detection globally with the flow-detection statement at the **[edit system ddos-protection global]** hierarchy level, you can include the flow-detection-mode statement to configure *how* flow detection operates globally for all for all protocol groups and packet types. By default, flow detection operates in automatic mode for all packet types, meaning that it monitors control traffic for suspicious flows only after a DDoS policer has been violated. You can also configure flow detection either to never monitor flows or to always monitor flows.

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. You can override the global configuration by including the flow-detection-mode statement at the **[edit system ddos-protection protocols *protocol-group packet-type*]** hierarchy level to configure how flow detection works for a protocol group or a packet type. You can use the flow-level-detection statement to specify

the behavior for one or more traffic flow aggregation levels (subscriber, logical interface, or physical interface).

Flow detection supports the following three modes:

- automatic—When a DDoS protection policer is violated, traffic flows where the violation occurred are monitored for suspicious behavior. Each suspicious flow is examined to determine whether it is the culprit flow that caused the violation.
- off—Traffic flows are never monitored for any protocol group or packet type.
- on—Traffic flows for all protocol groups and packet types are monitored for suspicious flows even when no DDoS protection policer is currently being violated.

To configure how flow detection operates at each flow aggregation level:

- Specify the detection mode.

  ```
  [edit system ddos-protection protocols global]
  user@host# set flow-detection-mode flow-detection-mode
  ```

For example, to configure flow detection to always monitor and detect flows for all protocol groups and packet types at all flow aggregation levels:

```
[edit system ddos-protection global]
user@host# set flow-detection-mode on
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69
- Configuring How Flow Detection Operates for Individual Protocol Groups or Packets on page 74
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75

Configuring How Flow Detection Operates for Individual Protocol Groups or Packets

By default, flow detection is disabled for all protocol groups and packet types. After you have turned on flow detection globally and configured the global operation mode, you can include the **flow-detection-mode** statement to configure flow detection to override the global setting for individual protocol groups and packet types. By default, flow detection operates in automatic mode for all packet types, meaning that it monitors control traffic for suspicious flows only after a DDoS policer has been violated. You can also configure flow detection either to never monitor flows or to always monitor flows.

NOTE: The flow detection mode at the packet level must be either automatic or on for flow detection to operate at individual flow aggregation levels.

To configure how flow detection operates:

- Disable suspicious flow detection for a packet type.

  ```
  [edit system ddos-protection protocols protocol-group packet-type]
  user@host# set flow-detection-mode off
  ```

- Set flow detection to operate automatically when a policer is violated.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-detection-mode **automatic**

- Specify that flow detection is always on for a packet type.

  [edit system ddos-protection protocols *protocol-group packet-type*]
  user@host# **set** flow-detection-mode **on**

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69
- Configuring How Flow Detection Operates Globally on page 73
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75

Configuring How Flow Detection Operates at Each Flow Aggregation Level

When flow detection is turned on, traffic flows are monitored by default for all protocol groups and packet types. When a policer violation occurs, each suspicious flow is examined to determine whether it is the culprit flow that caused the violation. You can include the **flow-level-detection** statement to configure how flow detection works at each flow aggregation level for a packet type: subscriber, logical interface, or physical interface.

NOTE: **The flow detection mode at the packet level must be either automatic or on for flow detection to operate at individual flow aggregation levels.**

Like flow detection at the protocol group and packet level, flow detection at the flow aggregation level supports three modes:

- automatic—When a DDoS protection policer is violated, traffic flows at this flow aggregation level are monitored for suspicious behavior only until flow detection determines that the suspect flow is not at this aggregation level and instead must be at a coarser level of aggregation. Flows at this level are subsequently not searched again until the policer is no longer violated at the coarser level.
- off—Traffic flows are never monitored at this flow aggregation level.
- on—Traffic flows at this flow aggregation level are monitored for suspicious flows even when no DDoS protection policer is currently being violated, if flow detection at the packet level is configured to **on**. Monitoring continues at this level regardless of whether a suspect flow is identified at this level. However, If the packet level mode is **automatic**, then the policer must be in violation for traffic flows to be checked at this level.

Flows are examined first at the finest-grained (lowest bandwidth) flow aggregation level, subscriber. If the suspect flow is not found at the subscriber level, then flows are checked at the logical interface level. Finally, if the suspect is not found there, then flows are checked at the physical interface level; barring some misconfiguration, the culprit flow must be found at this level.

To configure how flow detection operates at each flow aggregation level:

1. (Optional) Specify the detection mode at the subscriber level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
   user@host# set subscriber flow-detection-mode
   ```

2. (Optional) Specify the detection mode at the logical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
   user@host# set logical-interface flow-detection-mode
   ```

3. (Optional) Specify the detection mode at the physical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type flow-level-detection]
   user@host# set physical-interface flow-detection-mode
   ```

For example, include the following statements to configure flow detection to check for suspicious flows at the subscriber level only when the policer is being violated, to never check at the logical interface level, and to always check at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-detection
user@host# set subscriber automatic
user@host# set logical-interface off
user@host# set physical-interface on
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69
- Configuring How Flow Detection Operates Globally on page 73
- Configuring How Flow Detection Operates for Individual Protocol Groups or Packets on page 74

Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level

You can include the **flow-level-bandwidth** statement to configure the maximum acceptable bandwidth for traffic flows for individual packet types. You have to specify the bandwidth behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface. We recommend that you tune the bandwidth values for your entwork rather than rely on the defaults.

To configure the maximum bandwidth for traffic flows each flow aggregation level:

1. (Optional) Configure the bandwidth for flows at the subscriber level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type
     flow-level-bandwidth]
   user@host# set subscriber flow-bandwidth
   ```

2. (Optional) Configure the bandwidth for flows at the logical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type
     flow-level-bandwidth]
   user@host# set logical-interface flow-bandwidth
   ```

3. (Optional) Configure the bandwidth for flows at the physical interface level.

```
[edit system ddos-protection protocols protocol-group packet-type
  flow-level-bandwidth]
user@host# set physical-interface flow-bandwidth
```

For example, to configure the flow bandwidth to 1000 pps at the subscriber level, 5000 pps at the logical interface level, and 30,000 at the physical interface level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-bandwidth
user@host# set subscriber 1000
user@host# set logical-interface 5000
user@host# set physical-interface 30000
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring How Traffic in a Culprit Flow Is Controlled Globally

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure how flow detection controls traffic for one or more traffic flow aggregation levels globally for all protocol groups and packet types . You have to specify the control behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface.

You can configure flow detection flow control to employ one of the following modes for a packet type:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels.
- Police traffic—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- Keep all traffic—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for all packet types at all aggregation levels are within their limits, you can configure flow control to police the traffic at each level. Or if you want to detect culprit flows and suppress them at one level but only restrain traffic to the allowed bandwidth at another level, you can configure one level to drop all traffic and the other to police traffic.

- (Optional) Specify the control mode.

```
[edit system ddos-protection global]
user@host# set
```

To configure how flow detection controls traffic in a culprit flow for individual flow aggregation levels for all protocol groups and packet types:

1. (Optional) Specify the control mode at the subscriber level.

   ```
   [edit system ddos-protection global]
   user@host# set subscriber flow-control-mode
   ```

2. (Optional) Specify the control mode at the logical interface level.

   ```
   [edit system ddos-protection global]
   user@host# set logical-interface flow-control-mode
   ```

3. (Optional) Specify the control mode at the physical interface level.

   ```
   [edit system ddos-protection global]
   user@host# set physical-interface flow-control-mode
   ```

For example, to configure flow detection to keep all traffic for a physical interface under the configured bandwidth, but detect and suppress culprit flows at the subscriber level:

```
[edit system ddos-protection global]
user@host# set flow-level-control subscriber drop
user@host# set flow-level-control physical-interface police
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level

When flow detection is enabled, all traffic in a culprit flow is dropped by default for all protocol groups and packet types and at all flow aggregation levels. You can include the **flow-level-control** statement to configure flow detection to control traffic differently for individual packet types. You have to specify the control behavior at a particular flow aggregation level: subscriber, logical interface, or physical interface.

You can configure flow detection flow control to employ one of the following modes for a packet type:

- Drop all traffic—Configure flow control to drop all traffic when you think the flow that is violating a bandwidth limit is malicious. This behavior is the default at all flow aggregation levels.
- Police traffic—Configure flow control to police a flow that is violating bandwidth, forcing the rate below the bandwidth limit. Flow control acts as a simple policer in this case.
- Keep all traffic—Configure flow control to keep all traffic whether the flow is in violation or below the bandwidth limit. This mode is helpful when you need to debug traffic flow for your network.

Flow control mode enables great flexibility in how you manage control traffic in your network. For example, if you only want to ensure that control flows for a packet type at all aggregation levels are within their limits, you can configure flow control to police the traffic at each level. Or if you want to detect culprit flows and suppress them at one level

but only restrain traffic to the allowed bandwidth at another level, you can configure one level to drop all traffic and the other to police traffic.

To configure how flow detection controls traffic in a culprit flow:

1. (Optional) Specify the control mode at the subscriber level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type scfd
     flow-level-control]
   user@host# set subscriber flow-control-mode
   ```

2. (Optional) Specify the control mode at the logical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type scfd
     flow-level-control]
   user@host# set logical-interface flow-control-mode
   ```

3. (Optional) Specify the control mode at the physical interface level.

   ```
   [edit system ddos-protection protocols protocol-group packet-type scfd
     flow-level-control]
   user@host# set physical-interface flow-control-mode
   ```

For example, to configure flow detection to keep all traffic for a physical interface under the configured bandwidth, but detect and suppress culprit flows at the subscriber level:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# edit flow-level-control
user@host# set subscriber drop
user@host# set physical-interface police
user@host# edit flow-level-detection
user@host# set logical-interface off
```

In this example, you do not care about the logical interface, so flow detection is turned off for that level. Because flow detection is disabled, the state of flow control for that level does not matter.

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

Disabling Automatic Logging of Culprit Flow Events for a Packet Type

By default, flow detection automatically logs policer violation events associated with suspicious flows (violation reports) and culprit flow events (flow reports) for all protocol groups and packet types. You can include the **no-flow-logging** statement to prevent automatic logging of culprit flow events for individual packet types. Automatic logging of suspicious flow violation events is disabled with the **disable-logging** statement at the **[edit system ddos-protection global** hierarchy level.

To disable automatic culprit flow event logging for a packet type:

- Disable logging.

  ```
  [edit system ddos-protection protocols protocol-group packet-type]
  user@host# set no-flow-logging
  ```

To disable automatic suspicious flow violation event logging for a packet type:

- Disable logging.

  ```
  [edit system ddos-protection protocols protocol-group packet-type]
  user@host# set disable-logging
  ```

For example, include the following statement to disable automatic logging for DHCPv4 DISCOVER packet flows:

```
[edit system ddos-protection protocols dhcpv4 discover]
user@host# set no-flow-logging
```

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69
- Configuring DDoS Protection Policers for Individual Packet Types on page 54

Verifying and Managing Flow Detection

Purpose View or clear information about flow detection as part of a DDoS protection configuration.

Action

- To display configuration information for flow detection:

  ```
  user@host> show ddos-protection protocols flow-detection
  ```

- To display information about culprit flows identified by flow detection, including number of flows detected and tracked, source address of the flow, arriving interface, and rates:

  ```
  user@host> show ddos-protection protocols culprit-flows
  ```

- To clear culprit flows for all packet types in all protocol groups:

  ```
  user@host> clear ddos-protection protocols culprit-flows
  ```

- To clear culprit flows for all packet types in a particular protocol group:

  ```
  user@host> clear ddos-protection protocols protocol-group culprit-flows
  ```

Related Documentation

- Verifying and Managing DDoS Protection on page 62

PART 4

IPsec

CHAPTER 7

Understanding How IPsec Secures Network Traffic

Overview of IPSec

IP Security (IPSec) provides a secure way to authenticate senders and encrypt IP version 4 (IPv4) and version 6 (IPv6) traffic between network devices, such as routers and hosts. IPSec offers network administrators and their users the benefits of data confidentiality, data integrity, sender authentication, and anti-replay services. IPSec is increasingly becoming a critical component in today's contemporary IP networks.

IPSec is a framework for ensuring secure private communication over IP networks and is based on standards developed by the International Engineering Task Force (IETF). IPsec provides security services at the network layer of the Open Systems Interconnection (OSI) model by enabling a system to select required security protocols, determine the algorithms to use for the security services, and implement any cryptographic keys required to provide the requested services. You can use IPsec to protect one or more paths between a pair of hosts, between a pair of security gateways (such as routers), or between a security gateway and a host.

The terminology and components of IPSec can be intimidating to first-time users. However, if you learn a few key concepts, you can quickly master and deploy IPSec in your network. The main concepts you need to understand are as follows:

- IPsec-Enabled Line Cards on page 98
- Authentication Algorithms on page 84
- Encryption Algorithms on page 85
- IPsec Protocols on page 86
- IPsec Security Associations Overview on page 88
- IPSec Modes on page 89
- Digital Certificates on page 91
- Service Sets on page 93

Authentication Algorithms

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The Junos OS uses the following authentication algorithms:

- Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

  To verify that the message has not been tampered with, the Junos OS compares the calculated message digest against a message digest that is decrypted with a shared key. The Junos OS uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with authentication header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

- Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. The Junos OS uses the SHA-1 HMAC variant that provides an additional level of hashing. SHA-1 can be used with AH, ESP, and IKE.

- SHA-256, SHA-384, and SHA-512 (sometimes grouped under the name SHA-2) are variants of SHA-1 and use longer message digests. The Junos OS supports the SHA-256 version of SHA-2, which can process all versions of Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES) encryption.

Related Documentation

- *Understanding Junos VPN Site Secure*
- Encryption Algorithms on page 85

Encryption Algorithms

Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users. Like authentication algorithms, a shared key is used with encryption algorithms to verify the authenticity of the IPsec devices. The Junos OS uses the following encryption algorithms:

- Data Encryption Standard cipher-block chaining (DES-CBC) is a symmetric secret-key block algorithm. DES uses a key size of 64 bits, where 8 bits are used for error detection and the remaining 56 bits provide encryption. DES performs a series of simple logical operations on the shared key, including permutations and substitutions. CBC takes the first block of 64 bits of output from DES, combines this block with the second block, feeds this back into the DES algorithm, and repeats this process for all subsequent blocks.
- Triple DES-CBC (3DES-CBC) is an encryption algorithm that is similar to DES-CBC, but provides a much stronger encryption result because it uses three keys for 168-bit (3 x 56-bit) encryption. 3DES works by using the first key to encrypt the blocks, the second key to decrypt the blocks, and the third key to re-encrypt the blocks.
- Advanced Encryption Standard (AES) is a next-generation encryption method based on the Rijndael algorithm developed by Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen. It uses a 128-bit block and three different key sizes (128, 192, and 256 bits). Depending on the key size, the algorithm performs a series of computations (10, 12, or 14 rounds) that include byte substitution, column mixing, row shifting, and key addition. The use of AES in conjunction with IPsec is defined in RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

Related Documentation

- *Understanding Junos VPN Site Secure*
- *Configuring IKE Proposals*
- *Configuring IPsec Proposals*
- *encryption*

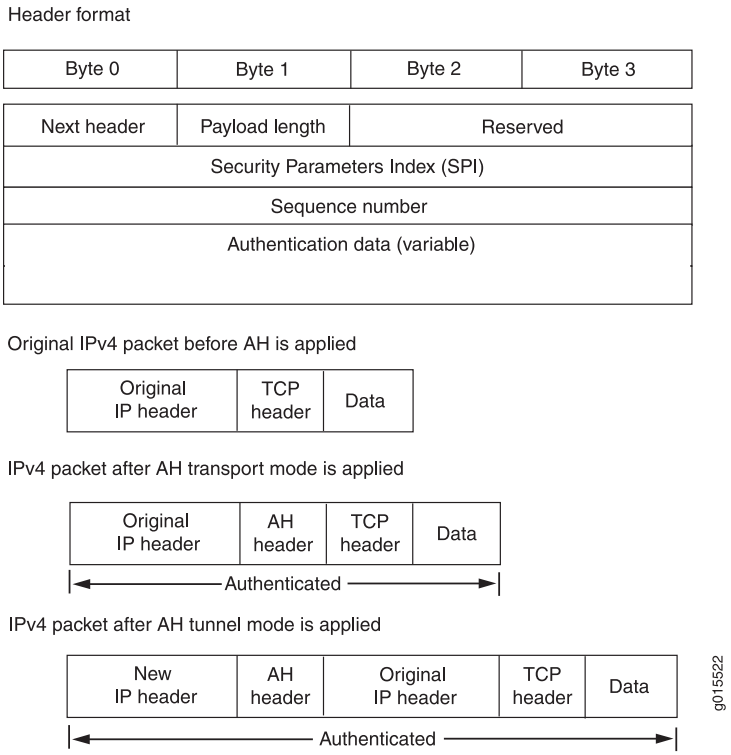
IPsec Protocols

IPsec protocols determine the type of authentication and encryption applied to packets that are secured by the router. The Junos OS supports the following IPsec protocols:

- AH—Defined in RFC 2402, AH provides connectionless integrity and data origin authentication for IPv4 and IPv6 packets. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper-level protocol data. However, some IP header fields might change in transit. Because the value of these fields might not be predictable by the sender, they cannot be protected by AH. In an IP header, AH can be identified with a value of **51** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by AH is shown in Figure 3 on page 86.

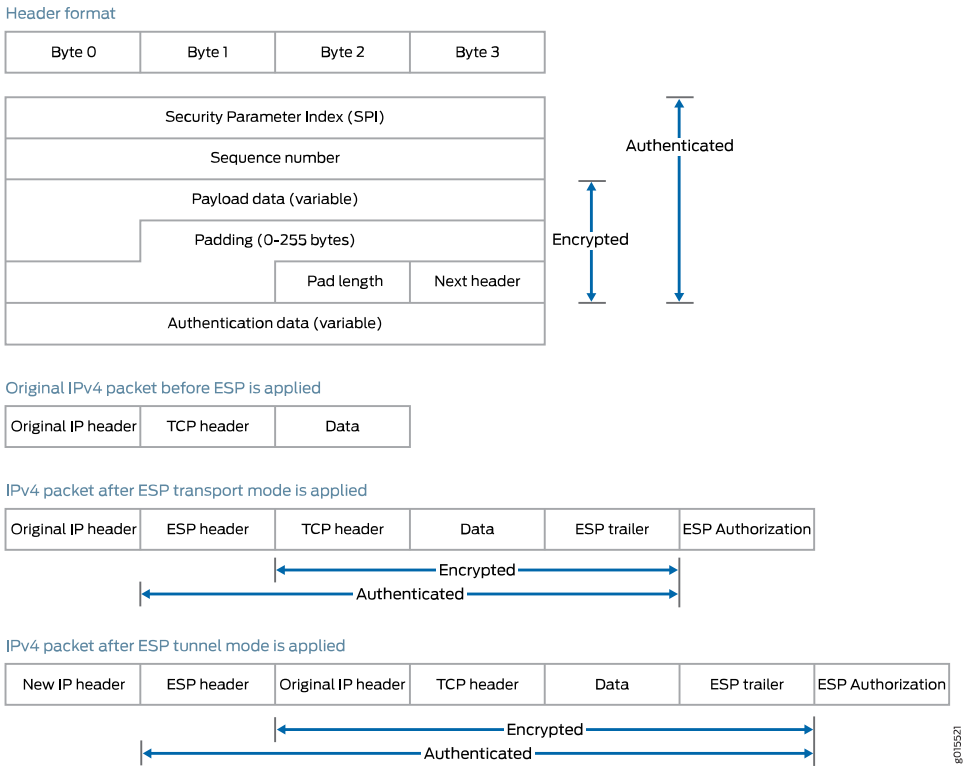
NOTE: AH is not supported on the T Series, M120, and M320 routers.

Figure 3: AH Protocol



- ESP—Defined in RFC 2406, ESP can provide encryption and limited traffic flow confidentiality, or connectionless integrity, data origin authentication, and an anti-replay service. In an IP header, ESP can be identified a value of **50** in the **Protocol** field of an IPv4 packet and the **Next Header** field of an IPv6 packet. An example of the IPsec protection offered by ESP is shown in Figure 4 on page 87.

Figure 4: ESP Protocol



- Bundle—When you compare AH with ESP, there are some benefits and shortcomings in both protocols. ESP provides a decent level of authentication and encryption, but does so only for part of the IP packet. Conversely, although AH does not provide encryption, it does provide authentication for the entire IP packet. Because of this, the Junos OS offers a third form of IPsec protocol called a protocol bundle. The bundle option offers a hybrid combination of AH authentication with ESP encryption.

Related Documentation

- *Understanding Junos VPN Site Secure*
- *Configuring IPsec Proposals*
- *Configuring Security Associations*
- *protocol (IPsec)*

IPsec Security Associations Overview

Another IPSec consideration is the type of security association (SA) that you wish to implement. An SA is a set of IPSec specifications that are negotiated between devices that are establishing an IPSec relationship. These specifications include preferences for the type of authentication, encryption, and IPSec protocol that should be used when establishing the IPSec connection. An SA can be either unidirectional or bidirectional, depending on the choices made by the network administrator. An SA is uniquely identified by a Security Parameter Index (SPI), an IPv4 or IPv6 destination address, and a security protocol (AH or ESP) identifier.

You can configure IPSec with a preset, preshared manual SA or use IKE to establish a dynamic SA. Manual SAs require you to specify all the IPSec requirements up front. Conversely, IKE dynamic SAs typically contain configuration defaults for the highest levels of authentication and encryption.

Security Associations Overview

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

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

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

Related Documentation

- IKE Key Management Protocol Overview on page 90
- IPsec Requirements for Junos-FIPS on page 98
- *[edit security] Hierarchy Level*

IPSec Modes

When configuring IPSec, the last major consideration is the type of IPSec mode you wish to implement in your network. The Junos OS supports the following IPSec modes:

- Tunnel mode is supported for both AH and ESP in the Junos OS and is the usual choice for a router. In tunnel mode, the SA and associated protocols are applied to tunneled IPv4 or IPv6 packets. For a tunnel mode SA, an outer IP header specifies the IPSec processing destination, and an inner IP header specifies the ultimate destination for the packet. The security protocol header appears after the outer IP header, and before the inner IP header. In addition, there are slight differences for tunnel mode when you implement it with AH and ESP:
  - For AH, portions of the outer IP header are protected, as well as the entire tunneled IP packet.
  - For ESP, only the tunneled packet is protected, not the outer header.

  When one side of a security association is a security gateway (such as a router), the SA must use tunnel mode. However, when traffic (for example, SNMP commands or BGP sessions) is destined for a router, the system acts as a host. Transport mode is allowed in this case because the system does not act as a security gateway and does not send or receive transit traffic.
- Transport mode provides a security association between two hosts. In transport mode, the protocols provide protection primarily for upper layer protocols. For IPv4 and IPv6 packets, a transport mode security protocol header appears immediately after the IP header and any options, and before any higher layer protocols (for example, TCP or UDP). There are slight differences for transport mode when you implement it with AH and ESP:
  - For AH, selected portions of the IP header are protected, as well as selected portions of the extension headers and selected options within the IPv4 header.
  - For ESP, only the higher layer protocols are protected, not the IP header or any extension headers preceding the ESP header.

NOTE: **Support for IPSec transport mode is primarily limited to routing authentication and to certain configurations only application when Junos FIPs code is used.**

Related Documentation

- Overview of IPSec on page 83
- Configuring Security Associations on page 105
- *Understanding OSPFv3 Authentication*
- *Example: Configuring IPsec Authentication for an OSPF Interface*

IKE Key Management Protocol Overview

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

IKE does the following:

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

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

NOTE: Starting in Junos OS Release 14.2, when you perform an SNMP walk of the jnxIkeTunnelEntry object in the jnxIkeTunnelTable table, the **Request failed: OID not increasing** error message might be generated. This problem occurs only when simultaneous Internet Key Exchange security associations (IKE SAs) are created, which occurs when both ends of the SA initiate IKE SA negotiations at the same time. When an SNMP MIB walk is performed to display IKE SAs, the snmpwalk tool expects the object identifiers (OIDs) to be in increasing order. However, in the case of simultaneous IKE SAs, the OIDs in the SNMP table might not be in increasing order. This behavior occurs because the tunnel IDs, which are part of the OIDs, are allocated based on the initiator of the IKE SA, which can be on either side of the IKE tunnel.

The following is an example of an SNMP MIB walk that is performed on IKE simultaneous SAs:

```
jnxIkeTunLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47885 = INTEGER:
 responder(2)   >>> This is Initiator SA
jnxIkeTunLocalRole."ipsec_ss_cust554".ipv4."192.0.2.41".47392 = INTEGER:
 initiator(1)   >>> This is Responder's SA
```

The OID comparison fails when the SNMP walk is tunnel ID (47885 and 47392). It cannot be ensured when an SNMP walk is performed that the tunnel IDs are in increasing order because tunnels might be initiated from either side.

To work around this problem, the SNMP MIB walk contains an option, -Cc, to disable check for increasing OIDs. The following is an example of the MIB walk performed on the jnxIkeTunnelEntry table with the -Cc option:

```
snmpwalk -Os -Cc -c public -v 1 vira jnxIkeTunnelEntry
```

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, when you perform an SNMP walk of the jnxIkeTunnelEntry object in the jnxIkeTunnelTable table, the **Request failed: OID not increasing** error message might be generated.

Related Documentation

- Security Associations Overview on page 88
- IPsec Requirements for Junos-FIPS on page 98
- *[edit security] Hierarchy Level*

Digital Certificates

For small networks, the use of preshared keys in an IPSec configuration is often sufficient. However, as a network grows, it can become a challenge to add new preshared keys on

the local router and all new and existing IPSec peers. One solution for scaling an IPSec network is to use digital certificates.

A digital certificate implementation uses the public key infrastructure (PKI), which requires you to generate a key pair consisting of a public key and a private key. The keys are created with a random number generator and are used to encrypt and decrypt data. In networks that do not use digital certificates, an IPSec-enabled device encrypts data with the private key and IPSec peers decrypt the data with the public key.

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

When you request a peering relationship with an IPSec peer, the peer receives a copy of your local certificate. Because the peer already has the CA certificate loaded, it can use the CA's public key contained in the CA certificate to decrypt your local certificate that has been signed by the CA's private key. As a result, the peer now has a copy of your public key. The peer encrypts data with your public key before sending it to you. When your local router receives the data, it decrypts the data with your private key.

In the Junos OS, you must implement the following steps to be able to initially use digital certificates:

- Configure a CA profile to request CA and local digital certificates—The profile contains the name and URL of the CA or registration authority (RA), as well as some retry timer settings.
- Configure certificate revocation list support—A certificate revocation list (CRL) contains a list of certificates canceled before their expiration date. When a participating peer uses a CRL, the CA acquires the most recently issued CRL and checks the signature and validity of a peer's digital certificate. You can request and load CRLs manually, configure an LDAP server to handle CRL processing automatically, or disable CRL processing that is enabled by default.
- Request a digital certificate from the CA—The request can be made either online or manually. Online CA digital certificate requests use the Simple Certificate Enrollment Protocol (SCEP) format. If you request the CA certificate manually, you must also load the certificate manually.
- Generate a private/public key pair—The public key is included in the local digital certificate and the private key is used to decrypt data received from peers.
- Generate and enroll a local digital certificate—The local certificate can be processed online using SCEP or generated manually in the Public-Key Cryptography Standards

#10 (PKCS-10) format. If you create the local certificate request manually, you must also load the certificate manually.

- Apply the digital certificate to an IPSec configuration—To activate a local digital certificate, you configure the IKE proposal to use digital certificates instead of preshared keys, reference the local certificate in the IKE policy, and identify the CA in the service set.

Optionally, you can do the following:

- Configure the digital certificate to automatically reenroll—Starting in Junos OS Release 8.5, you can configure automatic reenrollment for digital certificates.
- Monitor digital certificate events and delete certificates and requests—You can issue operational mode commands to monitor IPSec tunnels established using digital certificates and delete certificates or requests.

For more details on managing digital certificates, configuring them in an IPSec service set, and monitoring and clearing them, see "Using Digital Certificates for IPsec" on page 225 and "Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration" on page 136.

Service Sets

The Adaptive Services PIC supports two types of service sets when you configure IPSec tunnels. Because they are used for different purposes, it is important to know the differences between these service set types.

- Next-hop service set—Supports multicast and multicast-style dynamic routing protocols (such as OSPF) over IPSec. Next-hop service sets allow you to use *inside* and *outside* logical interfaces on the Adaptive Services PIC to connect with multiple routing instances. They also allow the use of Network Address Translation (NAT) and stateful firewall capabilities. However, next-hop service sets do not monitor Routing Engine traffic by default and require configuration of multiple service sets to support traffic from multiple interfaces.
- Interface service set—Applied to a physical interface and similar to a stateless firewall filter. They are easy to configure, can support traffic from multiple interfaces, and can monitor Routing Engine traffic by default. However, they cannot support dynamic routing protocols or multicast traffic over the IPSec tunnel.

In general, we recommend that you use next-hop service sets because they support routing protocols and multicast over the IPSec tunnel, they are easier to understand, and the routing table makes forwarding decisions without administrative intervention.

Related Documentation

- *Understanding Junos VPN Site Secure*
- *Configuring Junos VPN Site Secure or IPSec VPN*

IPsec Terms and Acronyms

A

Adaptive Services PIC — A next-generation Physical Interface Card (PIC) that provides IPsec services and other services, such as Network Address Translation (NAT) and stateful firewall, on M Series and T Series platforms.

Advanced Encryption Standard (AES) — A next-generation encryption method that is based on the Rijndael algorithm and uses a 128-bit block, three different key sizes (128, 192, and 256 bits), and multiple rounds of processing to encrypt data.

authentication header (AH) — A component of the IPsec protocol used to verify that the contents of a packet have not changed (data integrity), and to validate the identity of the sender (data source authentication). For more information about AH, see RFC 2402.

C

certificate authority (CA) — A trusted third-party organization that generates, enrolls, validates, and revokes digital certificates. The CA guarantees the identity of a user and issues public and private keys for message encryption and decryption.

certificate revocation list (CRL) — A list of digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the entities that have issued them. A CRL prevents usage of digital certificates and signatures that have been compromised.

cipher block chaining (CBC) — A cryptographic method that encrypts blocks of ciphertext by using the encryption result of one block to encrypt the next block. Upon decryption, the validity of each block of ciphertext depends on the validity of all the preceding ciphertext blocks. For more information on how to use CBC with DES and ESP to provide confidentiality, see RFC 2405.

D

Data Encryption Standard (DES) — An encryption algorithm that encrypts and decrypts packet data by processing the data with a single shared key. DES operates in increments of 64-bit blocks and provides 56-bit encryption.

digital certificate — Electronic file that uses private and public key technology to verify the identity of a certificate creator and distribute keys to peers.

E

Encapsulating Security Payload (ESP) — A component of the IPsec protocol used to encrypt data in an IPv4 or IPv6 packet, provide data integrity, and ensure data source authentication. For more information about ESP, see RFC 2406.

ES PIC — A PIC that provides first-generation encryption services and software support for IPsec on M Series and T Series platforms.

H

Hashed Message Authentication Code (HMAC) — A mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, such as MD5 or SHA-1, in combination with a secret shared key. For more information on HMAC, see RFC 2104.

I

Internet Key Exchange (IKE) — Establishes shared security parameters for any hosts or routers using IPsec. IKE establishes the SAs for IPsec. For more information about IKE, see RFC 2407.

M

Message Digest 5 (MD5) — An authentication algorithm that takes a data message of arbitrary length and produces a 128-bit message digest. For more information, see RFC 1321.

P

Perfect Forward Secrecy (PFS) — Provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

public key infrastructure (PKI) — A trust hierarchy that enables users of a public network to securely and privately exchange data through the use of public and private cryptographic key pairs that are obtained and shared with peers through a trusted authority.

R

registration authority (RA) — A trusted third-party organization that acts on behalf of a CA to guarantee the identity of a user.

Routing Engine — A PCI-based architectural portion of a Junos OS-based router that handles the routing protocol process, the interface process, some of the chassis components, system management, and user access.

S

Secure Hash Algorithm 1 (SHA-1) — An authentication algorithm that takes a data message of less than 264 bits in length and produces a 160-bit message digest. For more information on SHA-1, see RFC 3174.

Secure Hash Algorithm 2 (SHA-2) — A successor to the SHA-1 authentication algorithm that includes a group of SHA-1 variants (SHA-224, SHA-256, SHA-384, and SHA-512). SHA-2 algorithms use larger hash sizes and are designed to work with enhanced encryption algorithms such as AES.

security association (SA) — Specifications that must be agreed upon between two network devices before IKE or IPsec are allowed to function. SAs primarily specify protocol, authentication, and encryption options.

Security Association Database (SADB) — A database where all SAs are stored, monitored, and processed by IPsec.

Security Parameter Index (SPI) — An identifier that is used to uniquely identify an SA at a network host or router.

Security Policy Database (SPD) — A database that works with the SADB to ensure maximum packet security. For inbound packets, IPsec checks the SPD to verify if the incoming packet matches the security configured for a particular policy. For outbound packets, IPsec checks the SPD to see if the packet needs to be secured.

Simple Certificate Enrollment Protocol (SCEP) — A protocol that supports CA and registration authority (RA) public key distribution, certificate enrollment, certificate revocation, certificate queries, and certificate revocation list (CRL) queries.

T

Triple Data Encryption Standard (3DES) — An enhanced DES algorithm that provides 168-bit encryption by processing data three times with three different keys.

CHAPTER 8

IPsec System Requirements

IPsec System Requirements

To implement IPsec, your system must meet these minimum requirements:

- Junos OS Release 8.5 or later for automatic reenrollment of digital certificates.
- Junos OS Release 8.3 or later for IPsec support on OSPF version 2
- Junos OS Release 8.2 or later for support on M120 routers
- Junos OS Release 8.1 or later for IPsec IKE support in routing instances, and certificate revocation list support on AS and MultiServices PICs installed on M Series and T Series routers
- Junos OS Release 7.6 or later for AES encryption and SHA-256 authentication support on AS PICs installed in M Series routers, and IPv6-based IPsec for AS PICs installed in M Series and T Series routers
- Junos OS Release 7.5 or later for digital certificate support on AS PICs installed in M Series and T Series routers, and support of the IPsec Monitoring Management Information Base (MIB)
- Junos OS Release 7.4 or later for dynamic endpoint tunneling support and configuring multiple routed tunnels in a single next-hop service set
- Junos OS Release 7.2 or later for transport mode IPsec on Routing Engines running OSPF version 3 and support for the AS II FIPS PIC
- Junos OS Release 7.1 or later for IPsec on the ES PIC for T Series and M320 routers
- Junos OS Release 6.4 or later for IPsec on the AS PIC for T Series and M320 routers
- Junos OS Release 6.2 or later for IPsec on the AS PIC for M Series routers
- Junos OS Release 5.7 or later for multicast over IPsec tunnels on M Series routers
- Junos OS Release 5.2 or later for IPsec on the ES PIC for M Series routers

- Two Juniper Networks M Series or T Series routers
- Two ES PICs or AS PICs for M Series and T Series routers

IPsec Requirements for Junos-FIPS

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

Related Documentation

- Security Associations Overview on page 88
- IKE Key Management Protocol Overview on page 90
- *[edit security] Hierarchy Level*

IPsec-Enabled Line Cards

The first choice you need to make when implementing IPsec on a Junos OS-based router is the type of line card you wish to use. The term line card includes Physical Interface Cards (PICs), Modular Interface Cards (MICs), Dense Port Concentrators (DPCs), and Modular Port Concentrators (MPCs). The following line cards support IPsec implementation.

NOTE: **See the specific hardware documentation for your router to determine if the line cards on that router support IPsec.**

The following line cards support IPsec:

- The Encryption Services (ES) PIC provides encryption services and software support for IPsec.
- The Adaptive Services (AS) PIC and the Adaptive Services (AS) II PIC provide IPsec services and other services, such as Network Address Translation (NAT) and stateful firewall.
- The AS II Federal Information Processing Standards (FIPS) PIC is a special version of the AS PIC that communicates securely with the Routing Engine by using internal IPsec. You must configure IPsec on the AS II FIPS PIC when you enable FIPS mode on the router. For more information about implementing IPsec on an AS II FIPS PIC installed in a router configured in FIPS mode, see the *Secure Configuration Guide for Common Criteria and Junos-FIPS*.
- The Multiservices PICs supply hardware acceleration for an array of packet processing-intensive services. These services include IPsec services and other services, such as stateful firewall, NAT, IPsec, anomaly detection, and tunnel services.
- The Multiservices Dense Port Concentrators (DPCs) provide IPsec services.

- The Multiservices Modular Port Concentrators (MS-MPCs) support IPsec services.
- The Multiservices Modular Interface Cards (MS-MICs) support IPsec services.

NOTE: Junos OS extension-provider packages, including the IPsec service package, come preinstalled and preconfigured on MS-MPCs and MS-MICs.

Related Documentation

- Overview of IPSec on page 83
- Considering General IPsec Issues on page 101
- *Understanding Services PICs*
- *Enabling Service Packages*
- *Multiservices MIC and Multiservices MPC (MS-MIC and MS-MPC) Overview*

CHAPTER 9

IPsec Configuration Guidelines

Considering General IPsec Issues

Before you configure IPsec, it is helpful to understand some general guidelines.

- IPv4 and IPv6 traffic and tunnels—You can configure IPsec tunnels to carry traffic in the following ways: IPv4 traffic traveling over IPv4 IPsec tunnels, IPv6 traffic traveling over IPv4 IPsec tunnels, IPv4 traffic traveling over IPv6 IPsec tunnels, and IPv6 traffic traveling over IPv6 IPsec tunnels.
- Configuration syntax differences between the AS and MultiServices PICs and the ES PIC—There are slight differences in the configuration statements and operational mode commands that are used with the PICs that support IPsec. As a result, the syntax for the AS and MultiServices PICs cannot be used interchangeably with the syntax for the ES PIC. However, the syntax for one type of PIC can be converted to its equivalent syntax on the other PIC for interoperability. The syntax differences are highlighted in Table 5 on page 101.
- Configuring keys for authentication and encryption—When preshared keys are required for authentication or encryption, you must use the guidelines shown in Table 6 on page 103 to implement the correct key size.
- Rejection of weak and semiweak keys—The DES and 3DES encryption algorithms will reject weak and semiweak keys. As a result, do not create and use keys that contain the patterns listed in Table 7 on page 103.

Table 5: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC

AS and MultiServices PICs Statements and Commands	ES PIC Statements and Commands
Configuration Mode Statements	
[edit service-set *name*]	–

Table 5: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC *(continued)*

AS and MultiServices PICs Statements and Commands	ES PIC Statements and Commands
[edit services ipsec-vpn ike] • policy {...} • proposal {...}	[edit security ike] • policy {...} • proposal {...}
[edit services ipsec-vpn ipsec] • policy {...} • proposal {...}	[edit security ipsec] • policy {...} • proposal {...}
[edit services ipsec-vpn rule *rule-name*] • remote-gateway *address*	[edit interface es- *fpc / pic /port*] • tunnel destination *address*
[edit services ipsec-vpn rule *rule-name* term *term-name*] • from *match-conditions* {...} then dynamic {...} • from *match-conditions* {...} then manual {...}	[edit security ipsec] • security-association *name* dynamic {...} • security-association *name* manual {...}
[edit services ipsec-vpn rule-set]	–
[edit services service-set ipsec-vpn] • local-gateway *address*	[edit interface es- *fpc /pic /port*] • tunnel source *address*
Operational Mode Commands	
clear security pki ca-certificate	–
clear security pki certificate-request	–
clear security pki local-certificate	–
clear services ipsec-vpn certificates	–
request security pki ca-certificate enroll	request security certificate (unsigned)
request security pki ca-certificate load	request system certificate add
request security pki generate-certificate-request	–
request security pki generate-key-pair	request security key-pair
request security pki local-certificate enroll	request security certificate (signed)

Table 5: Comparison of IPsec Configuration Statements and Operational Mode Commands for the AS and MultiServices PICs and ES PIC *(continued)*

AS and MultiServices PICs Statements and Commands	ES PIC Statements and Commands
request security pki local-certificate load	request system certificate add
show security pki ca-certificate	show system certificate
show security pki certificate-request	–
show security pki crl	–
show security pki local-certificate	show system certificate
show services ipsec-vpn certificates	show ipsec certificates
show services ipsec-vpn ike security-associations	show ike security-associations
show services ipsec-vpn ipsec security-associations	show ipsec security-associations

Table 6: Authentication and Encryption Key Lengths

	Number of Hexadecimal Characters	Number of ASCII Characters
Authentication		
HMAC-MD5-96	32	16
HMAC-SHA1-96	40	20
Encryption		
AES-128-CBC	16	32
AES-192-CBC	24	48
AES-256-CBC	32	64
DES-CBC	16	8
3DES-CBC	48	24

Table 7: Weak and Semiweak Keys

Weak Keys			
0101	0101	0101	0101

Table 7: Weak and Semiweak Keys *(continued)*

Weak Keys			
1F1F	1F1F	1F1F	1F1F
E0E0	E0E0	E0E0	E0E0
FEFE	FEFE	FEFE	FEFE
Semiweak Keys			
01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FEF1	FEF1	FE0E	FE0E
1F01	1F01	0E01	0E01
FEE0	FEE0	FEF1	FEF1

Keep in mind the following limitations of IPsec services on the AS PIC:

- The AS PIC does not transport packets containing IPv4 options across IPsec tunnels. If you try to send packets containing IP options across an IPsec tunnel, the packets are dropped. Also, if you issue a **ping** command with the **record-route** option across an IPsec tunnel, the **ping** command fails.
- The AS PIC does not transport packets containing the following IPv6 options across IPsec tunnels: hop-by-hop, destination (Type 1 and 2), and routing. If you try to send packets containing these IPv6 options across an IPsec tunnel, the packets are dropped.
- Destination class usage is not supported with IPsec services on the AS PIC.

CHAPTER 10

Configuring IPsec Security Associations

Configuring Security Associations

The first IPsec configuration step is to select a type of security association (SA) for your IPsec connection. You must statically configure all specifications for manual SAs, but you can rely on some defaults when you configure an IKE dynamic SA. To configure a security association, see the following sections.

Configuring Manual SAs

On the ES PIC, you configure a manual security association at the **[edit security ipsec security-association *name*]** hierarchy level. Include your choices for authentication, encryption, direction, mode, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

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

```
            }
            auxiliary-spi auxiliary-spi;
            encryption {
              algorithm (des-cbc | 3des-cbc);
              key (ascii-text key  | hexadecimal key);
            }
            protocol (ah | esp | bundle);
            spi  spi-value;
          }
        }
        mode (tunnel | transport);
      }
    }
```

On the AS and MultiServices PICs, you configure a manual security association at the **[edit services ipsec-vpn rule *rule-name*]** hierarchy level. Include your choices for authentication, encryption, direction, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

```
[edit services ipsec-vpn]
rule rule-name {
  match-direction (input | output);
  term  term-name  {
    from {
      destination-address  address;
      source-address  address;
    }
    then {
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      manual {
        direction (inbound | outbound | bidirectional) {
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
          auxiliary-spi spi-value;
          encryption {
            algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
            # aes-256-cbc, des-cbc, or 3des-cbc.
            key (ascii-text key | hexadecimal key);
          }
          protocol (ah | bundle | esp);
          spi spi-value;
        }
      }
      no-anti-replay;
      remote-gateway  address;
      syslog;
    }
  }
}
rule-set  rule-set-name  {
  [ rule  rule-names  ];
}
```

Example: AS PIC Manual SA Configuration

Figure 5: AS PIC Manual SA Topology Diagram

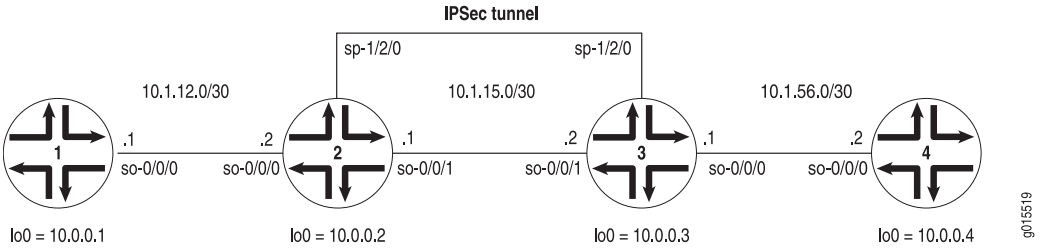


Figure 5 on page 107 shows a similar IPSec topology to the one used in the ES PIC manual SA example. The difference is that Routers 2 and 3 establish an IPSec tunnel using an AS PIC and use slightly modified manual SA settings. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R2 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.1;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA in a rule called rule-manual-SA-BiEspshades at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called service-set-manual-BiEspshades at the **[edit services service-set]** hierarchy level.

Configure all specifications for your manual SA. Use ESP for the protocol, **261** for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see Table 6 on page 103.)

To direct traffic into the AS PIC and the IPSec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 2

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R1 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R3 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    sp-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
                }
            }
        }
        unit 0 {
            family inet {
            }
            unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
                family inet;
                service-domain inside;
            }
            unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
                family inet;
                service-domain outside;
            }
        }
        lo0 {
            unit 0 {
                family inet {
                    address 10.0.0.2/32;
                }
            }
        }
    }
```

```
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
    }
  }
}
services {
  service-set service-set-manual-BiEspshades { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-manual-SA-BiEspshades; # Reference the IPSec rule here.
  }
  ipsec-vpn {
    rule rule-manual-SA-BiEspshades { # Define your IPSec VPN rule here.
      term term-manual-SA-BiEspshades {
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
          manual { # Define the manual SA specifications here.
            direction bidirectional {
              protocol esp;
              spi 261;
              authentication {
                algorithm hmac-sha1-96;
                key ascii-text "$ABC123";
                ## The unencrypted key is juniperjuniperjunipe (20 characters for
                   HMAC-SHA-1-96).
              }
              encryption {
                algorithm des-cbc;
                key ascii-text "$ABC123";
                ## The unencrypted key is juniperj (8 characters for DES-CBC).
              }
            }
          }
        }
      }
      match-direction input; # Correct match direction for next-hop service sets.
    }
  }
}
}
security {
  pki {
    auto-re-enrollment {
      certificate-id certificate-name {
```

```
        ca-profile ca-profile-name;
        challenge-password password;
        re-enroll-trigger-time-percentage percentage; #Percentage of validity-period
          # (specified in certificate) when automatic
          # reenrollment should be initiated.
        re-generate-keypair;
        validity-period number-of-days;
      }
    }
  }
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA in a rule called rule-manual-SA-BiEspshades at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called service-set-manual-BiEspshades at the **[edit services service-set]** hierarchy level.

Configure the same specifications for your manual SA that you specified on Router 2. Use ESP for the protocol, **261** for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see Table 6 on page 103.)

To direct traffic into the AS PIC and the IPSec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
    unit 0 {
      family inet {
      }
```

```
    unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
      family inet;
      service-domain inside;
    }
    unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
      family inet;
      service-domain outside;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.3/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
    }
  }
}
services {
  service-set service-set-manual-BiEspshades { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.2; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-manual-SA-BiEspshades; # Reference the IPSec rule here.
  }
  ipsec-vpn {
    rule rule-manual-SA-BiEspshades { # Define your IPSec VPN rule here.
      term term-manual-SA-BiEspshades {
        then {
          remote-gateway 10.1.15.1; # The remote IP address of the IPSec tunnel.
          manual { # Define the manual SA specifications here.
            direction bidirectional {
              protocol esp;
              spi 261;
              authentication {
                algorithm hmac-sha1-96;
                key ascii-text "$ABC123";
                ## The unencrypted key is juniperjuniperjunipe (20 characters for
                   HMAC-SHA-1-96).
              }
              encryption {
```

```
                    algorithm des-cbc;
                    key ascii-text "$ABC123";
                    ## The unencrypted key is juniperj (8 characters for DES-CBC).
                  }
                }
              }
            }
          }
          match-direction input; # Specify in which direction the rule should match.
        }
      }
    }
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

Verifying Your Work

To verify proper operation of a manual IPSec SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ipsec security-associations** (detail)
- **show services ipsec-vpn ipsec statistics**

The following sections show the output of these commands used with the configuration example:

Router 1

On Router 1, issue a **ping** command to the **lo0** interface on Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=254 time=1.375 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=254 time=18.375 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=254 time=1.120 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.120/6.957/18.375/8.075 ms
```

Router 2

To verify that the IPSec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the settings you specified, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-manual-BiEspshades
  Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
  Tunnel index: 1
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

    Direction: inbound, SPI: 261, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: Disabled

    Direction: outbound, SPI: 261, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: Disabled
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R2> show services ipsec-vpn ipsec statistics

PIC: sp-1/2/0, Service set: service-set-manual-BiEspshades

ESP Statistics:
  Encrypted bytes:            1616
  Decrypted bytes:            1560
  Encrypted packets:            20
```

```
  Decrypted packets:             19
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

Router 3

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-manual-BiEspshades
  Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
  Tunnel index: 1
  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

    Direction: inbound, SPI: 261, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: Disabled

    Direction: outbound, SPI: 261, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
    Anti-replay service: Disabled
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R3> show services ipsec-vpn ipsec statistics
PIC: sp-1/2/0, Service set: service-set-manual-BiEspshades
ESP Statistics:
  Encrypted bytes:            1560
  Decrypted bytes:            1616
  Encrypted packets:            19
  Decrypted packets:            20
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

Example: ES PIC Manual SA Configuration

Figure 6: ES PIC Manual SA Topology Diagram

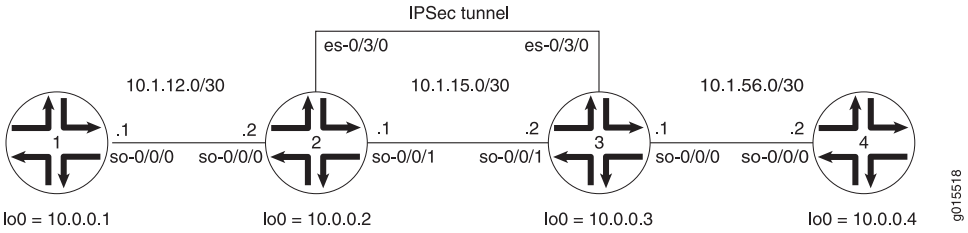


Figure 6 on page 115 shows an IPSec topology containing a group of four routers. Routers 2 and 3 establish an IPSec tunnel using an ES PIC and manual SA settings. Routers 1 and 4 provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R2 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.1;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA called **sa-manual** at the **[edit security ipsec security-association]** hierarchy level. Use AH for the protocol, **400** for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key for the MD5 authentication key. (For more information about key length, see Table 6 on page 103.) Because you are using AH, there is no need to configure encryption.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 1 destined for Router 4, whereas the **es-return** filter matches the return path from Router 4 to Router 1. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-manual** SA to the **es-0/3/0** interface.

Router 2

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.1;
        destination 10.1.15.2;
      }
      family inet {
        ipsec-sa sa-manual; # Apply the manual SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.2/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
```

```
        interface so-0/0/0.0;
        interface so-0/0/1.0;
        interface lo0.0;
      }
    }
}
security {
  ipsec {
    security-association sa-manual { # Define the manual SA specifications here.
      mode tunnel;
      manual {
        direction bidirectional {
          protocol ah;
          spi 400;
          authentication {
            algorithm hmac-md5-96;
            key hexadecimal "$ABC123";
          }
        }
      }
    }
  }
}

# The 32-bit unencrypted hexadecimal key is abcdef01abcdef01abcdef01abcdef01.
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-manual;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then accept;
```

```
    }
  }
}
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA called **sa-manual** at the **[edit security ipsec security-association]** hierarchy level. Use the exact same specifications that you used for the SA on Router 2: AH for the protocol, **400** for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key of **abcdef01abcdef01abcdef01abcdef01** for the MD5 authentication key. (For more information about authentication key length, see Table 6 on page 103.) Because you are using AH, there is no need to configure an encryption algorithm.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the **es-return** filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-manual** SA to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.2;
        destination 10.1.15.1;
      }
      family inet {
        ipsec-sa sa-manual; # Apply the manual SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
```

```
      unit 0 {
        family inet {
          address 10.0.0.3/32;
        }
      }
    }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    security-association sa-manual { # Define the manual SA specifications here.
      mode tunnel;
      manual {
        direction bidirectional {
          protocol ah;
          spi 400;
          authentication {
            algorithm hmac-md5-96;
            key hexadecimal "$ABC123";
          }
        }
      }
    }
  }
}


## The 32-bit unencrypted hexadecimal key is abcdef01abcdef01abcdef01abcdef01.
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-manual;
      }
    }
```

```
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then accept;
    }
  }
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.ping
    }
  }
}
```

Verifying Your Work

To verify proper operation of a manual IPSec SA on the ES PIC, use the following commands:

- **ping**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- Router 1 on page 121
- Router 2 on page 121
- Router 3 on page 122
- Router 4 on page 123

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.939 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.886 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.826 ms
^C
--- 10.1.56.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.826/0.884/0.939/0.046 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the second hop does not reference **10.1.15.2**—the physical interface on Router 3. Instead, the loopback address of **10.0.0.3** on Router 3 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1  10.1.12.1 (10.1.12.1)  0.655 ms  0.549 ms  0.508 ms
 2  10.0.0.3 (10.0.0.3)  0.833 ms  0.786 ms  0.757 ms
 3  10.1.56.2 (10.1.56.2)  0.808 ms  0.741 ms  0.716 ms
```

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. After you issue the **ping** command from Router 1 (three packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
```

```
Name                                                Bytes              Packets
ipsec-tunnel                                          252                    3
```

After you issue the **ping** command from both Router 1 (three packets) and Router 4 (two packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          420                    5
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA contains the settings you specified, such as AH for the protocol and HMAC-MD5-96 for the authentication algorithm.

```
user@R2> show ipsec security-associations detail
Security association: sa-manual, Interface family: Up

  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

   Direction: inbound, SPI: 400, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: AH, Authentication: hmac-md5-96, Encryption: None
    Anti-replay service: Disabled

    Direction: outbound, SPI: 400, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: AH, Authentication: hmac-md5-96, Encryption: None
    Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (three packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          252                    3
```

After you issue the **ping** command from both Router 1 (three packets) and Router 4 (two packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          420                    5
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
```

```
Security association: sa-manual, Interface family: Up

  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  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: 400, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: AH, Authentication: hmac-md5-96, Encryption: None
    Anti-replay service: Disabled

    Direction: outbound, SPI: 400, AUX-SPI: 0
    Mode: tunnel, Type: manual, State: Installed
    Protocol: AH, Authentication: hmac-md5-96, Encryption: None
    Anti-replay service: Disabled
```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface of Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=0.937 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.872 ms
^C
--- 10.1.12.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.872/0.905/0.937/0.032 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the loopback address of **10.0.0.2** on Router 2 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.56.1 (10.1.56.1)  0.670 ms  0.589 ms  0.548 ms
 2  10.0.0.2 (10.0.0.2)  0.815 ms  0.791 ms  0.763 ms
 3  10.1.12.2 (10.1.12.2)  0.798 ms  0.741 ms  0.714 ms
```

Configuring IKE Dynamic SAs

On the ES PIC, you configure an IKE dynamic SA at the **[edit security ike]** and **[edit security ipsec]** hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. The IKE policy must use the IP address of the remote end of the IPsec tunnel as the policy name. Also, include your choices for IPsec policies and proposals, which include options for authentication, encryption, protocols, Perfect Forward Secrecy (PFS), and IPsec modes. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

```
[edit security]
ike {
  proposal ike-proposal-name {
```

```
        authentication-algorithm (md5 | sha1 |sha-256 |sha-384);
        authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
        description description;
        dh-group (group1 | group2);
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
    }
    policy ike-peer-address {
        description description;
        encoding (binary | pem);
        identity identity-name;
        local-certificate certificate-filename;
        local-key-pair private-public-key-file;
        mode (aggressive | main);
        pre-shared-key (ascii-text key | hexadecimal key);
        proposals [ proposal-names ];
    }
}
ipsec {
    proposal ipsec-proposal-name  {
        authentication-algorithm (hmac-md5-96 | hmac-sha1-96 | hmac-sha-256-128);
        description description;
        encryption-algorithm (3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc | des-cbc);
        lifetime-seconds seconds;
        protocol (ah | esp | bundle);
    }
    policy ipsec-policy-name {
        description description;
        perfect-forward-secrecy {
            keys (group1 | group2);
        }
        proposals [ proposal-names ];
    }
    security-association sa-name {
        description description;
        dynamic {
            ipsec-policy policy-name;
            replay-window-size (32 | 64);
        }
        mode (tunnel | transport);
    }
}
```

On the AS and MultiServices PICs, you configure an IKE dynamic security association at the **[edit services ipsec-vpn ike]**, **[edit services ipsec-vpn ipsec]**, and **[edit services ipsec-vpn rule *rule-name*]** hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. Also, include your choices for IPsec policies and proposals, which include options for authentication, encryption, protocols, PFS, and IPsec modes. Be sure that these choices are configured exactly the same way on the remote IPsec gateway.

If you choose not to explicitly configure IKE and IPsec policies and proposals on the AS and MultiServices PICs, your configuration can default to some preset values. These default values are shown in Table 8 on page 125.

Table 8: IKE and IPsec Proposal and Policy Default Values for the AS and MultiServices PICs

IKE Policy Statement	Default Value
mode	main
proposals	default
IKE Proposal Statement	Default Value
authentication-algorithm	sha1
authentication-method	pre-shared-keys
dh-group	group2
encryption-algorithm	3des-cbc
lifetime-seconds	3600 (seconds)
IPsec Policy Statement	Default Value
perfect-forward-secrecy keys	group2
proposals	default
IPsec Proposal Statement	Default Value
authentication-algorithm	hmac-sha1-96
encryption-algorithm	3des-cbc
lifetime-seconds	28800 (seconds)
protocol	esp

NOTE: If you use the default IKE and IPsec policy and proposal values preset within the AS and MultiServices PICs, you must explicitly configure an IKE policy and include a preshared key. This is because the **pre-shared-keys** authentication method is one of the preset values in the default IKE proposal.

NOTE: Starting in Junos OS release 14.2, in an environment in which Juniper Networks MX Series routers interoperate with Cisco ASA devices, IKE security associations (SAs) and IPsec SAs are deleted immediately on the Cisco ASA devices, but they are retained on the MX Series routers.As a result, 100 percent traffic loss occurs on the MX routers when traffic is initiated from either the MX Series routers or Cisco ASA devices. This problem of excessive traffic loss occurs when a service PIC is restarted on MX Series routers, a line card is restarted on MX series routers, or when a shutdown/no shutdown command sequence or a change in speed setting is performed on the Cisco ASA devices. To prevent this problem of the preservation of IKE and IPsec SAs in such a deployment, you must manually delete the IPsec and IKE SAs by entering the **clear ipsec security-associations** and **clear ike security-associations** commands respectively.

If you decide to configure values manually, the following information shows the complete statement hierarchy and options for dynamic IKE SAs on the AS and MultiServices PICs:

```
[edit services ipsec-vpn]
ike {
   proposal proposal-name {
      authentication-algorithm (md5 | sha1 | sha256);
      authentication-method (pre-shared-keys | rsa-signatures);
      description description;
      dh-group (group1 | group2);
      encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
      # aes-256-cbc, des-cbc, or 3des-cbc.
      lifetime-seconds seconds;
   }
   policy policy-name {
      description description;
      local-id {
         ipv4_addr [ values ];
         key_id [ values ];
      }
      local-certificate certificate-id-name;
      mode (aggressive | main);
      pre-shared-key (ascii-text key | hexadecimal key);
      proposals [ proposal-names ];
      remote-id {
         ipv4_addr [ values ];
         key_id [ values ];
      }
   }
}
ipsec {
   proposal proposal-name {
      authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
      description description;
      encryption-algorithm algorithm; # This can be aes-128-cbc, aes-192-cbc,
      # aes-256-cbc, des-cbc, or 3des-cbc.
      lifetime-seconds seconds;
      protocol (ah | esp | bundle);
```

```
    }
    policy policy-name {
      description description;
      perfect-forward-secrecy {
        keys (group1 | group2);
      }
      proposals [ proposal-names ];
    }
  }
  rule rule-name {
    match-direction (input | output);
    term term-name {
      from {
        destination-address address;
        source-address address;
      }
      then {
        backup-remote-gateway address;
        clear-dont-fragment-bit;
        dynamic {
          ike-policy policy-name;
          ipsec-policy policy-name;
        }
        no-anti-replay;
        remote-gateway address;
        syslog;
      }
    }
  }
  rule-set rule-set-name {
    [ rule rule-names ];
  }
```

Release History Table

Release	Description
14.2	Starting in Junos OS release 14.2, in an environment in which Juniper Networks MX Series routers interoperate with Cisco ASA devices, IKE security associations (SAs) and IPsec SAs are deleted immediately on the Cisco ASA devices, but they are retained on the MX Series routers.

Example: AS PIC IKE Dynamic SA Configuration

Figure 7: AS PIC IKE Dynamic SA Topology Diagram

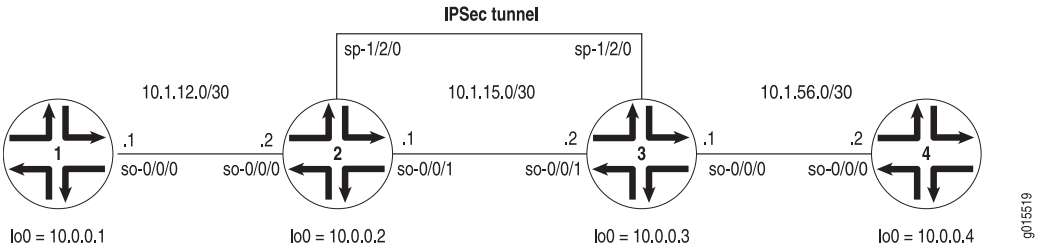


Figure 7 on page 127 shows the same IPSec topology as seen in the AS PIC manual SA example. However, this configuration requires Routers 2 and 3 to establish an IPSec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPSec tunnel is operational.

NOTE: When you do not specify an IKE proposal, an IPSec proposal, and an IPSec policy on an AS PIC, the Junos OS defaults to the highest level of encryption and authentication. As a result, the default authentication protocol is ESP, the default authentication mode is HMAC-SHA1-96, and the default encryption mode is 3DES-CBC. For more information about default IKE and IPSec policies and proposals on the AS PIC, see Table 8 on page 125.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R2 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.1;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Using default values in the AS PIC, you do not need to specify an IPsec proposal, IPsec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy

with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. (For more information about default IKE and IPsec policies and proposals on the AS PIC, see Table 8 on page 125.)

To direct traffic into the AS PIC and the IPSec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 2

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R1 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R3 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    sp-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
                }
            }
        }
        unit 0 {
            family inet {
            }
            unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
                family inet;
                service-domain inside;
            }
            unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
                family inet;
                service-domain outside;
            }
        }
        lo0 {
            unit 0 {
                family inet {
                    address 10.0.0.2/32;
                }
            }
        }
    }
    routing-options {
```

```
    router-id 10.0.0.2;
  }
  protocols {
    ospf {
      area 0.0.0.0 {
        interface so-0/0/0.0;
        interface lo0.0;
        interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
      }
    }
  }
  services {
    service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
      next-hop-service { # Required for dynamic routing protocols such as OSPF.
        inside-service-interface sp-1/2/0.1;
        outside-service-interface sp-1/2/0.2;
      }
      ipsec-vpn-options {
        local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
      }
      ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
    }
    ipsec-vpn {
      rule rule-ike { # Define your IPSec VPN rule here.
        term term-ike {
          then {
            remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
            dynamic { # This creates a dynamic SA.
              ike-policy ike-policy-preshared; # Reference your IKE policy here.
            }
          }
        }
        match-direction input; # Specify in which direction the rule should match.
      }
      ike {
        policy ike-policy-preshared { # Define your IKE policy specifications here.
          pre-shared-key ascii-text "$ABC123";
          ## The unencrypted preshared key for this example is juniper.
        }
      }
    }
  }
}
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Again, use the same default policies and proposals that you used on Router 2. However, remember to configure a preshared key in an IKE policy with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. The key must match the one you specified on Router 2. (For more information about default IKE and IPSec policies and proposals on the AS PIC, see Table 8 on page 125.)

To direct traffic into the AS PIC and the IPSec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 3

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R4 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R2 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    sp-1/2/0 {
        services-options {
            syslog {
                host local {
                    services info;
                }
            }
        }
        unit 0 {
            family inet {
            }
            unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
                family inet;
                service-domain inside;
            }
            unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
                family inet;
                service-domain outside;
            }
        }
        lo0 {
            unit 0 {
                family inet {
                    address 10.0.0.3/32;
                }
            }
        }
    }
    routing-options {
        router-id 10.0.0.3;
    }
    protocols {
        ospf {
            area 0.0.0.0 {
```

```
            interface so-0/0/0.0;
            interface lo0.0;
            interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
          }
        }
      }
      services {
        service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
          next-hop-service { # Required for dynamic routing protocols such as OSPF.
            inside-service-interface sp-1/2/0.1;
            outside-service-interface sp-1/2/0.2;
          }
          ipsec-vpn-options {
            local-gateway 10.1.15.2; # Specify the local IP address of the IPSec tunnel.
          }
          ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
        }
        ipsec-vpn {
          rule rule-ike { # Define your IPSec VPN rule here.
            term term-ike {
              then {
                remote-gateway 10.1.15.1; # The remote IP address of the IPSec tunnel.
                dynamic { # This creates a dynamic SA.
                  ike-policy ike-policy-preshared; # Reference your IKE policy here.
                }
              }
            }
            match-direction input; # Specify in which direction the rule should match.
          }
          ike {
            policy ike-policy-preshared { # Define your IKE policy specifications here.
              pre-shared-key ascii-text "$ABC123";
              ## The unencrypted preshared key for this example is juniper.
            }
          }
        }
      }
    }
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
```

```
        }
    }
}
routing-options {
    router-id 10.0.0.4;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **show services ipsec-vpn ipsec statistics**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- Router 1 on page 133
- Router 2 on page 134
- Router 3 on page 135
- Router 4 on page 135

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface on Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

Router 2

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command.

```
user@R2> show services ipsec-vpn ike security-associations
Remote Address  State         Initiator cookie  Responder cookie  Exchange type
10.1.15.2       Matured       03075bd3a0000003  4bff26a5c7000003  Main
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
    Direction: inbound, SPI: 2666326758, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26863 seconds
    Hard lifetime: Expires in 26998 seconds
    Anti-replay service: Enabled, Replay window size: 64
    Direction: outbound, SPI: 684772754, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26863 seconds
    Hard lifetime: Expires in 26998 seconds
    Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling over the bidirectional IPSec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R2> show services ipsec-vpn ipsec statistics
PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des
ESP Statistics:
  Encrypted bytes:             2248
  Decrypted bytes:             2120
  Encrypted packets:             27
  Decrypted packets:             25
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
```

Bad headers: 0, Bad trailers: 0

Router 3

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ike security-associations
Remote Address  State         Initiator cookie  Responder cookie  Exchange type
10.1.15.1       Matured       03075bd3a0000003  4bff26a5c7000003  Main
```

To verify that the IPsec SA is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
    Direction: inbound, SPI: 684772754, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26598 seconds
    Hard lifetime: Expires in 26688 seconds
    Anti-replay service: Enabled, Replay window size: 64
    Direction: outbound, SPI: 2666326758, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26598 seconds
    Hard lifetime: Expires in 26688 seconds
    Anti-replay service: Enabled, Replay window size: 64
```

To verify that traffic is traveling over the bidirectional IPsec tunnel, issue the **show services ipsec-vpn statistics** command:

```
user@R3> show services ipsec-vpn ipsec statistics
PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des
ESP Statistics:
  Encrypted bytes:             2120
  Decrypted bytes:             2248
  Encrypted packets:             25
  Decrypted packets:             27
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
```

Bad headers: 0, Bad trailers: 0

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
```

```
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

The final way you can confirm that traffic travels over the IPsec tunnel is by issuing the **traceroute** command to the **so-0/0/0** interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPSec tunnel through the adaptive services IPSec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the **so-0/0/0** interface on Router 1.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.15.2 (10.1.15.2)  0.987 ms  0.630 ms  0.563 ms
 2  10.0.0.2 (10.0.0.2)  1.194 ms  1.058 ms  1.033 ms
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.949 ms  0.932 ms
```

Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration

Figure 8: AS PIC IKE Dynamic SA Topology Diagram

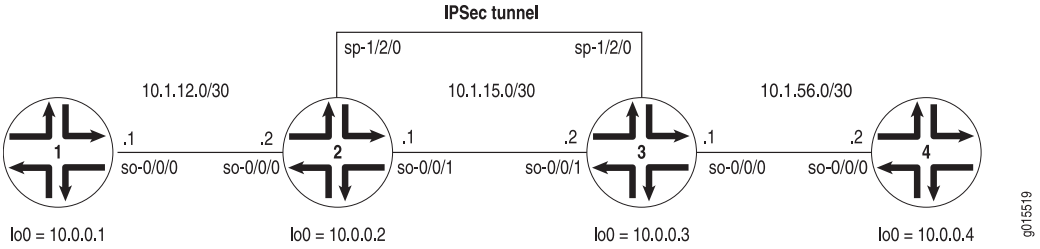


Figure 8 on page 136 shows the same IPSec topology as the AS PIC dynamic SA example on "Example: AS PIC IKE Dynamic SA Configuration" on page 127. However, this configuration requires Routers 2 and 3 to establish an IKE-based IPSec tunnel by using digital certificates in place of preshared keys. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R2 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
```

```
        family inet {
          address 10.0.0.1/32;
        }
      }
    }
  }
  routing-options {
    router-id 10.0.0.1;
  }
  protocols {
    ospf {
      area 0.0.0.0 {
        interface so-0/0/0.0;
        interface lo0.0;
      }
    }
  }
```

On Router 2, you must request a CA certificate, create a local certificate, and load these digital certificates into the router before you can reference them in your IPSec configuration. To begin, configure an IPSec profile by specifying the trusted CA and URL of the CA server that handles CA certificate processing:

```
[edit]
security {
  pki {
    ca-profile entrust {
      ca-identity entrust;
      enrollment {
        url http://ca-1.example.com/cgi-bin/pkiclient.exe;
      }
    }
  }
}
```

Certificate revocation list (CRL) verification is enabled by default. You can optionally specify the Lightweight Access Directory (LDAP) server where the CA stores the CRL. The certificate typically includes a certificate distribution point (CDP), which contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically. In this example, the LDAP URL is specified, which overrides the location provided in the certificate:

```
[edit]
security pki ca-profile entrust {
  revocation-check {
    crl {
      url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
    }
  }
}
```

After you configure the CA profile, you can request a CA certificate from the trusted CA. In this example, the certificate is enrolled online and installed into the router automatically.

```
user@R2> request security pki ca-certificate enroll ca-profile entrust
```

```
Received following certificates:
  Certificate: C=us, O=juniper
    Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or website download), you can install it with the **request security pki ca-certificate load** command.

Next, you must generate a private/public key pair before you can create a local certificate.

```
user@R2> request security pki generate-key-pair certificate-id local-entrust2
Generated key pair local-entrust2, key size 1024 bits
```

When the key pair is available, generate a local certificate request and send it to the CA for processing.

```
user@R2> request security pki generate-certificate-request
certificate-id local-entrust2 domain-name router2.example.com
filename entrust-req2 subject cn=router2.example.com
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8oOXyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH4O6gQ3G
3iHOZfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ7OfO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

NOTE: You can request the creation and installation of a local certificate online with the **request security pki local-certificate enroll** command. For more information, see "Generating and Enrolling a Local Digital Certificate" on page 228 or the *Junos System Basics and Services Command Reference*.

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

```
user@R2> request security pki local-certificate load filename /tmp/router2-cert   certificate-id
local-entrust2
Local certificate local-entrust2 loaded successfully
```

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

After the local and CA certificates have been loaded, you can reference them in your IPSec configuration.

Using default values in the AS PIC, you do not need to configure an IPSec proposal or IPSec policy. However, you must configure an IKE proposal that specifies the use of digital certificates, reference the IKE proposal and local certificate in an IKE policy, and apply the CA profile to the service set. To enable an IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name* authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

NOTE: For more information about default IKE and IPSec policies and proposals on the AS PIC, see Table 8 on page 125.

Optionally, you can configure automatic reenrollment of the certificate with the **auto-re-enrollment** statement at the [**edit security pki**] hierarchy level.

The remaining configuration components of your IKE-based IPSec tunnel are the same as when you use preshared keys. Enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPSec inside interface into the OSPF configuration.

Router 2

```
[edit]
interfaces {
   so-0/0/0 {
      description "To R1 so-0/0/0";
      unit 0 {
         family inet {
            address 10.1.12.1/30;
         }
      }
   }
   so-0/0/1 {
      description "To R3 so-0/0/1";
      unit 0 {
         family inet {
            address 10.1.15.1/30;
         }
```

```
    }
  }
  sp-1/2/0 {
    unit 0 {
      family inet;
    }
    unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
      family inet;
      service-domain inside;
    }
    unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
      family inet;
      service-domain outside;
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.2/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
      interface lo0.0;
    }
  }
}
security { # Configure CA profiles here, including the URLs used to reach the CAs.
  pki {
    ca-profile entrust {
      ca-identity entrust;
      enrollment {
        url http://ca-1.example.com/cgi-bin/pkiclient.exe;
      }
      revocation-check {
        crl {
          url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
          # Specify the URL of the LDAP server where the CA stores the CRL.
        }
      }
    }
    ca-profile microsoft {
      ca-identity microsoft;
      enrollment {
        url http://192.168.11.78:80/certsrv/mscep/mscep.dll;
      }
    }
    ca-profile verisign {
```

```
        ca-identity verisign;
        enrollment {
          url http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe;
        }
      }
    }
  }
  services {
    service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
      next-hop-service { # Required for dynamic routing protocols such as OSPF.
        inside-service-interface sp-1/2/0.1;
        outside-service-interface sp-1/2/0.2;
      }
      ipsec-vpn-options {
        trusted-ca entrust; # Reference the CA profile here.
        local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
      }
      ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
    }
    ipsec-vpn {
      rule rule-ike { # Define your IPSec VPN rule here.
        term term-ike {
          then {
            remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
            dynamic { # This creates a dynamic SA.
              ike-policy ike-digital-certificates; # Reference your IKE policy here.
            }
          }
        }
        match-direction input; # Specify in which direction the rule should match.
      }
      ike {
        proposal ike-proposal {
          authentication-method rsa-signatures; # Uses digital certificates
        }
        policy ike-digital-certificates {
          proposals ike-proposal; # Apply the IKE proposal here.
          local-id fqdn router2.example.com; # Provide an identifier for the local router.
          local-certificate local-entrust2; # Reference the local certificate here.
          remote-id fqdn router3.example.com; # Provide an ID for the remote router.
        }
      }
      establish-tunnels immediately;
    }
  }
```

On Router 3, you must repeat the digital certificate procedures you performed on Router 2. If the IPSec peers do not have a symmetrical configuration containing all the necessary components, they cannot establish a peering relationship.

You need to request a CA certificate, create a local certificate, load these digital certificates into the router, and reference them in your IPSec configuration. Begin by configuring an IPSec CA profile. Include the **ca-profile** statement at the **[edit security pki]** hierarchy level and specify the trusted CA and URL of the CA server that handles CA

certificate processing. Include the CRL statements found on Router 2 to complete your CA profile on Router 3.

After you configure the CA profile, request a CA certificate from the trusted CA. In this example, the certificate is enrolled online and installed into the router automatically.

```
user@R3> request security pki ca-certificate enroll ca-profile entrust
Received following certificates:
  Certificate: C=us, O=juniper
    Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

NOTE: If you obtain the CA certificate directly from the CA (for example, as an e-mail attachment or website download), you can install it with the request security pki ca-certificate load command.

Next, generate a private/public key pair.

```
user@R3> request security pki generate-key-pair certificate-id local-entrust3
Generated key pair local-entrust3, key size 1024 bits
```

When the key pair is available, you can generate a local certificate request and send it to the CA for processing.

```
user@R3> request security pki generate-certificate-request
certificate-id local-entrust3 domain-name router3.example.com
filename entrust-req3 subject cn=router3.example.com
Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIB8jCCAVsCAQAwZTEYMBYGA1UEAxMPdHA1Lmp1bmlwZXIubmV0MRQwEgYDVQQL
EwtFbmdpbmVlcmluZzEQMA4GA1UEChMHSnVuaXBlcjETMBEGA1UECBMKQ2FsaWZv
cm5pYTEMMAoGA1UEBhMDVVNBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCg
Wjo50w8jrnphs0sRFvqQMwC6PlYa65thrJ8nHZ2qgYgRbSrO8hdODhvU6/5VuD2/
zBtgV5ZSAOlyV6DXqlbVj/2XirQAJMRCr1eYu6DhYRBMNq/UaQv4Z8Sse1EJv+uR
HTNbD7xlwpw2zwzltRuGFtFr/FrGB0hF7IE+Xm5e2wIDAQABoE0wSwYJKoZIhvcN
AQkOMT4wPDAOBgNVHQ8BAf8EBAMCB4AwKgYDVR0RAQH/BCAwHocEwKhGk4IWdHA1
LmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQFAAOBgQBbiJ+ZCeQ59/eY
4Rd6awIpJFTzOsvRZLxxjFWogusVTmaD2dsqFBqftS1eJBdeiueRcYMF9vOnOGKm
FNfouegwei5+vzdNmNo55eIb3rs4pP62qOW5CUgmbHrjtp3lyJsvuOxTTcPNY8zw
b6GyM2Hdkk3Vh2ReX11tQUSqYujTjw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
7c:e8:f9:45:93:8d:a3:92:7f:18:29:02:f1:c8:e2:85:3d:ad:df:1f (sha1)
00:4e:df:a0:6b:ad:8c:50:da:7c:a1:cf:5d:37:b0:ea (md5)
```

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

```
user@R3> request security pki local-certificate load filename /tmp/router3-cert certificate-id
local-entrust3
Local certificate local-entrust3 loaded successfully
```

After the local and CA certificates have been loaded, you can reference them in your IPSec configuration. Using default values in the AS PIC, you do not need to configure an IPSec proposal or IPSec policy. However, you must configure an IKE proposal that uses digital certificates, reference the IKE proposal and local certificate in an IKE policy, and apply the CA profile to the service set. To enable the IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name* authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

The remaining configuration components of your IKE-based IPsec tunnel are the same as when you use preshared keys. Enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

To direct traffic into the AS PIC and the IPsec tunnel, configure a next-hop style service set and add the adaptive services logical interface used as the IPsec inside interface into the OSPF configuration.

Router 3

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R4 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.56.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R2 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.2/30;
            }
        }
    }
    sp-1/2/0 {
        unit 0 {
            family inet;
        }
        unit 1 { # sp-1/2/0.1 is the IPSec inside interface.
            family inet;
            service-domain inside;
        }
        unit 2 { # sp-1/2/0.2 is the IPSec outside interface.
            family inet;
            service-domain outside;
        }
    }
    lo0 {
```

```
      unit 0 {
        family inet {
          address 10.0.0.3/32;
        }
      }
    }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface sp-1/2/0.1; # This sends OSPF traffic over the IPSec tunnel.
      interface lo0.0;
    }
  }
}
security { # Configure CA profiles here, including the URLs used to reach the CAs.
  pki {
    ca-profile entrust {
      ca-identity entrust;
      enrollment {
        url http://ca-1.example.com/cgi-bin/pkiclient.exe;
      }
      revocation-check {
        crl {
          url ldap://10.157.90.185/o=juniper,c=uscertificateRevocationListbase;
          # Specify the URL of the LDAP server where the CA stores the CRL.
        }
      }
    }
    ca-profile microsoft {
      ca-identity microsoft;
      enrollment {
        url http://192.168.11.78:80/certsrv/mscep/mscep.dll;
      }
    }
    ca-profile verisign {
      ca-identity verisign;
      enrollment {
        url http://pilotonsiteipsec.verisign.com/cgi-bin/pkiclient.exe;
      }
    }
  }
}
services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    next-hop-service { # Required for dynamic routing protocols such as OSPF.
      inside-service-interface sp-1/2/0.1;
      outside-service-interface sp-1/2/0.2;
    }
    ipsec-vpn-options {
      trusted-ca entrust; # Reference the CA profile here.
      local-gateway 10.1.15.2; # Specify the local IP address of the IPSec tunnel.
```

```
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
        then {
          remote-gateway 10.1.15.1; # The remote IP address of the IPSec tunnel.
          dynamic { # This creates a dynamic SA.
            ike-policy ike-digital-certificates; # Reference your IKE policy here.
          }
        }
      }
      match-direction input; # Specify in which direction the rule should match.
    }
    ike {
      proposal ike-proposal {
        authentication-method rsa-signatures; # Uses digital certificates
      }
      policy ike-digital-certificates {
        proposals ike-proposal; # Apply the IKE proposal here.
        local-id fqdn router3.example.com; # Provide an identifier for the local router.
        local-certificate local-entrust3; # Reference the local certificate here.
        remote-id fqdn router2.example.com; # Provide an ID for the remote router.
      }
    }
    establish-tunnels immediately;
  }
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
```

```
        interface so-0/0/0.0;
        interface lo0.0;
      }
    }
  }
```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn certificates (detail)**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **show services ipsec-vpn ipsec statistics**
- **traceroute**

To verify and manage digital certificates in your router, use the following commands:

- **show security pki ca-certificate (detail)**
- **show security pki certificate-request (detail)**
- **show security pki local-certificate (detail)**

The following sections show the output of these commands used with the configuration example:

- Router 1 on page 146
- Router 2 on page 147
- Router 3 on page 150
- Router 4 on page 153

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface on Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

If you ping the loopback address of Router 4, the operation succeeds because the address is part of the OSPF network configured on Router 4.

```
user@R1> ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=62 time=1.318 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=62 time=1.084 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=62 time=3.260 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.084/1.887/3.260/0.975 ms
```

Router 2

To verify that matched traffic is being diverted to the bidirectional IPSec tunnel, view the IPSec statistics:

```
user@R2> show services ipsec-vpn ipsec statistics

PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des

ESP Statistics:
  Encrypted bytes:           162056
  Decrypted bytes:           161896
  Encrypted packets:           2215
  Decrypted packets:           2216
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command:

```
user@R2> show services ipsec-vpn ike security-associations
Remote Address  State         Initiator cookie  Responder cookie  Exchange type
10.1.15.2       Matured       d82610c59114fd37  ec4391f76783ef28  Main
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des

  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  IPSec inside interface: sp-1/2/0.1
  Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

    Direction: inbound, SPI: 857451461, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
```

```
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 9052 seconds
    Hard lifetime: Expires in 9187 seconds
    Anti-replay service: Enabled, Replay window size: 64

    Direction: outbound, SPI: 1272330309, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 9052 seconds
    Hard lifetime: Expires in 9187 seconds
    Anti-replay service: Enabled, Replay window size: 64
```

To display the digital certificates that are used to establish the IPSec tunnel, issue the **show services ipsec-vpn certificates** command:

```
user@R2> show services ipsec-vpn certificates
Service set: service-set-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Flags: Non-root Trusted
    Issued to: router3.example.com, Issued by: juniper
    Alternate subject: router3.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:33:58 GMT
      Not after: 2008 Nov 22nd, 00:03:58 GMT

  Certificate cache entry: 2
    Flags: Non-root Trusted
    Issued to: router2.example.com, Issued by: juniper
    Alternate subject: router2.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:28:22 GMT
      Not after: 2008 Nov 21st, 23:58:22 GMT

  Certificate cache entry: 1
    Flags: Root Trusted
    Issued to: juniper, Issued by: juniper
    Validity:
      Not before: 2005 Oct 18th, 23:54:22 GMT
      Not after: 2025 Oct 19th, 00:24:22 GMT
```

To display the CA certificate, issue the **show security pki ca-certificate detail** command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

```
user@R2> show security pki ca-certificate detail
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
```

```
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: CRL signing, Certificate signing

Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
    23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925b
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
    d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
    00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
    e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
    90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
    b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
    af:44:bf:53:aa:d4:5f:67
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
    ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
```

```
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature
```

To display the local certificate request, issue the **show security pki certificate-request** command:

```
user@R2> show security pki certificate-request
Certificate identifier: local-entrust2
  Issued to: router2.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

To display the local certificate, issue the **show security pki local-certificate** command:

```
user@R2> show security pki local-certificate
Certificate identifier: local-entrust2
  Issued to: router2.example.com, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

Router 3

To verify that matched traffic is being diverted to the bidirectional IPSec tunnel, view the IPSec statistics:

```
user@R3> show services ipsec-vpn ipsec statistics

PIC: sp-1/2/0, Service set: service-set-dynamic-BiEspsha3des

ESP Statistics:
  Encrypted bytes:           161896
  Decrypted bytes:           162056
  Encrypted packets:           2216
  Decrypted packets:           2215
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ike security-associations
Remote Address  State         Initiator cookie  Responder cookie  Exchange type
10.1.15.1       Matured       d82610c59114fd37  ec4391f76783ef28  Main
```

To verify that the IPsec SA is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
```

```
Service set: service-set-dynamic-BiEspsha3des

  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  IPSec inside interface: sp-1/2/0.1
  Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

    Direction: inbound, SPI: 1272330309, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 7219 seconds
    Hard lifetime: Expires in 7309 seconds
    Anti-replay service: Enabled, Replay window size: 64

    Direction: outbound, SPI: 857451461, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 7219 seconds
    Hard lifetime: Expires in 7309 seconds
    Anti-replay service: Enabled, Replay window size: 64
```

To display the digital certificates that are used to establish the IPsec tunnel, issue the **show services ipsec-vpn certificates** command:

```
user@R3> show services ipsec-vpn certificates
Service set: service-set-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Flags: Non-root Trusted
    Issued to: router3.example.com, Issued by: juniper
    Alternate subject: router3.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:33:58 GMT
      Not after: 2008 Nov 22nd, 00:03:58 GMT

  Certificate cache entry: 2
    Flags: Non-root Trusted
    Issued to: router2.example.com, Issued by: juniper
    Alternate subject: router2.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:28:22 GMT
      Not after: 2008 Nov 21st, 23:58:22 GMT

  Certificate cache entry: 1
    Flags: Root Trusted
    Issued to: juniper, Issued by: juniper
    Validity:
      Not before: 2005 Oct 18th, 23:54:22 GMT
      Not after: 2025 Oct 19th, 00:24:22 GMT
```

To display the CA certificate, issue the **show security pki ca-certificate detail** command. Notice that there are three separate certificates: one for certificate signing, one for key encipherment, and one for the CA's digital signature.

```
user@R3> show security pki ca-certificate detail
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: juniper, Country: us
  Subject:
```

```
    Organization: juniper, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
    23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925b
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
    d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
    00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
    e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
```

```
    90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
    b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
    af:44:bf:53:aa:d4:5f:67
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
    ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature
```

To display the local certificate request, issue the **show security pki certificate-request** command:

```
user@R3> show security pki certificate-request
Certificate identifier: local-entrust3
  Issued to: router3.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

To display the local certificate, issue the **show security pki local-certificate** command:

```
user@R3> show security pki local-certificate
Certificate identifier: local-entrust3
  Issued to: router3.example.com, Issued by: juniper
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

The final way you can confirm that traffic travels over the IPsec tunnel is by issuing the **traceroute** command to the **so-0/0/0** interface on Router 1. Notice that the physical interface between Routers 2 and 3 is not referenced in the path; traffic enters the IPSec tunnel through the adaptive services IPSec inside interface on Router 3, passes through the loopback interface on Router 2, and ends at the **so-0/0/0** interface on Router 1.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.15.2 (10.1.15.2)  0.987 ms  0.630 ms  0.563 ms
 2  10.0.0.2 (10.0.0.2)  1.194 ms  1.058 ms  1.033 ms
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.949 ms  0.932 ms
```

For additional information on using digital certificates, see the *Junos Services Interfaces Configuration Guide* and the *Junos System Basics and Services Command Reference*.

Example: ES PIC IKE Dynamic SA Configuration

Figure 9: ES PIC IKE Dynamic SA Topology Diagram

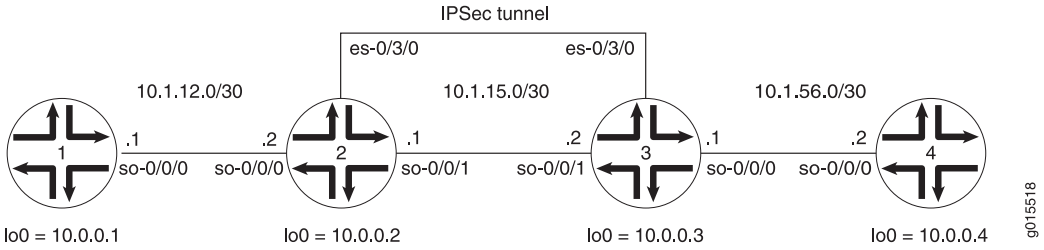


Figure 9 on page 154 shows the same IPSec topology as seen in the ES PIC manual SA example. However, this time the configuration requires Routers 2 and 3 to establish an IPSec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R2 so-0/0/0";
        unit 0 {
            family inet {
                address 10.1.12.2/30;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.1/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.1;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface lo0.0;
        }
    }
}
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 1 destined for Router 4, whereas the **es-return** filter matches the return path from Router 4 to Router 1. Apply the **es-traffic** filter to the **so-0/0/0** interface, and then apply both the **es-return** filter and the **sa-dynamic** SA to the **es-0/3/0** interface.

Router 2

```
[edit]
interfaces {
    so-0/0/0 {
        description "To R1 so-0/0/0";
        unit 0 {
            family inet {
                filter {
                    input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
                }
                address 10.1.12.1/30;
            }
        }
    }
    so-0/0/1 {
        description "To R3 so-0/0/1";
        unit 0 {
            family inet {
                address 10.1.15.1/30;
            }
        }
    }
    es-0/3/0 {
        unit 0 {
            tunnel { # Specify the IPSec tunnel endpoints here.
                source 10.1.15.1;
                destination 10.1.15.2;
            }
            family inet {
                ipsec-sa sa-dynamic; # Apply the dynamic SA here.
                filter {
                    input es-return; # Apply the filter that matches return IPSec traffic here.
                }
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.2/32;
```

```
        }
      }
    }
}
routing-options {
    router-id 10.0.0.2;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface so-0/0/1.0;
            interface lo0.0;
        }
    }
}
security {
    ipsec {
        proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 28800;
        }
        policy es-ipsec-policy { # Define your IPSec policy specifications here.
            perfect-forward-secrecy {
                keys group2;
            }
            proposals es-ipsec-proposal; # Reference the IPSec proposal here.
        }
        security-association sa-dynamic { # Define your dynamic SA here.
            mode tunnel;
            dynamic {
                ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
            }
        }
    }
    ike {
        proposal es-ike-proposal { # Define your IKE proposal specifications here.
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 3600;
        }
        policy 10.1.15.2 { # Define your IKE policy specifications here.
            mode main;
            proposals es-ike-proposal; # Reference the IKE proposal here.
            pre-shared-key ascii-text "$ABC123";
            ## The unencrypted preshared key for this example is juniper.
        }
    }
}
firewall {
    filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
        term to-es {
```

```
        from {
          source-address {
            10.1.12.0/24;
          }
          destination-address {
            10.1.56.0/24;
          }
        }
        then {
          count ipsec-tunnel;
          ipsec-sa sa-dynamic;
        }
      }
      term other {
        then accept;
      }
    }
    filter es-return { # Define a filter that matches return IPSec traffic here.
      term return {
        from {
          source-address {
            10.1.56.0/24;
          }
          destination-address {
            10.1.12.0/24;
          }
        }
        then accept;
      }
    }
  }
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. Use the same policies and proposals that you used on Router 2.

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the **es-return** filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-dynamic** SA to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
```

```
        family inet {
          filter {
            input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
          }
          address 10.1.56.1/30;
        }
      }
    }
    so-0/0/1 {
      description "To R2 so-0/0/1";
      unit 0 {
        family inet {
          address 10.1.15.2/30;
        }
      }
    }
    es-0/3/0 {
      unit 0 {
        tunnel { # Specify the IPSec tunnel endpoints here.
          source 10.1.15.2;
          destination 10.1.15.1;
        }
        family inet {
          ipsec-sa sa-dynamic; # Apply the dynamic SA here.
          filter {
            input es-return; # Apply the filter that matches return IPSec traffic here.
          }
        }
      }
    }
    lo0 {
      unit 0 {
        family inet {
          address 10.0.0.3/32;
        }
      }
    }
}
routing-options {
    router-id 10.0.0.3;
}
protocols {
    ospf {
      area 0.0.0.0 {
        interface so-0/0/0.0;
        interface so-0/0/1.0;
        interface lo0.0;
      }
    }
}
security {
    ipsec {
      proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm 3des-cbc;
```

```
        lifetime-seconds 28800;
      }
      policy es-ipsec-policy { # Define your IPSec policy specifications here.
        perfect-forward-secrecy {
          keys group2;
        }
        proposals es-ipsec-proposal; # Reference the IPSec proposal here.
      }
      security-association sa-dynamic { # Define your dynamic SA here.
        mode tunnel;
        dynamic {
          ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
        }
      }
    }
    ike {
      proposal es-ike-proposal { # Define your IKE proposal specifications here.
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 3600;
      }
      policy 10.1.15.1 { # Define your IKE policy specifications here.
        mode main;
        proposals es-ike-proposal; # Reference the IKE proposal here.
        pre-shared-key ascii-text "$ABC123";
        ## The unencrypted preshared key for this example is juniper.
      }
    }
  }
  firewall {
    filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
      term to-es {
        from {
          source-address {
            10.1.56.0/24;
          }
          destination-address {
            10.1.12.0/24;
          }
        }
        then {
          count ipsec-tunnel;
          ipsec-sa sa-dynamic;
        }
      }
      term other {
        then accept;
      }
    }
    filter es-return { # Define a filter that matches return IPSec traffic here.
      term return {
        from {
          source-address {
            10.1.12.0/24;
```

```
            }
            destination-address {
              10.1.56.0/24;
            }
          }
          then accept;
        }
      }
    }
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

- **ping**
- **show ike security-associations (detail)**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.917 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.881 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.897 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=0.871 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=253 time=0.890 ms
64 bytes from 10.1.56.2: icmp_seq=5 ttl=253 time=0.858 ms
64 bytes from 10.1.56.2: icmp_seq=6 ttl=253 time=0.904 ms
^C
--- 10.1.56.2 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.858/0.888/0.917/0.019 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the second hop does not reference **10.1.15.2**—the physical interface on Router 3. Instead, the loopback address of **10.0.0.3** on Router 3 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1  10.1.12.1 (10.1.12.1)  0.655 ms  0.549 ms  0.508 ms
 2  10.0.0.3 (10.0.0.3)  0.833 ms  0.786 ms  0.757 ms
```

3 10.1.56.2 (10.1.56.2) 0.808 ms 0.741 ms 0.716 ms

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. After you issue the **ping** command from Router 1 (seven packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          588                    7
```

After you issue the **ping** command from both Router 1 (seven packets) and Router 4 (five packets), the **es-traffic** firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
```

```
Name                                                Bytes              Packets
ipsec-tunnel                                         1008                   12
```

To verify that the IKE SA negotiation between Routers 2 and 3 is successful, issue the **show ike security-associations detail** command. Notice that the SA contains the settings you specified, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show ike security-associations detail
IKE peer 10.1.15.2
  Role: Initiator, State: Matured
  Initiator cookie: b5dbdfe2f9000000, Responder cookie: a24c868410000041
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.1:500, Remote: 10.1.15.2:500
  Lifetime: Expires in 401 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 1736
   Output bytes  :                 2652
   Input  packets:                    9
   Output packets:                   15
  Flags: Caller notification sent
  IPSec security associations: 3 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA contains the settings you specified, such as ESP for the protocol, HMAC-SHA1-96 for the authentication algorithm, and 3DES-CBC for the encryption algorithm.

```
user@R2> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
    Direction: inbound, SPI: 2133029543, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26212 seconds
    Hard lifetime: Expires in 26347 seconds
    Anti-replay service: Disabled
    Direction: outbound, SPI: 1759450863, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26212 seconds
    Hard lifetime: Expires in 26347 seconds
    Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (seven packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
```

```
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          588                    7
```

After you issue the **ping** command from both Router 1 (seven packets) and Router 4 (five packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                         1008                   12
```

To verify the success of the IKE security association, issue the **show ike security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
IKE peer 10.1.15.1
  Role: Responder, State: Matured
  Initiator cookie: b5dbdfe2f9000000, Responder cookie: a24c868410000041
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.2:500, Remote: 10.1.15.1:500
  Lifetime: Expires in 564 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 2652
   Output bytes  :                 1856
   Input  packets:                   15
   Output packets:                   10
  Flags: Caller notification sent
  IPSec security associations: 3 created, 4 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up
  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
    Direction: inbound, SPI: 1759450863, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26427 seconds
    Hard lifetime: Expires in 26517 seconds
    Anti-replay service: Disabled
    Direction: outbound, SPI: 2133029543, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 26427 seconds
    Hard lifetime: Expires in 26517 seconds
    Anti-replay service: Disabled
```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface of Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=13.528 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.873 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=253 time=32.145 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=253 time=0.921 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=253 time=0.899 ms
^C
--- 10.1.12.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.873/9.673/32.145/12.255 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the loopback address of **10.0.0.2** on Router 2 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.56.1 (10.1.56.1)  0.681 ms  0.624 ms  0.547 ms
 2  10.0.0.2 (10.0.0.2)  0.800 ms  0.770 ms  0.737 ms
 3  10.1.12.2 (10.1.12.2)  0.793 ms  0.742 ms  0.716 ms
```

Example: IKE Dynamic SA Between an AS PIC and an ES PIC Configuration

Figure 10: AS PIC to ES PIC IKE Dynamic SA Topology Diagram

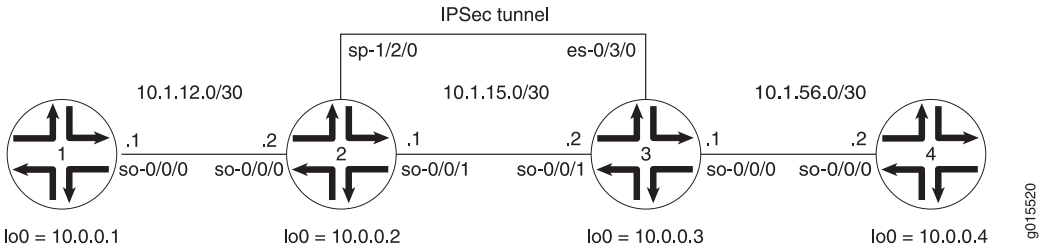


Figure 10 on page 164 shows a hybrid configuration that allows you to create an IPSec tunnel between the AS PIC and the ES PIC. Router 2 contains an AS PIC at **sp-1/2/0** and Router 3 has an ES PIC at **es-0/3/0**. To establish an IPSec tunnel using an IKE dynamic SA, the key is to learn the default IKE SA and IPSec SA settings built into the AS PIC and configure them explicitly on the ES PIC. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

Router 1

```
[edit]
interfaces {
   so-0/0/0 {
      description "To R2 so-0/0/0";
```

```
        unit 0 {
          family inet {
            address 10.1.12.2/30;
          }
        }
      }
      lo0 {
        unit 0 {
          family inet {
            address 10.0.0.1/32;
          }
        }
      }
    }
    routing-options {
      router-id 10.0.0.1;
    }
    protocols {
      ospf {
        area 0.0.0.0 {
          interface so-0/0/0.0;
          interface lo0.0;
        }
      }
    }
```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called **rule-ike** at the **[edit ipsec-vpn rule]** hierarchy level. Reference this rule in a service set called **service-set-dynamic-BiEspsha3des** at the **[edit services service-set]** hierarchy level.

Using default values in the AS PIC, you do not need to specify an IPSec proposal, IPSec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy with the **pre-shared-key** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. (For more information about default IKE and IPSec policies and proposals on the AS PIC, see Table 8 on page 125.)

To direct traffic into the AS PIC and the IPSec tunnel, include match conditions in the **rule-ike** IPSec VPN rule to match inbound traffic from Router 1 that is destined for Router 4. Because the rule is already referenced by the service set, apply the service set to the **so-0/0/1** interface. To count the amount of traffic that enters the IPsec tunnel, configure a firewall filter called **ipsec-tunnel** and apply it to the **sp-1/2/0** interface.

Router 2

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
```

```
        unit 0 {
          family inet {
            service { # Apply the service set here.
              input {
                service-set service-set-dynamic-BiEspsha3des;
              }
              output {
                service-set service-set-dynamic-BiEspsha3des;
              }
            }
            address 10.1.15.1/30;
          }
        }
      }
      sp-1/2/0 {
        services-options {
          syslog {
            host local {
              services info;
            }
          }
        }
        unit 0 {
          family inet {
            filter {
              input ipsec-tunnel; # Apply the firewall filter with the counter here.
            }
          }
        }
      }
      lo0 {
        unit 0 {
          family inet {
            address 10.0.0.2/32;
          }
        }
      }
    }
    routing-options {
      router-id 10.0.0.2;
    }
    protocols {
      ospf {
        area 0.0.0.0 {
          interface so-0/0/0.0;
          interface so-0/0/1.0;
          interface lo0.0;
        }
      }
    }
    firewall {
      filter ipsec-tunnel { # Configure a firewall filter to count IPsec traffic here.
        term 1 {
          then {
            count ipsec-tunnel;
            accept;
```

```
        }
      }
    }
  }
  services {
    service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
      interface-service {
        service-interface sp-1/2/0; # Specify an interface to process IPsec.
      }
      ipsec-vpn-options {
        local-gateway 10.1.15.1; # Specify the local IP address of the IPsec tunnel.
      }
      ipsec-vpn-rules rule-ike; # Reference your IPsec VPN rule here.
    }
    ipsec-vpn {
      rule rule-ike { # Define your IPsec VPN rule here.
        term term-ike {
          from {
            source-address {
              10.1.12.0/24;
            }
            destination-address {
              10.1.56.0/24;
            }
          }
          then {
            remote-gateway 10.1.15.2; # The remote IP address of the IPsec tunnel.
            dynamic { # This creates a dynamic SA.
              ike-policy ike-policy-preshared; # Reference your IKE proposal here.
            }
          }
        }
        match-direction output; # Specify in which direction the rule should match.
      }
      ike {
        policy ike-policy-preshared { # Define your IKE policy specifications here.
          pre-shared-key ascii-text "$ABC123";
          ## The unencrypted preshared key for this example is juniper.
        }
      }
    }
  }
```

Router 2

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
```

```
        family inet {
          service { # Apply the service set here.
            input {
              service-set service-set-dynamic-BiEspsha3des;
            }
            output {
              service-set service-set-dynamic-BiEspsha3des;
            }
          }
          address 10.1.15.1/30;
        }
      }
    }
    sp-1/2/0 {
      services-options {
        syslog {
          host local {
            services info;
          }
        }
      }
      unit 0 {
        family inet {
          filter {
            input ipsec-tunnel; # Apply the firewall filter with the counter here.
          }
        }
      }
    }
    lo0 {
      unit 0 {
        family inet {
          address 10.0.0.2/32;
        }
      }
    }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
```

```
        }
      }
    }
    services {
      service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
        interface-service {
          service-interface sp-1/2/0; # Specify an interface to process IPSec.
        }
        ipsec-vpn-options {
          local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
        }
        ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
      }
      ipsec-vpn {
        rule rule-ike { # Define your IPSec VPN rule here.
          term term-ike {
            from {
              source-address {
                10.1.12.0/24;
              }
              destination-address {
                10.1.56.0/24;
              }
            }
            then {
              remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
              dynamic { # This creates a dynamic SA.
                ike-policy ike-policy-preshared; # Reference your IKE proposal here.
              }
            }
          }
          match-direction output; # Specify in which direction the rule should match.
        }
        ike {
          policy ike-policy-preshared { # Define your IKE policy specifications here.
            pre-shared-key ascii-text "$ABC123";
            ## The unencrypted preshared key for this example is juniper.
          }
        }
      }
    }
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called **sa-dynamic** at the **[edit security ipsec security-association]** hierarchy level. To allow the ES PIC to communicate with the IKE dynamic SA established on Router 2, you must explicitly configure the same policies and proposals on the ES PIC that are available by default on the AS PIC. (For more information about default IKE and IPSec policies and proposals on the AS PIC, see Table 8 on page 125.)

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of **juniper** for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The **es-traffic** filter matches inbound traffic from Router 4 destined for Router 1, whereas the **es-return** filter matches the return path from Router 1 to Router 4. Apply the **es-traffic** filter to the **so-0/0/0** interface; then apply both the **es-return** filter and the **sa-dynamic SA** to the **es-0/3/0** interface.

Router 3

```
[edit]
interfaces {
   so-0/0/0 {
      description "To R4 so-0/0/0";
      unit 0 {
         family inet {
            filter {
               input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
            }
            address 10.1.56.1/30;
         }
      }
   }
   so-0/0/1 {
      description "To R2 so-0/0/1";
      unit 0 {
         family inet {
            address 10.1.15.2/30;
         }
      }
   }
   es-0/3/0 {
      unit 0 {
         tunnel { # Specify the IPSec tunnel endpoints here.
            source 10.1.15.2;
            destination 10.1.15.1;
         }
         family inet {
            ipsec-sa sa-dynamic; # Apply the dynamic SA here.
            filter {
               input es-return; # Apply the filter that matches return IPSec traffic here.
            }
         }
      }
   }
   lo0 {
      unit 0 {
         family inet {
            address 10.0.0.3/32;
         }
      }
   }
}
routing-options {
   router-id 10.0.0.3;
}
protocols {
   ospf {
      area 0.0.0.0 {
         interface so-0/0/0.0;
```

```
        interface so-0/0/1.0;
        interface lo0.0;
      }
    }
}
security {
  ipsec {
    proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 28800;
    }
    policy es-ipsec-policy { # Define your IPSec policy specifications here.
      perfect-forward-secrecy {
        keys group2;
      }
      proposals es-ipsec-proposal; # Reference the IPSec proposal here.
    }
    security-association sa-dynamic { # Define your dynamic SA here.
      mode tunnel;
      dynamic {
        ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
      }
    }
  }
  ike {
    proposal es-ike-proposal { # Define your IKE proposal specifications here.
      authentication-method pre-shared-keys;
      dh-group group2;
      authentication-algorithm sha1;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 3600;
    }
    policy 10.1.15.1 { # Define your IKE policy specifications here.
      mode main;
      proposals es-ike-proposal; # Reference the IKE proposal here.
      pre-shared-key ascii-text "$ABC123";
      ## The unencrypted preshared key for this example is juniper.
    }
  }
}
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
```

```
        }
      }
      term other {
        then accept;
      }
    }
    filter es-return { # Define a filter that matches return IPSec traffic here.
      term return {
        from {
          source-address {
            10.1.12.0/24;
          }
          destination-address {
            10.1.56.0/24;
          }
        }
        then accept;
      }
    }
}
```

On Router 4, provide basic OSPF connectivity to Router 3.

Router 4

```
[edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}
```

Verifying Your Work

To verify proper operation of an IKE-based dynamic SA on the AS PIC, use the following commands:

- **ping**
- **show services ipsec-vpn ike security-associations (detail)**
- **show services ipsec-vpn ipsec security-associations (detail)**
- **traceroute**

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

- **ping**
- **show ike security-associations (detail)**
- **show ipsec security-associations (detail)**
- **traceroute**

The following sections show the output of these commands used with the configuration example:

- Router 1 on page 173
- Router 2 on page 174
- Router 3 on page 175
- Router 4 on page 176

Router 1

On Router 1, issue a **ping** command to the **so-0/0/0** interface of Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=1.020 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.998 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=1.037 ms
^C
--- 10.1.56.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.998/1.057/1.172/0.068 ms
```

You can also issue the **traceroute** command to verify that traffic to **10.1.56.2** travels over the IPsec tunnel between Router 2 and Router 3. Notice that the traced path does not reference **10.1.15.2**—the physical interface on Router 3. Instead, traffic arriving at Router 2 is immediately filtered into the IPSec tunnel and the path is listed as unknown with the *** notation. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
```

```
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1  * * *
 2  10.1.56.2 (10.1.56.2)  1.045 ms  0.915 ms  0.850 ms
```

Router 2

One way to verify that matched traffic is being diverted to the bidirectional IPSec tunnel is to view the firewall filter counter. Before any traffic flows, the **ipsec-tunnel** firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                            0                    0
```

After you issue the **ping** command from Router 1 (four packets) to **10.1.56.2**, the **ipsec-tunnel** firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          336                    4
```

After you issue the **ping** command from both Router 1 to **10.1.56.2** (four packets) and from Router 4 to **10.1.12.2** (six packets), the **ipsec-tunnel** firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          840                   10
```

To verify that the IKE SA negotiation is successful, issue the **show services ipsec-vpn ike security-associations detail** command. Notice that the SA contains the default IKE settings inherent in the AS PIC, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show services ipsec-vpn ike security-associations detail
IKE peer 10.1.15.2
  Role: Responder, State: Matured
  Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.1:500, Remote: 10.1.15.2:500
  Lifetime: Expires in 3535 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                  840
   Output bytes  :                  756
   Input  packets:                    5
   Output packets:                    4
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show services ipsec-vpn ipsec security-associations detail** command. Notice that the SA contains the default settings inherent in the AS PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
  Rule: rule-ike, Term: term-ike, Tunnel index: 1
  Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
    Direction: inbound, SPI: 407204513, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 24546 seconds
    Hard lifetime: Expires in 24636 seconds
    Anti-replay service: Disabled
    Direction: outbound, SPI: 2957235894, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 24546 seconds
    Hard lifetime: Expires in 24636 seconds
    Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the **ping** command from Router 1 (four packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          336                    4
```

After you issue the **ping** command from both Router 1 (four packets) and Router 4 (six packets), the **es-traffic** firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                                                Bytes              Packets
ipsec-tunnel                                          840                   10
```

To verify the success of the IKE security association on the ES PIC, issue the **show ike security-associations detail** command. Notice that the IKE SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
IKE peer 10.1.15.1
  Role: Initiator, State: Matured
  Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.2:500, Remote: 10.1.15.1:500
  Lifetime: Expires in 3441 seconds
  Algorithms:
   Authentication        : sha1
   Encryption            : 3des-cbc
```

```
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                  756
   Output bytes  :                  840
   Input  packets:                    4
   Output packets:                    5
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the **show ipsec security-associations detail** command. Notice that the IPsec SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up
  Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
  Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
  Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
    Direction: inbound, SPI: 2957235894, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 28555 seconds
    Hard lifetime: Expires in 28690 seconds
    Anti-replay service: Disabled
    Direction: outbound, SPI: 407204513, AUX-SPI: 0
    Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 28555 seconds
    Hard lifetime: Expires in 28690 seconds
    Anti-replay service: Disabled
```

Router 4

On Router 4, issue a **ping** command to the **so-0/0/0** interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

Again, the **traceroute** command verifies that traffic to **10.1.12.2** travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference **10.1.15.1**—the physical interface on Router 2. Instead, the second hop is listed as unknown with the *** notation. This indicates that the IPsec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1  10.1.56.1 (10.1.56.1)  3.561 ms  0.613 ms  0.558 ms
 2  * * *
 3  10.1.12.2 (10.1.12.2)  1.073 ms  0.862 ms  0.818 ms
```

Option: Configuring Multiple Routed Tunnels in a Single Next-Hop Service Set

To save you time and simplify your configurations, an enhancement to the Junos OS enables you to configure several routed IPSec tunnels within a single next-hop service set. To configure, establish multiple services interfaces as inside interfaces by including the **service-domain inside** statement at the **[edit interfaces sp-*fpc/pic/port* unit *logical-unit-number*] hierarchy level. Then, include the ipsec-inside-interface statement at the [edit services ipsec-vpn rule *rule-name* term *term-name* from] hierarchy level.**

NOTE: The full IPsec and IKE proposals and policies are not shown in the following example for the sake of brevity. For more information on proposals and policies, see "Configuring IKE Dynamic SAs" on page 123.

```
[edit]
interfaces {
   sp-3/3/0 {
      unit 3 {
         family inet;
         service-domain inside;
      }
      unit 4 {
         family inet;
         service-domain outside;
      }
      unit 5 {
         family inet;
         service-domain inside;
      }
   }
}
services {
   service-set link_type_ss_1 {
      next-hop-service {
         inside-service-interface sp-3/3/0.3;
         outside-service-interface sp-3/3/0.4;
      }
      ipsec-vpn-options {
         local-gateway 10.8.7.2;
      }
      ipsec-vpn-rules link_rule_1;
   }
   ipsec-vpn {
      rule link_rule_1 {
         term 1 {
            from {
               ipsec-inside-interface sp-3/3/0.3;
            }
            then {
               remote-gateway 10.10.7.3;
               backup-remote-gateway 10.8.7.1;
               dynamic {
```

```
            ike-policy main_mode_ike_policy;
            ipsec-policy dynamic_ipsec_policy;
          }
        }
      }
      term 2 {
        from {
          ipsec-inside-interface sp-3/3/0.5;
        }
        then {
          remote-gateway 10.12.7.5;
          dynamic {
            ike-policy main_mode_ike_policy;
            ipsec-policy dynamic_ipsec_policy;
          }
        }
      }
      match-direction input;
    }
  }
}
```

To confirm that your configuration is working, issue the **show services ipsec-vpn ipsec security-associations** command. Notice that each IPsec inside interface that you assigned to each IPsec tunnel is included in the output of this command.

```
user@router> show services ipsec-vpn ipsec security-associations
Service set: link_type_ss_1

  Rule: link_rule_1, Term: 1, Tunnel index: 1
  Local gateway: 10.8.7.2, Remote gateway: 10.8.7.1
  IPSec inside interface: sp-3/3/0.3
    Direction SPI         AUX-SPI     Mode       Type     Protocol
    inbound   3216392497  0           tunnel     dynamic  ESP
    outbound  398917249   0           tunnel     dynamic  ESP

  Rule: link_rule_1, Term: 2, Tunnel index: 2
  Local gateway: 10.8.7.2, Remote gateway: 10.12.7.5
  IPSec inside interface: sp-3/3/0.5
    Direction SPI         AUX-SPI     Mode       Type     Protocol
    inbound   762146783   0           tunnel     dynamic  ESP
    outbound  319191515   0           tunnel     dynamic  ESP
```

CHAPTER 11

Configuring IPsec on an ES PIC

IPsec Configuration for an ES PIC Overview

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

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

Related Documentation

- Configuring Minimum Manual Security Associations for IPsec on an ES PIC on page 180
- Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC on page 180
- Configuring Security Associations for IPsec on an ES PIC on page 181
- Configuring an IKE Proposal for Dynamic SAs on page 193

- Example: Configuring an IKE Proposal on page 195

Configuring Minimum Manual Security Associations for IPsec on an ES PIC

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

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

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 179

Configuring Minimum IKE Requirements for IPsec on an ES PIC

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

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

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 179

Configuring Minimum Digital Certificate Requirements for IKE on an ES PIC

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

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

Related Documentation

- IPsec Configuration for an ES PIC Overview on page 179

Configuring Security Associations for IPsec on an ES PIC

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

- Manual—Requires no negotiation; all values, including the keys, are static and specified in the configuration. As a result, each peer must have the same configured options for communication to take place. For information about how to configure a manual SA, see "Configuring Manual IPsec Security Associations for an ES PIC" on page 183.
- Dynamic—Specify proposals to be negotiated with the tunnel peer. The keys are generated as part of the negotiation and therefore do not need to be specified in the configuration. The dynamic SA includes one or more **proposal** statements, which allow you to prioritize a list of protocols and algorithms to be negotiated with the peer. For information about how to configure a dynamic SA, see "Associating the Configured Security Association with a Logical Interface" on page 21.

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

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

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

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

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

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

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

1. Configuring the Description for an SA on page 182
2. Configuring IPsec Transport Mode on page 182
3. Configuring IPsec Tunnel Mode on page 183
4. Configuring Manual IPsec Security Associations for an ES PIC on page 183
5. Configuring Dynamic IPsec Security Associations on page 187
6. Enabling Dynamic IPsec Security Associations on page 188

Configuring the Description for an SA

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

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

Configuring IPsec Transport Mode

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

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

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

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

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

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

Configuring IPsec Tunnel Mode

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

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

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

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

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

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

- Configuring Security Associations for IPsec on an ES PIC on page 181
- Configuring an IKE Proposal for Dynamic SAs on page 193
- Associating the Configured Security Association with a Logical Interface on page 21
- IPsec Tunnel Traffic Configuration Overview on page 207

Configuring Manual IPsec Security Associations for an ES PIC

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

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

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

```
[edit security ipsec security-association sa-name]
manual {
   direction (inbound | outbound | bi-directional) {
      authentication {
```

```
        algorithm (hmac-md5-96 | hmac-sha1-96);
        key (ascii-text key | hexadecimal key);
      }
      auxiliary-spiauxiliary-spi-value;
      encryption {
        algorithm (des-cbc | 3des-cbc);
        key (ascii-text key | hexadecimal key);
      }
      protocol (ah | esp | bundle);
      spi spi-value;
    }
  }
```

Tasks to configure a manual SA are:

1. Configuring the Processing Direction on page 184
2. Configuring the Protocol for a Manual SA on page 185
3. Configuring the Security Parameter Index on page 185
4. Configuring the Auxiliary Security Parameter Index on page 186
5. Configuring the Authentication Algorithm and Key on page 186
6. Configuring the Encryption Algorithm and Key on page 187

Configuring the Processing Direction

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

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

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

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

```
[edit security ipsec security-association sa-name]
manual {
  direction inbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 2345678901234567890234;
    }
    protocol esp;
    spi 16384;
  }
  direction outbound {
    encryption {
      algorithm 3des-cbc;
      key ascii-text 1234567890123456789abcd;
    }
```

```
    protocol esp;
    spi 24576;
  }
}
```

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

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

Configuring the Protocol for a Manual SA

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

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

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

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

Configuring the Security Parameter Index

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

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

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

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

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

Configuring the Auxiliary Security Parameter Index

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

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

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

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

Configuring the Authentication Algorithm and Key

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

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

The algorithm can be one of the following:

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

The key can be one of the following:

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

Configuring the Encryption Algorithm and Key

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

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

The algorithm can be one of the following:

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

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

The key can be one of the following:

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

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

Configuring Dynamic IPsec Security Associations

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

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

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

```
dynamic {
   ipsec-policy policy-name;
   replay-window-size (32 | 64);
}
```

Enabling Dynamic IPsec Security Associations

To enable a dynamic SA, follow these steps:

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

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

The replay window is not used with manual SAs.

Configuring Manual IPsec Security Associations for an ES PIC

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

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

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

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

```
}
```

Tasks to configure a manual SA are:

1. Configuring the Processing Direction on page 189
2. Configuring the Protocol for a Manual SA on page 190
3. Configuring the Security Parameter Index on page 190
4. Configuring the Auxiliary Security Parameter Index on page 190
5. Configuring the Authentication Algorithm and Key on page 191
6. Configuring the Encryption Algorithm and Key on page 191

Configuring the Processing Direction

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

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

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

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

```
[edit security ipsec security-association sa-name]
manual {
    direction inbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 2345678901234567890234;
        }
        protocol esp;
        spi 16384;
    }
    direction outbound {
        encryption {
            algorithm 3des-cbc;
            key ascii-text 1234567890123456789abcd;
        }
        protocol esp;
        spi 24576;
    }
}
```

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

```
[edit security ipsec security-association sa-name manual]
direction bidirectional {
    authentication {
```

```
        algorithm hmac-md5-96;
        key ascii-text 123456789012abcd;
    }
    protocol ah;
    spi 20001;
}
```

Configuring the Protocol for a Manual SA

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

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

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

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

Configuring the Security Parameter Index

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

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

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

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

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

Configuring the Auxiliary Security Parameter Index

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

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

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

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

Configuring the Authentication Algorithm and Key

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

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

The algorithm can be one of the following:

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

The key can be one of the following:

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

Configuring the Encryption Algorithm and Key

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

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

The algorithm can be one of the following:

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

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

The key can be one of the following:

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

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

Configuring Dynamic IPsec Security Associations

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

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

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

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 183

Configuring an IKE Proposal for Dynamic SAs

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

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

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

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

For information about associating an IKE proposal with an IKE policy, see "Configuring an IKE Policy for Preshared Keys" on page 195.

Tasks for configuring the IKE proposal are:

1. Configuring the Authentication Algorithm for an IKE Proposal on page 193
2. Configuring the Authentication Method for an IKE Proposal on page 193
3. Configuring the Description for an IKE Proposal on page 194
4. Configuring the Diffie-Hellman Group for an IKE Proposal on page 194
5. Configuring the Encryption Algorithm for an IKE Proposal on page 194
6. Configuring the Lifetime for an IKE SA on page 195

Configuring the Authentication Algorithm for an IKE Proposal

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

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

The authentication algorithm can be one of the following:

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

Configuring the Authentication Method for an IKE Proposal

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

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

The authentication method can be one of the following:

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

Configuring the Description for an IKE Proposal

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

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

Configuring the Diffie-Hellman Group for an IKE Proposal

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

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

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

The group can be one of the following:

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

group2 provides more security but requires more processing time.

Configuring the Encryption Algorithm for an IKE Proposal

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

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

The encryption algorithm can be one of the following:

- **3des-cbc**—Encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.
- **des-cbc**—Encryption algorithm that has a key size of 8 bytes; its key size is 56 bits long.

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

Configuring the Lifetime for an IKE SA

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

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

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

Example: Configuring an IKE Proposal

The following example shows how to configure an IKE proposal:

```
[edit security ike]
proposal ike-proposal {
   authentication-method pre-shared-keys;
   dh-group group1;
   authentication-algorithm sha1;
   encryption-algorithm 3des-cbc;
}
```

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 193

Configuring an IKE Policy for Preshared Keys

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

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

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

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

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

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

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

Tasks for configuring an IKE policy are:

1. Configuring the Description for an IKE Policy on page 196
2. Configuring the Mode for an IKE Policy on page 196
3. Configuring the Preshared Key for an IKE Policy on page 197
4. Associating Proposals with an IKE Policy on page 197

Configuring the Description for an IKE Policy

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

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

Configuring the Mode for an IKE Policy

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

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

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

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

For Junos OS in FIPS mode, the aggressive option for IKEv1 is not supported with the mode statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level.

Configuring the Preshared Key for an IKE Policy

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

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

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

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

Associating Proposals with an IKE Policy

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

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

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

Related Documentation

- Example: Configuring an IKE Policy on page 197

Example: Configuring an IKE Policy

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

```
[edit security]
ike {
  proposal proposal-1 {
    authentication-method pre-shared-keys;
    dh-group group1;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 1000;
  }
  proposal proposal-2 {
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
    lifetime-seconds 10000;
  }
  proposal proposal-3 {
    authentication-method rsa-signatures;
    dh-group group2;
    authentication-algorithm md5;
    encryption-algorithm des-cbc;
```

```
    lifetime-seconds 10000;
  }
  policy 10.1.1.2 {
    mode main;
    proposals [ proposal-1 proposal-2 ];
    pre-shared-key ascii-text example-pre-shared-key;
  }
  policy 10.1.1.1 {
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode aggressive;
    proposals [ proposal-2 proposal-3 ]
    pre-shared-key hexadecimal 0102030abbcd;
  }
}
```

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

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

Related Documentation

- Configuring an IKE Policy for Preshared Keys on page 195

Configuring an IPsec Proposal for an ES PIC

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

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

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

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

- Configuring the Authentication Algorithm for an IPsec Proposal on page 199
- Configuring the Description for an IPsec Proposal on page 199
- Configuring the Encryption Algorithm for an IPsec Proposal on page 199
- Configuring the Lifetime for an IPsec SA on page 199
- Configuring the Protocol for a Dynamic IPsec SA on page 200

Configuring the Authentication Algorithm for an IPsec Proposal

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

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

The authentication algorithm can be one of the following:

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

Configuring the Description for an IPsec Proposal

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

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

Configuring the Encryption Algorithm for an IPsec Proposal

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

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

The encryption algorithm can be one of the following:

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

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

Configuring the Lifetime for an IPsec SA

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

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

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

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

Configuring the Protocol for a Dynamic IPsec SA

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

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

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

Configuring the IPsec Policy for an ES PIC

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

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

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

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

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

```
[edit security ipsec]
```

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

Configuring Perfect Forward Secrecy

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

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

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

The key can be one of the following:

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

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

Related Documentation

- Example: Configuring an IPsec Policy on page 201
- IPsec Configuration for an ES PIC Overview on page 179

Example: Configuring an IPsec Policy

The following example shows how to configure an IPsec policy:

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

```
security-association dynamic-sa1 {
  dynamic {
    replay-window-size 64;
    ipsec-policy dynamic-policy-1;
  }
}
```

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

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

Related Documentation

- Configuring the IPsec Policy for an ES PIC on page 200
- IPsec Configuration for an ES PIC Overview on page 179

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

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

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

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

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

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

To configure internal IPsec, include the **security-association** statement at the **[edit security]** hierarchy level. You can configure parameters, such as the direction in which the manual

IPsec SAs must be applied, the SPI value that uniquely identifies the SA to use at the receiving Routing Engine, and the IPsec key that defines the authentication and encryption keys for the manual IPsec SA.

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

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

1. Configuring the SA Direction on page 203
2. Configuring the IPsec SPI on page 204
3. Configuring the IPsec Key on page 204

Configuring the SA Direction

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

```
direction (bidirectional | inbound | outbound);
```

The value can be one of the following:

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

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

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

```
[edit security]
ipsec {
  internal {
    security-association {
      manual {
        direction inbound {
          protocol esp;
          spi 512;
          encryption {
            algorithm 3des-cbc;
            key hexadecimal 309fc4be20f04e53e011b00744642d3fe66c2c7c;
          }
        }
        direction outbound {
          protocol esp;
          spi 513;
          encryption {
            algorithm 3des-cbc;
            key hexadecimal b0344c61d8db38535ca8afceaf0bf12b881dc200c9833da7;
          }
        }
      }
    }
  }
}
```

Configuring the IPsec SPI

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

```
spi value;
```

The value must be from 256 through 16,639.

Configuring the IPsec Key

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

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

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

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

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

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

Related Documentation

- Example: Configuring Internal IPsec on page 205

Example: Configuring Internal IPsec

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

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

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 202

CHAPTER 12

Configuring Traffic Filters to Direct Traffic Through the Desired IPsec Tunnel

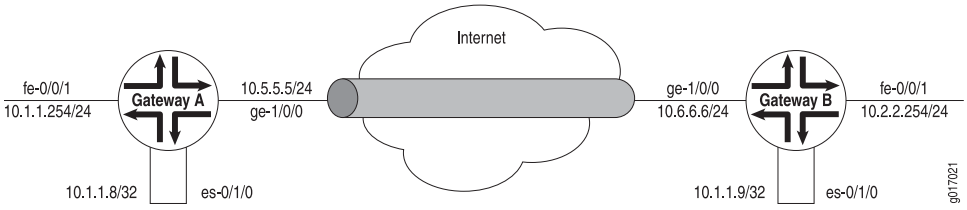
IPsec Tunnel Traffic Configuration Overview

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

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

In Figure 11 on page 208, Gateway A protects the network **10.1.1.0/24**, and Gateway B protects the network **10.2.2.0/24**. The gateways are connected by an IPsec tunnel.

Figure 11: Example: IPsec Tunnel Connecting Security Gateways



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

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

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

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

```
            key ascii-text 12345678900987654321 1234;
          }
        }
      }
    }
[edit interfaces es-0/1/0]
unit 0 {
  tunnel {
    source 10.6.6.6;
    destination 10.5.5.5;
  }
  family inet {
    ipsec-sa manual-sa1;
    address 10.1.1.9/32; {
      destination 10.1.1.8;
    }
  }
}
```

Related Documentation

- Example: Configuring an Outbound Traffic Filter on page 212
- Example: Applying an Outbound Traffic Filter on page 213
- Example: Configuring an Inbound Traffic Filter for a Policy Check on page 214
- ES Tunnel Interface Configuration for a Layer 3 VPN on page 237

Using a Filter to Select Traffic to Be Secured

For the ES PIC, you need to configure a firewall filter to direct traffic into the IPsec tunnel. To apply a security association to traffic that matches a firewall filter, include the **ipsec-sa** ***sa-name*** statement at the **[edit firewall filter** ***filter-name*** **term** ***term-name*** **then]** hierarchy level.

```
[edit firewall filter filter-name]
term term-name {
  from {
    source-address {
      ip-address;
    }
    destination-address {
      ip-address;
    }
  }
  then {
    count counter-name;
    ipsec-sa sa-name;
  }
}
term other {
  then accept;
}
```

For the AS and MultiServices PICs, you do not need to configure a separate firewall filter. A filter is already built into the IPsec VPN **rule** statement at the **[edit services ipsec-vpn]**

hierarchy level. To apply a security association to traffic that matches the IPsec VPN rule, include the **dynamic** or **manual** statement at the **[edit services rule *rule-name* term *term-name* then]** hierarchy level. To specify whether the rule should match input or output traffic, include the **match-direction** statement at the **[edit services rule *rule-name*]** hierarchy level.

After defining the rules for your IPsec VPNs, you must apply the rules to a service set. To do this, include the **ipsec-vpn-rules *rule-name*** statement at the **[edit services service-set *service-set-name*]** hierarchy level. Include an IPv4 or IPv6 IPsec gateway with the **local-gateway *local-ip-address*** statement at the **[edit services service-set *service-set-name*]** hierarchy level.

Also, you must select either a single interface or a pair of interfaces that participate in IPsec. To select a single interface, include the interface-service ***interface-name*** statement at the **[edit services service-set *service-set-name*]** hierarchy level. To select a pair of interfaces and a next hop, include the **next-hop-service** statement at the **[edit services service-set *service-set-name*]** hierarchy level and specify an inside interface and an outside interface. Only next-hop service sets support IPsec within Layer 3 VPNs and use of routing protocols over the IPsec tunnel.

```
[edit services]
service-set service-set-name {
    interface-service {
        service-interface interface-name;
    }
    next-hop-service {
        inside-service-interface interface-name;
        outside-service-interface interface-name;
    }
    ipsec-vpn-options {
        local-gateway local-ip-address <routing-instance instance-name>;
        trusted-ca ca-profile-name;
    }
    ipsec-vpn-rules rule-name;
}
ipsec-vpn {
    rule rule-name {
        term term-name {
            from {
                source-address {
                    ip-address;
                }
                destination-address {
                    ip-address;
                }
            }
            then {
                remote-gateway remote-ip-address;
                (dynamic | manual);
            }
        }
        match-direction output;
    }
}
```

Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured

For the ES PIC, apply your firewall filter on the input interface receiving the traffic that you wish to send to the IPsec tunnel. To do this, include the **filter** statement at the **[edit interfaces *interface-name* unit *unit-number* family inet]** hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
filter {
   input filter-name;
}
```

For the AS and MultiServices PICs, apply your IPsec-based interface service set to the input interface receiving the traffic that you wish to send to the IPsec tunnel. To do this, include the **service-set *service-set-name*** statement at the **[edit interfaces *interface-name* unit *unit-number* family inet service (input | output)]** hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
service {
   input {
      service-set service-set-name;
   }
   output {
      service-set service-set-name;
   }
}
```

To configure a next-hop-based service set on the AS and MultiServices PICs, include the **service-domain** statement at the **[edit interfaces *interface-name* unit *unit-number*]** hierarchy level and specify one logical interface on the AS PIC as an inside interface and a second logical interface on the AS PIC as an outside interface.

```
[edit interfaces sp-fpc/pic/port]
unit 0 {
   family inet {
      address ip-address;
   }
}
unit 1 {
   family inet;
   service-domain inside;
}
unit 2 {
   family inet;
   service-domain outside;
}
```

Using Filter-Based Forwarding to Select Traffic to Be Secured

Instead of using a firewall filter, you can also forward traffic into an IPsec security association by using a filter-based forwarding instance. First, configure the filter-based forwarding instance. Then, configure a routing table group to advertise the routes from the filter-based forwarding instance. Next, create a firewall filter for the ES PIC and

reference the filter-based forwarding instance. Lastly, apply the filter and IPsec security association to the ES PIC.

```
[edit]
routing-instances {
    forwarding {
        instance-type forwarding;
        routing-options {
            static {
                route 10.10.10.0/24 next-hop 192.168.0.5;
            }
        }
    }
}
routing-options {
    rib-groups {
        group-name  {
            import-rib [ inet.0 forwarding.inet.0 ];
        }
    }
}
firewall {
    family inet {
        filter filter-name {
            term term-name {
                then routing-instance instance-name;
            }
        }
    }
}
[edit]
interfaces {
    es-0/0/0 {
        unit 0 {
            tunnel {
                source source-ip-address;
                destination destination-ip-address;
            }
            family inet {
                ipsec-sa sa-name;
                filter {
                    input filter-name;
                }
                address ip-address;
            }
        }
    }
}
```

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 11 on page 208). Here, an outbound firewall filter is created on security Gateway A; it identifies

the traffic to be encrypted and adds it to the input side of the interface that carries the internal VPN traffic:

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

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

Related Documentation

- Example: Applying an Outbound Traffic Filter on page 213
- IPsec Tunnel Traffic Configuration Overview on page 207

Example: Applying an Outbound Traffic Filter

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

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

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

interface, which is configured with the **manual-sa1** SA. The ES PIC receives the packet, applies the **manual-sa1** SA, and sends the packet through the tunnel.

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

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 207

Example: Configuring an Inbound Traffic Filter for a Policy Check

Requirements

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

Overview

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

Configuration

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

To configure this example, perform the following tasks:

CLI Quick Configuration

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

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

Configuring the firewall filter

Step-by-Step Procedure

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

1. Create the firewall filter:

   ```
   [edit]
   user@host# edit firewall family inet filter ipsec-decrypt-policy-filter
   ```

2. Configure matching for source and destination addresses:

   ```
   [edit firewall family inet filter ipsec-decrypt-policy-filter]
   user@host# set term term1 from source-address 10.2.2.0/24
   user@host# set term term1 from destination-address 10.1.1.0/24
   ```

3. Configure the filter to accept the matched traffic:

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

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

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

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

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

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

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

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

Related Documentation
- IPsec Tunnel Traffic Configuration Overview on page 207
- Example: Applying an Inbound Traffic Filter to an ES PIC for a Policy Check on page 216

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

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

```
[edit interfaces]
es-1/2/0 {
  unit 0 {
    tunnel {
      source 10.5.5.5; # tunnel source address
      destination 10.6.6.6; # tunnel destination address
    }
    family inet {
      filter {
        input ipsec-decrypt-policy-filter;
      }
    ipsec-sa manual-sa1; # SA name applied to packet
      address 10.1.1.8/32 { # local interface address inside local VPN
        destination 10.2.2.254; # destination address inside remote VPN
      }
  }
}
```

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

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

Related Documentation
- IPsec Tunnel Traffic Configuration Overview on page 207

CHAPTER 13

Configuring IPsec Dynamic Endpoints

Option: Configuring IPSec Dynamic Endpoints

IPSec tunnels can also be established using *dynamic peer* security gateways, in which the remote end of the tunnels do not have a statically assigned IPv4 or IPv6 address. Since the remote address is not known and is assigned from an address pool each time the remote host reboots, establishment of the tunnel relies on using IKE main mode with preshared global keys. Both policy-based and link-type tunnels are supported as follows:

- Policy-based tunnels used shared mode.
- Link-type or routed tunnels use dedicated mode. Each tunnel allocates a service interface from a pool of interfaces configured for the dynamic peers. Routing protocols can be configured to run on these service interfaces to learn routes over the IPSec tunnel that is used as a link.

This section includes the following topics:

IPsec Dynamic Endpoint Tunnel Architecture

When you configure dynamic endpoint tunnels, the following components are used:

Authentication Process

The remote dynamic peer initiates IKE and negotiations with the local (Juniper Networks) router. The local router uses a default set of authentication and encryption values to match the and IKE proposals sent by the remote peer to establish the SA. If any of the values match, the tunnel establishment process continues. The default values are shown in Table 9 on page 218.

Table 9: Default IKE and Proposals for Dynamic SA Negotiations

Statement Name	Values
Implicit IKE Proposal	
authentication-method	preshared keys
dh-group	group1, group2
authentication-algorithm	sha1, md5
encryption-algorithm	3des-cbc, des-cbc
lifetime-seconds	3600 seconds
Implicit Proposal	
protocol	esp, ah, bundle
authentication-algorithm	hmac-sha1-96, hmac-md5-96
encryption-algorithm	3des-cbc, des-cbc
lifetime-seconds	28,800 seconds (8 hours)

Phase 2 of the authentication process matches the *proxy identities* of the protected hosts and networks sent by the peer against a list of configured proxy identities. The accepted proxy identity is used to create the dynamic rules for encrypting the traffic. You can configure proxy identities by including the **allowed-proxy-pair** statement in an IKE access profile at the **[edit access profile *profile-name* client * ike]** hierarchy level. If no configured entry matches, the negotiation is rejected.

However, if you do not configure the **allowed-proxy-pair** statement, the default value **ANY(0.0.0.0/0)-ANY** is applied, and the local router accepts any proxy identities sent by the peer.

Once the phase 2 negotiation has been successfully completed, the router builds dynamic rules and inserts the reverse route into the routing table using the accepted proxy identity.

Dynamic Implicit Rules

After successful negotiation with the dynamic peer, the key management process (kmd) creates a dynamic rule for the accepted phase 2 proxy and applies it on the local AS or MultiServices PIC. The source and destination addresses are specified by the accepted proxy. This rule is used to encrypt traffic directed to one of the end hosts in the phase 2 proxy identity.

NOTE: You do not configure this rule; it is created by the key management process (kmd).

The **ipsec-inside-interface** value is the interface name assigned to the dynamic tunnel. The **source-address** and **destination-address** values are accepted from the proxy ID. The **match-direction** value is **input** for next-hop-style service sets.

Rule lookup for static tunnels is unaffected by the presence of a dynamic rule; it is performed in the order configured. When a packet is received for a service-set, static rules are always matched first. Dynamic rules are matched only after the rule match for static rules has failed.

Reverse Route Insertion

Static routes are automatically inserted into the route table for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities.

Each route is created based on the remote proxy network and prefix length sent by the peer and is inserted in the relevant route table after successful phase 1 and phase 2 negotiations.

The route preference for each of these static reverse routes is 1. This value is necessary to avoid conflict with similar routes that might be added by the routing protocol process (rpd).

No routes are added if the accepted remote proxy address is the default (**0.0.0.0/0**). In this case, you can run routing protocols over the tunnel to learn routes and add static routes for the traffic you want to be protected over this tunnel.

For next-hop style service sets, the reverse routes include next hops pointing to the locations specified by the **inside-service-interface** statements.

The selection of the routing table in which these routes are inserted depends on where you configure the **inside-service-interface** statement. If these interfaces are present in a

VRF routing instance, then routes are added to the corresponding VRF routing table; otherwise, the routes are added to **inet.0**.

NOTE: Reverse route insertion takes place only for tunnels to dynamic peers. These routes are added only for next-hop style service sets.

Configuring an IKE Access Profile for IPsec Dynamic Endpoint Tunnels

You can configure only one tunnel profile per service set for all dynamic peers. The configured preshared key in the profile is used for IKE authentication of all dynamic peers terminating in that service set.

The IKE tunnel profile specifies all the information needed to complete the IKE negotiation. For more information on access profiles, see the *Junos System Basics Configuration Guide*.

```
[edit access]
profile profile-name {
   client * {
      ike {
         allowed-proxy-pair {
            remote remote-proxy-address local local-proxy-address;
         }
         pre-shared-key ([ ascii-text key-string ] | [hexadecimal key-string ]);
         interface-id string-value;
         ipsec-policy ipsec-policy;
      }
   }
}
```

NOTE: For dynamic peers, the Junos OS supports only IKE main mode with the preshared key method of authentication. In this mode, an IPv4 or IPv6 address is used to identify a tunnel peer to get the preshared key information. The client value * (wildcard) means that the configuration within this profile is valid for all dynamic peers terminating within the service set accessing this profile.

The following statements are the parts of the IKE profile:

- **allowed-proxy-pair**—During phase 2 IKE negotiation, the remote peer supplies its network address (**remote**) and its peer's network address (**local**). Since multiple dynamic tunnels are authenticated through the same mechanism, this statement must include the list of possible combinations. If the dynamic peer does not present a valid combination, the phase 2 IKE negotiation fails.

  By default, remote 0.0.0.0/0 local 0.0.0.0/0 is used if no values are configured.

- **pre-shared-key**—Mandatory key used to authenticate the dynamic peer during IKE phase 1 negotiation. This key must be configured on both ends of the tunnel and

distributed through an out-of-band secure mechanism. You can configure the key value either in **hexadecimal** or **ascii-text** format.

- **interface-id**—Interface identifier, a mandatory attribute used to derive the logical service interface information for the session.
- **ipsec-policy**—Name of the IPsec policy that defines the IPsec policy information for the session. You define the IPsec policy at the **[edit services ipsec-vpn ipsec policy *policy-name*]** hierarchy level. If no policy is set, any policy proposed by the dynamic peer is accepted.

Configuring the Service Set for IPsec Dynamic Endpoint Tunnels

To complete a dynamic endpoint tunnel configuration, you need to reference the IKE access profile configured at the [**edit access**] hierarchy level in the service set. To do this, include the **ike-access-profile** statement at the [**edit services service-set *name* ipsec-vpn-options**] hierarchy level:

```
[edit services]
service-set name {
    next-hop-service {
        inside-service-interface interface-name;
        outside-service-interface interface-name;
    }
    ipsec-vpn-options {
        local-gateway address;
        ike-access-profile profile-name;
    }
}
```

You can reference only one access profile in each service set. This profile is used to negotiate IKE and IPsec security associations with dynamic peers only.

NOTE: If you configure an IKE access profile in a service set, no other service set can share the same **local-gateway** address.

Configuring the Interface Identifier for IPsec Dynamic Endpoint Tunnels

You can configure an interface identifier for a group of dynamic peers, which specifies which adaptive services logical interface(s) take part in the dynamic IPsec negotiation. By assigning the same interface identifier to multiple logical interfaces, you can create a pool of interfaces for this purpose. To configure, include the **ipsec-interface-id** statement at the [**edit interfaces *interface-name***] hierarchy level:

```
[edit interfaces sp-fpc/pic/port]
unit logical-unit-number {
    dial-options {
        ipsec-interface-id identifier;
        (shared | dedicated);
    }
}
```

Specifying the interface identifier in the **dial-options** statement makes this logical interface part of the pool identified by the IPsec interface identifier.

NOTE: Only one interface identifier can be specified at a time. You can include the **ipsec-interface-id** statement or the **l2tp-interface-id** statement, but not both simultaneously.

The **shared** statement enables one logical interface to be shared across multiple tunnels. The **dedicated** statement specifies that the logical interface is associated with a single tunnel, which is necessary when you are configuring an IPsec link-type tunnel. You must include the **dedicated** statement when you specify an **ipsec-interface-id** value.

Example: Dynamic Endpoint Tunneling Configuration

Figure 12: IPSec Dynamic Endpoint Tunneling Topology Diagram

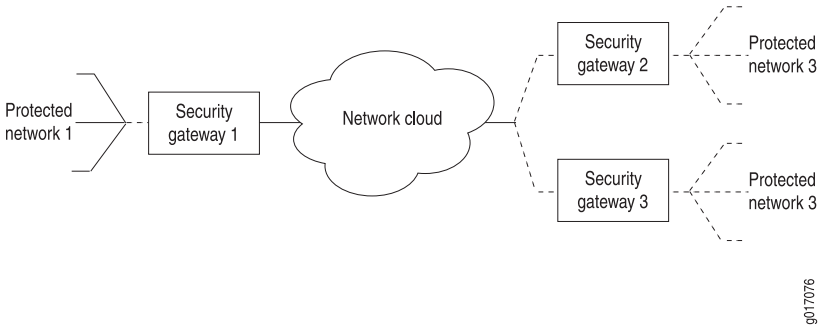


Figure 12 on page 222 shows a local network N-1 located behind security gateway SG-1. SG-1 is a Juniper Networks router terminating dynamic peer endpoints. The tunnel termination address on SG-1 is **10.7.7.2** and the local network address is **172.16.1.0/24**.

A remote peer router obtains addresses from an ISP pool and runs RFC-compliant IKE. Remote network N-2 has address **172.16.2.0/24** and is located behind security gateway SG-2 with tunnel termination address **10.7.7.1**.

On Router SG-1, configure an IKE access profile to accept proposals from SG-2. Apply the interface identifier from the access profile to the inside services interface and apply the IKE access profile itself to the IPSec next-hop style service set.

Router SG-1

```
[edit]
access {
  profile ike_access {
    client * { # Accepts proposals from specified peers that use the preshared key.
      ike {
        allowed-proxy-pair local 10.255.14.63/32 remote 10.255.14.64/32;
        pre-shared-key ascii-text "$ABC123"; # SECRET-DATA
        interface-id test_id; # Apply this ID to the inside services interfaces.
      }
    }
  }
}
interfaces {
```

```
    fe-0/0/0 {
      description "Connection to the local network";
      unit 0 {
        family inet {
          address 172.16.1.1/24;
        }
      }
    }
    so-1/0/0 {
      description "Connection to SG-2";
      no-keepalives;
      encapsulation cisco-hdlc;
      unit 0 {
        family inet {
          address 10.7.7.2/30;
        }
      }
    }
    sp-3/3/0 {
      unit 0 {
        family inet;
      }
      unit 3 {
        dial-options {
          ipsec-interface-id test_id; # Accepts dynamic endpoint tunnels.
          shared;
        }
        service-domain inside;
      }
      unit 4 {
        family inet;
        service-domain outside;
      }
    }
  }
  services {
    service-set dynamic_nh_ss { # Create a next-hop service set
      next-hop-service { # for the dynamic endpoint tunnels.
        inside-service-interface sp-3/3/0.3;
        outside-service-interface sp-3/3/0.4;
      }
      ipsec-vpn-options {
        local-gateway 10.7.7.2;
        ike-access-profile ike_access; # Apply the IKE access profile here.
      }
    }
  }
```

Verifying Your Work

To verify proper operation of a dynamic endpoint tunnel configured on the AS PIC, use the following command:

```
show services ipsec-vpn ipsec security-associations (detail)
```

The following section shows output from this command used with the configuration example. The dynamically created rule **_junos_** appears in the output, as well as the establishment of the inbound and outbound dynamically created tunnels.

```
user@router> show services ipsec-vpn ipsec security-associations detail
Service set: dynamic_nh_ss

  Rule:  _junos_ , Term: tunnel4, Tunnel index: 4
  Local gateway: 10.7.7.2, Remote gateway: 10.7.7.1
  Local identity: ipv4(any:0,[0..3]=10.255.14.63)
  Remote identity: ipv4(any:0,[0..3]=10.255.14.64)

    Direction: inbound , SPI: 428111023, AUX-SPI: 0
     Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 27660 seconds
    Hard lifetime: Expires in 27750 seconds
    Anti-replay service: Enabled, Replay window size: 64

    Direction: outbound , SPI: 4035429231, AUX-SPI: 0
     Mode: tunnel, Type: dynamic, State: Installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
    Soft lifetime: Expires in 27660 seconds
    Hard lifetime: Expires in 27750 seconds
    Anti-replay service: Enabled, Replay window size: 64
```

CHAPTER 14

Configuring Digital Certificates for IPsec

Using Digital Certificates for IPsec

A popular way for network administrators to scale an IPsec network is to use digital certificates instead of preshared keys. To enable digital certificates in your network, you need to use a combination of operational mode commands and configuration statements. The following tasks enable you to implement digital certificates on AS and MultiServices PICs installed in M Series and T Series routers:

Related Documentation

- Digital Certificates on page 91

Configuring a CA Profile

The CA profile contains the name and URL of the CA or RA, as well as some retry timer settings. CA certificates issued by Entrust, VeriSign, and Microsoft are all compatible with M Series, and T Series routers. To configure the domain name of the CA or RA, include the **ca-identity** statement at the **[edit security pki ca-profile *ca-profile-name*]** hierarchy level. To configure the URL of the CA, include the **url** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level. To configure the number of enrollment attempts the router should perform, include the **retry** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level. To configure the amount of time the router should wait between enrollment attempts, include the **retry-interval** statement at the **[edit security pki ca-profile *ca-profile-name* enrollment]** hierarchy level.

```
[edit security pki]
ca-profile ca-profile-name {
   ca-identity ca-identity;
   enrollment {
      url url-name;
      retry number-of-enrollment-attempts; # The range is 0 though 100 attempts.
      retry-interval seconds; # The range is 0 though 3600 seconds.
   }
}
```

NOTE: When you delete the entire public key infrastructure (PKI) configuration, all the CA certificates in the device are not deleted as expected. These CA certificates are accessible after you create the CA profiles again.

Configuring a Certificate Revocation List

A certificate revocation list (CRL) contains a list of digital certificates that have been canceled before their expiration date. When a participating peer uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL. By default, CRL verification is enabled on any CA profile running on Junos OS Release 8.1 or later. To disable CRL verification, include the **disable** statement at the [**edit security pki ca-profile *ca-profile-name* revocation-check**] hierarchy level.

To specify the URL for the Lightweight Directory Access Protocol (LDAP) server where your CA stores its current CRL, include the **url** statement at the [**edit security pki ca-profile *ca-profile-name* revocation-check crl**] hierarchy level. If the LDAP server requires a password to access the CRL, include the **password** statement at the [**edit security pki ca-profile *ca-profile-name* revocation-check crl url**] hierarchy level.

NOTE: You do not need to specify a URL for the LDAP server if the certificate includes a certificate distribution point (CDP). The CDP is a field within the certificate that contains information about how to retrieve the CRL for the certificate. The router uses this information to download the CRL automatically. Any LDAP URL you configure takes precedence over the CDP included in the certificate.

If you manually downloaded the CRL, you must manually install it on the router. To manually install the CRL, issue the **request security pki crl load ca-profile** *ca-profile-name* **filename** *path/filename* command.

To configure the time interval between CRL updates, include the **refresh-interval** statement at the [**edit security ca-profile** *ca-profile-name* **revocation-check crl**] hierarchy level.

To override the default behavior and permit IPsec peer authentication to continue when the CRL fails to download, include the **disable on-download-failure** statement at the [**edit security ca-profile** *ca-profile-name* **revocation-check crl**] hierarchy level.

```
[edit security pki ca-profile ca-profile-name]
revocation-check {
    disable;
    crl {
        disable on-download-failure;
        refresh-interval number-of-hours { # The range is 0 through 8784 hours.
            url {
                url-name;
                password;
            }
        }
    }
}
```

Requesting a CA Digital Certificate

You can request a CA digital certificate either online or manually. To request a digital certificate from a CA or RA online by using SCEP, issue the **request security pki ca-certificate enroll ca-profile** *ca-profile-name* command.

If you obtained the CA digital certificate manually through e-mail or other out-of-band mechanism, you must load it manually. To manually install a certificate in your router, issue the **request security pki local-certificate load** command.

Generating a Private/Public Key Pair

A key pair is a critical element of a digital certificate implementation. The public key is included in the local digital certificate and the private key is used to decrypt data received from peers. To generate a private/public key pair, issue the **request security pki generate-key-pair certificate-id** *certificate-id-name* command.

Generating and Enrolling a Local Digital Certificate

You can generate and enroll a local digital certificate either online or manually. To generate and enroll a local certificate online by using SCEP, issue the **request security pki local-certificate enroll** command. To generate a local certificate request manually in the PKCS-10 format, issue the **request security pki generate-certificate-request** command.

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

Applying the Local Digital Certificate to an IPsec Configuration

To activate a local digital certificate, you configure the IKE proposal to use digital certificates instead of preshared keys, reference the local certificate in the IKE policy, and identify the CA or RA in the service set. To enable the IKE proposal for digital certificates, include the **rsa-signatures** statement at the **[edit services ipsec-vpn ike proposal *proposal-name* authentication-method]** hierarchy level. To reference the local certificate in the IKE policy, include the **local-certificate** statement at the **[edit services ipsec-vpn ike policy *policy-name*]** hierarchy level. To identify the CA or RA in the service set, include the **trusted-ca** statement at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level.

```
[edit services]
service-set service-set-name {
   .....
   ipsec-vpn-options {
      trusted-ca ca-profile-name;
   }
}
ipsec-vpn {
   ike {
      proposal proposal-name  {
         .....
         authentication-method [pre-shared-keys | rsa-signatures];
      }
      policy policy-name {
         ....
         local-certificate certificate-id-name;
      }
   }
}
```

Configuring Automatic Reenrollment of Digital Certificates

You can configure automatic reenrollment for digital certificates. This feature is by default not enabled. To configure automatic reenrollment for digital certificates, include the **auto-re-enrollment** statement at the [**edit security pki**] hierarchy level:

```
[edit]
security {
```

```
pki {
  auto-re-enrollment {
    certificate-id certificate-name {
      ca-profile ca-profile-name;
      challenge-password password;
      re-enroll-trigger-time-percentage percentage; # Percentage of validity-period
        # (specified in certificate) when automatic
        # reenrollment should be initiated.
      re-generate-keypair;
      validity-period number-of-days;
    }
  }
}
```

Monitoring Digital Certificates

Purpose You can issue various forms of the **show security pki** command to view digital certificates and certificate requests and certificate revocation lists:

Action

- To display the CA digital certificate, issue the **show security pki ca-certificate ca-profile** ***ca-profile-name*** command.
- To display the local digital certificate and the public key used to enroll the certificate, issue the **show security pki local-certificate certificate-id** ***certificate-id-name*** command.
- To display the local certificate request in PKCS-10 format, issue the **show security pki certificate-request certificate-id** ***certificate-id-name*** command.
- You can also view which digital certificates are used in IKE negotiations to establish tunnels by issuing the **show services ipsec-vpn certificates** command.
- To display the certificate revocation list, issue the **show security pki crl ca-profile** ***ca-profile-name*** command.
- To determine if a certificate is enabled for automatic-reenrollment, issue the **show security pki** command.

Clearing Digital Certificates

Purpose Variations of the **clear security pki** command enable you to delete certificates or requests and certificate revocation lists:

Action

- To delete the CA digital certificate, issue the **clear security pki ca-certificate ca-profile** ***ca-profile-name*** command.
- To delete the local digital certificate and the associated private/public key pair, issue the **clear security pki local-certificate certificate-id** ***certificate-id-name*** command.
- To delete the local certificate request, issue the **clear security pki certificate-request certificate-id** ***certificate-id-name*** command.

- To clear the digital certificates that were used in IKE negotiations to establish tunnels, issue the **clear services ipsec-vpn certificates** command.
- To delete the certificate revocation list, issue the **clear security pki crl ca-profile *ca-profile-name*** command.

Related Documentation

- Example: AS PIC IKE Dynamic SA with Digital Certificates Configuration on page 136
- *Security Services Administration Guide for Routing Devices*
- *Understanding Junos VPN Site Secure*

CHAPTER 15

Securing Layer 3 Protocol Traffic with IPsec Transport Mode

Securing BGP Sessions with IPsec Transport Mode

For the ES PIC, you can use IPsec to secure BGP sessions between Routing Engines in M Series and T Series platforms. To configure, create a transport mode security association and apply the SA to the BGP configuration by including the **ipsec-sa** statement at the **[edit protocols bgp group *group-name*]** hierarchy level.

```
[edit]
protocols {
   bgp {
      group group-name  {
         local-address ip-address;
         export export-policy;
         peer-as as-number;
         ipsec-sa sa-name;
         neighbor peer-ip-address;
      }
   }
}
```

Related Documentation

- IPSec Modes on page 89

Securing OSPFv2 Networks with IPsec Transport Mode

By default, you can configure MD5 or simple text password-based authentication over OSPFv2 links. In addition to these basic authentications, the Junos OS supports OSPFv2 with a security authentication header (AH), Encapsulating Security Payload (ESP), or an IPsec protocol bundle that supports both AH and ESP. You can configure IPsec over OSPFv2 using transport mode security associations on physical, sham, or virtual links.

Because the Junos OS supports only bidirectional security associations over OSPFv2, OSPFv2 peers must be configured with the same IPsec security association. Configuring OSPFv2 peers with different security associations or with dynamic IKE will prevent adjacencies from being established. In addition, you must configure identical security associations for sham links with the same remote endpoint address, for virtual links with the same remote endpoint address, for all neighbors on OSPF nonbroadcast multiaccess (NBMA) or point-to-multipoint links, and for every subnet that is part of a broadcast link.

To create a manual bidirectional security association, include the **security-association** ***security-association-name*** statement at the [**edit security ipsec**] hierarchy level:

```
[edit]
security {
  ipsec {
    security-association security-association name {
      mode transport;
      manual {
        direction bidirectional {
          protocol (ah | esp | bundle);
          spi spi--value;
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
        }
      }
    }
  }
}
```

To configure IPsec on an OSPFv2 interface, create a transport mode security association and include the **ipsec-sa name** statement at the [**edit protocols ospf area** ***area-id***] hierarchy level:

```
[edit]
protocols {
  ospf {
    area area-id {
      interface interface-name {
        ipsec-sa sa-name;
      }
      virtual-link neighbor-id a.b.c.d transit-area x.x.x.x {
        ipsec-sa sa-name;
      }
      sham-link-remote {
        ipsec-sa sa-name;
      }
    }
  }
}
```

To verify your configuration, enter the **show ospf interface detail** command. This command gives detailed information about the **ospfv2** interface and displays the interface's security

association at the bottom of the output. In the example below, the security association configured on this router is **sa1**.

```
user@router> show ospf interface detail
Interface              State     Area            DR ID           BDR ID Nbrs
fe-0/0/1.0             BDR      0.0.0.0         192.168.37.12   10.255.245.215 1
Type LAN, address 192.168.37.11, Mask 255.255.255.248, MTU 4460, Cost 40
DR addr 192.168.37.12, BDR addr 192.168.37.11, Adj count 1, Priority 128
Hello 10, Dead 40, ReXmit 5, Not Stub
t1-0/2/1.0             PtToPt   0.0.0.0         0.0.0.0         0.0.0.0 0
Type P2P, Address 0.0.0.0, Mask 0.0.0.0, MTU 1500, Cost 2604
Adj count 0
Hello 10, Dead 40, ReXmit 5, Not Stub
Auth type: MD5, Active key ID 3, Start time 2002 Nov 19 10:00:00 PST
IPsec SA Name: sa1
```

Related Documentation

- IPSec Modes on page 89

Securing OSPFv3 Networks with IPsec Transport Mode

OSPF version 3 (OSPFv3), unlike OSPF version 2, does not have a built-in authentication method and relies on IPsec to provide this functionality. Using the ES PIC syntax, you can use IPsec to secure OSPFv3 between Routing Engines in M Series and T Series platforms. You can secure specific OSPFv3 interfaces and protect OSPFv3 virtual links. To configure, create a transport mode security association and apply the SA to the OSPFv3 configuration by including the **ipsec-sa** statement at the **[edit protocols ospf3 area** *area-number* **interface** *interface-name***]** or **[edit protocols ospf3 area** *area-number* **virtual-link neighbor-id** *neighbor-ip-address* **transit-area** *area-number***]** hierarchy level.

```
[edit]
protocols {
  ospf3 {
    area area-number {
      interface interface-name {
        ipsec-sa sa-name;
      }
      virtual-link neighbor-id neighbor-ip-address transit-area area-number {
        ipsec-sa sa-name;
      }
    }
  }
}
```

Related Documentation

- IPSec Modes on page 89

CHAPTER 16

Using IPsec with a Layer 3 VPN

Using IPsec with a Layer 3 VPN

Some key concepts to keep in mind when configuring IPsec within a VPN include the following:

- Add the outside services interface for a next-hop style service set into the routing instance by including the **interface sp-*fpc/pic/port*** statement at the **[edit routing-instances *instance-name*]** hierarchy level.
- For interface style service sets, add the interface on which you apply the service set and the services interface by including both interfaces at the **[edit routing-instances *instance-name*]** hierarchy level.
- To define a routing instance for the local gateway within the service set, include the **routing-instance *instance-name*** option at the **[edit services service-set *service-set-name* ipsec-vpn-options local-gateway *address*]** hierarchy level.

The following configuration for an AS PIC on a provider edge (PE) router demonstrates the use of next-hop service sets with an IKE dynamic SA in a VPN routing and forwarding (VRF) routing instance.

```
[edit]
interfaces {
   so-0/0/0 {
      description "Interface connected to the customer edge (CE) router";
      unit 0 {
         family inet {
            address 10.6.6.6/32;
         }
      }
   }
   so-2/2/0 {
      description "Source IPsec tunnel interface to the network core";
      unit 0 {
         family inet {
            address 10.10.1.1/30;
         }
```

```
    }
  }
  sp-3/1/0 {
    description "AS PIC interface";
    unit 0 {
      family inet {
        address 10.7.7.7/32;
      }
    }
    unit 1 {
      family inet;
      service-domain inside;
    }
    unit 2 {
      family inet;
      service-domain outside;
    }
  }
}
policy-options {
  policy-statement vpn-export-policy {
    then {
      community add community-name;
      accept;
    }
  }
  policy-statement vpn-import-policy {
    term term-name {
      from community community-name;
      then accept;
    }
  }
  community community-name members target:100:20;
}
routing-instances {
  vrf {
    instance-type vrf;
    interface sp-3/1/0.1; # Inside sp interface.
    interface so-0/0/0.0; # Interface that connects to the CE router.
    route-distinguisher route-distinguisher;
    vrf-import vpn-import-policy;
    vrf-export vpn-export-policy;
    routing-options {
      static {
        route ip-address/prefix next-hop so-0/0/0.0; # Routes for the CE router.
        route ip-address/prefix next-hop sp-3/1/0.1; # Routes for IPsec.
      }
    }
  }
}
services {
  service-set service-set-name {
    next-hop-service {
      inside-service-interface sp-3/1/0.1;
      outside-service-interface sp-3/1/0.2;
    }
```

```
    ipsec-vpn-options {
      local-gateway 10.10.1.1;
    }
    ipsec-vpn-rules rule-name;
  }
  ipsec-vpn {
    rule rule-name {
      term term-name {
        from {
          source-address {
            source-ip-address;
          }
        }
        then {
          remote-gateway 10.10.1.2;
          dynamic {
            ike-policy ike-policy-name;
          }
        }
      }
      match-direction direction;
    }
    ike {
      policy  ike-policy-name  {
        pre-shared-key ascii-text preshared-key;
      }
    }
  }
}
```

For more information on VRF routing instances, see the *Junos VPNs Configuration Guide*. For more information on next-hop service sets, see the *Junos Services Interfaces Configuration Guide*.

ES Tunnel Interface Configuration for a Layer 3 VPN

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

Related Documentation

- IPsec Tunnel Traffic Configuration Overview on page 207

PART 5

Monitoring and Troubleshooting Information

CHAPTER 17

Tracing Security Services Operations for Troubleshooting Purposes

Configuring Tracing Operations for Security Services

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

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

You can include these statements at the following hierarchy levels:

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

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

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

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

Related Documentation

- Configuring Tracing Operations for IPsec Events for Adaptive Services PICs on page 242
- Security Associations Overview on page 88

Configuring Tracing Operations for IPsec Events for Adaptive Services PICs

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

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

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

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

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

Related Documentation

- Configuring Tracing Operations for Security Services on page 241

CHAPTER 18

Monitoring IPsec Traffic

Monitoring IPsec by Using SNMP

In Junos OS Release 7.5 and later, the IPsec Monitoring MIB provides a way to monitor IPsec information on AS PICs installed in M Series and T Series routers by using the Simple Network Management Protocol (SNMP). The MIB provides an IKE tunnel table to monitor IKE security associations and view related statistics, an IPsec tunnel table to view IPsec tunnel statistics, and an IPsec security associations table to view all IPsec SAs. For more information, see the *Junos Network Management Configuration Guide*.

PART 6

Configuration Statements and Operational Commands

CHAPTER 19

Configuration Statements: DDoS

bandwidth (DDoS)

Syntax bandwidth *packets-per-second*;

Hierarchy Level

- For MX Series routers, T4000 routers, and EX9200 switches:

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

- For QFX10000 switches:

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the DDoS bandwidth rate limit; that is, the maximum traffic rate (packets per second) allowed by the specified policer . When the value is exceeded, a violation is declared.

Options ***packets-per-second***—Number of packets per second that are allowed by the aggregate or packet-type policer.

Range: 1 through 100,000 packets per second

Default: The default bandwidth value varies by packet type or protocol. You can view the default values for all packet types or protocols before you begin DDoS protection configuration by entering the **show ddos-protection protocols parameters brief** command from operational mode. For QFX10000 switches, the default bandwidth limits are also provided in the *protocols (DDoS)* statement description.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

bandwidth-scale (DDoS)

Syntax bandwidth-scale *percentage*;

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the percentage by which the DDoS bandwidth rate limit is scaled down for the aggregate or packet-type policer on the card in the specified slot.

Options ***percentage***—Percentage multiplied by the bandwidth rate limit to reduce the number of packets per second allowed for the packet type or protocol.

Range: 1 through 100 percent

Default: 100

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

burst (DDoS)

Syntax burst *size*;

Hierarchy Level

- For MX Series routers, T4000 routers, and EX9200 switches:

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

- For QFX10000 switches:

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the DDoS burst limit; that is, the maximum number of packets that is allowed in a burst of traffic by the specified policer. When this value is exceeded, a violation is declared.

Options ***size***—Number of packets that are allowed in a burst by the aggregate or packet-type policer.

Range: 1 through 100,000 packets

Default: The default burst value varies by packet type or protocol. You can view the default values for all packet types or protocols on an unconfigured router or switch by entering the **show ddos-protection protocols parameters brief** command from operational mode. For QFX10000 switches, the default bandwidth limits are also provided in the *protocols (DDoS)* statement description.

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

burst-scale (DDoS)

Syntax burst-scale *percentage*;

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Configure the percentage by which the DDoS burst limit is scaled down for the aggregate or packet-type policer on the card in the specified slot.

Options ***percentage***—Percentage multiplied by the burst limit to reduce the number of packets allowed in a burst for the packet type or protocol.

Range: 1 through 100 percent

Default: 100

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

bypass-aggregate (DDoS)

Syntax bypass-aggregate;

Hierarchy Level
- For MX Series routers, T4000 routers, and EX9200 switches:

  [edit system ddos-protection protocols *protocol-group packet-type*]
- For QFX10000 and QFX5200 switches:

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Prevent this packet type from being considered by the DDoS aggregate policer. Traffic for the packet type is still included in traffic statistics.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

ddos-protection (DDoS)

Syntax

```
ddos-protection
  global {
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection;
    flow-level-control;
    flow-detection-mode;
    flow-report-rate;
    violation-report-rate;
  }
  protocols protocol-group (aggregate | packet-type) {
    bandwidth packets-per-second;
    burst size;
    bypass-aggregate;
    disable-fpc;
    disable-logging;
    disable-routing-engine;
    flow-detection-mode (automatic | off | on);
    flow-detect-time seconds;
    flow-level-bandwidth {
      logical-interface flow-bandwidth;
      physical-interface flow-bandwidth;
      subscriber flow-bandwidth;
    }
    flow-level-control {
      logical-interface flow-control-mode;
      physical-interface flow-control-mode;
      subscriber flow-control-mode;
    }
    flow-level-detection {
      logical-interface flow-detection-mode;
      physical-interface flow-detection-mode;
      subscriber flow-detection-mode;
    }
    flow-recover-time seconds;
    flow-timeout-time seconds;
    fpc slot-number {
      bandwidth-scale percentage;
      burst-scale percentage;
      disable-fpc;
    }
    no-flow-logging
    priority level;
    recover-time seconds;
    timeout-active-flows;
  }
  traceoptions{
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
```

```
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure DDoS policers.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Protection Against DDoS Attacks on page 43
- Configuring Flow Detection for DDoS Protection on page 69

disable-fpc (DDoS)

Syntax disable-fpc;

Hierarchy Level [edit system ddos-protection global],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)],
[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*) fpc *slot-number*]

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Disable DDoS policers for debugging purposes on the card in the specified slot for a particular packet type within a protocol group, on all cards for a particular packet type within a protocol group, or globally on all cards and for all packet types in all protocols. This statement does not affect the state of the Routing Engine policers.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 57
- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

disable-logging (DDoS)

Syntax disable-logging;

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

Release Information Statement introduced in Junos OS Release 11.2.
Support at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level introduced in Junos OS Release 12.1.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Disable device-wide logging of all DDoS violation and flow detection events globally. Disable only logging of events other than flow detection culprit flow events for a particular packet type or for a protocol group. Typically used for debugging purposes.

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 57
- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*
- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 79

disable-routing-engine (DDoS)

Syntax disable-routing-engine;

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Disable DDoS Routing Engine policers for debugging purposes for a particular packet type within a protocol group or globally for all packet types in all protocols. This statement does not affect the state of the line card policers.

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

Related Documentation
- Disabling DDoS Protection Policers and Logging Globally on page 57

flow-detection (DDoS Flow Detection)

Syntax flow-detection;

Hierarchy Level [edit system ddos-protection global]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Enable flow detection globally for all protocol groups and packet types except the following, which do not have typical Ethernet, IP, or IPv6 headers:

- Protocol groups: **fab-probe**, **frame-relay**, **inline-ka**, **isis**, **jfm**, **mlp**, **pfe-alive**, **pos**, and **services**.
- Packet type: **unclassified** in the **ip-options** protocol group.

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

Related Documentation
- Enabling Flow Detection for All Protocol Groups and Packet Types on page 70
- Configuring Flow Detection for DDoS Protection on page 69

flow-detection (DDoS Packet Level)

Syntax

```
flow-detection {
  flow-detect-time detect-period;
  no-flow-logging;
  timeout-active-flows enable-period;
  flow-level-bandwidth {
    logical-interface flow-bandwidth;
    physical-interface flow-bandwidth;
    subscriber flow-bandwidth;
  }
  flow-level-control {
    logical-interface flow-control-mode;
    physical-interface flow-control-mode;
    subscriber flow-control-mode;
  }
  flow-level-detection {
    logical-interface operation-mode;
    physical-interface operation-mode;
    subscriber operation-mode;
  }
  flow-detection-mode (automatic |off | on);
  flow-recover-time recover-period;
  flow-timeout-time timeout-period;
}
```

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure DDoS protection suspicious control flow detection for a packet type.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Flow Detection for DDoS Protection on page 69

flow-detection-mode (DDoS Flow Detection)

Syntax flow-detection-mode (automatic | off | on)

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection for a protocol group or packet type. Use this statement to override global flow detection settings configured with the **flow-detection-mode** statement at the **[edit system ddos-protection global]** hierarchy level. The operation mode is effective only when flow detection is enabled.

Default The default mode for all protocol groups and packet types is **automatic**.

Options **automatic**—Detect flows only when the policer is being violated.

off—Disable flow detection.

on—Always monitor and detect flows, even when the policer is not being violated.

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

Related Documentation

- Configuring How Flow Detection Operates for Individual Protocol Groups or Packets on page 74
- Configuring Flow Detection for DDoS Protection on page 69

flow-detection-mode (DDoS Global Flow Detection)

Syntax flow-detection-mode (automatic | off | on)

Hierarchy Level [edit system ddos-protection global]

Release Information Statement introduced in Junos OS Release 17.1.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection globally for all protocol groups and packet types. The operation mode is effective only when flow detection is enabled.

To override the global configuration for a protocol group or packet type, use the **flow-detection-mode** statement at the **[edit system ddos-protection protocols *protocol-group packet-type*]** hierarchy level.

Default The default global mode is **automatic**.

Options **automatic**—Detect flows only when the policer is being violated.

off—Disable flow detection.

on—Always monitor and detect flows, even when the policer is not being violated.

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

Related Documentation

- Configuring How Flow Detection Operates for Individual Protocol Groups or Packets on page 74
- Configuring Flow Detection for DDoS Protection on page 69

flow-detect-time (DDoS Flow Detection)

Syntax flow-detect-time *seconds*;

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is confirmed to be a culprit flow.

BEST PRACTICE: We recommend that you use the default value for the detection period.

Options *seconds*—Period of excessive bandwidth required for flow to be a culprit flow.

Range: 1 through 60 seconds

Default: 3 seconds

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

Related Documentation

- Configuring the Detection Period for Suspicious Flows on page 71
- Configuring Flow Detection for DDoS Protection on page 69

flow-level-bandwidth (DDoS Flow Detection)

Syntax

```
flow-level-bandwidth {
  logical-interface flow-bandwidth;
  physical-interface flow-bandwidth;
  subscriber flow-bandwidth;
}
```

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure allowed flow bandwidth for the packet type at each flow aggregation level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 76
- Configuring Flow Detection for DDoS Protection on page 69

flow-level-control (DDoS Flow Detection)

Syntax

```
flow-level-control {
  logical-interface flow-control-mode;
  physical-interface flow-control-mode;
  subscriber flow-control-mode;
}
```

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Specify how traffic in the detected flow is handled for the protocol group or packet type at one or more flow aggregation levels. Use this statement to override global flow control mode settings configured with the **flow-level-control** statement at the **[edit system ddos-protection global]** hierarchy level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 78
- Configuring Flow Detection for DDoS Protection on page 69

flow-level-control (DDoS Global Flow Detection)

Syntax flow-level-control *flow-control-mode*;

Hierarchy Level [edit system ddos-protection global]

Release Information Statement introduced in Junos OS Release 17.1.

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Specify how traffic in the detected flow is handled globally for all protocol groups and packet types at all flow aggregation levels.

To override the global configuration for a protocol group or packet type, use the **flow-level-control** statement at the **[edit system ddos-protection protocols** ***protocol-group packet-type*****]** hierarchy level to specify the flow control mode at one or more flow aggregation levels.

Options ***flow-control-mode***—Mode for how traffic in the detected flow is controlled globally.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

Default: drop

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

Related Documentation

- Configuring How Traffic in a Culprit Flow Is Controlled Globally on page 77
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 78
- Configuring Flow Detection for DDoS Protection on page 69

flow-level-detection (DDoS Flow Detection)

Syntax

```
flow-level-detection {
  logical-interface flow-detection-mode;
  physical-interface flow-detection-mode;
  subscriber flow-detection-mode;
}
```

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the mode of operation for flow detection for the packet type at each flow aggregation level.

The remaining statements are explained separately.

NOTE: **Flow detection operates for individual flow aggregation levels only when the flow detection mode at the packet level is configured to either automatic or on.**

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

Related Documentation

- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75
- Configuring Flow Detection for DDoS Protection on page 69

flow-recover-time (DDoS Flow Detection)

Syntax flow-recover-time *seconds*;

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure how much time must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.

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

Range: 1 through 3600 seconds

Default: 60 seconds

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

Related Documentation

- Configuring the Recovery Period for a Culprit Flow on page 72
- Configuring Flow Detection for DDoS Protection on page 69

flow-report-rate (DDoS Flow Detection)

Syntax flow-report-rate *report-rate*;

Hierarchy Level [edit system ddos-protection global]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Set the rate at which culprit flow events are reported by system log messages, for all protocol groups and packet types on all line cards.

Options *report-rate*—Number of flows per second.

Range: 1 through 50,000

Default: 10

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

Related Documentation

- Configuring the Culprit Flow Reporting Rate for All Protocol Groups and Packet Types on page 71
- Configuring Flow Detection for DDoS Protection on page 69

flow-timeout-time (DDoS Flow Detection)

Syntax flow-timeout-time *seconds*;

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

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure the period of time that a culprit flow is suppressed for the packet type. The timeout period is effective only when timing out has been enabled with the timeout-active-flows statement.

Options *seconds*—Period that the traffic is suppressed.

Range: 1 through 7200 seconds

Default: 300 seconds

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

Related Documentation

- Configuring the Timeout Period for a Culprit Flow on page 73
- Configuring Flow Detection for DDoS Protection on page 69

fpc (DDoS)

Syntax

```
fpc slot-number;
  bandwidth-scale percentage;
  burst-scale percentage;
  disable-fpc;
}
```

Hierarchy Level

- For MX Series routers, T4000 routers, and EX9200 switches:

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

- For QFX10000 and QFX5200 switches:

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

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description

(MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, or QFX10000 switches) Modify the aggregate or packet-type policer on the specified line card.

Options

slot-number—Slot number of the card.

Range: Depends on the router or switch model

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

global (DDoS)

Syntax

```
global {
  disable-fpc;
  disable-logging;
  disable-routing-engine;
  flow-detection;
  flow-level-control;
  flow-detection-mode;
  flow-report-rate;
  violation-report-rate;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches,or QFX10000 switches) Modify DDoS policers, event logging, and flow detection globally for all protocols.

NOTE: The following statements are not supported on QFX5200 and QFX10000 switches: **disable-routing-engine, flow-detection, flow-report-rate, and violation-report-rate.**

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Disabling DDoS Protection Policers and Logging Globally on page 57

logical-interface (DDoS Flow Detection)

Syntax logical-interface (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode for flow detection at the logical interface flow aggregation level for the packet type.

Options ***flow-bandwidth***—Bandwidth for the flow at the logical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 200 packets per second

Range: 1 through 30,000 packets per second

flow-control-mode—Mode for how traffic in the detected flow is controlled at the logical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

Default: drop

flow-detection-mode—Mode for how flow detection operates at the logical interface level when a policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the flow-detection-mode statement at the [edit system ddos-protection global] hierarchy level.

- **automatic**—Search flows at the logical interface level only when a DDoS policer is being violated and only when the flow causing the policer violation is not discovered at the finer flow aggregation level, subscriber. When the suspicious flow is not found at this level, then the search moves to a coarser level of flow aggregation (physical interface). Flows at the logical interface level are subsequently not searched again until the policer is no longer violated at the coarser level, and a subsequent violation occurs that cannot be found at the subscriber level.
- **off**—Disable flow detection at the logical interface level so that flows are never searched at this level.
- **on**—Search flows at the logical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

Required Privilege Level

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 76
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 78
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75
- Configuring Flow Detection for DDoS Protection on page 69

no-flow-logging (DDoS Flow Detection)

Syntax no-flow-logging;

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

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

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

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

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

Related Documentation

- Disabling Automatic Logging of Culprit Flow Events for a Packet Type on page 79
- Configuring Flow Detection for DDoS Protection on page 69

physical-interface (DDoS Flow Detection)

Syntax physical-interface (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the physical interface flow aggregation level for the packet type.

Options ***flow-bandwidth***—Bandwidth for the flow at the physical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 20,000 packets per second

Range: 1 through 50,000 packets per second

flow-control-mode—Mode for how traffic in the detected flow is controlled at the physical interface level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the **flow-level-control** statement at the **[edit system ddos-protection global]** hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

Default: drop

flow-detection-mode—Mode for how flow detection operates at the physical interface level when a policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the **flow-detection-mode** statement at the **[edit system ddos-protection global]** hierarchy level.

- **automatic**—Search flows at the physical interface level only when a DDoS policer is being violated and only when the policer violation is not discovered at the finer aggregation levels, logical interface or subscriber. Flows at the physical interface level are subsequently not searched again until a subsequent violation occurs that cannot be found at the subscriber or logical interface levels.
- **off**—Disable flow detection at the physical interface level so that flows are never searched at this level.
- **on**—Search flows at the physical interface level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

Required Privilege Level

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

Related Documentation

- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 76
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 78
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75
- Configuring Flow Detection for DDoS Protection on page 69

priority (DDoS)

Syntax priority *level*;

Hierarchy Level
- For MX Series routers, T4000 routers, and EX9200 switches:

  [edit system ddos-protection protocols *protocol-group packet-type*]
- For QFX10000 and QFX5200 switches:

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

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Configure the priority for the packet type within the parent protocol group. In the event of downstream traffic congestion, high priority packets are provided bandwidth before medium priority packets. In turn, medium priority packets are provided bandwidth before low priority packets. Packets are dropped when there is insufficient available bandwidth.

Options ***level***—Priority of the packet type, low, medium, or high.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- *Configuring DDoS Protection Policers on QFX Series Switches*

protocols (DDoS)

Syntax

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

Hierarchy Level [edit system ddos-protection]

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

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

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

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

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

- **relay-reply**—RELAY-REPLY packets.
- **release**—RELEASE packets.
- **renew**—RENEW packets.
- **reply**—REPLY packets.
- **request**—REQUEST packets.
- **solicit**—SOLICIT packets.
- **unclassified**—All unclassified packets in the protocol group.

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

- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **mld**—Snooped MLD traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
  - **add**—Add requests; internal MAC address learning request packets sent to the host.
  - **delete**—Delete requests; internal MAC address learning request packets sent to the host.
  - **lookup**—Lookup requests; internal MAC address learning request packets sent to the host.
  - **unclassified**—All unclassified packets in the protocol group.
- **ndpv6**—The following NDPv6 packet types are available, except where noted, starting in 14.1R8, 14.2R8, 15.1R5, 15.1F7, and 16.1R1:
  - **invalid-hop-limit**—(Starting in 16.1R2) Invalid hop limit packets. These messages might represent crafted packets in a malicious network-based packet flood.
  - **neighbor-advertisement**—Neighbor advertisement packets. These are messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.
  - **neighbor-solicitation**—Neighbor solicitation packets. These are messages used for duplicate address detection and to test reachability of neighbors.
  - **redirect**—Redirect packets.
  - **router-advertisement**—Router advertisement packets. These are messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
  - **router-solicitation**—Router solicitation packets. These are messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.

- **ndpv6**—The following NDPv6 packet types are available:
  - **neighbor-advertisement**—Neighbor advertisement packets. These are messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.
  - **neighbor-solicitation**—Neighbor solicitation packets. These are messages used for duplicate address detection and to test reachability of neighbors.
  - **redirect**—Redirect packets.
  - **router-advertisement**—Router advertisement packets. These are messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
  - **router-solicitation**—Router solicitation packets. These are messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **echo-rep**—LCP echo reply packets.
  - **echo-req**—LCP echo request packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mlppp-lcp**—MLPPP LCP packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.
  - **pads**—PADS packets.
  - **padt**—PADT packets.

- **radius**—The following RADIUS packet types are available:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.
  - **unclassified**—All unclassified packets in the protocol group.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect:
  - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
  - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
  - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
  - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
  - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
  - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
  - **host**—Host packets.
  - **pfe**—Packet Forwarding Engine packets.
  - **syslog**—System log message packets.
  - **tap**—TAP packets.
- **tcp-flags**—The following TCP-flagged packet types are available:
  - **established**—TCP packets with ACK or RST flags set.
  - **initial**—TCP packets with SYN flag set and ACK flag not set.
  - **unclassified**—TCP packets with flags set any other way than the established and initial packets.

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

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

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

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

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

The remaining statements are explained separately.

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 54
- Understanding Distributed Denial-of-Service Protection with IPv6 Neighbor Discovery Protocol on page 41

recover-time (DDoS)

Syntax
recover-time *seconds*;

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

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

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

Options
seconds—Period required for the traffic to recover.
Range: 1 through 3600 seconds
Default: 300

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

Related Documentation
- Configuring DDoS Protection Policers for Individual Packet Types on page 54

subscriber (DDoS Flow Detection)

Syntax subscriber (*flow-bandwidth* | *flow-control-mode* | *flow-detection-mode*)

Hierarchy Level [edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control],
[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Configure flow bandwidth, flow control mode, or flow detection mode at the subscriber flow aggregation level for the packet type.

Options ***flow-bandwidth***—Specify the bandwidth for the flow at the subscriber level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-bandwidth]** hierarchy level.

Default: 100 packets per second

Range: 1 through 10,000 packets per second

flow-control-mode—Specify how traffic in the detected flow is controlled at the subscriber level. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-control]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the flow-level-control statement at the [edit system ddos-protection global] hierarchy level.

- **drop**—Drop all traffic in flow.
- **keep**—Keep all traffic in flow.
- **police**—Police the traffic to within its allowed bandwidth.

Default: drop

flow-detection-mode—Specify how flow detection operates at the subscriber level when a policer has been violated. Available only at the **[edit system ddos-protection protocols *protocol-group packet-type* flow-level-detection]** hierarchy level.

NOTE: The configuration at this level overrides the global configuration using the flow-detection-mode statement at the [edit system ddos-protection global] hierarchy level.

- **automatic**—Search flows at the subscriber level only when a DDoS policer is being violated and only until it is established that the flow causing the violation is not at this level. When the suspicious flow is not at this level, then the search moves to a coarser level of flow aggregation (logical interface). Flows at the subscriber level are subsequently not searched again until the policer is no longer violated at the coarser level.
- **off**—Disable flow detection at the subscriber level so that flows are never searched at this level.
- **on**—Search flows at the subscriber level, even when no DDoS protection policer is currently being violated. Monitoring continues at this level regardless of whether a suspect flow is identified at this level.

Default: automatic

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

Related Documentation
- Configuring the Maximum Flow Bandwidth at Each Flow Aggregation Level on page 76
- Configuring How Traffic in a Culprit Flow Is Controlled at Each Flow Aggregation Level on page 78
- Configuring How Flow Detection Operates at Each Flow Aggregation Level on page 75
- Configuring Flow Detection for DDoS Protection on page 69

timeout-active-flows (DDoS Flow Detection)

Syntax
timeout-active-flows;

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

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

Description
(MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Enable culprit flows for the packet type to time out according to the timeout period. The culprit flow is suppressed for the duration of the timeout period. When the period expires, the flow times out and is released from suppression.

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

Related Documentation
- Configuring the Timeout Period for a Culprit Flow on page 73
- Configuring Flow Detection for DDoS Protection on page 69

traceoptions (DDoS)

Syntax

```
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
```

Hierarchy Level [edit system ddos-protection]

Release Information

Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Statement introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Statement introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description (MX Series routers with only MPCs, T4000 routers with only FPC5s, EX9200 switches, QFX5200 switches, or QFX10000 switches) Define tracing operations for DDoS protection processes.

Options

file *filename*—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory **/var/log**.

files *number*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the **size** option.

Range: 2 through 1000

Default: 3 files

flag *flag*—Tracing operation to perform. To specify more than one tracing operation, include multiple **flag** statements. You can include the following flags:

- **all**—Trace all operations.
- **config**—Trace processing of the DDoS configuration at an extensive level.
- **events**—Trace jddosd event processing; currently only exit events are traced.
- **gres**—Trace messages exchanged with the kernel and jddosd process that could affect graceful Routing Engine switchover (GRES).
- **init**—Trace jddosd initialization.
- **ipc**—Trace interface interprocess communication (IPC) messages.
- **memory**—Trace memory management code. This flag is not currently supported.
- **protocol**—Trace DDoS protocol state processing. Only the violation state is currently traced.
- **rtsock**—Trace messages exchanged with the kernel and jddosd process.

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

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

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

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

no-remote-trace—Disable remote tracing.

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

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

Syntax: ***size*****k** to specify KB, ***size*****m** to specify MB, or ***size*****g** to specify GB

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

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

Required Privilege Level

trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- Tracing DDoS Protection Operations on page 58

violation-report-rate (DDoS Flow Detection)

Syntax violation-report-rate *report-rate*;

Hierarchy Level [edit system ddos-protection global]

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

Description (MX Series routers with only MPCs, T4000 Core Routers with only FPC5s, or EX9200 switches) Limit the rate at which bandwidth violations (violation reports) are reported from an FPC to the Routing Engine, for all protocol groups and packet types on all line cards.

Options *report-rate*—Number of violations per second.

Range: 1 through 50,000

Default: 100

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

Related Documentation

- Configuring the Violation Reporting Rate for All Protocol Groups and Packet Types on page 71
- Configuring Flow Detection for DDoS Protection on page 69

CHAPTER 20

Configuration Statements: IPsec and Digital Certificates

algorithm (Authentication Keychain)

Syntax algorithm (hmac-sha-1 | md5);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Configure the authentication algorithm for IS-IS.

Options **hmac-sha-1**—96-bit hash-based message authentication code (SHA-1).

md5—Message digest 5.
Default: md5

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

Related Documentation
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*
- *Understanding Hitless Authentication Key Rollover for IS-IS*

algorithm (Junos FIPS)

Syntax algorithm 3des-cbc;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description Select the encryption algorithm for the internal Routing-Engine–to–Routing-Engine IPsec security association (SA) configuration.

Options Only **3des-cbc** is supported.

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

authentication (Security IPsec)

Syntax

```
authentication {
  algorithm (hmac-sha1-96 | hmac-sha2-256);
  key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level

[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Configure IP Security (IPsec) authentication parameters for manual security association (SA).

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

Options

algorithm—Hash algorithm that authenticates packet data. It can be one of the following:

- **hmac-md5-96**—Produces a 128-bit digest.
- **hmac-sha1-96**—Produces a 160-bit digest.

key—Type of authentication key. It can be one of the following:

- **ascii-text *key***—ASCII text key. For **hmac-md5-96**, the key is 16 ASCII characters; for **hmac-sha1-96**, the key is 20 ASCII characters.
- **hexadecimal *key***—Hexadecimal key. For **hmac-md5-96**, the key is 32 hexadecimal characters; for **hmac-sha1-96**, the key is 40 hexadecimal characters.

Required Privilege Level

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

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 183

authentication-algorithm (Security IKE)

Syntax authentication-algorithm (md5 | sha1);

Hierarchy Level [edit security ike proposal *ike-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the Internet Key Exchange (IKE) authentication algorithm.

Options **authentication-algorithm**—Hash algorithm that authenticates packet data. It can be one of two algorithms:

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

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

Related Documentation

- Configuring the Authentication Algorithm for an IKE Proposal on page 193

authentication-algorithm (Security IPsec)

Syntax authentication-algorithm (hmac-md5-96 | hmac-sha1-96);

Hierarchy Level [edit security ipsec proposal *ipsec-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the IPsec authentication algorithm.

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

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

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

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

Options

authentication-algorithm—Hash algorithm that authenticates packet data. It can be one of two algorithms:

- **hmac-md5-96**—Produces a 128-bit digest.
- **hmac-sha1-96**—Produces a 160-bit digest.

Required Privilege Level

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

Related Documentation

- Configuring the Authentication Algorithm for an IPsec Proposal on page 199

authentication-key-chains

Syntax

```
authentication-key-chains {
  key-chain key-chain-name {
    description text-string;
    key key {
      algorithm (md5 | hmac-sha-1);
      options (basic | isis-enhanced);
      secret secret-data;
      start-time yyyy-mm-dd.hh:mm:ss;
    }
    tolerance seconds;
  }
}
```

Hierarchy Level [edit security]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure authentication key updates for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol. When the **authentication-key-chains** statement is configured at the **[edit security]** hierarchy level, and is associated with the BGP, LDP, or IS-IS protocols at the **[edit protocols]** hierarchy level or with the BFD protocol using the **bfd-liveness-detection** statement, authentication key updates can occur without interrupting routing and signaling protocols such as Open Shortest Path First (OSPF) and Resource Reservation Setup Protocol (RSVP).

The remaining statements are explained separately.

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

authentication-method

Syntax authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);

Hierarchy Level [edit security ike proposal *ike-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the IKE authentication method.

Options

dsa-signatures—Digital Signature Algorithm (DSA)

rsa-signatures—A public key algorithm, which supports encryption and digital signatures

pre-shared-keys—A key derived from an out-of-band mechanism; the key authenticates the exchange

Required Privilege Level

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

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 183

auto-re-enrollment

Syntax

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

Hierarchy Level [edit security pki]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify auto-reenrollment parameters for a certificate authority (CA) issued router certificate. Auto-reenrollment requests that the issuing CA replace a router certificate before its specified expiration date.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- Configuring Digital Certificates for Adaptive Services Interfaces on page 21

auxiliary-spi (Security IPsec)

Syntax auxiliary-spi *auxiliary-spi-value*;

Hierarchy Level [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the auxiliary Security Parameter Index (SPI) for a manual SA. Use the auxiliary SPI when you configure the **protocol** statement to use the **bundle** option.

Options ***auxiliary-spi-value***—Arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).

Range: 256 through 16,639

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

Related Documentation
- Configuring Manual IPsec Security Associations for an ES PIC on page 183
- spi on page 356

ca-identity

Syntax ca-identity *ca-identity*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement introduced in Junos OS Release 7.5.

Description Specify the certificate authority (CA) identity to use in requesting digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.

Options ***ca-identity***—The name of the CA identity. This name is typically the domain name of the CA.

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

Related Documentation
- Specifying the CA Profile Name on page 23

ca-name

Syntax ca-name *ca-identity*;

Hierarchy Level [edit security certificates certification-authority]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the certificate authority (CA) identity to use in the certificate request.

Options ***ca-identity***—CA identity to use in the certificate request.

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

Related Documentation
- Specifying the Certificate Authority Name on page 16

ca-profile

Syntax

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

Hierarchy Level [edit security pki]

Release Information Statement introduced in Junos OS Release 7.5.
revocation-check and **crl** statements added in Junos OS Release 8.1.

Description Specify the name of the certificate authority (CA) profile for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M Series and T Series routers.

The remaining statements are explained separately.

Options *ca-profile-name*—Name of the trusted CA.

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

Related Documentation

- Specifying the CA Profile Name on page 23

cache-size

Syntax cache-size *bytes*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.

Options ***bytes***—Cache size for digital certificates.

Range: 64 through 4,294,967,295

Default: 2 megabytes (MB)

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

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

Related Documentation

- Configuring the Cache Size on page 18

cache-timeout-negative

Syntax cache-timeout-negative *seconds*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.

Options ***seconds***—Negative time to cache digital certificates, in seconds.

Range: 10 through 4,294,967,295

Default: 20

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

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

Related Documentation

- Configuring the Negative Cache on page 18

certificate-id

Syntax

```
certificate-id {
  ca-profile ca-profile-name;
  challenge-password password;
  re-enroll-trigger-time-percentage percentage;
  re-generate-keypair;
  validity-period days;
}
```

Hierarchy Level [edit security auto-re-enrollment]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify a router certificate for auto-reenrollment. The ID is the same as that used to get the end entity's certificate from the issuing certificate authority.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- auto-re-enrollment on page 303

certificates

Syntax

```
certificates {
  cache-size bytes;
  cache-timeout-negative seconds;
  certification-authority ca-profile-name {
    ca-name ca-identity;
    crl file-name;
    encoding (binary | pem);
    enrollment-url url-name;
    file certificate-filename;
    ldap-url url-name;
  }
  enrollment-retry attempts;
  local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
  }
  maximum-certificates number;
  path-length certificate-path-length;
}
```

Hierarchy Level [edit security]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificates for IPsec.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring Digital Certificates for an ES PIC on page 15

certification-authority

Syntax

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

Hierarchy Level [edit security certificates]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced before Junos OS Release 12.1 for the SRX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure a certificate authority profile name.

Configure certification authority (CA) for X.509 certificate.

Options

- *profile-name*—Name of this CA configuration.
- **ca-name** ***name***—Name of the CA.
- **crl** ***filename***—Certificate revocation list (CRL) filename.
- **encoding**—Certificate encoding, either **binary** or **pem** (privacy-enhanced mail).
- **enrollment-url** ***url***—Enrollment URL.
- **file** ***filename***—Certificate filename.
- **ldap-url** ***url***—Lightweight Directory Access Protocol (LDAP) URL.

Required Privilege Level

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

Related Documentation

- Configuring the Certificate Authority Properties for an ES PIC on page 16
- *Network Monitoring and Troubleshooting Guide for Security Devices*
- *Security Basics*
- Configuring the Certificate Authority Properties for an ES PIC on page 16

challenge-password

Syntax challenge-password *password*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS Release 8.5.

Description Specify the challenge password used by the certificate authority (CA) for router certificate enrollment and revocation. This challenge password must be the same used when the router certificate was originally configured.

Options ***password***—The password required by the CA.

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

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- **auto-re-enrollment on page 303**

crl (Adaptive Services Interface)

Syntax

```
crl {
  disable on-download-failure;
  refresh-interval number-of-hours;
  url {
    url-name;
    password;
  }
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name* revocation-check]

Release Information Statement introduced in Junos OS Release 8.1.

Description Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options

disable on-download-failure—Permit the authentication of the IPsec peer when the CRL is not downloaded.

password—Password to access the URLs.

refresh-interval *number-of-hours*—Time interval, in hours, between CRL updates.

Range: 0 through 8784

Default: 24

url *url-name*—Location from which to retrieve the CRL through the Lightweight Directory Access Protocol (LDAP). You can configure as many as three URLs for each configured CA profile.

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

Related Documentation

- Configuring the Certificate Revocation List on page 24

crl (Encryption Interface)

Syntax crl *file-name*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.

Options ***file-name***—Specify the file from which to read the CRL.

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

Related Documentation
- Configuring the Certificate Authority Properties for an ES PIC on page 16

description (Authentication Keychain)

Syntax description *text-string*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in JUNOS OS Release 11.2.

Description Configure a description for an authentication key-chain.

Options ***text-string***—A text string describing the **authentication-key-chain**. Put the text string in quotes (“text description”).

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

Related Documentation
- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

description (IKE policy)

Syntax description *description*;

Hierarchy Level [edit security ike policy *ike-peer-address*],
[edit security ike proposal *ike-proposal-name*],
[edit security ipsec policy *ipsec-policy-name*],
[edit security ipsec proposal *ipsec-proposal-name*],
[edit security ipsec security-association *sa-name*]

Description Specify a text description for an IKE proposal or policy, or an IPsec proposal, policy, or SA.

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

Related Documentation

- Configuring Security Associations for IPsec on an ES PIC on page 181
- Configuring the Description for an IKE Proposal on page 194
- Configuring the Description for an IKE Policy on page 196
- Configuring an IPsec Proposal for an ES PIC on page 198
- Configuring the IPsec Policy for an ES PIC on page 200

dh-group

Syntax dh-group (group1 | group2 | group5 | group14);

Hierarchy Level [edit security ike proposal *ike-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the IKE Diffie-Hellman group.

Options **dh-group**—Type of Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange. It can be one of the following:

- **group1**—768-bit.
- **group2**—1024-bit.
- **group5**—1536-bit.
- **group14**—2048-bit.

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

Related Documentation

- Configuring the Diffie-Hellman Group for an IKE Proposal on page 194

direction (Junos OS)

Syntax

```
direction (inbound | outbound | bidirectional) {
  authentication {
    algorithm (hmac-md5-96 | hmac-sha1-96);
    key (ascii-text key | hexadecimal key);
  }
  auxiliary-spi auxiliary-spi-value;
  encryption {
    algorithm (des-cbc | 3des-cbc);
    key (ascii-text key | hexadecimal key);
  }
  protocol (ah | esp | bundle);
  spi spi-value;
}
```

Hierarchy Level [edit security ipsec security-association *sa-name* manual]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the direction of IPsec processing.

Options

inbound—Inbound SA—Define algorithms, keys, or security parameter index (SPI) values to decrypt and authenticate incoming traffic coming from the peer.

outbound—Outbound SA—Define algorithms, keys, or SPI values to decrypt and authenticate outbound traffic to the peer.

bidirectional—Bidirectional SA—Decrypt and authenticate the incoming and outgoing traffic using the same algorithm, keys, or SPI in both directions, unlike inbound and outbound SAs that use different attributes in both directions.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 183
- *Example: Using IPsec to Protect BGP Traffic*

direction (Junos-FIPS Software)

Syntax

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

Hierarchy Level [edit security ipsec internal security-association manual],
[edit security trusted-channel ipsec security-association manual]

Release Information Statement introduced before Junos OS Release 7.4.

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

Options

bidirectional—Apply the same SA values in both directions between Routing Engines.

inbound—Apply these SA properties only to the inbound IPsec tunnel.

outbound—Apply these SA properties only to the outbound IPsec tunnel.

The remaining statements are explained separately.

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

dynamic

Syntax

```
dynamic {
  ipsec-policy ipsec-policy-name;
  replay-window-size (32 | 64);
}
```

Hierarchy Level [edit security ipsec security-association *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a dynamic IPsec SA.

Options

ipsec-policy *ipsec-policy-name*—Name of the IPsec policy.

replay-window-size—(Optional) Antireplay window size. It can be one of the following values:

- **32**—32-packet window size.
- **64**—64-packet window size.

Required Privilege Level

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

Related Documentation

- Configuring Dynamic IPsec Security Associations on page 187
- Associating the Configured Security Association with a Logical Interface on page 21

encoding

Syntax encoding (binary | pem);

Hierarchy Level [edit security ike policy *ike-peer-address*],
[edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the **local-certificate** and **local-key-pair** statements.

Options **binary**—Binary file format.

pem—Privacy-enhanced mail (PEM), an ASCII base 64 encoded format.

Default: binary

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

Related Documentation

- Configuring the Type of Encoding Your CA Supports on page 17
- Configuring the Type of Encoding Your CA Supports on page 20

encryption (Junos OS)

Syntax

```
encryption {
    algorithm (des-cbc | 3des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);
    key (ascii-text key | hexadecimal key);
}
```

Hierarchy Level

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

Release Information

Statement introduced before Junos OS Release 7.4.
aes-128-cbc, **aes-192-cbc**, and **aes-256-cbc** algorithm options added in Junos OS Release 15.1.

Description

Configure an encryption algorithm and key for a manual Security Association.

Options

algorithm—Type of encryption algorithm. It can be one of the following:

- **des-cbc**—Has a block size of 8 bytes (64 bits); its key size is 48 bits long.
- **3des-cbc**—Has block size of 8 bytes (64 bits); its key size is 192 bits long.

NOTE: For **3des-cbc**, we recommend that the first 8 bytes be different from the second 8 bytes, and the second 8 bytes be the same as the third 8 bytes.

- **aes-128-cbc**—Has a block size of 128 bits; its key size is 128 bits long.
- **aes-192-cbc**—Has a block size of 128 bits; its key size is 192 bits long.
- **aes-256-cbc**—Has a block size of 128 bits; its key size is 256 bits long.

NOTE: The **aes-*-cbc** algorithms support both IKE and IPsec configurations at the **[security]** hierarchy level.

key—Type of encryption key. It can be one of the following:

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

Required Privilege Level

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

Related Documentation

- *Example: Using IPsec to Protect BGP Traffic*
- Configuring Manual IPsec Security Associations for an ES PIC on page 183

encryption (Junos-FIPS Software)

Syntax

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

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

Release Information Statement introduced before Junos OS Release 7.4.

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

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

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

encryption-algorithm (Security)

Syntax encryption-algorithm (3des-cbc | des-cbc | aes-128-cbc | aes-192-cbc | aes-256-cbc);

Hierarchy Level [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an IKE or IPsec encryption algorithm.

Options

3des-cbc—Encryption algorithm with key size of 24 bytes; its key size is 192 bits long.

des-cbc—Encryption algorithm with key size of 8 bytes; its key size is 48 bits long.

aes-128-cbc—Advanced encryption algorithm that has a key size of 16 bytes; its key size is 128 bits long.

aes-192-cbc—Advanced encryption algorithm that has a key size of 24 bytes; its key size is 192 bits long.

aes-256-cbc—Advanced encryption algorithm that has a key size of 32 bytes; its key size is 256 bits long.

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

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 193
- Configuring an IPsec Proposal for an ES PIC on page 198

enrollment

Syntax

```
enrollment {
  url url-name;
  retry number-of-enrollment-attempts;
  retry-interval seconds;
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement introduced in Junos OS Release 7.5.

Description Specify the URL and enrollment parameters of the certificate authority (CA) for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed on M Series and T Series routers.

Options

url *url-name*—Location of the CA to which the router sends the Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests for the configured CA profile. Use the CA host DNS name or IP address.

retry *number-of-enrollment-attempts*—Number of enrollment retries.

Range: 0 through 100

Default: 0

retry-interval *seconds*—Length of time, in seconds, that a router should wait between enrollment attempts.

Range: 0 through 3600

Default: 0

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

Related Documentation

- Specifying an Enrollment URL on page 23
- Specifying the Enrollment Properties on page 24

enrollment-retry

Syntax enrollment-retry *attempts*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.

Options ***attempts***—Number of enrollment retries.

Range: 0 through 100

Default: 0

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

Related Documentation

- Configuring the Number of Enrollment Retries on page 18

enrollment-url

Syntax enrollment-url *url-name*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).

Options *url-name*—Certificate authority URL.

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

Related Documentation

- Specifying an Enrollment URL on page 17

file

Syntax file *certificate-filename*;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.

Options *certificate-filename*—File from which to read the digital certificate.

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

Related Documentation
- Specifying a File to Read the Digital Certificate on page 17

identity

Syntax identity *identity-name*;

Hierarchy Level [edit security ike]

Release Information Statement introduced before Junos OS Release 7.4.

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

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

Related Documentation
- Configuring the Identity to Define the Remote Certificate Name on page 20

ike (Security)

Syntax

```
ike {
  policy ike-peer-address {
    description policy-description;
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
  }
  proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Configure IKE.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 193
- Configuring an IKE Policy for Preshared Keys on page 195

internal

Syntax

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

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

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

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 202
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

ipsec (Security)

Syntax

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

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

Hierarchy Level [edit security]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure IPsec on encryption interfaces.

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

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Security Associations for IPsec on an ES PIC on page 181

key (Authentication Keychain)

Syntax

```
key key {
  algorithm (md5 | hmac-sha-1);
  options (basic | isis-enhanced);
  secret secret-data;
  start-time yyyy-mm-dd.hh:mm:ss;
}
```

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure the authentication element.

Options

key—Each key within a keychain is identified by a unique integer value.

Range: 0 through 63

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

key (Junos FIPS)

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

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

Release Information Statement introduced before Junos OS Release 7.4.

Description The key used for the internal Routing-Engine–to–Routing-Engine IPsec security association (SA) configuration.

Options ***ascii-text-key***—The encrypted ASCII text key.

hexadecimal key—The encrypted hexadecimal key.

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

key-chain (Security)

Syntax

```
keychain key-chain-name {
  description text-string;
  key key {
    algorithm (md5 | hmac-sha-1);
    options (basic | isis-enhanced);
    secret secret-data;
    start-time yyyy-mm-dd.hh:mm:ss;
  }
  tolerance seconds;
}
```

Hierarchy Level [edit security authentication-key-chains]

Release Information

Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Create the key-chain configuration for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options

key-chain-name—Authentication keychain name. It can be up to 126 characters. Characters can include any ASCII strings. If you include spaces, enclose all characters in quotation marks (“ ”).

Required Privilege Level

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

Related Documentation

- authentication-key-chains on page 301
- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

ldap-url

Syntax <ldap-url *url-name*>;

Hierarchy Level [edit security certificates certification-authority *ca-profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,

Description (Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.

Options ***url-name***—Name of the LDAP URL.

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

Related Documentation
- Specifying an LDAP URL on page 17

lifetime-seconds (Security)

Syntax <lifetime-seconds *seconds*>;

Hierarchy Level [edit security ike proposal *ike-proposal-name*],
[edit security ipsec proposal *ipsec-proposal-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description (Optional) Configure the lifetime of IKE or IPsec SA. When the SA expires, it is replaced by a new SA (and SPI) or terminated.

Options ***seconds***—Lifetime, in seconds.
Range: 180 through 86,400

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

Related Documentation
- Configuring the Lifetime for an IKE SA on page 195
- Configuring the Lifetime for an IPsec SA on page 199

local

Syntax

```
local certificate-name {
    certificate-key-string;
    load-key-file URL filename;
}
```

Hierarchy Level [edit security certificates]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.

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

Options

certificate-key-string—String of alphanumeric characters that constitute the private key and certificate.

certificate-name—Name that uniquely identifies the certificate.

load-key-file *URL filename*—File that contains the private key and certificate. It can be one of two types of values:

- Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk)
- URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)

Required Privilege Level

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

Related Documentation

- Importing SSL Certificates for Junos XML Protocol Support on page 5

local-certificate (Security)

Syntax local-certificate *certificate-filename*;

Hierarchy Level [edit security ike policy *ike-peer-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the certificate filename from which to read the local certificate.

Options ***certificate-filename***—File from which to read the local certificate.

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

Related Documentation
- Specifying the Certificate Filename on page 20

local-key-pair

Syntax local-key-pair *private-public-key-file*;

Hierarchy Level [edit security ike policy *ike-peer-address*]

Release Information Statement introduced before Junos 7.4.

Description Specify private and public keys.

Options ***private-public-key-file***—Specify the file from which to read the private and public key pair.

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

Related Documentation
- Specifying the Private and Public Key File on page 20

manual (Junos OS)

Syntax

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

Hierarchy Level [edit security ipsec security-association]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define a manual IPsec SA.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Manual IPsec Security Associations for an ES PIC on page 183

manual (Junos-FIPS Software)

Syntax

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

Hierarchy Level [edit security ipsec internal security-association]

Release Information Statement introduced before Junos OS Release 7.4.

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

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 202
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

maximum-certificates

Syntax maximum-certificates *number*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.

Options ***number***—Maximum number of peer digital certificates to be cached.

Range: 64 through 4,294,967,295 peer certificates

Default: 1024 peer certificates

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

Related Documentation

- Configuring the Maximum Number of Peer Certificates on page 19

mode (IKE)

Syntax mode (aggressive | main);

Hierarchy Level [edit security ike policy *ike-peer-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IKE policy mode.

NOTE: IKEv2 protocol does not negotiate using mode configuration.

Default main

Options

aggressive—Take half the number of messages of main mode, has less negotiation power, and does not provide identity protection.

main—Use six messages, in three peer-to-peer exchanges, to establish the IKE SA. These three steps include the IKE SA negotiation, a Diffie-Hellman exchange, and authentication of the peer. Also provides identity protection.

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

Related Documentation

- Configuring the Mode for an IKE Policy on page 196

mode (IPsec)

Syntax mode (transport | tunnel);

Hierarchy Level [edit security ipsec security-association *name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the mode for the IPsec security association.

Default tunnel

Options

transport—Protect traffic when the communication endpoint and cryptographic endpoint are the same. The data portion of the IP packet is encrypted, but the IP header is not. Virtual Private Network (VPN) gateways that provide encryption and decryption services for protected hosts cannot use transport mode for protected VPN communications.

tunnel—Protect traffic using preshared keys with IKE to authenticate peers or digital certificates with IKE to authenticate peers.

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

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

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

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

Related Documentation

- *Example: Using IPsec to Protect BGP Traffic*
- Configuring IPsec Tunnel Mode on page 183

options (Security)

Syntax options (basic | isis-enhanced);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description For IS-IS only, configure the protocol transmission encoding format for encoding the message authentication code in routing protocol packets.

Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.

Options

basic—RFC 5304 based encoding. Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices.

isis-enhanced—RFC 5310 based encoding. Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices.

Default: basic

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

Related Documentation

- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*
- *Understanding Hitless Authentication Key Rollover for IS-IS*

path-length

Syntax path-length *certificate-path-length*;

Hierarchy Level [edit security certificates]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description (Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.

Options ***certificate-path-length***—Digital certificate path length.

Range: 2 through 15 certificates

Default: 15 certificates

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

Related Documentation

- Configuring the Path Length for the Certificate Hierarchy on page 19

perfect-forward-secrecy (Security)

Syntax

```
perfect-forward-secrecy {
  keys (group1 | group2);
}
```

Hierarchy Level [edit security ipsec policy *ipsec-policy-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the Perfect Forward Secrecy (PFS) protocol. Create single-use keys.

Options **keys**—Type of Diffie-Hellman prime modulus group that IKE uses when performing the new Diffie-Hellman exchange.

The key can be one of the following:

- **group1**—768-bit.
- **group2**—1024-bit.

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

Related Documentation

- Configuring Perfect Forward Secrecy on page 201

pki

Syntax

```
pki {
  auto-re-enrollment {
    certificate-id {
      ca-profile ca-profile-name;
      challenge-password password;
      re-enroll-trigger-time-percentage percentage;
      re-generate-keypair;
      validity-period days;
    }
  }
  ca-profile ca-profile-name {
    ca-identity ca-identity;
    enrollment {
      url url-name;
      retry number-of-enrollment-attempts;
      retry-interval seconds;
    }
    revocation-check {
      disable;
      crl {
        disable on-download-failure;
        refresh-interval hours;
        url {
          url-name;
          password;
        }
      }
    }
  }
  traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag;
  }
}
```

Hierarchy Level [edit security]

Release Information Statement introduced in Junos OS Release 7.5.
revocation-check and **crl** statements added in Junos OS Release 8.1.

Description Configure an IPsec profile to request digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.

Options The remaining statements are explained separately.

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

Related Documentation

- Configuring Digital Certificates for Adaptive Services Interfaces on page 21

- *Junos OS, Release 15.1*
- CLI Explorer

policy (Security IKE)

Syntax

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

Hierarchy Level [edit security ike]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IKE policy.

Options ***ike-peer-address***—A tunnel address configured at the **[edit interfaces es]** hierarchy level.

The remaining statements are explained separately.

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

Related Documentation

- Configuring an IKE Policy for Preshared Keys on page 195
- Configuring an IKE Policy for Digital Certificates for an ES PIC on page 19

policy (Security IPsec)

Syntax

```
policy ipsec-policy-name {
  description description;
    perfect-forward-secrecy {
    keys (group1 | group 14 | group2 | group 5);
  }
  proposals [ proposal-names ];
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IPsec policy.

Options ***ipsec-policy-name***—Specify an IPsec policy name.

The remaining statements are explained separately.

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

Related Documentation

- Configuring the IPsec Policy for an ES PIC on page 200

pre-shared-key (Security)

Syntax pre-shared-key (ascii-text *key* | hexadecimal *key*);

Hierarchy Level [edit security ike policy *ike-peer-address*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the key used to authenticate a dynamic peer during IKE phase 1 negotiation. Specify the key in either ASCII or hexadecimal format.

Options **ascii-text *key***—Authentication key in ASCII format.

hexadecimal *key*—Authentication key in hexadecimal format.

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

Related Documentation

- Configuring the Preshared Key for an IKE Policy on page 197

proposal (Security IKE)

Syntax

```
proposal ike-proposal-name {
  authentication-algorithm (md5 | sha1 | sha-256);
  authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
  description description;
  dh-group (group1 | group2 | group 5 | group14);
  encryption-algorithm algorithm;
  lifetime-seconds seconds;
}
```

Hierarchy Level [edit security ike]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IKE proposal for a dynamic SA.

Options ***ike-proposal-name***—Specify an IKE proposal name.

The remaining statements are explained separately.

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

Related Documentation

- Configuring an IKE Proposal for Dynamic SAs on page 193

proposal (Security IPsec)

Syntax

```
proposal ipsec-proposal-name {
  authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
  encryption-algorithm algorithm;
  lifetime-seconds seconds;
  protocol (ah | bundle | esp);
}
```

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define an IPsec proposal for a dynamic SA.

Options ***ipsec-proposal-name***—Specify an IPsec proposal name.

The remaining statements are explained separately.

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

Related Documentation

- Configuring an IPsec Proposal for an ES PIC on page 198

proposals

Syntax proposals [*proposal-names*];

Hierarchy Level [edit security ike policy *ike-peer-address*],
[edit security ipsec policy *ipsec-policy-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Associate one or more proposals with an IKE or IPsec policy.

Options ***proposal-names***—Name of one or more proposals.

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

Related Documentation

- Associating Proposals with an IKE Policy on page 197
- Configuring the IPsec Policy for an ES PIC on page 200

protocol (Junos OS)

Syntax protocol (ah | esp | bundle);

Hierarchy Level [edit security ipsec proposal *ipsec-proposal-name*],
[edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bidirectional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Define the IPsec protocol for a manual or dynamic SA.

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

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

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

Options **ah**—Authentication Header protocol

bundle—AH and ESP protocols

esp—ESP protocol (the **tunnel** statement must be included at the **[edit security ipsec security-association *sa-name* mode** hierarchy level)

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

Related Documentation

- *Example: Using IPsec to Protect BGP Traffic*
- Configuring Manual IPsec Security Associations for an ES PIC on page 183
- Configuring the Protocol for a Dynamic IPsec SA on page 200

protocol (Junos-FIPS Software)

Syntax protocol esp;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description The protocol used for the internal Routing-Engine–to–Routing-Engine IPsec security association (SA) configuration.

Options Only **esp** is supported.

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

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 202
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

re-enroll-trigger-time-percentage

Syntax re-enroll-trigger-time-percentage *percentage*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS Release 8.5.

Description Percentage of the router certificate validity-period statement value, in days, when auto-reenrollment should start before expiration.

Options ***percentage***—Percentage for the reenroll trigger time.
Range: 1 through 99

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

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- auto-re-enrollment on page 303

re-generate-keypair

Syntax <re-generate-keypair>;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS Release 8.5.

Description (Optional) Automatically generate a new key pair when auto-reenrolling a router certificate. If this statement is not configured, the current key pair is used.

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

Related Documentation
- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- auto-re-enrollment on page 303

refresh-interval

Syntax refresh-interval *number-of-hours*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* revocation-check crl]

Release Information Statement introduced in Junos OS Release 8.1.

Description (Adaptive services interfaces only) Specify the amount of time between certificate revocation list (CRL) updates.

Options ***number-of-hours***—Time interval, in hours, between CRL updates.
Range: 0 through 8784
Default: 24

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

Related Documentation
- Configuring the Certificate Revocation List on page 24
- crl on page 313

retry (Adaptive Services Interface)

Syntax retry *number-of-attempts*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* enrollment]

Release Information Statement introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Specify how many times a router can resend a digital certificate request.

Options ***number-of-attempts***—Number of enrollment retries.
Range: 0 through 100
Default: 0

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

Related Documentation
- Specifying the Enrollment Properties on page 24
- enrollment on page 323

retry-interval

Syntax retry-interval *seconds*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* enrollment]

Release Information Statement introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Specify the amount of time the router should wait between enrollment retries.

Options ***seconds***—Time interval, in seconds, between enrollment retries.
Range: 0 through 3600
Default: 0

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

Related Documentation
- Specifying the Enrollment Properties on page 24
- enrollment on page 323

revocation-check

Syntax

```
revocation-check {
  disable;
  crl {
    refresh-interval number-of-hours;
    url {
      url-name;
    }
  }
}
```

Hierarchy Level [edit security pki ca-profile *ca-profile-name*]

Release Information Statement introduced in Junos OS Release 8.1.

Description Specify the method to verify revocation status of digital certificates for J Series Services Routers and Adaptive Services (AS) and MultiServices PICs installed in M Series and T Series routers.

Options

disable—Disable verification of status of digital certificates.

crl—Only certificate revocation list (CRL) is supported. A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis. By default, **crl** is enabled.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- Configuring the Certificate Revocation List on page 24

secret

Syntax secret *secret-data*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a password in encrypted text or plain text format. The secret password always appears in encrypted format.

Options ***secret-data***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

security-association (Junos OS)

Syntax

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

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

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

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately.

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

Related Documentation

- Configuring Security Associations for IPsec on an ES PIC on page 181

security-association (Junos-FIPS Software)

Syntax

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

Hierarchy Level [edit security ipsec]

Release Information Statement introduced before Junos OS Release 7.4.

NOTE: We recommend that you configure the IPsec keys as hexadecimal keys for maximum key strength with Junos OS in FIPS mode.

Description Configure an IPsec security association.

Options *sa-name*—Name of the security association.

The remaining statements are explained separately.

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

spi (Junos OS)

Syntax spi *spi-value*;

Hierarchy Level [edit security ipsec security-association *sa-name* manual direction (inbound | outbound | bi-directional)]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure the security parameter index (SPI) for a security association (SA).

Options ***spi-value***—An arbitrary value that uniquely identifies which SA to use at the receiving host (the destination address in the packet).

Range: 256 through 16,639

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

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

spi (Junos-FIPS Software)

Syntax spi *spi-value*;

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

Release Information Statement introduced before Junos OS Release 7.4.

Description The security parameter index (SPI) value used for the internal Routing Engine-to-Routing Engine IPsec security association (SA) configuration.

Options ***spi-value***—Integer to use for this SPI.

Range: 256 through 16,639

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

Related Documentation

- Configuring IPsec for Enabling Internal Communications Between Routing Engines for Junos OS in FIPS Mode on page 202
- *Secure Configuration Guide for Common Criteria and Junos-FIPS*

ssh-known-hosts

Syntax

```
ssh-known-hosts {
  host host-name {
    dsa-key key;
    fetch-from-server host-name;
    load-key-file URL filename;
    rsa-key key;
    rsa1-key key;
  }
}
```

Hierarchy Level [edit security ssh-known-hosts]

Release Information Statement introduced in Junos OS Release 7.5.

Description Configure SSH support for known hosts and for administering SSH host key updates.

Options **host *host-name***—Hostname of the SSH known host entry. This option has the following suboptions:

- **dsa-key *key***—Base64 encoded Digital Signature Algorithm (DSA) key for SSH version 2.
- **fetch-from-server *host-name***—Retrieve SSH public host key information from a specified server.
- **load-key-file *filename***—Import SSH host key information from the **/var/tmp/ssh-known-hosts** file.
- **rsa-key *key***—Base64 encoded public key algorithm that supports encryption and digital signatures for SSH version 1 and SSH version 2.
- **rsa1-key *key***—Base64 encoded RSA public key algorithm, which supports encryption and digital signatures for SSH version 1.

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

Related Documentation

- Configuring SSH Host Keys for Secure Copying of Data on page 3

start-time (Authentication Key Transmission)

Syntax start-time (now | *yyyy-mm-dd.hh:mm:ss*);

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name* key *key*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Specify a start time for key transmission. You do not need to specify an end time for the key. If a new key is present with a new start time, the keychain rolls over to the new one. The start time must be unique within the keychain.

Options **now**—Start time as the current year, month, day, hour, minute, and second.

***day*days**—Start time as the specified number of days after the current day. For example, if the current day is the 12th and you configure **start-time 2day**, the start time will be on the 14th, exactly two days after the configuration is entered.

***hour*hours**—Start time as the specified number of hours after the current hour. For example, if the current hour is 9:00 and you configure **start-time 3hour**, the start time will be in 12:00, exactly three hours after the configuration is entered.

***minute*minutes**—Start time as the specified number of minutes after the current minute. For example, if the current minute is 27 minutes after the hour and you configure **start-time 5min**, the start time will be in 32 minutes after the hour, exactly five minutes after the configuration is entered.

***month*months**—Start time as the specified number of months after the current month. For example, if the current month is March and you configure **start-time 4month**, the start time will be in July, exactly four months after the configuration is entered.

***second*seconds**—Start time as the specified number of seconds after the current second. For example, if the current second is 10:20:40 and you configure **start-time 10seconds**, the start time will be 10:20:50, exactly 10 seconds after the configuration is entered.

***year*years**—Start time as the specified number of years after the current year. For example, if the current year is 2011 and you configure **start-time 1year**, the start time will be in 2012, exactly one year after the configuration is entered.

yyyy–mm-dd.hh:mm:ss—Start time in UTC (Coordinated Universal Time). The start time must be unique within the keychain.

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

tolerance

Syntax tolerance *seconds*;

Hierarchy Level [edit security authentication-key-chains key-chain *key-chain-name*]

Release Information Statement introduced in Junos OS Release 7.6.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Support for the BFD protocol introduced in Junos OS Release 9.6.
Support for the BFD protocol introduced in Junos OS Release 9.6 for EX Series switches.
Support for IS-IS introduced in Junos OS Release 11.2.

Description Configure the clock-skew tolerance for accepting keys for a key chain.

Options ***seconds***—Number of seconds to accept for clock-skew.

Default: 0 seconds

Range: 0 through 999,999,999

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

Related Documentation

- *Configuring the Authentication Key Update Mechanism for BGP and LDP Routing Protocols*
- *Example: Configuring BFD Authentication for Securing Static Routes*
- *Example: Configuring Hitless Authentication Key Rollover for IS-IS*

traceoptions

Syntax

```
traceoptions {
  file filename <files number> <size size>;
  flag all;
  flag certificates;
  flag database;
  flag general;
  flag ike;
  flag parse;
  flag policy-manager;
  flag routing-socket;
  flag timer;
  level
  no-remote-trace
}
```

Hierarchy Level

[edit security],
[edit services ipsec-vpn]

Trace options can be configured at either the **[edit security]** or the **[edit services ipsec-vpn]** hierarchy level, but not at both levels.

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description

Configure security trace options.

To specify more than one trace option, include multiple **flag** statements. Trace option output is recorded in the **/var/log/kmd** file.

NOTE: The **traceoptions**statement is not supported on QFabric systems.

Options

files ***number***—(Optional) Maximum number of trace files. When a trace file (for example, **kmd**) reaches its maximum size, it is renamed **kmd.0**, then **kmd.1**, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option.

Range: 2 through 1000 files

Default: 0 files

size ***size***—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, **kmd**) reaches this size, it is renamed, **kmd.0**, then **kmd.1** and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

Default: 1024 KB

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

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

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

Required Privilege Level

admin—To view the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- Configuring Tracing Operations for Security Services on page 241

url (Security)

Syntax url *url-name*;

Hierarchy Level [edit security pki ca-profile *ca-profile-name* enrollment],
[edit security pki ca-profile *ca-profile-name* revocation-check crl]

Release Information Statement introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Specify the certificate authority (CA) URL to use in requesting digital certificates or the URL for the Lightweight Access Directory Protocol (LDAP) location from which retrieve the certificate revocation list (CRL).

Options ***url-name***—URL of CA or URL of LDAP location of CRL.

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

Related Documentation

- Specifying an Enrollment URL on page 23
- Specifying an LDAP URL on page 24
- **crl on page 313**
- **enrollment on page 323**

validity-period

Syntax validity-period *days*;

Hierarchy Level [edit security pki auto-re-enrollment certificate-id]

Release Information Statement introduced in Junos OS Release 8.5.

Description Certificate validity period, in days, from the enrollment start date. If not specified, the issuing certificate authority (CA) sets this time as per its own policy. The start time is when auto-reenrollment is initiated.

Options ***days***—Number of days that the certificate is valid.

Range: 1 through 4095 days

Default: Per CA policy

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

Related Documentation

- Configuring the Auto-Reenrollment Properties for Automatic Renewal of the Router Certificate from the CA on page 27
- **auto-re-enrollment on page 303**

Security Services Configuration Statements

The following table lists the security services configuration statements available at the **[edit security]** hierarchy level:

Table 10: Security Services Configuration Statements

A-C	D-G	H-M	N-R	S-Z
algorithm (Authentication Keychain)	description (Authentication Keychain)	identity	options (Security)	secret
algorithm (Junos FIPS)	description (IKE policy)	ike	path-length	security-association (Junos OS)
authentication (Security IPsec)	dh-group	internal	perfect-forward-secrecy (Security)	security-association (Junos-FIPS Software)
authentication-algorithm (Security IKE)	direction (Junos OS)	ipsec (Security)	pki	spi (Junos OS)
authentication-algorithm (Security IPsec)	direction (Junos-FIPS Software)	key (Authentication Keychain)	policy (Security IKE)	spi (Junos-FIPS Software)
authentication-key-chains	dynamic	key (Junos FIPS)	policy (Security IPsec)	ssh-known-hosts
authentication-method	encoding	key-chain (Security)	pre-shared-key (Security)	start-time (Authentication Key Transmission)
auto-re-enrollment	encryption (Junos OS)	ldap-url	proposal (Security IKE)	tolerance
auxiliary-spi	encryption (Junos-FIPS Software)	lifetime-seconds (Security)	proposal (Security IPsec)	traceoptions
ca-identity	encryption-algorithm	local	proposals	url
ca-name	enrollment	local-certificate (Security)	protocol (Junos OS)	validity-period
ca-profile	enrollment-retry	local-key-pair	protocol (Junos-FIPS Software)	
cache-size	enrollment-url	manual (Junos OS)	re-enroll-trigger-time-percentage	
cache-timeout-negative	file	manual (Junos-FIPS Software)	re-generate-keypair	
certificate-id		maximum-certificates	refresh-interval	
certificates		mode (IKE)	retry (Adaptive Services Interface)	

Table 10: Security Services Configuration Statements *(continued)*

A-C	D-G	H-M	N-R	S-Z
certification-authority		mode (IPsec)	retry-interval	
challenge-password			revocation-check	
crl (Adaptive Services Interface)				
crl (Encryption Interface)				

Related Documentation

- *[edit security] Hierarchy Level*

CHAPTER 21

Operational Commands: DDoS

clear ddos-protection protocols

Syntax **clear ddos-protection protocols**
<*protocol-group* <*packet-type*>> (culprit-flows | states | statistics)

Release Information Command introduced in Junos OS Release 11.2.
Option **culprit-flows** introduced in Junos OS Release 12.3.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Clear current DDoS protection statistics, violation states, or culprit flows for all packet types in all protocol groups, for all packet types in a particular protocol group, or for a particular packet type in a particular protocol group.

Options ***protocol-group***—(Optional) Protocol group that is cleared. See show ddos-protection protocols for a list of available groups.

packet-type—(Optional) Packet type in a particular protocol group that is cleared. See show ddos-protection protocols for a list of available packet types.

culprit-flows—Clear culprit flows for a packet type, for a protocol group, or for all protocol groups. This option is not supported on QFX Series switches.

states—Clear DDoS protection violation states for a packet type, for a protocol group, or for all protocol groups.

statistics—Clear DDoS protection statistics such as packet counts and rates for a packet type, for a protocol group, or for all protocol groups.

Required Privilege Level clear

Related Documentation
- show ddos-protection protocols on page 368
- show ddos-protection statistics on page 415
- show ddos-protection version on page 418

List of Sample Output
clear ddos-protection protocols (Clear Statistics for All Protocols) on page 366
clear ddos-protection protocols (Clear Violation States for Packet Type) on page 367

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ddos-protection protocols (Clear Statistics for All Protocols)

```
user@host> clear ddos-protection protocols statistics
```

clear ddos-protection protocols (Clear Violation States for Packet Type)

```
user@host> clear ddos-protection protocols radius server states
```

show ddos-protection protocols

Syntax **show ddos-protection protocols <*protocol-group* (aggregate | *packet-type*)>**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display DDoS protection configuration and statistics for protocol groups or individual packet types.

Options **none**—Display information for all packet types in all protocol groups.

aggregate—(Optional) Display DDoS protection information for the aggregate policer. The **aggregate** option is available for all protocol groups.

packet-type—(Optional) Display DDoS protection information for the specified packet type in the protocol group. The available packet types vary by protocol group.

On QFX10000 switches, only aggregate policers are available for protocol groups that are not in the following list:

- **mcast-snoop**—The following packet types are available for the **mcast-snoop** protocol group:
  - **igmp**—Control packets for IGMP snooping.
  - **mld**—Control packets for MLD snooping.
  - **pim**—Control packets for PIM snooping.
- **radius**—The following packet types are available for the **radius** protocol group:
  - **accounting**—RADIUS accounting packets.
  - **authorization**—RADIUS authorization packets.
  - **server**—RADIUS server traffic.

On MX Series routers, T4000 routers, and EX9200 switches, only aggregate policers are available for protocol groups that are not in the following list:

- **dhcpv4**—The following packet types are available for DHCPv4 traffic:
  - **ack**—DHCPACK packets.
  - **bad-packets**—DHCPv4 packets with bad formats.
  - **bootp**—DHCPBOOTP packets.
  - **decline**—DHCPDECLINE packets.
  - **discover**—DHCDISCOVER packets.
  - **force-renew**—DHCPFORCERENEW packets.

- **inform**—DHCPINFORM packets.
- **lease-active**—DHCPLEASEACTIVE packets.
- **lease-query**—DHCPLEASEQUERYpackets.
- **lease-unassigned**—DHCPLEASEUNASSIGNED packets.
- **lease-unknown**—DHCPLEASEUNKNOWN packets.
- **nak**—DHCPNAK packets.
- **no-message-type**—DHCP packets that are missing the message type.
- **offer**—DHCOFFER packets.
- **release**—DHCPACK packets.
- **renew**—DHCPRENEW packets.
- **request**—DHCPREQUEST packets.
- **unclassified**— All unclassified packets in the protocol group.

- **dhcpv6**—The following packet types are available for DHCPv6 traffic:
  - **advertise**—ADVERTISE packets.
  - **confirm**—CONFIRM packets.
  - **decline**—DECLINE packets.
  - **information-request**—INFORMATION-REQUEST packets.
  - **leasequery**—LEASEQUERY packets.
  - **leasequery-data**—LEASEQUERY-DATA packets.
  - **leasequery-done**—LEASEQUERY-DONE packets.
  - **leasequery-reply**—LEASEQUERY-REPLY packets.
  - **rebind**—REBIND packets.
  - **reconfigure**—RECONFIGURE packets.
  - **relay-forward**—RELAY-FORWARD packets.
  - **relay-reply**—RELAY-REPLY packets.
  - **release**—RELEASE packets.
  - **renew**—RENEW packets.
  - **reply**—REPLY packets.
  - **request**—REQUEST packets.
  - **solicit**—SOLICIT packets.
  - **unclassified**— All unclassified packets in the protocol group.

- **filter-action**—The following packet types are available for unclassified firewall filter action packets, sent to the host because of reject terms in firewall filters:

- **filter-v4**—Unclassified IPv4 filter action packets.
- **filter-v6**—Unclassified IPv6 filter action packets.
- **other**—All other unclassified filter action packets that are not IPv4 or IPv6.

- **frame-relay**—The following packet types are available for Frame Relay traffic:
  - **frf15**—Multilink frame relay FRF.15 packets.
  - **frf16**—Multilink frame relay FRF.16 packets.
- **ip-fragments**—The following packet types are available for IP fragments:
  - **first-fragment**—First IP fragment.
  - **trail-fragment**—Last IP fragment.
- **ip-options**—The following packet types are available for IP option traffic:
  - **non-v4v6**—Options packets other than IPv4/v6.
  - **router-alert**—Router alert options packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **l2tp**—The following packet types are available for L2TP traffic:
  - **cdn**—Call-Disconnect-Notify message packets.
  - **hello**—Hello message packets.
  - **iccn**—Incoming-Call-Connected message packets.
  - **icrq**—Incoming-Call-Request message packets.
  - **scccn**—Start-Control-Connection-Connected message packets.
  - **sccrq**—Start-Control-Connection-Request message packets.
  - **stopccn**—Stop-Control-Connection-Notification message packets.
  - **unclassified**—All unclassified packets in the protocol group.
- **mcast-snoop**—Control traffic for multicast snooping.
  - **igmp**—Snooped IGMP traffic.
  - **pim**—Snooped PIM control traffic.
- **mlp**—The following MLP packet types are available:
  - **add**—Add requests; internal MAC address learning request packets sent to the host.
  - **delete**—Delete requests; internal MAC address learning request packets sent to the host.
  - **lookup**—Lookup requests; internal MAC address learning request packets sent to the host.
  - **unclassified**— All unclassified packets in the protocol group.

- **ndpv6**—The following packet types are available for NDPv6 traffic, except where noted, starting in 14.1R8, 14.2R8, 15.1R5, 15.1F7, and 16.1R1:
  - **invalid-hop-limit**—(Starting in 16.1R2) Invalid hop limit packets. These messages might represent crafted packets in a malicious network-based packet flood.
  - **neighbor-advertisement**—Neighbor advertisement packets. These are messages used for duplicate address detection and to test reachability of neighbors. Neighbor advertisements are sent in response to neighbor solicitation messages.
  - **neighbor-solicitation**—Neighbor solicitation packets. These are messages used for duplicate address detection and to test reachability of neighbors.
  - **redirect**—Redirect packets.
  - **router-advertisement**—Router advertisement packets. These are messages sent to announce the presence of the router, advertise prefixes, assist in address configuration, and share other link information such as MTU size and hop limit. The IPv6 nodes on the link can use this information to configure themselves with an IPv6 address and routing information such as the default gateway.
  - **router-solicitation**—Router solicitation packets. These are messages sent by IPv6 nodes when they come online to solicit immediate router advertisements from the router.
- **ppp**—The following PPP packet types are available:
  - **authentication**—PPP authentication protocol packets.
  - **echo-rep**—LCP echo reply packets.
  - **echo-req**—LCP echo request packets.
  - **ipcp**—IP Control Protocol packets.
  - **ipv6cp**—IPv6 Control Protocol packets.
  - **isis**—IS-IS packets.
  - **lcp**—Link Control Protocol packets.
  - **mlppp-lcp**—MLPPP LCP packets.
  - **mplscp**—MPLS Control Protocol packets.
  - **unclassified**— All unclassified packets in the protocol group.
- **pppoe**—The following PPPoE packet types are available:
  - **padi**—PADI packets.
  - **padm**—PADM packets.
  - **padn**—PADN packets.
  - **pado**—PADO packets.
  - **padr**—PADR packets.

    - **pads**—PADS packets.
    - **padt**—PADT packets.
- **radius**—The following RADIUS packet types are available:
    - **accounting**—RADIUS accounting packets.
    - **authorization**—RADIUS authorization packets.
    - **server**—RADIUS server traffic.
    - **unclassified**— All unclassified packets in the protocol group.
- **re-services**—The following packet type is available for Routing Engine-based HTTP redirect:
    - **captive-portal**—Routing Engine-based captive portal content delivery packets.
- **resolve**—The following packet types are available for unclassified resolve packets, which are sent to the host because of a traffic request resolve action:
    - **mcast-v4**—Unclassified IPv4 multicast resolve packets.
    - **mcast-v6**—Unclassified IPv6 multicast resolve packets.
    - **ucast-v4**—Unclassified IPv4 unicast resolve packets.
    - **ucast-v6**—Unclassified IPv6 unicast resolve packets.
    - **other**—All other unclassified resolve packets.
- **sample**—The following sample packet types are available:
    - **host**—Host packets.
    - **pfe**—Packet Forwarding Engine packets.
    - **syslog**—System log message packets.
    - **tap**—TAP packets.
- **tcp-flags**—The following TCP-flagged packet types are available:
    - **established**—TCP packets with ACK or RST flags set.
    - **initial**—TCP packets with SYN flag set and ACK flag not set.
    - **unclassified**—TCP packets with flags set any other way than the established and initial packets.
- **unclassified**—The following unclassified packet types are available:
    - **control-layer2**—Unclassified layer 2 control packets.
    - **control-v4**—Unclassified IPv4 control packets.
    - **control-v6**—Unclassified IPv6 control packets.
    - **fw-host**—Unclassified send-to-host firewall packets.

- **host-route-v4**—Unclassified IPv4 routing protocol and host packets in traffic sent to the router local interface address.
- **host-route-v6**—Unclassified IPv6 routing protocol and host packets in traffic sent to the router local interface address.
- **other**—All unclassified packets that do not belong to another type.

- **virtual-chassis**—The following packet types are available for virtual chassis packets:
  - **control-low**—Low-priority control packets.
  - **control-high**—High-priority control packets.
  - **unclassified**— All unclassified packets in the protocol group.
  - **vc-packets**—All exception packets on the virtual chassis link.
  - **vc-ttl-errors**—Virtual chassis TTL error packets.

protocol-group—(Optional) Display DDoS protection information for a protocol group. Table 11 on page 373 lists the protocol groups and the platforms they are supported on.

Table 11: Supported Protocol Groups

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
all-fiber-channel-enode	Fiber channel ENode traffic	–	X
amtv4	IPv4 AMT traffic	X	–
amtv6	IPv6 AMT traffic	X	–
ancp	ANCP traffic	X	–
ancpv6	ANCPv6 traffic	X	–
arp	ARP traffic	X	X
arp-snoop	ARP snooping traffic	–	X
atm	ATM traffic	X	–
bfd	Single-hop BFD traffic	X	X
bfdv6	BFDv6 traffic	X	X
bgp	BGP traffic	X	X
bgpv6	BGPv6 traffic	X	–
bridge-control	Bridge Control traffic	–	X

Table 11: Supported Protocol Groups *(continued)*

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
control	Control traffic	X	–
demux-autosense	Demux autosensing traffic	X	–
dhcpv4	DHCPv4 traffic	X	–
dhcpv6	DHCPv6 traffic	X	–
dhcpv4v6	DHCPv4 and DHCPv6 traffic	–	X
diameter	Diameter and Gx-Plus traffic	X	X
dns	DNS traffic	X	X
dtcp	DTCP traffic	X	X
dynamic-vlan	Dynamic VLAN exception traffic	X	–
egpv6	EGPv6 traffic	X	X
eoam	EOAM traffic	X	–
esmc	ESMC traffic	X	–
ethernet-tcc	TCC-encapsulated Ethernet traffic	–	X
fab-probe	Fab out probe packets	X	–
filter-action	IPv4 and IPv6 firewall filter action packets sent to the host because of reject terms in firewall filters	X	–
frame-relay	Frame relay traffic	X	–
ftp	FTP traffic	X	X
ftpv6	FTPv6 traffic	X	–
garp-reply	Gratuitous ARP reply traffic	–	X
gre	GRE traffic	X	X
icmp	ICMP traffic	X	X

Table 11: Supported Protocol Groups *(continued)*

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
igmp	IGMP traffic	X	X
igmpv4v6	IGMP and MLD traffic	X	–
igmpv6	MLD traffic	X	–
inline-ka	Inline service interfaces keepalive traffic	X	–
inline-svcs	Inline services traffic	X	–
ip-fragments	IP fragments traffic	X	–
ip-options	IP traffic with IP packet header options	X	X
isis	IS-IS traffic	X	X
iso-tcc	TCC-encapsulated ISO traffic	–	X
jfm	JFM traffic	X	–
l2tp	Layer 2 protocol tunneling traffic	X	X
lacp	LACP traffic	X	X
ldp	LDP traffic	X	X
ldp-hello	LDP hello packets	–	X
ldpv6	LDPv6 traffic	X	–
lldp	LLDP traffic	X	X
lmp	LMP traffic	X	X
lmpv6	LMPv6 traffic	X	–
mac-host	Layer 2 MAC send-to-host traffic	X	–
martian-address	Martian address	–	–
mcast-snoop	Control traffic for multicast snooping	X	X

Table 11: Supported Protocol Groups *(continued)*

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
mld	MLD traffic	–	X
mlp	MLP traffic	X	–
msdp	MSDP traffic	X	X
multihop-bfd	Multihop BFD traffic	–	X
mld	MLD traffic	–	X
msdpv6	MSDPv6 traffic	X	–
multicast-copy	Host copy traffic due to multicast routing	X	–
mvrp	MVRP traffic	X	–
ndpv6	NDPv6 traffic	X	X
ntp	NTP traffic	X	X
oam-cfm	OAM CFM traffic	–	X
oam-lfm	OAM LFM traffic	X	X
ospf	OSPF traffic	X	X
ospf-hello	OSPF hello packets	–	X
ospfv3v6	OSPFv3/IPv6 traffic	X	–
pfe-alive	Packet Forwarding Engine keepalive traffic	X	–
pim	PIM traffic	X	–
pim-ctrl	PIM control packets	–	X
pim-data	PIM data	–	X
pimv6	PIMv6 traffic	X	–
pmvrp	PMVRP traffic	X	–
pos	POS traffic	X	–

Table 11: Supported Protocol Groups *(continued)*

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
ppp	PPP traffic	X	–
pppoe	PPPoE traffic	X	–
proto-802-1x	802.1X traffic	–	X
ptp	PTP traffic	X	X
pvstp	PVSTP traffic	X	X
radius	RADIUS traffic	X	X
re-services	Captive portal content delivery traffic for Routing Engine HTTP redirect	X	–
redirect	Traffic that triggers ICMP redirects	X	–
reject	Packets rejected by a next-hop forwarding decision	X	X
rejectv6	IPv6 packets rejected by a next-hop forwarding decision	X	–
resolve	Unclassified IPv4 and IPv6 resolve packets sent to the host because of a traffic request resolve action	X	X
rip	RIP traffic	X	X
ripv6	RIPv6 traffic	X	–
rsvp	RSVP traffic	X	X
rsvpv6	RSVPv6 traffic	X	–
snmp	SNMP traffic	X	X
snmpv6	SNMPv6 traffic	X	–
ssh	SSH traffic	X	X
sshv6	SSHv6 traffic	X	–
stp	STP traffic	X	X

Table 11: Supported Protocol Groups *(continued)*

Protocol Group	Description	MX Series Routers, T4000 Routers, EX9200 Switches	QFX10000 Switches
syslog	System log messages UDP traffic on port 6333 for the Routing Engine syslog server	X	–
tacacs	TACACS+ traffic	--	X
tcp-flags	Traffic with TCP flags	X	–
telnet	Telnet traffic	X	X
telnetv6	Telnetv6 traffic	X	–
ttl	Time to Live packets	X	X
tunnel-fragment	Tunnel fragments traffic	X	–
tunnel-ka	Tunnel keepalive traffic	X	–
unclassified	Unclassified traffic	X	–
virtual-chassis	Virtual chassis traffic	X	–
vrrp	VRRP traffic	X	X
vrrpv6	VRRPv6 traffic	X	–

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols culprit-flows on page 388
- show ddos-protection protocols flow-detection on page 392
- show ddos-protection protocols parameters on page 396
- show ddos-protection protocols statistics on page 403
- show ddos-protection protocols violations on page 413

List of Sample Output

show ddos-protection protocols on page 383
show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled) on page 385
show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic) on page 386

show ddos-protection protocols (Specific Packet Type with Bandwidth Violation) on page 386

Output Fields Table 12 on page 379 lists the output fields for the **show ddos-protection protocols** command. Output fields are listed in the approximate order in which they appear.

Table 12: show ddos-protection protocols Output Fields

Field Name	Field Description
Packet types	Number of packet types
Modified	Number of packets for which policer values have been modified from the default.
Received traffic	Number of traffic flows received.
Currently violated	Number of flows that are currently violating the flow bandwidth limit.
Currently tracked flows	Number of active flows that are being tracked as culprit flows by flow detection.
Total detected flows	Total number of culprit flows that have been detected, including those that have recovered or timed out.
Protocol Group	Name of protocol group.
Packet type	Name of packet type in protocol group.
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared.
Priority	Priority of the packet type for individual packet policers that enables more important traffic to pass through in the event of traffic congestion: **low**, **medium**, or **high**. Lower priority packets can be dropped when insufficient bandwidth is available.
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires.

Table 12: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Enabled	State of the policer: • **Yes**—The policer is enabled on both the Routing Engine and the FPC (line card). This is the default state. • **No**—The policer is disabled on both the Routing Engine and the FPC by global configuration. It is not disabled by the packet type level configuration. • **No***—The policer is disabled on both the Routing Engine and the FPC. The asterisk (*) indicates that one or both of these instances is disabled at the packet type level; it may also be disabled globally. • **Partial**—The policer is disabled on either the Routing Engine or the FPC, but not both. It is disabled by global configuration. It is not disabled by the packet type level configuration. • **Partial***—The policer is disabled on either the Routing Engine or the FPC, but not both. The asterisk (*) indicates that the instance is disabled by the packet type level configuration; it may also be disabled globally. Disabling can occur globally for all packet types at the **[edit system ddos-protection global]** hierarchy level, for a specific packet type at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*]** hierarchy level, or at both levels.
Bypass aggregate	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. This field appears only for individual policers.
Flow detection configuration	State of flow detection configured on the router: • Detection mode—Mode of operation for suspicious flow detection: automatic, off, or on. • Log flows—State of automatic logging of suspicious traffic flows: on (**Yes**) or off (**No**). • Timeout flows—State of culprit flow timeout behavior: flow is suppressed for a configured timeout period (**Yes**) or flow is suppressed until it is no longer in violation (**No**). • Detect time—Time in seconds that must pass before a suspicious flow that has exceeded the bandwidth allowed for the packet type is considered to be a culprit flow. • Recover time—Time in seconds that must pass before a culprit flow is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation. • Timeout time—Time in seconds that a culprit flow is suppressed, if timeouts have been enabled. • Flow aggregation level configuration—Flow detection mode, flow control mode, and flow bandwidth for traffic at each of the traffic flow aggregation levels: subscriber, logical interface, and physical interface. ◦ Detection mode—State of flow detection: automatic, off, or on. Control mode—Mode of controlling culprit traffic: dropped, kept, or policed back to within the allowed bandwidth. Flow rate—Bandwidth allowed for the control traffic in packets per second.

Table 12: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
System-wide information	The following information collected for the router: • A message indicates whether the policer has been violated. • No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. • No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at all card slots and the Routing Engine. • Dropped—Number of packets dropped regardless of where they were dropped. • Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. • Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.

Routing Engine information	The following information collected for the Routing Engine:
	• Bandwidth—Maximum number of packets per second that is allowed.
	• Burst—Maximum number of packets that is allowed in a burst.
	• State of the policer:
	  • **enabled**—The Routing Engine policer is enabled. This is the default state.
	  • **disabled**—The Routing Engine policer is disabled globally. It is not disabled by the packet type level configuration.
	  • **disabled***—The Routing Engine policer is disabled by the packet type level configuration; it may also be disabled globally.
	• A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value.
	• Violation first detected at—Timestamp of the first violation.
	• Violation last seen at—Timestamp of the last observed violation.
	• Duration of violation—Length of the violation.
	• Number of violations—Number of times the violation has occurred.
	• Received—Number of packets received at the Routing Engine from all cards.
	• Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers.
	• Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards.
	• Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards.
	• Dropped by aggregate policer—Number of packets dropped by the aggregate policer.
	• Dropped by individual policers—Number of packets dropped by individual policer.

Table 12: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description

FPC slot information	The following information collected for the card in the indicated slot:
	• Bandwidth—Bandwidth scaling percentage and the number of packets per second that is allowed before a violation is declared.
	• Burst—Burst scaling percentage and the maximum number of packets that is allowed in a burst before a violation is declared.
	• State of the policer:
	  ◦ **enabled**—The FPC policer is enabled. This is the default state.
	  ◦ **disabled**—The FPC policer is disabled globally. It is not disabled by the packet type level configuration.
	  ◦ **disabled***—The FPC policer is disabled by the packet type level configuration; it may also be disabled globally.
	• A message indicates whether the policer has been violated.
	• Violation first detected at—Timestamp of the first violation.
	• Violation last seen at—Timestamp of the last observed violation.
	• Duration of violation—Length of the violation.
	• Number of violations—Number of times the violation has occurred.
	• Received—Number of packets received on the line card.
	• Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers.
	• Arrival rate—Current traffic rate for packets arriving at the line card.
	• Max arrival rate—Highest traffic rate for packets arriving at the line card.
	• Dropped by this policer—Number of packets dropped by the individual policer.
	• Dropped by aggregate policer—Number of packets dropped by the aggregate policer.
	NOTE: On MX Series routers with built-in MPCs—the MX5, MX10, MX40, MX80, and MX104 routers—this field actually displays information for tfeb0 because these routers have no Flexible PIC Concentrator (FPC) slots. Instead, the Packet Forwarding Engine has two “pseudo” FPCs (FPC 0 and FPC1).

Bypass aggr.	State of the bypass aggregate configuration: • Yes—The aggregate policer configuration is bypassed. • No—The aggregate policer configuration is enforced. Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.
FPC Mod	Indicates whether configuration has changed from the default for any line cards. • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type
Op mode	Mode of operation for suspicious flow detection for the packet type: always-on (**on**), (**auto**), or disabled (**off**).

Table 12: show ddos-protection protocols Output Fields *(continued)*

Field Name	Field Description
Policer BW (pps)	Bandwidth policer value; number of packets per second that is allowed before a violation is declared.
Aggr level Op:Fc:Bwidth (pps)	Flow operation mode, flow control mode, and flow bandwidth for traffic of the packet type at each traffic flow aggregation level: subscriber (**sub**), logical interface (**ifl**), and physical interface (**ifd**).
Log flow	State of automatic logging of suspicious traffic flows for the packet type: on (**Yes**) or off (**No**).
Time out	State of culprit flow timeout behavior for the packet type: flow is suppressed or monitored for a configured timeout period (**Yes**) or flow is suppressed or monitored until it is no longer in violation (**No**).

Sample Output

show ddos-protection protocols

```
user@host> show ddos-protection protocols

Packet types: 190, Modified: 0, Received traffic: 12, Currently violated: 3
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: IPv4-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:        2000 pps
      Burst:            10000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 2000 pps, Burst: 10000 packets, enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Bandwidth: 100% (2000 pps), Burst: 100% (10000 packets), enabled
      Aggregate policer is never violated
```

```
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0

…

Protocol Group: PPPoE

  Packet type: aggregate (Aggregate for all PPPoE control traffic)
    Aggregate policer configuration:
      Bandwidth:        2000 pps
      Burst:            2000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 2000 pps, Burst: 2000 packets, enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Bandwidth: 100% (2000 pps), Burst: 100% (2000 packets), enabled
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
        Dropped by flow suppression:    0

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
```

```
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Bandwidth: 500 pps, Burst: 500 packets, enabled
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
      Dropped by flow suppression:  0
...
```

show ddos-protection protocols (Specific Packet Type with Flow Detection Disabled)

```
user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Off*       Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
```

show ddos-protection protocols (Specific Packet Type with Flow Detection Enabled and Automatic)

```
user@host> show ddos-protection protocols pppoe padi
Currently tracked flows: 0, Total detected flows: 0
* = User configured value

Protocol Group: PPPoE

  Packet type: padi (PPPoE PADI)
    Individual policer configuration:
      Bandwidth:        500 pps
      Burst:            500 packets
      Priority:         Low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          500 pps
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Bandwidth: 500 pps, Burst: 500 packets, enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
        Dropped by flow suppression:  0
```

show ddos-protection protocols (Specific Packet Type with Bandwidth Violation)

```
user@host> show ddos-protection protocols bfd
Packet types: 1, Modified: 0, Received traffic: 1, Currently violated: 1
Currently tracked flows: 1, Total detected flows: 1
* = User configured value

Protocol Group: BFD

  Packet type: aggregate (Aggregate for all bfd traffic)
    Aggregate policer configuration:
      Bandwidth:        20000 pps
      Burst:            20000 packets
      Recover time:     300 seconds
      Enabled:          Yes
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
```

```
  Timeout flows:  No         Timeout time: 300 seconds
  Flow aggregation level configuration:
    Aggregation level   Detection mode  Control mode  Flow rate
    Subscriber          Automatic       Drop          10 pps
    Logical interface   Automatic       Drop          10 pps
    Physical interface  Automatic       Drop          20000 pps
System-wide information:
  Aggregate bandwidth is being violated!
    No. of FPCs currently receiving excess traffic: 1
    No. of FPCs that have received excess traffic:  1
    Violation first detected at: 2012-10-24 23:40:20 EDT
    Violation last seen at:      2012-10-25 10:25:48 EDT
    Duration of violation: 10:45:28 Number of violations: 1
  Received:  1173471731          Arrival rate:     30304 pps
  Dropped:   399135607           Max arrival rate: 30331 pps
  Flow counts:
    Aggregation level     Current       Total detected
    Subscriber            1             1
    Total                 1             1
Routing Engine information:
  Bandwidth: 20000 pps, Burst: 20000 packets, enabled
  Aggregate policer is never violated
  Received:  366831604           Arrival rate:     0 pps
  Dropped:   0                   Max arrival rate: 9522 pps
    Dropped by individual policers: 0
FPC slot 1 information:
  Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled
  Aggregate policer is currently being violated!
    Violation first detected at: 2012-10-24 23:40:21 EDT
    Violation last seen at:      2012-10-25 10:25:48 EDT
    Duration of violation: 10:45:27 Number of violations: 1
  Received:  1173471731          Arrival rate:     30304 pps
  Dropped:   399135607           Max arrival rate: 30331 pps
    Dropped by individual policers: 0
    Dropped by aggregate policer:   398854530
    Dropped by flow suppression:    281077
  Flow counts:
    Aggregation level     Current       Total detected   State
    Subscriber            1             1                Active
    Logical-interface     0             0                Active
    Physical-interface    0             0                Active
    Total                 1             1
```

show ddos-protection protocols culprit-flows

Syntax **show ddos-protection protocols <*protocol-group* (aggregate | *packet-type*)> culprit-flows**

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

Description Display culprit flow information for protocol groups or individual packet types.

Options **none**—Display information for all protocol groups and packet types.

brief | detail —(Optional) Display the specified level of output.

fpc-slot—(Optional) Display information for the specified Flexible PIC Concentrator (FPC) slot.

Default: system-wide, that is; include all the FPC slots.

Range: 0 through 2

summary—(Optional) Display flow information summary.

aggregate—(Optional) Display DDoS protection information for the aggregate policer. The **aggregate** option is available for all protocol groups.

packet-type—(Optional) Display information for the specified packet type in the protocol group. The available packet types vary by protocol group.

See show ddos-protection protocols for a list of available packet types.

protocol-group—(Optional) Display information for a particular protocol group.

See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection protocols flow-detection on page 392
- show ddos-protection protocols parameters on page 396
- show ddos-protection protocols statistics on page 403
- show ddos-protection protocols violations on page 413

List of Sample Output

show ddos-protection protocols culprit-flows brief on page 389
show ddos-protection protocols culprit-flows summary on page 390
show ddos-protection protocols culprit-flows detail(Specific Protocol Group) on page 390
show ddos-protection protocols culprit-flows fpc-slot on page 390

Output Fields Table 13 on page 389 lists the output fields for the **show ddos-protection protocols culprit-flows** command. Output fields are listed in the approximate order in which they appear.

Table 13: show ddos-protection protocols culprit-flows Output Fields

Field Name	Field Description	Level of Output
Currently tracked flows	Number of active flows that are being tracked as culprit flows by flow detection.	All levels
Total detected flows	Total number of culprit flows that have been detected, including those that have recovered or timed out.	All levels
Protocol Group	Name of protocol group.	**detail**
Packet type	Name of packet type in protocol group.	**detail**
Arriving Interface	Logical interface on which the traffic flow arrived.	**detail**
Source Address MAC or IP	Source address of the traffic flow, either a MAC address or an IP address.	**detail**
Destination Address MAC or IP	Destination address of the traffic flow, either a MAC address or an IP address.	**detail**
Source Port	Source port number.	**detail**
Destination Port	Destination port number.	**detail**
pps	Rate of the traffic flow in packets per second.	**brief**
Rate	Rate of the traffic flow in packets per second.	**detail**
pkts	Number of packets received in the traffic flow.	**brief**
received packets	Number of packets received in the traffic flow.	**detail**
Additional information	Flow ID numbers automatically assigned to flow, with embedded slot ID. The flow ID is prefixed by **sub**, **ifl**, or **ifd**, which indicate the subscriber, logical interface, and physical interface flow aggregation levels. Timestamp that identifies when the flow arrived on the interface.	**detail**

Sample Output

show ddos-protection protocols culprit-flows brief

```
user@host> show ddos-protection protocols culprit-flows brief
Currently tracked flows: 1000, Total detected flows: 1000
Protocol Packet Arriving Source Address
group type Interface MAC or IP
ndpv6 router-adv ge-1/1/0.0
```

```
2001:db8::03d4 sub:0001000000000384 2015-03-13 00:21:07 PDT pps:72 pkts:547072
ndpv6 router-adv ge-1/1/0.0
2001:db8::013f
sub:0001000000000385 2015-03-13 00:21:07 PDT pps:72 pkts:552704
ndpv6 router-adv ge-1/1/0.0
2001:db8::02e4
sub:0001000000000386 2015-03-13 00:21:07 PDT pps:72 pkts:726784
ndpv6 router-adv ge-1/1/0.0
2001:0db8::0102
 sub:0001000000000387 2015-03-13 00:21:07 PDT pps:72 pkts:762880
```

show ddos-protection protocols culprit-flows summary

```
user@host> show ddos-protection protocols ndpv6 culprit-flows summary
Currently tracked flows: 2, Total detected flows: 2
```

```
user@host> show ddos-protection protocols pppoe culprit-flows summary
Currently tracked flows: 2, Total detected flows: 2
```

show ddos-protection protocols culprit-flows detail (Specific Protocol Group)

```
user@host> show ddos-protection protocols pppoe culprit-flows detail
Currently tracked flows: 1, Total detected flows: 1000
Protocol Packet Arriving Aggr Flow Id
group type Interface level
pppoe padi ge-1/1/0.1 sub 0001000000000022
Ethertype: 0x0 outer-vlan: 100 inner-vlan: ---
Source Address: 2001:db8::02
Destination Address: 2001:db8::FF
Found at: 2014-10-07 07:11:27 PDT
Last Violation: 2014-10-07 07:43:24 PDT
Rate: 9995 pps received packets: 18546724
```

```
user@host> show ddos-protection protocols icmp aggregate culprit-flows detail
Currently tracked flows: 1, Total detected flows: 1
Protocol Packet Arriving Aggr Flow Id
group type Interface level
icmp aggregate ge-1/1/0.3 sub 0001000000000003
Source Address: 192.0.2.2
Destination Address: 198.51.100.111
Type: 15 Code: 0
Found at: 2014-10-23 12:06:14 PDT
Last Violation: 2014-10-23 12:06:27 PDT
Rate: 25000 pps received packets: 384112
```

```
user@host> show ddos-protection protocols ndpv6 culprit-flows detail
Currently tracked flows: 1, Total detected flows: 1
Protocol Packet Arriving Aggr Flow Id
group type Interface level
ndpv6 router-sol ge-1/1/0.2 sub 0001000000000001
Source Address: 2001:db8::03
Destination Address: 2001:0db8::0111
Type: 133 Code: 0
Found at: 2014-10-23 11:55:20 PDT
Last Violation: 2014-10-23 11:55:21 PDT
Rate: 30000 pps received packets: 43469
```

show ddos-protection protocols culprit-flows fpc-slot

```
user@host> show ddos-protection protocols ndpv6 culprit-flows fpc-slot 1
Currently tracked flows: 2, Total detected flows: 2
```

show ddos-protection protocols flow-detection

Syntax **show ddos-protection protocols <*protocol-group*> flow-detection <brief | detail | terse>**

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

Description Display flow detection information for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups.

protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection protocols culprit-flows on page 388
- show ddos-protection protocols parameters on page 396
- show ddos-protection protocols statistics on page 403
- show ddos-protection protocols violations on page 413

List of Sample Output show ddos-protection protocols flow-detection on page 394
show ddos-protection protocols flow-detection brief (Parameters for a Specific Protocol) on page 395

Output Fields Table 14 on page 393 lists the output fields for the **show ddos-protection protocols flow-detection** command. Output fields are listed in the approximate order in which they appear.

Table 14: show ddos-protection protocols flow-detection Output Fields

Field Name	Field Description	Level of Output
Packet types	Number of packet types.	All levels
Modified	Number of packets for which policer values have been modified from the default.	All levels
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
Flow detection configuration	Configuration of flow detection at the packet level.	**detail** none
Detection mode or **Op mode**	Mode of operation for flow detection at the packet level: • **Automatic** or **a**—Search flows only when a policer is being violated. • **Off** or **x**—Never search flows even when a policer is being violated. • **On** or **o**—Search flows even when no policer is being violated.	All levels
Policer BW (pps)	Bandwidth allowed at the packet level.	**brief terse**
Detect time	Time in seconds that a suspicious flow that has exceeded the bandwidth allowed for the packet type must remain in violation to be confirmed as a culprit flow.	**detail** none
Log flows or **Log flow**	State of automatic logging of suspicious traffic flows for the packet type: on (**Yes**) or off (**No**).	All levels
Recover time	Time in seconds that must pass before a culprit flow for the packet type is considered to have returned to normal. The period starts when the flow drops below the threshold that triggered the last violation.	**detail** none
Timeout flows or **Time out**	State of timeout enabling for culprit flows: • **Yes**—Enabled; flows can time out (released from suppression) when a timeout period expires, regardless of whether flow is still in violation. • **No**—Disabled; flows are not allowed to time out.	All levels
Timeout time	Time in seconds that a culprit flow is suppressed. On expiration, the flow times out even if it is still violating the bandwidth limit.	**detail** none
Flow aggregation level configuration	Configuration of flow detection for each flow aggregation level.	**detail** none
Aggregation level or **Agg level**	One of three levels of flow aggregation • **Subscriber** or **sub** • **Logical interface** or **ifl** • **Physical interface** or **ifd**	All levels

Table 14: show ddos-protection protocols flow-detection Output Fields *(continued)*

Field Name	Field Description	Level of Output
Detection mode or **Op**	Mode of operation for flow detection at the flow aggregation level: • **Automatic**—Search flows only when a policer is being violated. • **Off**—Never search flows even when a policer is being violated. • **On**—Search flows even when no policer is being violated.	All levels
Control mode or **Fc**	Mode by which traffic in a culprit flow is handled. • **drop**—Drop all traffic in flow. • **keep**—Keep all traffic in flow. • **police**—Police the traffic to within its allowed bandwidth.	All levels
Flow rate or BWidth (pps)	Bandwidth allowed at the flow aggregation level.	**brief terse**

Sample Output

show ddos-protection protocols flow-detection

```
user@host> show ddos-protection protocols flow-detection
Packet types: 190, Modified: 2
* = User configured value

Protocol Group: IPv4-Unclassified

  Packet type: aggregate
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps


Protocol Group: IPv6-Unclassified

  Packet type: aggregate
    Flow detection configuration:
      Detection mode: Automatic  Detect time:  3 seconds
      Log flows:      No         Recover time: 60 seconds
      Timeout flows:  No         Timeout time: 300 seconds
      Flow aggregation level configuration:
        Aggregation level   Detection mode  Control mode  Flow rate
        Subscriber          Automatic       Drop          10 pps
        Logical interface   Automatic       Drop          10 pps
        Physical interface  Automatic       Drop          2000 pps

...
```

show ddos-protection protocols flow-detection brief (Parameters for a Specific Protocol)

```
user@host> show ddos-protection protocols dhcpv4 flow-detection brief
Packet types: 19, Modified: 1
* = User configured value

Detection mode(Op): a = automatic    Flow control mode(Fc): d = drop
                    o = on                                  k = keep
                    x = off                                 p = police

Protocol    Packet      Op   Policer  Aggr level Op:Fc:BWidth(pps)   Log  Time
group       type        mode BW(pps)  sub       ifl       ifd        flow out
dhcpv4      aggregate   auto 5000     a:d:10    a:d:10    a:d:5000   No   No
dhcpv4      unclass..   auto 300      a:d:10    a:d:10    a:d:300    No   No
dhcpv4      discover    auto 777*     a:d:10    a:d:10    a:d:500    No   No
dhcpv4      offer       auto 1000     a:d:10    a:d:10    a:d:1000   No   No
dhcpv4      request     auto 1000     a:d:10    a:d:10    a:d:1000   No   No
dhcpv4      decline     auto 500      a:d:10    a:d:10    a:d:500    No   No
dhcpv4      ack         auto 500      a:d:10    a:d:10    a:d:500    No   No
dhcpv4      nak         auto 500      a:d:10    a:d:10    a:d:500    No   No
dhcpv4      release     auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      inform      auto 500      a:d:10    a:d:10    a:d:500    No   No
dhcpv4      renew       auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      forcerenew  auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      leasequery  auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      leaseuna..  auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      leaseunk..  auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      leaseact..  auto 2000     a:d:10    a:d:10    a:d:2000   No   No
dhcpv4      bootp       auto 300      a:d:10    a:d:10    a:d:300    No   No
dhcpv4      no-msgtype  auto 0        a:d:10    a:d:10    a:d:0      No   No
dhcpv4      bad-pack..  auto 0        a:d:10    a:d:10    a:d:0      No   No
```

show ddos-protection protocols parameters

Syntax **show ddos-protection protocols <*protocol-group*> parameters <brief | detail | terse>**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display DDoS protection configuration information for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups—groups that show traffic in the **Received (packets)** column.

protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection protocols culprit-flows on page 388
- show ddos-protection protocols flow-detection on page 392
- show ddos-protection protocols statistics on page 403
- show ddos-protection protocols violations on page 413

List of Sample Output

show ddos-protection protocols parameters on page 398
show ddos-protection protocols parameters brief on page 399
show ddos-protection protocols dhcpv4 parameters brief on page 400
show ddos-protection protocols dhcpv4 parameters terse on page 401
show ddos-protection protocols dhcpv4 parameters on page 401

Output Fields Table 15 on page 397 lists the output fields for the **show ddos-protection protocols parameters** command. Output fields are listed in the approximate order in which they appear.

Table 15: show ddos-protection protocols parameters Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
Bandwidth	Bandwidth policer value; number of packets per second that is allowed before a violation is declared. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Burst	Burst policer value; the maximum number of packets that is allowed in a burst before a violation is declared. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Priority	Priority of the packet type in the event of traffic congestion: **low**, **medium**, or **high**. Lower priority packets can be dropped when insufficient bandwidth is available. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Recover time	Time that must pass since the last violation before the traffic flow is considered to have recovered from the attack. A notification is generated when the timer expires. In the **brief** output, an asterisk indicates the value has been modified from the default.	All levels
Enabled	State of the policer, enabled (**Yes**) or disabled (**No**).	**detail** none
Bypass aggregate	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. This field appears only for individual policers.	**detail** none
FPC slot information	The following configuration information for the card in the indicated slot: • Bandwidth—Bandwidth scale and the number of packets per second that is allowed before a violation is declared • Burst—Burst scale and the maximum number of packets that is allowed in a burst before a violation is declared • **enabled** or **disabled**—State of the line card policer	**detail** none

Table 15: show ddos-protection protocols parameters Output Fields *(continued)*

Field Name	Field Description	Level of Output
Number of policers modified	Number of policers that have been changed from the default configuration. An asterisk by a particular value indicates that value has been modified.	**brief terse**
Policer Enabled	State of the policer, enabled (**Yes**), disabled (**No**), or partially disabled (**part.**); **part.** indicates that only some of the policer instances are disabled for the policer.	**brief terse**
Bypass aggr.	State of the bypass aggregate configuration: • Yes—The aggregate policer is bypassed. • No—The aggregate policer is enforced. Dashes indicate that the bypass aggregate configuration is not available; this is possible only for aggregate policers.	**brief terse**
FPC Mod	Indicates whether configuration has changed from the default for any line cards. • No—The default configuration has not changed from the default for the packet type. • Yes—The default configuration has changed from the default for the packet type	**brief terse**

Sample Output

show ddos-protection protocols parameters

```
user@host> show ddos-protection protocols parameters
Protocol Group: IPv4-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:        20000 pps
      Burst:            20000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
    FPC slot 1 information:
      Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

Protocol Group: IPv6-Unclassified

  Packet type: aggregate (Aggregate for unclassified host-bound IPv6 traffic)
    Aggregate policer configuration:
      Bandwidth:        20000 pps
      Burst:            20000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
    FPC slot 1 information:
      Bandwidth: 100% (20000 pps), Burst: 100% (20000 packets), enabled

...

Protocol Group: PPPoE
```

```
Packet type: aggregate (Aggregate for all PPPoE control traffic)
  Aggregate policer configuration:
    Bandwidth:        800 pps
    Burst:            2000 packets
    Priority:         medium
    Recover time:     300 seconds
    Enabled:          Yes
  FPC slot 1 information:
    Bandwidth: 100% (800 pps), Burst: 100% (2000 packets), enabled

Packet type: padi (PPPoE PADI)
  Individual policer configuration:
    Bandwidth:        500 pps
    Burst:            500 packets
    Priority:         low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  FPC slot 1 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled

Packet type: pado (PPPoE PADO)
  Individual policer configuration:
    Bandwidth:        0 pps
    Burst:            0 packets
    Priority:         low
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  FPC slot 1 information:
    Bandwidth: 100% (0 pps), Burst: 100% (0 packets), enabled

Packet type: padr (PPPoE PADR)
  Individual policer configuration:
    Bandwidth:        500 pps
    Burst:            500 packets
    Priority:         medium
    Recover time:     300 seconds
    Enabled:          Yes
    Bypass aggregate: No
  FPC slot 1 information:
    Bandwidth: 100% (500 pps), Burst: 100% (500 packets), enabled
```

show ddos-protection protocols parameters brief

```
user@host> show ddos-protection protocols parameters brief
Number of policers modified: 3
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
ipv4-uncls  aggregate   20000     20000  medium   300       yes     --     no
ipv6-uncls  aggregate   20000     20000  medium   300       yes     --     no
dynvlan     aggregate   1000      500    low      300       yes     --     no
ppp         aggregate   16000     16000  medium   300       yes     --     no
ppp         unclass     1000      500    low      300       yes     no     no
ppp         lcp         12000     12000  low      300       yes     no     no
ppp         auth        2000      2000   medium   300       yes     no     no
ppp         ipcp        2000      2000   high     300       yes     no     no
ppp         ipv6cp      2000      2000   high     300       yes     no     no
ppp         mplscp      2000      2000   high     300       yes     no     no
ppp         isis        2000      2000   high     300       yes     no     no
```

```
pppoe       aggregate   800*      2000    medium   300       part.*  --      no
pppoe       padi        500       500     low      300       part.   no      no
pppoe       pado        0         0       low      300       part.   no      no
pppoe       padr        500       500     medium   300       part.   no      no
pppoe       pads        0         0       low      300       part.   no      no
pppoe       padt        1000      1000    high     300       part.   no      no
pppoe       padm        0         0       low      300       part.   no      no
pppoe       padn        0         0       low      300       part.   no      no
dhcpv4      aggregate   669*      5000    medium   300       yes     --      no
dhcpv4      unclass..   300       150     low      300       yes     no      no
dhcpv4      discover    100*      500     low      300       yes     no      no
dhcpv4      offer       1000      1000    low      300       yes     no      no
dhcpv4      request     1000      1000    medium   300       yes     no      no
dhcpv4      decline     500       500     low      300       yes     no      no
dhcpv4      ack         500       500     medium   300       yes     no      no
dhcpv4      nak         500       500     low      300       yes     no      no
dhcpv4      release     2000      2000    high     300       yes     no      no
dhcpv4      inform      500       500     low      300       yes     no      no
dhcpv4      renew       2000      2000    high     300       yes     no      no
dhcpv4      forcerenew  2000      2000    high     300       yes     no      no
dhcpv4      leasequery  2000      2000    high     300       yes     no      no
dhcpv4      leaseuna..  2000      2000    high     300       yes     no      no
dhcpv4      leaseunk..  2000      2000    high     300       yes     no      no
dhcpv4      leaseact..  2000      2000    high     300       yes     no      no
dhcpv4      bootp       300       300     low      300       yes     no      no
dhcpv4      no-msgtype  0         0       low      300       yes     no      no
dhcpv4      bad-pack..  0         0       low      300       yes     no      no

...

icmp        aggregate   20000     20000   high     300       yes     --      no
igmp        aggregate   20000     20000   high     300       yes     --      no
ospf        aggregate   20000     20000   high     300       yes     --      no
rsvp        aggregate   20000     20000   high     300       yes     --      no
pim         aggregate   20000     20000   high     300       yes     --      no
rip         aggregate   20000     20000   high     300       yes     --      no
ptp         aggregate   20000     20000   high     300       yes     --      no
bfd         aggregate   20000     20000   high     300       yes     --      no
lmp         aggregate   20000     20000   high     300       yes     --      no
ldp         aggregate   20000     20000   high     300       yes     --      no
msdp        aggregate   20000     20000   high     300       yes     --      no
bgp         aggregate   20000     20000   low      300       yes     --      no
vrrp        aggregate   20000     20000   high     300       yes     --      no
telnet      aggregate   20000     20000   low      300       yes     --      no
ftp         aggregate   20000     20000   low      300       yes     --      no
ssh         aggregate   20000     20000   low      300       yes     --      no
snmp        aggregate   20000     20000   low      300       yes     --      no
ancp        aggregate   20000     20000   low      300       yes     --      no

...
```

show ddos-protection protocols dhcpv4 parameters brief

```
user@host> show ddos-protection protocols dhcpv4 parameters brief
Number of policers modified: 2
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
dhcpv4      aggregate   669*      5000   medium   300       yes     --     no
dhcpv4      unclass..   300       150    low      300       yes     no     no
dhcpv4      discover    100*      500    low      300       yes     no     no
dhcpv4      offer       1000      1000   low      300       yes     no     no
```

```
dhcpv4      request     1000      1000    medium   300       yes     no      no
dhcpv4      decline     500       500     low      300       yes     no      no
dhcpv4      ack         500       500     medium   300       yes     no      no
dhcpv4      nak         500       500     low      300       yes     no      no
dhcpv4      release     2000      2000    high     300       yes     no      no
dhcpv4      inform      500       500     low      300       yes     no      no
dhcpv4      renew       2000      2000    high     300       yes     no      no
dhcpv4      forcerenew  2000      2000    high     300       yes     no      no
dhcpv4      leasequery  2000      2000    high     300       yes     no      no
dhcpv4      leaseuna..  2000      2000    high     300       yes     no      no
dhcpv4      leaseunk..  2000      2000    high     300       yes     no      no
dhcpv4      leaseact..  2000      2000    high     300       yes     no      no
dhcpv4      bootp       300       300     low      300       yes     no      no
dhcpv4      no-msgtype  0         0       low      300       yes     no      no
dhcpv4      bad-pack..  0         0       low      300       yes     no      no
```

show ddos-protection protocols dhcpv4 parameters terse

```
user@host> show ddos-protection protocols dhcpv4 parameters terse
Number of policers modified: 2
Protocol    Packet      Bandwidth Burst  Priority Recover   Policer Bypass FPC
group       type        (pps)     (pkts)         time(sec) enabled aggr.  mod
dhcpv4      aggregate   669*      5000   medium   300       yes     --     no
dhcpv4      discover    100*      500    low      300       yes     no     no
```

show ddos-protection protocols dhcpv4 parameters

```
user@host> show ddos-protection protocols dhcpv4 parameters
Protocol Group: DHCPv4

  Packet type: aggregate (aggregate for all DHCPv4 traffic)
    Aggregate policer configuration:
      Bandwidth:          669 pps
      Burst:              5000 packets
      Priority:           medium
      Recover time:       300 seconds
      Enabled:            Yes
    FPC slot 1 information:
      Bandwidth: 100% (669 pps), Burst: 100% (5000 packets), enabled

  Packet type: unclassified (Unclassified DHCPv4 traffic)
    Individual policer configuration:
      Bandwidth:          300 pps
      Burst:              150 packets
      Priority:           low
      Recover time:       300 seconds
      Enabled:            Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (300 pps), Burst: 100% (150 packets), enabled

  Packet type: discover (DHCPv4 DHCPDISCOVER)
    Individual policer configuration:
      Bandwidth:          100 pps
      Burst:              500 packets
      Priority:           low
      Recover time:       300 seconds
      Enabled:            Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (100 pps), Burst: 100% (500 packets), enabled
```

```
  Packet type: offer (DHCPv4 DHCPOFFER)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         low
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

  Packet type: request (DHCPv4 DHCPREQUEST)
    Individual policer configuration:
      Bandwidth:        1000 pps
      Burst:            1000 packets
      Priority:         medium
      Recover time:     300 seconds
      Enabled:          Yes
      Bypass aggregate: No
    FPC slot 1 information:
      Bandwidth: 100% (1000 pps), Burst: 100% (1000 packets), enabled

...
```

show ddos-protection protocols statistics

Syntax **show ddos-protection protocols <*protocol-group*> statistics <brief | detail | terse>**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display traffic statistics and DDoS policer violation statistics for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

brief | detail | terse—(Optional) Display the specified level of output.

- **brief**—Display basic function information.
- **detail**—Add information to the **brief** output; it is identical to the output displayed when you choose no option. The **brief** and **detail** options display information for all protocol groups, which can be a long list.
- **terse**—Display the same level of information as the **brief** option but only for active protocol groups—groups that show traffic in the **Received (packets)** column.

protocol-group—(Optional) Display information for a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection protocols culprit-flows on page 388
- show ddos-protection protocols flow-detection on page 392
- show ddos-protection protocols parameters on page 396
- show ddos-protection protocols violations on page 413

List of Sample Output

show ddos-protection protocols statistics on page 405
show ddos-protection protocols statistics brief on page 408
show ddos-protection protocols statistics terse on page 409
show ddos-protection protocols pppoe statistics on page 410
show ddos-protection protocols pppoe statistics brief on page 412

Output Fields Table 16 on page 404 lists the output fields for the **show ddos-protection protocols statistics** command. Output fields are listed in the approximate order in which they appear.

Table 16: show ddos-protection protocols statistics Output Fields

Field Name	Field Description	Level of Output
Protocol Group	Name of protocol group.	All levels
Packet type	Name of packet type in protocol group.	All levels
System-wide information	The following information collected for the router: • A message indicates whether the policer has been violated. • No. of FPCs currently receiving excess traffic—Number of cards that are currently in violation of a policer. • No. of FPCs that have received excess traffic—Number of cards that have at some point been in violation of a policer. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at all card slots and the Routing Engine. • Dropped—Number of packets dropped regardless of where they were dropped. • Arrival rate—Current traffic rate for packets arriving from all cards and at the Routing Engine. • Max arrival rate—Highest traffic rate for packets arriving from all cards and at the Routing Engine.	**detail** none
Routing Engine information	The following information collected for the Routing Engine: • A message indicates whether the policer has been violated; the policer might be passed at the individual cards, but the combined rate of packets arriving at the Routing Engine can exceed the configured policer value. • Violation first detected at—Timestamp of the first violation. • Violation last seen at—Timestamp of the last observed violation. • Duration of violation—Length of the violation. • Number of violations—Number of times the violation has occurred. • Received—Number of packets received at the Routing Engine from all cards. • Dropped—Number of packets dropped at the Routing Engine; includes packets dropped by the aggregate policer and by individual protocol policers. • Arrival rate—Current traffic rate for packets arriving at the Routing Engine from all cards. • Max arrival rate—Highest traffic rate for packets arriving at the Routing Engine from all cards. • Dropped by aggregate policer—Number of packets dropped by the aggregate policer. • Dropped by individual policers—Number of packets dropped by individual policer.	**detail** none

Table 16: show ddos-protection protocols statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
FPC slot information	The following information collected for the card in the indicated slot: • A message indicates whether the policer has been violated • Violation first detected at—Timestamp of the first violation • Violation last seen at—Timestamp of the last observed violation • Duration of violation—Length of the violation • Number of violations—Number of times the violation has occurred • Received—Number of packets received on the line card • Dropped—Number of packets dropped at the line card; includes packets dropped by the aggregate policer and by individual protocol policers • Arrival rate—Current traffic rate for packets arriving at the line card • Max arrival rate—Highest traffic rate for packets arriving at the line card • Dropped by this policer—Number of packets dropped by the individual policer • Dropped by aggregate policer—Number of packets dropped by the aggregate policer	**detail** none
Received (packets)	Number of packets of this packet type or protocol group received at all cards and the Routing Engine.	**brief terse**
Dropped (packets)	Number of packets dropped for this packet type or protocol group, regardless of where the packets were dropped.	**brief terse**
Rate (pps)	Highest observed traffic rate for this packet type or protocol group.	**brief terse**
Violation counts	Number of violations of the policer bandwidth.	**brief terse**
State	Violation state of the packet type: • **ok**—Policer has not been violated for this packet type • **viol**—Policer has been violated for this packet type	**brief terse**

Sample Output

show ddos-protection protocols statistics

```
user@host> show ddos-protection protocols statistics
Protocol Group: IPv4-Unclassified

  Packet type: aggregate
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
```

```
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0

Protocol Group: IPv6-Unclassified

  Packet type: aggregate
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Aggregate policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by individual policers: 0


Protocol Group: PPPoE

  Packet type: aggregate
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  61961244           Arrival rate:     4000 pps
      Dropped:   0                  Max arrival rate: 4002 pps
    Routing Engine information:
      Aggregate policer is never violated
      Received:  15488871           Arrival rate:     1001 pps
      Dropped:   0                  Max arrival rate: 1011 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Aggregate policer is never violated
      Received:  61961244           Arrival rate:     4000 pps
      Dropped:   46473017           Max arrival rate: 4002 pps
        Dropped by individual policers: 46473017

  Packet type: padi
    System-wide information:
      Bandwidth is being violated!
        No. of FPCs currently receiving excess traffic: 1
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:41:23 PDT
        Duration of violation: 04:18:06 Number of violations: 1
      Received:  30980622           Arrival rate:     2000 pps
      Dropped:   23236505           Max arrival rate: 2001 pps
    Routing Engine information:
      Policer is never violated
      Received:  7744433            Arrival rate:     500 pps
      Dropped:   0                  Max arrival rate: 505 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is currently being violated!
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:41:23 PDT
        Duration of violation: 04:18:06 Number of violations: 1
      Received:  30980622           Arrival rate:     2000 pps
```

```
    Dropped:   23236505            Max arrival rate: 2001 pps
      Dropped by this policer: 23236505
      Dropped by aggregate policer: 0

Packet type: pado
  System-wide information:
    Bandwidth is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padr
  System-wide information:
    Bandwidth is being violated!
      No. of FPCs currently receiving excess traffic: 1
      No. of FPCs that have received excess traffic:  1
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:43:23 PDT
      Duration of violation: 04:20:06 Number of violations: 1
    Received:  31220846            Arrival rate:     2000 pps
    Dropped:   23416690            Max arrival rate: 2001 pps
  Routing Engine information:
    Policer is never violated
    Received:  7806417             Arrival rate:     499 pps
    Dropped:   0                   Max arrival rate: 506 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is currently being violated!
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:43:23 PDT
      Duration of violation: 04:20:06 Number of violations: 1
    Received:  31220846            Arrival rate:     2000 pps
    Dropped:   23416690            Max arrival rate: 2001 pps
      Dropped by this policer: 23416690
      Dropped by aggregate policer: 0

Packet type: pads
  System-wide information:
    Bandwidth is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                   Arrival rate:     0 pps
    Dropped:   0                   Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
```

```
  Packet type: padt
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0

  Packet type: padm
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0

  Packet type: padn
    System-wide information:
      Bandwidth is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
    Routing Engine information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is never violated
      Received:  0                  Arrival rate:     0 pps
      Dropped:   0                  Max arrival rate: 0 pps
        Dropped by aggregate policer: 0

...
```

show ddos-protection protocols statistics brief

```
user@host> show ddos-protection protocols statistics brief

Protocol    Packet      Received        Dropped         Rate     Violation State
group       type        (packets)       (packets)       (pps)    counts
ipv4-uncls  aggregate   0               0               0        0         ok
ipv6-uncls  aggregate   0               0               0        0         ok
dynvlan     aggregate   0               0               0        0         ok
ppp         aggregate   0               0               0        0         ok
ppp         unclass     0               0               0        0         ok
```

```
ppp             lcp             0               0               0       0       ok
ppp             auth            0               0               0       0       ok
ppp             ipcp            0               0               0       0       ok
ppp             ipv6cp          0               0               0       0       ok
ppp             mplscp          0               0               0       0       ok
ppp             isis            0               0               0       0       ok
pppoe           aggregate       61561238        0               4000    0       ok
pppoe           padi            30780619        23086506        2000    1       viol
pppoe           pado            0               0               0       0       ok
pppoe           padr            30780619        23086499        2000    1       viol
pppoe           pads            0               0               0       0       ok
pppoe           padt            0               0               0       0       ok
pppoe           padm            0               0               0       0       ok
pppoe           padn            0               0               0       0       ok
dhcpv4          aggregate       0               0               0       0       ok
dhcpv4          unclass..       0               0               0       0       ok
dhcpv4          discover        0               0               0       0       ok
dhcpv4          offer           0               0               0       0       ok
dhcpv4          request         0               0               0       0       ok
dhcpv4          decline         0               0               0       0       ok
dhcpv4          ack             0               0               0       0       ok
dhcpv4          nak             0               0               0       0       ok
dhcpv4          release         0               0               0       0       ok
dhcpv4          inform          0               0               0       0       ok
dhcpv4          renew           0               0               0       0       ok
dhcpv4          forcerenew      0               0               0       0       ok
dhcpv4          leasequery      0               0               0       0       ok
dhcpv4          leaseuna..      0               0               0       0       ok
dhcpv4          leaseunk..      0               0               0       0       ok
dhcpv4          leaseact..      0               0               0       0       ok
dhcpv4          bootp           0               0               0       0       ok
dhcpv4          no-msgtype      0               0               0       0       ok
dhcpv4          bad-pack..      0               0               0       0       ok

...

icmp            aggregate       0               0               0       0       ok
igmp            aggregate       0               0               0       0       ok
ospf            aggregate       0               0               0       0       ok
rsvp            aggregate       0               0               0       0       ok
pim             aggregate       0               0               0       0       ok
rip             aggregate       0               0               0       0       ok
ptp             aggregate       0               0               0       0       ok
bfd             aggregate       0               0               0       0       ok
lmp             aggregate       0               0               0       0       ok
ldp             aggregate       0               0               0       0       ok
msdp            aggregate       0               0               0       0       ok
bgp             aggregate       0               0               0       0       ok
vrrp            aggregate       0               0               0       0       ok
telnet          aggregate       0               0               0       0       ok

...
```

show ddos-protection protocols statistics terse

```
user@host> show ddos-protection protocols statistics terse
Protocol        Packet          Received        Dropped         Rate    Violation State
group           type            (packets)       (packets)       (pps)   counts
ipv4-uncls      aggregate       241             0               0       0       ok
icmp            aggregate       20              0               0       0       ok
```

```
igmp         aggregate   55              0              0         0          ok
ospf         aggregate   956             0              0         0          ok
rsvp         aggregate   784             0              0         0          ok
ldp          aggregate   2984            0              0         0          ok
bgp          aggregate   312             0              0         0          ok
lacp         aggregate   1744            0              0         0          ok
stp          aggregate   9791            0              0         0          ok
arp          aggregate   19              0              0         0          ok
pvstp        aggregate   393             0              0         0          ok
mlp          aggregate   624774          0              0         0          ok
mlp          packets     1714371         223937         0         3          ok
mcast-copy   aggregate   3018038         0              0         0          ok
igmp-snoop   aggregate   43              0              0         0          ok
fw-host      aggregate   95547           0              0         0          ok
uncls        aggregate   10000           0              0         0          ok
```

show ddos-protection protocols pppoe statistics

```
user@host> show ddos-protection protocols pppoe statistics
Protocol Group: PPPoE

  Packet type: aggregate
    System-wide information:
      Aggregate bandwidth is never violated
      Received:  60381200            Arrival rate:     4000 pps
      Dropped:   0                   Max arrival rate: 4002 pps
    Routing Engine information:
      Aggregate policer is never violated
      Received:  15095242            Arrival rate:     1001 pps
      Dropped:   0                   Max arrival rate: 1011 pps
        Dropped by individual policers: 0
    FPC slot 1 information:
      Aggregate policer is never violated
      Received:  60381200            Arrival rate:     4000 pps
      Dropped:   45287921            Max arrival rate: 4002 pps
        Dropped by individual policers: 45287921

  Packet type: padi
    System-wide information:
      Bandwidth is being violated!
        No. of FPCs currently receiving excess traffic: 1
        No. of FPCs that have received excess traffic:  1
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:34:48 PDT
        Duration of violation: 04:11:31 Number of violations: 1
      Received:  30190600            Arrival rate:     2000 pps
      Dropped:   22643960            Max arrival rate: 2001 pps
    Routing Engine information:
      Policer is never violated
      Received:  7547621             Arrival rate:     499 pps
      Dropped:   0                   Max arrival rate: 505 pps
        Dropped by aggregate policer: 0
    FPC slot 1 information:
      Policer is currently being violated!
        Violation first detected at: 2011-04-19 08:23:17 PDT
        Violation last seen at:      2011-04-19 12:34:48 PDT
        Duration of violation: 04:11:31 Number of violations: 1
      Received:  30190600            Arrival rate:     2000 pps
      Dropped:   22643960            Max arrival rate: 2001 pps
        Dropped by this policer: 22643960
        Dropped by aggregate policer: 0
```

```
Packet type: pado
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padr
  System-wide information:
    Bandwidth is being violated!
      No. of FPCs currently receiving excess traffic: 1
      No. of FPCs that have received excess traffic:  1
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:34:48 PDT
      Duration of violation: 04:11:31 Number of violations: 1
    Received:  30190600           Arrival rate:     2000 pps
    Dropped:   22643961           Max arrival rate: 2001 pps
  Routing Engine information:
    Policer is never violated
    Received:  7547621            Arrival rate:     501 pps
    Dropped:   0                  Max arrival rate: 506 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is currently being violated!
      Violation first detected at: 2011-04-19 08:23:17 PDT
      Violation last seen at:      2011-04-19 12:34:48 PDT
      Duration of violation: 04:11:31 Number of violations: 1
    Received:  30190600           Arrival rate:     2000 pps
    Dropped:   22643961           Max arrival rate: 2001 pps
      Dropped by this policer: 22643961
      Dropped by aggregate policer: 0

Packet type: pads
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padt
  System-wide information:
    Bandwidth is never violated
```

```
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  Routing Engine information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padm
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  :
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0

Packet type: padn
  System-wide information:
    Bandwidth is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
  :
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
  FPC slot 1 information:
    Policer is never violated
    Received:  0                  Arrival rate:     0 pps
    Dropped:   0                  Max arrival rate: 0 pps
      Dropped by aggregate policer: 0
```

show ddos-protection protocols pppoe statistics brief

```
user@host> show ddos-protection protocols pppoe statistics brief
Protocol    Packet      Received        Dropped         Rate     Violation State
group       type        (packets)       (packets)       (pps)    counts
pppoe       aggregate   60901227        0               4000     0         ok
pppoe       padi        30450613        22838981        2000     1         viol
pppoe       pado        0               0               0        0         ok
pppoe       padr        30450614        22838977        2000     1         viol
pppoe       pads        0               0               0        0         ok
pppoe       padt        0               0               0        0         ok
pppoe       padm        0               0               0        0         ok
pppoe       padn        0               0               0        0         ok
```

show ddos-protection protocols violations

Syntax **show ddos-protection protocols <*protocol-group*> violations**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display information about DDoS policer violations for all protocol groups or for a particular protocol group.

Options **none**—Display information for all protocol groups.

protocol-group—(Optional) Name of a particular protocol group. See show ddos-protection protocols for a list of available groups.

Required Privilege Level view

Related Documentation

- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection protocols culprit-flows on page 388
- show ddos-protection protocols flow-detection on page 392
- show ddos-protection protocols parameters on page 396
- show ddos-protection protocols statistics on page 403

List of Sample Output

show ddos-protection protocols violations on page 414
show ddos-protection protocols lldp violations on page 414
show ddos-protection protocols pppoe violations on page 414

Output Fields Table 17 on page 413 lists the output fields for the **show ddos-protection protocols violations** command. Output fields are listed in the approximate order in which they appear.

Table 17: show ddos-protection protocols violations Output Fields

Field Name	Field Description
Number of packet types that are being violated	Number of individual policers and aggregate policers that are currently being violated
Protocol Group	Name of protocol group
Packet type	Name of packet type in protocol group
Bandwidth (pps)	Policer bandwidth

Table 17: show ddos-protection protocols violations Output Fields *(continued)*

Field Name	Field Description
Arrival rate (pps)	Current traffic rate for packets arriving from all cards and at the Routing Engine
Peak rate (pps)	Highest traffic rate for packets arriving from all cards and at the Routing Engine
Policer bandwidth violation detected at	Timestamp of the policer violation
Detected on	Slot number of the card on which the violation was detected

Sample Output

show ddos-protection protocols violations

```
user@host> show ddos-protection protocols violations
Number of packet types that are being violated: 2
Protocol    Packet      Bandwidth  Arrival   Peak      Policer bandwidth
group       type        (pps)      rate(pps) rate(pps) violation detected at
pppoe       padi        500        2000      2001      2011-04-19 08:23:17 PDT
            Detected on: FPC-1
pppoe       padr        500        1999      2001      2011-04-19 08:23:17 PDT
            Detected on: FPC-1
```

show ddos-protection protocols lldp violations

```
user@host> show ddos-protection protocols lldp violations
Number of packet types that are being violated: 0
```

show ddos-protection protocols pppoe violations

```
user@host> show ddos-protection protocols pppoe violations
Number of packet types that are being violated: 2
Protocol    Packet      Bandwidth  Arrival   Peak      Policer bandwidth
group       type        (pps)      rate(pps) rate(pps) violation detected at
pppoe       padi        500        2000      2001      2011-04-19 08:23:17 PDT
            Detected on: FPC-1
pppoe       padr        500        1999      2001      2011-04-19 08:23:17 PDT
            Detected on: FPC-1
```

show ddos-protection statistics

Syntax **show ddos-protection statistics**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display DDoS protection global statistics for bandwidth violations.

Options This command has no options.

Required Privilege Level view

Related Documentation
- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection version on page 418

List of Sample Output show ddos-protection statistics on page 416
[xref target has no title]

Output Fields Table 18 on page 415 lists the output fields for the **show ddos-protection statistics** command. Output fields are listed in the approximate order in which they appear.

Table 18: show ddos-protection statistics Output Fields

Field Name	Field Description
Policing on routing engine	Shows whether or not policing is enabled on the Routing Engine.
Policing on FPC	Shows whether or not policing is enabled on the line card.
Flow detection	Shows whether or not flow detection in enabled.
Logging	Shows whether or not DDoS event logging is enabled.
Policer violation report rate	Shows the violation report rate as a percentage.
Flow report rate	Shows the flow report rate as a percentage.
Default flow detection mode	Flow detection and tracking mode configured at the global level for all protocol groups and packet types.
Default flow level detection mode	Flow detection and tracking mode configured at the flow aggregation level for all protocol groups and packet types.

Table 18: show ddos-protection statistics Output Fields *(continued)*

Field Name	Field Description
Default flow level control mode	Default behavior configured for how traffic in detected flows is controlled for all protocol groups and packet types.
Currently violated packet types	Number of packet types currently experiencing a bandwidth violation.
Packet types have seen violations	Number of packet types that have experienced a bandwidth violation since statistics were cleared.
Total violation counts	Total number of bandwidth violations.

Sample Output

show ddos-protection statistics

```
user@host> show ddos-protection statistics
DDOS protection global statistics:

  Policing on routing engine:         Yes

  Policing on FPC:                    Yes

  Flow detection:                     No

  Logging:                            Yes

  Policer violation report rate:      100

  Flow report rate:                   100

  Currently violated packet types:    2

  Packet types have seen violations:  2

  Total violation counts:             2

  Currently tracked flows:            0

  Total detected flows:               0
```

```
user@host> show ddos-protection statistics
DDOS protection global statistics:
  Policing on routing engine:         Yes
  Policing on FPC:                    Yes
  Flow detection:                     No
  Logging:                            Yes
  Policer violation report rate:      100
  Flow report rate:                   100
  Default flow detection mode         Automatic
  Default flow level detection mode   Automatic
  Default flow level control mode     Drop
  Currently violated packet types:    2
```

```
Packet types have seen violations:  4
Total violation counts:             4
Currently tracked flows:            0
Total detected flows:               0
```

show ddos-protection version

Syntax **show ddos-protection version**

Release Information Command introduced in Junos OS Release 11.2.
Command introduced in Junos OS Release 12.3R2 on EX9200 switches and T4000 routers.
Command introduced in Junos OS Release 15.1X53 on QFX10000 switches.
Command introduced in Junos OS Release 15.1X53-D30 on QFX5200 switches.

Description Display the DDoS protection version and the total numbers of protocol groups and packet types that this version can be configured in this version.

Options This command has no options.

Required Privilege Level view

Related Documentation
- clear ddos-protection protocols on page 366
- show ddos-protection protocols on page 368
- show ddos-protection statistics on page 415

List of Sample Output show ddos-protection version on page 418

Output Fields Table 19 on page 418 lists the output fields for the **show ddos-protection version** command. Output fields are listed in the approximate order in which they appear.

Table 19: show ddos-protection version Output Fields

Field Name	Field Description
Version	Version number of the DDoS protection code.
Total protocol groups	Number of protocol groups configured with DDoS protection.
Total tracked packet types	Number of protocol packet types configured with DDoS protection.

Sample Output

show ddos-protection version

```
user@host> show ddos-protection version
DDOS protection, Version 1.0
  Total protocol groups       = 83
  Total tracked packet types  = 154
```

CHAPTER 22

Operational Commands: IPsec and Digital Certificates

- clear security pki ca-certificate
- clear security pki certificate-request
- clear security pki crl
- clear security pki key-pair
- clear security pki local-certificate
- clear services ipsec-vpn certificates
- clear services ipsec-vpn ipsec statistics
- clear services ipsec-vpn ike security-associations
- clear services ipsec-vpn ipsec security-associations
- request security certificate enroll (Signed)
- request security certificate enroll (Unsigned)
- request security key-pair
- request security pki ca-certificate enroll
- request security pki ca-certificate load
- request security pki ca-certificate verify
- request security pki crl load
- request security pki generate-certificate-request
- request security pki generate-key-pair
- request security pki local-certificate enroll
- request security pki local-certificate generate-self-signed
- request security pki local-certificate load
- request security pki local-certificate verify
- request system certificate add
- show ike security-associations
- show ipsec certificates
- show ipsec security-associations

- show security keychain
- show security pki ca-certificate
- show security pki certificate-request
- show security pki crl
- show security pki local-certificate
- show services ipsec-vpn certificates
- show services ipsec-vpn ike security-associations
- show services ipsec-vpn ipsec security-associations
- show services ipsec-vpn ipsec statistics
- show system certificate

clear security pki ca-certificate

Syntax clear security pki ca-certificate (all | ca-profile *ca-profile-name*)

Release Information Command introduced in Junos OS Release 7.5.

Description Delete certificate authority (CA) digital certificates from the router.

Options **all**—Delete all CA digital certificates from the router.

ca-profile *ca-profile-name*—Delete the specified CA profile.

Required Privilege Level clear

Related Documentation

- request security pki ca-certificate enroll on page 434
- request security pki ca-certificate load on page 435
- show security pki ca-certificate on page 460

List of Sample Output clear security pki ca-certificate all on page 421

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki ca-certificate all

```
user@host> clear security pki ca-certificate all
```

clear security pki certificate-request

Syntax clear security pki certificate-request (all | certificate-id *certificate-id-name*)

Release Information Command introduced in Junos OS Release 7.5.

Description Delete manually generated local digital certificate requests from the router.

Options **all**—Delete all local digital certificate requests from the router.

certificate-id *certificate-id-name*—Delete the specified local digital certificate and corresponding public/private key pair.

Required Privilege Level clear

Related Documentation
- show security pki certificate-request on page 464

List of Sample Output clear security pki certificate-request all on page 422

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki certificate-request all

```
user@host> clear security pki certificate-request all
```

clear security pki crl

Syntax clear security pki crl (all | ca-profile *ca-profile-name*)

Release Information Command introduced in Junos 8.1

Description Delete certificate revocation lists (CRLs) from the router.

Options **all**—Delete all CRLs from the router.

ca-profile *ca-profile-name*—Delete CRLs associated with the specified CA profile.

Required Privilege Level clear

List of Sample Output clear security pki crl ca-profile all on page 423

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear security pki crl ca-profile all

```
user@host> clear security pki crl ca-profile all
```

clear security pki key-pair

Syntax clear security pki key-pair (all | certificate-id *certificate-id-name*)

Release Information Command introduced in Junos OS Release 8.5.

Description Clear public key infrastructure (PKI) key pair information for local digital certificates from the router.

Options

all—Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

certificate-id *certificate-id-name*—Delete the specified local digital certificate and corresponding public/private key pair.

Required Privilege Level clear

Related Documentation

- request security pki local-certificate enroll on page 441
- show security pki local-certificate on page 468

Output Fields This command produces no output.

Sample Output

```
user@host> clear security pki key pair
```

clear security pki local-certificate

Syntax clear security pki local-certificate
<all | certificate-id *certificate-id-name* | system-generated>

Release Information Command introduced in Junos OS Release 7.5.

Description Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the router.

Options

all—(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.

certificate-id *certificate-id-name*—(Optional) Delete the specified local digital certificate and corresponding public and private key pair.

system-generated—(Optional) Auto-generated self-signed certificate.

Required Privilege Level clear

Related Documentation

- request security pki local-certificate enroll on page 441
- show security pki local-certificate on page 468

List of Sample Output clear security pki local-certificate all on page 425

Output Fields This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@host> clear security pki local-certificate all
```

clear services ipsec-vpn certificates

Syntax clear services ipsec-vpn certificates (all | service-set *service-set*) <certificate-cache-entry *number*>

Release Information Command introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Delete digital certificates from the IPsec configuration memory cache. Issuing this command also clears the certificate revocation list (CRL) from the cache along with the certificates.

Options **all**—Delete digital certificates for all service sets.

service-set *service-set*—Delete digital certificates for the specified service set.

Required Privilege Level clear

List of Sample Output clear services ipsec-vpn certificates all on page 426

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn certificates all

```
user@host> clear services ipsec-vpn certificates all
```

clear services ipsec-vpn ipsec statistics

Syntax clear services ipsec-vpn ipsec statistics
<remote-gateway *address*>
<service-set *service-set-name*>

Release Information Command introduced in Junos OS Release 8.1.

Description (Adaptive services interface only) Clear IP Security (IPsec) statistics.

Options **remote-gateway *address***—(Optional) Clear statistics for the specified remote system.

service-set *service-set-name*—(Optional) Clear statistics for the specified service set.

Required Privilege Level view

Related Documentation
- show services ipsec-vpn ipsec statistics on page 482

List of Sample Output clear services ipsec-vpn ipsec statistics on page 427

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec statistics

```
user@host> clear services ipsec-vpn ipsec statistics
```

clear services ipsec-vpn ike security-associations

Syntax clear services ipsec-vpn ike security-associations
<*peer-address-name*>
<service-set *service-set-name*>

Release Information Command introduced before Junos OS Release 7.4.
service-set option added in Junos OS Release 8.5.

Description (Adaptive services interfaces only) Clear Internet Key Exchange (IKE) security associations.

Options ***peer-address-name***—(Optional) Clear only the security association specified by the peer address.

service-set *service-set-name*—(Optional) Clear only the security association specified by the service-set name.

Required Privilege Level view

Related Documentation
- show services ipsec-vpn ike security-associations on page 474

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ike security-associations

```
user@host> clear services ipsec-vpn ike security-associations
```

clear services ipsec-vpn ipsec security-associations

Syntax
clear services ipsec-vpn security-associations
<*peer-address-name*>
<remote-gateway *remote-gateway-address*>
<*service-set-name*>
<tunnel-index *tunnel-index-number*>

Release Information
Command introduced before Junos OS Release 7.4.
remote-gateway, ***service-set-name***, and **tunnel-index** options added in Junos OS Release 8.4.

Description
(Adaptive services interfaces only) Clear IP Security (IPsec) security associations. You can combine the options for greater specificity.

Options
peer-address-name—(Optional) Clear only the security association specified by the peer address.

remote-gateway ***remote-gateway-address***—(Optional) Clear only the security association specified by the remote gateway address.

service-set-name—(Optional) Clear only the security association specified by the service-set name.

tunnel-index ***tunnel-index-number***—(Optional) Clear only the security association specified by the tunnel index number.

Required Privilege Level
view

Related Documentation
- show services ipsec-vpn ipsec security-associations on page 478

Output Fields
When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear services ipsec-vpn ipsec security-associations

```
user@host> clear services ipsec-vpn ipsec security-associations
```

request security certificate enroll (Signed)

Syntax request security certificate enroll filename *filename* subject *subject* alternative-subject *alternative-subject* certification-authority *certification-authority* encoding (binary | pem) key-file *key-file* domain-name *domain-name*

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (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 **/var/etc/ikecert** directory.

NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard. The request security key-pair command is deprecated and not available with Junos in FIPS mode because it generates RSA and DSA keys with sizes of 512 and 1024 bits that are not compliant with the NIST SP 800-131A standard.

Options

filename *filename*—File that stores the certificate.

subject *subject*—Distinguished name (**dn**), which consists of a set of components—for example, an organization (**o**), an organization unit (**ou**), a country (**c**), and a locality (**l**).

alternative-subject *alternative-subject*—Tunnel source address.

certification-authority *certification-authority*—Name of the certificate authority profile in the configuration.

encoding (binary | pem)—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.

key-file *key-file*—File containing a local private key.

domain-name *domain-name*—Fully qualified domain name.

Required Privilege Level maintenance

List of Sample Output request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (Signed) on page 431

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename subject alternative-subject certification-authority key-file domain-name (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.example.com
CA name: example.com CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.example.com
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 enroll (Unsigned)

Syntax request security certificate enroll filename *filename* ca-file *ca-file* ca-name *ca-name* encoding (binary | perm) url *url*

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (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 **/var/etc/ikecert** directory.

Options

filename *filename*—File that stores the public key certificate.

ca-file *ca-file*—Name of the certificate authority profile in the configuration.

ca-name *ca-name*—Name of the certificate authority.

encoding (binary | pem)—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 **binary**.

url *url*—Certificate authority URL.

Required Privilege Level maintenance

List of Sample Output request security certificate enroll filename ca-file ca-name url (Unsigned) on page 432

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate enroll filename ca-file ca-name url (Unsigned)

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
example.com urlxyzcompany URL
http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: example.com
 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. <--------------
```

request security key-pair

Syntax request security key-pair *filename*
<size *key-size*>
<type (rsa | dsa)>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 9.0 for EX Series switches.

Description (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.

NOTE: The request security-certificates command is deprecated and are not available with Junos in FIPS mode because security certificates are not compliant with the NIST SP 800-131A standard.

Options ***filename***—Name of a file in which to store the key pair.

size *key-size*—(Optional) Key size, in bits. The key size can be **512**, **1024**, or **2048**. The default value is **1024**.

type—(Optional) Algorithm used to encrypt the key:

- **rsa**—RSA algorithm. This is the default.
- **dsa**—Digital signature algorithm with Secure Hash Algorithm (SHA).

Required Privilege Level maintenance

List of Sample Output request security key-pair on page 433

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security key-pair

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

request security pki ca-certificate enroll

Syntax request security pki ca-certificate enroll ca-profile *ca-profile-name*

Release Information Command introduced in Junos OS Release 7.5.

Description Request a digital certificate from a certificate authority (CA) online by using the Simple Certificate Enrollment Protocol (SCEP).

Options **ca-profile *ca-profile-name***—CA profile name.

Required Privilege Level maintenance

Related Documentation
- clear security pki ca-certificate on page 421
- show security pki ca-certificate on page 460

List of Sample Output request security pki ca-certificate enroll on page 434

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate enroll

```
user@host> request security pki ca-certificate enroll ca-profile entrust
Received following certificates:
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: 46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f
  Certificate: C=us, O=juniper, CN=First Officer
    Fingerprint: bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17
  Certificate: C=us, O=juniper
    Fingerprint: 00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10
Do you want to load the above CA certificate ? [yes,no] (no) yes
```

request security pki ca-certificate load

Syntax request security pki ca-certificate load ca-profile *ca-profile-name* filename *path/filename*

Release Information Command introduced in Junos OS Release 7.5.

Description Manually load a certificate authority (CA) digital certificate from a specified location.

Options **ca-profile *ca-profile-name***—Load the specified CA profile.

filename *path/filename*—Directory location and filename of the CA digital certificate.

Required Privilege Level maintenance

Related Documentation
- clear security pki ca-certificate on page 421
- show security pki ca-certificate on page 460

List of Sample Output request security pki ca-certificate load on page 435

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki ca-certificate load

```
user@host> request security pki ca-certificate load ca-profile ca-private filename pki-file
```

request security pki ca-certificate verify

Syntax request security pki ca-certificate verify ca-profile *ca-profile-name*

Release Information Command introduced in Junos OS Release 8.5.

Description Verify the digital certificate installed for the specified certificate authority (CA).

Options **ca-profile *ca-profile-name***—Name of the local digital certificate identifier.

Required Privilege Level maintenance

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki ca-certificate verify ca-profile ca1 (CRL not downloaded)
user@host> request security pki ca-certificate verify ca-profile ca1

CA certificate ca1: CRL verification in progress. Please check the PKId debug
logs for completion status
```

request security pki crl load

Syntax request security pki crl load ca-profile *ca-profile-name* filename *path/filename*

Release Information Command introduced in Junos OS Release 8.1.

Description Manually install a certificate revocation list (CRL) on the router from a specified location.

Options **ca-profile *ca-profile-name*** —Load the specified certificate authority (CA) profile.

filename *path/filename* —Directory location and filename of the CRL.

Required Privilege Level maintenance

List of Sample Output request security pki crl load on page 437

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki crl load

```
user@host> request security pki crl load ca-profile ca-private filename pki-file
```

request security pki generate-certificate-request

Syntax

request security pki generate-certificate-request certificate-id *certificate-id-name*
domain-name *domain-name* subject *subject-distinguished-name*
<email *email-address*>
<filename (*path* | terminal)>
<ip-address *ip-address*>

Release Information

Command introduced in Junos OS Release 7.5.

Description

Manually generate a local digital certificate request in the Public-Key Cryptography Standards #10 (PKCS-10) format.

Options

certificate-id *certificate-id-name*—Name of the local digital certificate and the public/private key pair.

domain-name *domain-name*—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

subject *subject-distinguished-name*—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

email *email-address*—(Optional) E-mail address of the certificate holder.

filename (*path* | terminal)—(Optional) Location where the local digital certificate request should be placed or the login terminal.

ip-address *ip-address*—(Optional) IP address of the router.

Required Privilege Level

maintenance

Related Documentation

- clear security pki certificate-request on page 422
- show security pki certificate-request on page 464

List of Sample Output

request security pki generate-certificate-request on page 439

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-certificate-request

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

Generated certificate request
-----BEGIN CERTIFICATE REQUEST-----
MIIBoTCCAQoCAQAwGjEYMBYGA1UEAxMPdHAxLmp1bmlwZXIubmV0MIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCiUFklQws1Ud+AqN5DDxRs2kVyKEhh9qoVFnz+
Hz4c9vsy3B8ElwTJlkmIt2cB3yifB6zePd+6WYpf57Crwre7YqPkiXM31F6z3YjX
H+1BPNbCxNWYvyrnSyVYDbFj8oOXyqog8ACDfVL2JBWrPNBYy7imq/K9soDBbAs6
5hZqqwIDAQABoEcwRQYJKoZIhvcNAQkOMTgwNjAOBgNVHQ8BAf8EBAMCB4AwJAYD
VR0RAQH/BBowGIIWdHAxLmVuZ2xhYi5qdW5pcGVyLm5ldDANBgkqhkiG9w0BAQQF
AAOBgQBc2rq1v5SOQXH7LCb/FdqAL8ZM6GoaN5d6cGwq4bB6a7UQFgtoH4O6gQ3G
3iHOZfz4xMIBpJYuGd1dkqgvcDoH3AgTsLkfn7Wi3x5H2qeQVs9bvL4P5nvEZLND
EIMUHwteolZCiZ7OfO9Fer9cXWHSQs1UtXtgPqQJy2xIeImLgw==
-----END CERTIFICATE REQUEST-----
Fingerprint:
0d:90:b8:d2:56:74:fc:84:59:62:b9:78:71:9c:e4:9c:54:ba:16:97 (sha1)
1b:08:d4:f7:90:f1:c4:39:08:c9:de:76:00:86:62:b8 (md5)
```

request security pki generate-key-pair

Syntax request security pki generate-key-pair certificate-id *certificate-id-name* <size (512 | 1024 | 2048)>

Release Information Command introduced in Junos OS Release 7.5.

Description Generate a Public Key Infrastructure (PKI) public and private key pair for a local digital certificate.

Options **certificate-id *certificate-id-name***—Name of the local digital certificate and the public/private key pair.

size—(Optional) Key pair size. The key pair size can be **512**, **1024**, or **2048** bits.

Required Privilege Level maintenance

List of Sample Output request security pki generate-key-pair on page 440

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

```
user@host> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate enroll

Syntax

request security pki local-certificate enroll ca-profile *ca-profile-name*
certificate-id *certificate-id-name* challenge-password *password* domain-name *domain-name* subject *subject-distinguished-name*
<email *email-address*>
<ip-address *ip-address*>

Release Information

Command introduced in Junos OS Release 7.5.

Description

Request that a certificate authority (CA) enroll and install a local digital certificate online by using the Simple Certificate Enrollment Protocol (SCEP).

Options

ca-profile ***ca-profile-name***—CA profile name.

certificate-id ***certificate-id-name***—Name of the local digital certificate and the public/private key pair.

challenge-password ***password***—Password set by the administrator and normally obtained from the SCEP enrollment webpage of the CA. The password is 16 characters in length.

domain-name ***domain-name***—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

subject ***subject-distinguished-name***—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

email ***email-address***—(Optional) E-mail address of the certificate holder.

ip-address ***ip-address***—(Optional) IP address of the router.

Required Privilege Level

maintenance

Related Documentation

- show security pki local-certificate on page 468

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate enroll certificate-id r3-entrust-scep ca-profile
entrust domain-name router3.example.net subject "CN=router3,OU=Engineering,O=juniper,C=US"
challenge-password 123

Certificate enrollment has started. To view the status of your enrollment, check
 the public key infrastructure log (pkid) log file at /var/log/pkid. Please save
 the challenge-password for revoking this certificate in future.  Note that this
 password is not stored on the router.
```

request security pki local-certificate generate-self-signed

Syntax request security pki local-certificate generate-self-signed certificate-id *certificate-id-name* domain-name *domain-name* ip-address *ip-address* email *email-address* subject *subject-distinguished-name*

Release Information Command introduced in Junos OS Release 9.1.

Description Manually generate a self-signed certificate for the given distinguished name.

Options

certificate-id ***certificate-id-name***—Name of the local digital certificate and the public/private key pair.

domain-name ***domain-name***—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.

email ***email-address***—E-mail address of the certificate holder.

ip-address ***ip-address***—IP address of the router.

subject ***subject-distinguished-name***—Distinguished name format that contains the common name, department, company name, state, and country:

- **CN**—Common name
- **OU**—Organizational unit name
- **O**—Organization name
- **ST**—State
- **C**—Country

Required Privilege Level maintenance
security

Related Documentation

- *Requesting for and Installing a Digital Certificates on Your Router*

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
user@host> request security pki local-certificate generate-self-signed certificate-id self-cert
subject cn=abc domain-name example.net email user1@example.net
Self-signed certificate generated and loaded successfully
```

request security pki local-certificate load

Syntax request security pki local-certificate load certificate-id *certificate-id-name* filename *path*

Release Information Command introduced in Junos OS Release 7.5.

Description Manually load a local digital certificate from a specified location.

Options

certificate-id *certificate-id-name*—Name of the public/private key pair mapped to the local digital certificate.

filename *path/filename*—Directory location and filename of the local digital certificate provided by the CA.

Required Privilege Level maintenance

List of Sample Output request security pki local-certificate load on page 444

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate load

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

request security pki local-certificate verify

Syntax request security pki local-certificate verify certificate-id *certificate-id-name*

Release Information Command introduced in Junos OS Release 8.5.

Description Verify the validity of the local digital certificate identifier.

Options **certificate-id *certificate-id-name*** —Display the specified certificate identifier name.

Required Privilege Level maintenance

Related Documentation
- show security pki local-certificate on page 468

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

You receive the following response before the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate-id bme1 (not downloaded)
user@host> request security pki local-certificate verify certificate-id bme1

Local certificate bme1: CRL verification in progress. Please check the PKId debug
 logs for completion status
```

You receive the following response after the certificate revocation list (CRL) is downloaded:

```
request security pki local-certificate verify certificate bme1 (downloaded)
user@host> request security pki local-certificate verify certificate-id bme1
Local certificate bme1 verification success
```

request system certificate add

Syntax request system certificate add (*filename* | terminal)

Release Information Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 11.1 for the QFX Series.

Description (Encryption interface on M Series and T Series routers, PTX Series, and QFX Series switches only) Add a certificate provided by the Juniper Networks certificate authority (CA).

Options ***filename***—Filename (URL, local, or remote).

terminal—Use login terminal.

Required Privilege Level maintenance

List of Sample Output request system certificate add terminal on page 446

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system certificate add terminal

```
user@host> request system certificate add terminal
```

show ike security-associations

Syntax
show ike security-associations
<brief | detail>
<*peer-address*>

Release Information
Command introduced before Junos OS Release 7.4.

Description
(Encryption interface on M Series and T Series routers only) Display information about Internet Key Exchange (IKE) security associations.

Options
none—Display standard information about all IKE security associations.

brief | detail—(Optional) Display the specified level of output.

peer-address—(Optional) Display IKE security associations for the specified peer address.

Required Privilege Level
view

Related Documentation
- *clear ike security-associations*

List of Sample Output
show ike security-associations on page 450
show ike security-associations detail on page 450

Output Fields
Table 20 on page 447 lists the output fields for the **show ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 20: show ike security-associations Output Fields

Field Name	Field Description	Level of Output
IKE peer	Remote end of the IKE negotiation.	**detail**
Role	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.	**detail**
Remote Address	Responder's address.	none specified
State	State of the IKE security association: • **Matured**—The IKE security association is established. • **Not matured**—The IKE security association is in the process of negotiation.	none specified
Initiator cookie	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels

Table 20: show ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Responder cookie	The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received. 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).	All levels
Exchange type	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: • **Main**—The exchange is done with six messages. **Main** encrypts the payload, protecting the identity of the neighbor. • **Aggressive**—The exchange is done with three messages. **Aggressive** does not encrypt the payload, leaving the identity of the neighbor unprotected.	All Levels
Authentication method	Type of authentication determines which payloads are exchanged and when they are exchanged. The Junos OS supports only **pre-shared keys**.	**detail**
Local	Prefix and port number of the local end.	**detail**
Remote	Prefix and port number of the remote end.	**detail**
Lifetime	Number of seconds remaining until the IKE security association expires.	**detail**
Algorithms	Header for the IKE algorithms output. • **Authentication**—Type of authentication algorithm used:**md5** or **sha1**. • **Encryption**—Type of encryption algorithm used: **des-cbc**, **3des-cbc**, or **None**. • **Pseudo random function**—Function that generates highly unpredictable random numbers:**hmac-md5** or**hmac-sha1**.	**detail**
Traffic statistics	Number of bytes and packets received and transmitted on the IKE security association. • **Input bytes, Output bytes**—Number of bytes received and transmitted on the IKE security association. • **Input packets, Output packets**—Number of packets received and transmitted on the IKE security association.	**detail**

Table 20: show ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flags	Notification to the key management process of the status of the IKE negotiation: • **caller notification sent**—Caller program notified about the completion of the IKE negotiation. • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.	**detail**
IPsec security associates	Number of IPsec security associations created and deleted with this IKE security association.	**detail**

Phase 2 negotiations in progress	Number of phase 2 IKE negotiations in progress and status information:
	• **Negotiation type**—Type of phase 2 negotiation. The Junos OS currently supports **quick mode**.
	• **Message ID**—Unique identifier for a phase 2 negotiation.
	• **Local identity**—Identity of the local phase 2 negotiation. The format is *id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*)
	• **Remote identity**—Identity of the remote phase 2 negotiation. The format is *id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*)
	• **Flags**—Notification to the key management process of the status of the IKE negotiation:
	  ◦ **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  ◦ **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  ◦ **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  ◦ **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.
		detail

Sample Output

show ike security-associations

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

show ike security-associations detail

```
user@host>  show ike security-associations detail
IKE peer 192.0.2.4
  Role: Initiator, State: Matured
  Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  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: 192.0.2.5:500, Remote: 192.0.2.4:500
    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

Syntax show ipsec certificates
<brief | detail>
<crl *crl-name* | *serial-number*>

Release Information Command introduced before Junos OS Release 7.4.

Description (Encryption interface on M Series and T Series routers only) Display information about the IPsec certificate database.

Options **none**—Display standard information about all of the entries in the IPsec certificate database.

brief | detail—(Optional) Display the specified level of output.

crl *crl-name* | *serial-number*—(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.

Required Privilege Level view

Related Documentation
- *clear ipsec security-associations*

List of Sample Output show ipsec certificates detail on page 452

Output Fields Table 21 on page 451 lists the output fields for the **show ipsec certificates** command. Output fields are listed in the approximate order in which they appear.

Table 21: show ipsec certificates Output Fields

Field Name	Field Description	Level of Output
Database	Display information about the IPsec certificate database. • **Total entries**—Number of database entries, including entries that are not trusted or that are in the process of being deleted. • **Active entries**—Number of database entries, excluding entries that are marked as deleted. • **Locked entries**—Number of statically configured database entries that cannot expire, such as CA certificates that are root or trusted.	All levels
Subject	Distinguished name for the certificate for **C**, **O**, **CN**, as described in RFC 3280, *Internet x.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.*	All levels
ID	Identification number of the database entry. **ID** is generated by the internal certificate database.	All levels

Table 21: 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. • **Trusted**—Passed validity checks. • **Not trusted**—Failed validity checks. • **Root**—Entry is locked and may have been learned through IKE or a locally configured CA certificate. • **Non-root**—Entry is not locked. • **Crl-issuer**—Entity issues CRLs. • **Non-crl-issuer**—Entity does not issue CRLs.	**detail**
Validity period starts	Start time that the certificate is valid, in the format ***yyyy mon dd***, ***hh:mm:ss*** **GMT**.	**detail**
Validity period ends	End time that the certificate is valid, in the format ***yyyy mon dd***, ***hh:mm:ss*** **GMT**.	**detail**
Alternative name information	Auxiliary identity for the certificate: ***dns-name***, ***email-address***, ***ip-address***, or ***uri*** (uniform resource identifier).	**detail**
Issuer	Information about the entity that has signed and issued the CRL as described in RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile.*	**detail**

Sample Output

show ipsec certificates detail

```
user@host> show ipsec certificates 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 security-associations

Syntax show ipsec security-associations
<brief | detail>
<*sa-name*>

Release Information Command introduced before Junos OS Release 7.4.

Description Display information about the IPsec security associations applied to the local or transit traffic stream.

Options **none**—Display standard information about all IPsec security associations.

brief | detail—(Optional) Display the specified level of output.

sa-name—(Optional) Display the specified IPsec security association.

Required Privilege Level view

List of Sample Output show ipsec security-associations sa-name on page 456
show ipsec security-associations sa-name detail on page 456

Output Fields Table 22 on page 454 lists the output fields for the **show ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 22: show ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Security association	Name of the security association.	All levels
Interface family	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: • **Up**—The security association is referenced in the interface family and the interface family is up. • **Down**—The security association is referenced in the interface family and the interface family is down. • **No reference**—The security association is not referenced in the interface family.	All levels
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
Local identity	Prefix and port number of the local end	All levels
Remote identity	Prefix and port number of the remote end.	All levels
Direction	Direction of the security association: **inbound** or **outbound**.	All levels
SPI	Value of the security parameter index.	All levels

Table 22: show ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
AUX-SPI	Value of the auxiliary security parameter index. • When the value is **AH** or **ESP**, **AUX-SPI** is always **0**. • When the value is**AH+ESP**, **AUX-SPI** is always a positive integer.	All levels
State	Status of the security association: • **Installed**—The security association is installed in the security association database. (For transport mode security associations, the value of **State** must always be **Installed**.) • **Not installed**—The security association is not installed in the security association database.	**detail**
Mode	Mode of the security association: • **transport**—Protects single host-to-host protections. • **tunnel**—Protects connections between security gateways.	All levels
Type	Type of security association:. • **manual**—Security parameters require no negotiation. They are static, and are configured by the user. • **dynamic**—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode.	All levels
Protocol	Protocol supported: • **transport** mode—Supports Encapsulation Security Protocol (**ESP**) or Authentication Header (**AH**). • **tunnel** mode—Supports **ESP** or **AH+ESP**.	All levels
Authentication	Type of authentication used: **hmac-md5-96**, **hmac-sha1-96**, or **None**.	**detail**
Encryption	Type of encryption used: **des-cbc**, **3des-csc**, or **None**.	**detail**
Soft lifetime **Hard lifetime**	(**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 **hard lifetime** specifies the lifetime of the SA. The **soft lifetime**, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This allows the key management system to negotiate a new SA before the hard lifetime expires. • **Expires in** *seconds* **seconds**—Number of seconds left until the security association expires. • **Expires in** *kilobytes* **kilobytes**—Number of kilobytes left until the security association expires.	**detail**
Anti-replay service	State of the service that prevents packets from being replayed: **Enabled** or **Disabled**.	**detail**

Table 22: 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: **32** or **64**. The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is **0**, 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: 192.0.2.1, Remote gateway: 198.51.100.1
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: 192.0.2.1, Remote gateway: 198.51.100.1
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 security keychain

Syntax
show security keychain
<brief | detail>

Release Information
Command introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3X50 for the QFX Series.

Description
Display information about authentication keychains configured for the Border Gateway Protocol (BGP), the Label Distribution Protocol (LDP) routing protocols, the Bidirectional Forwarding Detection (BFD) protocol, and the Intermediate System-to-Intermediate System (IS-IS) protocol.

Options
none—Display information about authentication keychains.

brief | detail—(Optional) Display the specified level of output.

Required Privilege Level
view

List of Sample Output
show security keychain brief on page 458
show security keychain detail on page 459

Output Fields
Table 23 on page 457 describes the output fields for the **show security keychain** command. Output fields are listed in the approximate order in which they appear.

Table 23: show security keychain Output Fields

Field Name	Field Description	Level of Output
keychain	The name of the keychain in operation.	All levels
Active-ID Send	Number of routing protocols packets sent with the active key.	All levels
Active-ID Receive	Number of routing protocols packets received with the active key.	All levels
Next-ID Send	Number of routing protocols packets sent with the next key.	All levels
Next-ID Receive	Number of routing protocols packets received with the next key.	All levels
Transition	Amount of time until the current key will be replaced with the next key in the keychain.	All levels
Tolerance	Configured clock-skew tolerance, in seconds, for accepting keys for a key chain.	All levels
Id	Identification number configured for the current key.	**detail**
Algorithm	Authentication algorithm configured for the current key.	**detail**

Table 23: show security keychain Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	State of the current key. The value can be: • **receive** • **send** • **send-receive** For the active key, the **State** can be **send-receive**, **send**, or **receive**. For keys that have a future start time, the **State** is **inactive**. Compare the **State** field to the **Mode** field.	**detail**
Option	For IS-IS only, the option determines how Junos OS encodes the message authentication code in routing protocol packets. The values can be: • **basic**—Based on RFC 5304. • **isis-enhanced**—Based on RFC 5310. The default value is **basic**. When you configure the **isis-enhanced** option, Junos OS sends RFC 5310-encoded routing protocol packets and accepts both RFC 5304-encoded and RFC 5310-encoded routing protocol packets that are received from other devices. When you configure **basic** (or do not include the **options** statement in the key configuration) Junos OS sends and receives RFC 5304-encoded routing protocols packets, and drops 5310-encoded routing protocol packets that are received from other devices. Because this setting is for IS-IS only, the TCP and the BFD protocol ignore the encoding option configured in the key.	**detail**
Start-time	Time that the current key became active.	**detail**
Mode	Mode of each key (Informational only.) The value can be • **receive** • **send** • **send-receive** The mode of the key is based on the configuration. Suppose you configure two keys, one with a start-time of today and the other with a start-time of next week. For both keys, the **Mode** can be **send-receive**, **send**, or **receive**, regardless of the configured start-time. Compare the **Mode** field to the **State** field.	**detail**

Sample Output

show security keychain brief

```
user@host> show security keychain brief
```

```
keychain                 Active-ID       Next-ID       Transition  Tolerance
                        Send  Receive   Send  Receive
 hakr                     3     3        1     1        1d 23:58    3600
```

show security keychain detail

```
user@host> show security keychain detail
keychain                 Active-ID       Next-ID       Transition  Tolerance
                        Send  Receive   Send  Receive
 hakr                     3     3        1     1        1d 23:58    3600
  Id 3, Algorithm hmac-md5, State send-receive, Option basic
  Start-time Wed Aug 11 16:28:00 2010, Mode send-receive
  Id 1, Algorithm hmac-md5, State inactive, Option basic
  Start-time Fri Aug 20 11:30:57 2010, Mode send-receive
```

show security pki ca-certificate

Syntax show security pki ca-certificate
<brief | detail>
<ca-profile *ca-profile-name*>

Release Information Command introduced in Junos OS Release 7.5.

Description Display information about certificate authority (CA) digital certificates installed in the router.

Options **none**—(Same as brief) Display information about all CA digital certificates.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display information about only the specified CA profile.

Required Privilege Level view

List of Sample Output show security pki ca-certificate on page 461
show security pki ca-certificate detail on page 462

Output Fields Table 24 on page 460 lists the output fields for the **show security pki ca-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 24: show security pki ca-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	**none brief**
Issued to	Device that was issued the digital certificate.	**none brief**
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**

Table 24: show security pki ca-certificate Output Fields *(continued)*

Field Name	Field Description	Level of Output
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the requestor. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption(1024 bits)**.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki ca-certificate

```
user@host> show security pki ca-certificate
Certificate identifier: entrust
  Issued to: juniper, Issued by: juniper
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier: entrust
  Issued to: First Officer, Issued by: juniper
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)

Certificate identifier: entrust
  Issued to: First Officer, Issued by: juniper
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
```

```
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
```

show security pki ca-certificate detail

```
user@host> show security pki ca-certificate detail
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 9235
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us
  Validity:
    Not before: 2005 Oct 18th, 23:54:22 GMT
    Not after: 2025 Oct 19th, 00:24:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    cb:9e:2d:c0:70:f8:ea:3c:f2:b5:f0:02:48:87:dc:68:99:a3:57:4f
    0e:b9:98:0b:95:47:0d:1f:97:7c:53:17:dd:1a:f8:da:e5:08:d1:1c
    78:68:1f:2f:72:9f:a2:cf:81:e3:ce:c5:56:89:ce:f0:97:93:fa:36
    19:3e:18:7d:8c:9d:21:fe:1f:c3:87:8d:b3:5d:f3:03:66:9d:16:a7
    bf:18:3f:f0:7a:80:f0:62:50:43:83:4f:0e:d7:c6:42:48:c0:8a:b2
    c7:46:30:38:df:9b:dc:bc:b5:08:7a:f3:cd:64:db:2b:71:67:fe:d8
    04:47:08:07:de:17:23:13
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
    71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: CRL signing, Certificate signing
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925c
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: First Officer
  Validity:
    Not before: 2005 Oct 18th, 23:55:59 GMT
    Not after: 2008 Oct 19th, 00:25:59 GMT
  Public key algorithm: rsaEncryption(1024 bits)
    c0:a4:21:32:95:0a:cd:ec:12:03:d1:a2:89:71:8e:ce:4e:a6:f9:2f
    1a:9a:13:8c:f6:a0:3d:c9:bd:9d:c2:a0:41:77:99:1b:1e:ed:5b:80
    34:46:f8:5b:28:34:38:2e:91:7d:4e:ad:14:86:78:67:e7:02:1d:2e
    19:11:b7:fa:0d:ba:64:20:e1:28:4e:3e:bb:6e:64:dc:cd:b1:b4:7a
    ca:8f:47:dd:40:69:c2:35:95:ce:b8:85:56:d7:0f:2d:04:4d:5d:d8
    42:e1:4f:6b:bf:38:c0:45:1e:9e:f0:b4:7f:74:6f:e9:70:fd:4a:78
    da:eb:10:27:bd:46:34:33
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    bc:78:87:9b:a7:91:13:20:71:db:ac:b5:56:71:42:ad:1a:b6:46:17 (sha1)
    23:79:40:c9:6d:a6:f0:ca:e0:13:30:d4:29:6f:86:79 (md5)
  Distribution CRL:
    C=us, O=example, CN=CRL1
    http://CA-1/CRL/example_us_crlfile.crl
  Use for key: Key encipherment
Certificate identifier: entrust
  Certificate version: 3
  Serial number: 4355 925b
```

```
Issuer:
  Organization: example, Country: us
Subject:
  Organization: example, Country: us, Common name: First Officer
Validity:
  Not before: 2005 Oct 18th, 23:55:59 GMT
  Not after: 2008 Oct 19th, 00:25:59 GMT
Public key algorithm: rsaEncryption(1024 bits)
  ea:75:c4:f3:58:08:ea:65:5c:7e:b3:de:63:0a:cf:cf:ec:9a:82:e2
  d7:e8:b9:2f:bd:4b:cd:86:2f:f1:dd:d8:a2:95:af:ab:51:a5:49:4e
  00:10:c6:25:ff:b5:49:6a:99:64:74:69:e5:8c:23:5b:b4:70:62:8e
  e4:f9:a2:28:d4:54:e2:0b:1f:50:a2:92:cf:6c:8f:ae:10:d4:69:3c
  90:e2:1f:04:ea:ac:05:9b:3a:93:74:d0:59:24:e9:d2:9d:c2:ef:22
  b9:32:c7:2c:29:4f:91:cb:5a:26:fe:1d:c0:36:dc:f4:9c:8b:f5:26
  af:44:bf:53:aa:d4:5f:67
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  46:71:15:34:f0:a6:41:76:65:81:33:4f:68:47:c4:df:78:b8:e3:3f (sha1)
  ee:cc:c7:f4:5d:ac:65:33:0a:55:db:59:72:2c:dd:16 (md5)
Distribution CRL:
  C=us, O=example, CN=CRL1
  http://CA-1/CRL/example_us_crlfile.crl
Use for key: Digital signature
```

show security pki certificate-request

Syntax
show security pki certificate-request
<brief | detail>
<certificate-id *certificate-id-name*>

Release Information
Command introduced in Junos OS Release 7.5.

Description
Display information about manually generated local digital certificate requests that are stored in the router.

Options
none—(same as brief) Display information about all local digital certificate requests.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified local digital certificate request

Required Privilege Level
view

Related Documentation
- clear security pki certificate-request on page 422

List of Sample Output
show security pki certificate-request on page 465
show security pki certificate-request detail on page 465

Output Fields
Table 25 on page 464 lists the output fields for the **show security pki certificate-request** command. Output fields are listed in the approximate order in which they appear.

Table 25: show security pki certificate-request Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Issued to	Device that was issued the digital certificate.	**none brief**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	**detail**

Table 25: show security pki certificate-request Output Fields *(continued)*

Field Name	Field Description	Level of Output
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption(1024 bits)**.	All levels
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.	All levels
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki certificate-request

```
user@host> show security pki certificate-request
Certificate identifier: local-microsoft-2
  Issued to: router2.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

show security pki certificate-request detail

```
user@host> show security pki certificate-request detail
Certificate identifier: local-entrust3
  Certificate version: 3
  Subject:
    Common name: router3.example.com
  Alternate subject: router3.example.com
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
    fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
    d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
    23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
    ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
    7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
    72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
    79:54:da:4f:d3:6f:52:1f
  Fingerprint:
    7c:e8:f9:45:93:8d:a3:92:7f:18:29:02:f1:c8:e2:85:3d:ad:df:1f (sha1)
    00:4e:df:a0:6b:ad:8c:50:da:7c:a1:cf:5d:37:b0:ea (md5)
  Use for key: Digital signature
```

show security pki crl

Syntax
show security pki crl
<brief | detail>
<ca-profile *ca-profile-name*>

Release Information
Command introduced in Junos OS Release 8.1.

Description
Display information about the certificate revocation lists (CRLs) that are stored in the router.

Options
none—(same as brief) Display information about all CRLs.

brief | detail—(Optional) Display the specified level of output.

ca-profile *ca-profile-name*—(Optional) Display CRL information about only the specified CA profile.

Required Privilege Level
view

Related Documentation
- clear security pki crl on page 423

List of Sample Output
show security pki crl on page 467
show security pki crl detail on page 467

Output Fields
Table 26 on page 466 shows the output fields for the **show security pki crl** command. Output fields are listed in the approximate order in which they appear.

Table 26: show security pki crl Output Fields

Field Name	Field Description	Level of Output
CA profile	Name of the configured CA profile.	All levels
CRL version	Revision number of the certificate revocation list.	All levels
CRL number	Number of the certificate revocation list	All levels
CRL Issuer	Device that was issued the certificate revocation list.	All levels
Issuer	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Effective date	Date and time the certificate revocation list becomes valid.	All levels

Table 26: show security pki crl Output Fields *(continued)*

Field Name	Field Description	Level of Output
Next update	Date and time the router will download the latest version of the certificate revocation list.	All levels
Revocation List	List of digital certificates that have been revoked before their expiration date. Values are: • **Serial number**—Unique serial number of the digital certificate • **Revocation date**—Date and time that the digital certificate was revoked.	**detail**

Sample Output

show security pki crl

```
user@host> show security pki crl
 CA profile entrust
 CRL version: V2
 CRL number: 24
 CRL issuer: C=CA, O=juniper
 Effective date: 2006 May 31st, 05:35:25 GMT
 Next update: 2006 Jun 1st, 06:35:25 GMT
```

show security pki crl detail

```
user@host> show security pki crl detail
  CA profile: entrust
 CRL version: V2
 CRL number: 24
 Issuer:
  Organization: juniper, Country: ca
 Validity:
  Effective date: 2006 May 31st, 05:35:25 GMT
  Next update: 2006 Jun 1st, 06:35:25 GMT
 Revocation List:
  Serial number      Revocation date
  4451aca3 2006      May 25th, 09:13:38 GMT
  4451aca4 2006      May 25th, 10:11:33 GMT
  4451acb4 2006      May 29th, 11:28:54 GMT
  4451aceb 2006      May 29th, 11:29:01 GMT
  4451acfe 2006      May 29th, 11:29:17 GMT
  4451acff 2006      May 31st, 05:29:55 GMT
```

show security pki local-certificate

Syntax
show security pki local-certificate
<brief | detail>
<certificate-id *certificate-id-name*>
<system-generated>

Release Information
Command introduced in Junos OS Release 7.5.

Description
Display information about the local digital certificates and the corresponding public keys installed in the router.

Options
none—(same as brief) Display information about all local digital certificates and corresponding public keys.

brief | detail—(Optional) Display the specified level of output.

certificate-id *certificate-id-name*—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.

system-generated—(Optional) Auto-generated self-signed certificate.

Required Privilege Level
view

Related Documentation
- clear security pki local-certificate on page 425

List of Sample Output
show security pki local-certificate on page 469
show security pki local-certificate detail on page 470

Output Fields
Table 27 on page 468 lists the output fields for the **show security pki local-certificate** command. Output fields are listed in the approximate order in which they appear.

Table 27: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Issued by	Authority that issued the digital certificate.	none **brief**
Issued to	Device that was issued the digital certificate.	none **brief**

Table 27: show security pki local-certificate Output Fields *(continued)*

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: • **Common name**—Name of the authority. • **Organization**—Organization of origin. • **Organizational unit**—Department within an organization. • **State**—State of origin. • **Country**—Country of origin.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	**detail**
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	All levels
Public key algorithm	Encryption algorithm used with the private key, such as **rsaEncryption (1024 bits)**.	All levels
Public key verification status	Public key verification status: **Failed** or **Passed**. The **detail** output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show security pki local-certificate

```
user@host> show security pki local-certificate
Certificate identifier: local-entrust2
  Issued to: router2.example.com, Issued by: juniper
```

```
  Validity:
    Not before: 2005 Nov 21st, 23:28:22 GMT
    Not after: 2008 Nov 21st, 23:58:22 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
```

show security pki local-certificate detail

```
user@host> show security pki local-certificate detail
Certificate identifier: local-entrust3
  Certificate version: 3
  Serial number: 4355 94f9
  Issuer:
    Organization: juniper, Country: us
  Subject:
    Organization: juniper, Country: us, Common name: router3.example.com
  Alternate subject: router3.example.com
  Validity:
    Not before: 2005 Nov 21st, 23:33:58 GMT
    Not after: 2008 Nov 22nd, 00:03:58 GMT
  Public key algorithm: rsaEncryption(1024 bits)
  Public key verification status: Passed
    fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
    d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
    23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
    ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
    7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
    72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
    79:54:da:4f:d3:6f:52:1f
  Signature algorithm: sha1WithRSAEncryption
  Fingerprint:
    61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
    60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
  Distribution CRL:
    C=us, O=juniper, CN=CRL1
    http://CA-1/CRL/juniper_us_crlfile.crl
  Use for key: Digital signature
```

show services ipsec-vpn certificates

Syntax show services ipsec-vpn certificates
<brief | detail>
<service-set *service-set*>

Release Information Command introduced in Junos OS Release 7.5.

Description (Adaptive services interfaces only) Display local and remote certificates installed in the IPsec configuration memory cache that are used for the IKE negotiation.

Options **none**—(same as brief) Display information about local and remote certificates associated with all service sets.

brief | detail—(Optional) Display the specified level of output.

service-set *service-set*—(Optional) Display information about local and remote certificates associated with only the specified service set.

Required Privilege Level view

List of Sample Output show services ipsec-vpn certificates on page 472
show security ipsec-vpn certificates detail on page 472

Output Fields Table 28 on page 471 lists the output fields for the **show services ipsec-vpn certificates** command. Output fields are listed in the approximate order in which they appear.

Table 28: show services ipsec-vpn certificates Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the IPsec service set.	All levels
Total entries	Number of certificate cache entries.	All levels
Certificate cache entry	Identification number of the certificate cache entry.	All levels
Flags	Information about the digital certificate, including whether the certificate is a root certificate and trusted.	none **brief**
Issued to	Device that was issued the digital certificate.	none **brief**
Issued by	Authority that issued the digital certificate.	none **brief**
Certificate version	Revision number of the digital certificate.	**detail**
Serial number	Unique serial number of the digital certificate.	**detail**
Alternate subject	Domain name or IP address of the device related to the digital certificate.	All levels

Table 28: show services ipsec-vpn certificates Output Fields *(continued)*

Field Name	Field Description	Level of Output
Validity	Time period when the digital certificate is valid. Values are: • **Not before**—Start time when the digital certificate becomes valid. • **Not after**—End time when the digital certificate becomes invalid.	none **brief**
Public key algorithm	Specifies the encryption algorithm used with the private key, such as **rsaEncryption (1024 bits)**.	**detail**
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as **sha1WithRSAEncryption**.	**detail**
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	**detail**
Distribution CRL	Distinguished name information and the URL for the certificate revocation list (CRL) server.	**detail**
Use for key	Use of the public key, such as **Certificate signing**, **CRL signing**, **Digital signature**, or **Key encipherment**.	**detail**

Sample Output

show services ipsec-vpn certificates

```
user@host> show services ipsec-vpn certificates
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Flags: Non-root Trusted
    Issued to: router3.example.com, Issued by: juniper
    Alternate subject: router3.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:33:58 GMT
      Not after: 2008 Nov 22nd, 00:03:58 GMT

 Certificate cache entry: 2
    Flags: Non-root Trusted
    Issued to: router2.example.com, Issued by: juniper
    Alternate subject: router2.example.com
    Validity:
      Not before: 2005 Nov 21st, 23:28:22 GMT
      Not after: 2008 Nov 21st, 23:58:22 GMT

  Certificate cache entry: 1
    Flags: Root Trusted
    Issued to: juniper, Issued by: juniper
    Validity:
      Not before: 2005 Oct 18th, 23:54:22 GMT
      Not after: 2025 Oct 19th, 00:24:22 GMT
```

show security ipsec-vpn certificates detail

```
user@host> show services ipsec-vpn certificates detail
```

```
Service set: serviceset-dynamic-BiEspsha3des, Total entries: 3
  Certificate cache entry: 3
    Certificate version: 3
    Serial number: 4355 94f9
    Alternate subject: router3.example.com
    Public key algorithm: rsaEncryption
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
      60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
    Distribution CRL:
      C=us, O=juniper, CN=CRL1
      http://CA-1/CRL/juniper_us_crlfile.crl
    Use for key: Digital signature

  Certificate cache entry: 2
    Certificate version: 3
    Serial number: 4355 94f8
    Alternate subject: router2.example.com
    Public key algorithm: rsaEncryption
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      30:c3:a4:04:da:33:9d:60:23:5a:48:75:48:2c:f0:c6:96:6c:31:fa (sha1)
      9a:a2:ce:ef:7e:10:80:a0:c8:4d:2f:e7:e1:d3:69:9d (md5)
    Distribution CRL:
      C=us, O=juniper, CN=CRL1
      http://CA-1/CRL/juniper_us_crlfile.crl
    Use for key: Digital signature

  Certificate cache entry: 1
    Certificate version: 3
    Flags: Root
    Serial number: 4355 9235
    Public key algorithm: rsaEncryption
    Signature algorithm: sha1WithRSAEncryption
    Fingerprint:
      00:8e:6f:58:dd:68:bf:25:0a:e3:f9:17:70:d6:61:f3:53:a7:79:10 (sha1)
      71:6f:6a:76:17:9b:d6:2a:e7:5a:72:97:82:6d:26:86 (md5)
    Distribution CRL:
      C=us, O=juniper, CN=CRL1
      http://CA-1/CRL/juniper_us_crlfile.crl
    Use for key: CRL signing, Certificate signing
```

show services ipsec-vpn ike security-associations

Syntax show services ipsec-vpn ike security-associations
<brief | detail>
<*peer-address*>

Release Information Command introduced before Junos OS Release 7.4.
Statistics for Internet Key Exchange (IKE) security associations for each services PIC introduced in Junos OS Release 12.1.

Description (Adaptive services interface only) Display information for Internet Key Exchange (IKE) security associations. If no security association is specified, the information for all security associations is displayed.

Options **none**—(same as brief) Display standard information for all IPsec security associations.

brief | detail—(Optional) Display the specified level of output.

peer-address—(Optional) Display information about a particular security association address.

Required Privilege Level view

List of Sample Output show services ipsec-vpn ike security-associations on page 476
show services ipsec-vpn ike security-associations detail on page 477

Output Fields Table 29 on page 474 lists the output fields for the **show services ipsec-vpn ike security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 29: show services ipsec-vpn ike security-associations Output Fields

Field Name	Field Description	Level of Output
IKE peer	Remote end of the IKE negotiation.	**detail**
Role	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.	**detail**
Remote Address	Responder's address.	none specified
State	State of the IKE security association: • **Matured**—IKE security association is established. • **Not matured**—The IKE security association is in the process of negotiation.	none specified
Initiator cookie	When the IKE negotiation is triggered, a random number is sent to the remote node.	All levels

Table 29: show services ipsec-vpn ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Responder cookie	The remote node generates its own random number and sends it back to the initiator as a verification that the packets were received. 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).	All levels
Exchange type	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: • **Main**—The exchange is done with six messages. **Main** encrypts the payload, protecting the identity of the neighbor. • **Aggressive**—The exchange is done with three messages. **Aggressive** does not encrypt the payload, leaving the identity of the neighbor unprotected. • **IKEv2**—The exchange is negotiated using IKE version 2.	All levels
PIC	The services PIC for which the IKE security associations are displayed.	All levels
Authentication method	Type of authentication determines which payloads are exchanged and when they are exchanged. The Junos OS supports only **pre-shared keys**.	**detail**
Local	Prefix and port number of the local end.	**detail**
Remote	Prefix and port number of the remote end.	**detail**
Lifetime	Number of seconds remaining until the IKE security association expires.	**detail**
Algorithms	Header for the IKE algorithms output. • **Authentication**—(**detail** output only) Type of authentication algorithm used: **md5** or **sha1** • **Encryption**—(**detail** output only) Type of encryption algorithm used: **des-cbc**, **3des-cbc**, or **None**. • **Pseudo random function**—Function that generates highly unpredictable random numbers: **hmac-md5** or **hmac-sha1**.	**detail**
Traffic statistics	Number of bytes and packets received and transmitted on the IKE security association. • **Input bytes, Output bytes**—Number of bytes received and transmitted on the IKE security association. • **Input packets, Output packets**—Number of packets received and transmitted on the IKE security association.	**detail**

Table 29: show services ipsec-vpn ike security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Flags	Notification to the key management process of the status of the IKE negotiation: • **caller notification sent**—Caller program notified about the completion of the IKE negotiation. • **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire. • **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation. • **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.	**detail**
IPsec security associates	Number of IPsec security associations created and deleted with this IKE security association.	**detail**

Phase 2 negotiations in progress	Number of phase 2 negotiations in progress and status information:
	• Negotiation type—Type of phase 2 negotiation. The Junos OS currently supports **quick mode**.
	• Message ID—Unique identifier for a phase 2 negotiation.
	• Local identity—Identity of the local phase 2 negotiation. The format is *id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*).
	• Remote identity—Identity of the remote phase 2 negotiation. The format is *id-type-name* (*proto-name*:*port-number*,[0..*id-data-len*] = *iddata-presentation*)
	• Flags—Notification to the key management process of the status of the IKE negotiation:
	  ◦ **caller notification sent**—Caller program notified about the completion of the IKE negotiation.
	  ◦ **waiting for done**—Negotiation is done. The library is waiting for the remote end retransmission timers to expire.
	  ◦ **waiting for remove**—Negotiation has failed. The library is waiting for the remote end retransmission timers to expire before removing this negotiation.
	  ◦ **waiting for policy manager**—Negotiation is waiting for a response from the policy manager.
		detail

Sample Output

show services ipsec-vpn ike security-associations

```
user@host> show services ipsec-vpn ike security-associations
Remote Address  State         Initiator cookie  Responder cookie  Exchange type

192.0.2.1        Matured       062d291d21275fc7  82ef00e3d1f1c981  Main

192.0.2.2        Matured       cd6d581d7bb1664d  88a707779f3ad8d1  Main

192.0.2.3        Matured       86621051e3e78360  6bc5cc83fd67baa4  IKEv2
```

```
PIC: sp-0/3/0

192.0.2.7         Matured       565e2813075e6fdb  67886757a74edcd6  IKEv2
```

show services ipsec-vpn ike security-associations detail

```
user@host> show services ipsec-vpn ike security-associations detail
IKE peer 198.51.100.2
      Role: Responder, State: Matured
      Initiator cookie: d91c9f20f78e1d4e, Responder cookie: 727a04ed8d5021a1
      Exchange type: IKEv2, Authentication method: Pre-shared-keys
      Local: 2013.0.113.2:500, Remote: 198.51.100:500
      Lifetime: Expires in 1357 seconds
      Algorithms:
       Authentication        : sha1
       Encryption            : 3des-cbc
       Pseudo random function: hmac-sha1
      Traffic statistics:
       Input  bytes  :               22244
       Output bytes  :               22236
       Input  packets:                 263
       Output packets:                 263
      Flags: Caller notification sent
      IPSec security associations: 0 created, 0 deleted
      Phase 2 negotiations in progress: 0

IKE peer 192.0.2.4
  Role: Initiator, State: Matured
  Initiator cookie: cf22bd81a7000001, Responder cookie: fe83795c2800002e
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 192.0.2.5:500, Remote: 192.0.2.4:500
  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: 192.0.2.5:500, Remote: 192.0.2.4:500
    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 services ipsec-vpn ipsec security-associations

Syntax show services ipsec-vpn ipsec security-associations
<brief | detail | extensive>
<service-set *service-set-name*>

Release Information Command introduced before Junos OS Release 7.4.

Description (Adaptive services interface only) Display IPsec security associations for the specified service set. If no service set is specified, the security associations for all service sets are displayed.

Options **none**—Display standard information about IPsec security associations for all service sets.

brief | detail | extensive—(Optional) Display the specified level of output.

service-set *service-set-name*—(Optional) Display information about a particular service set.

Required Privilege Level view

List of Sample Output show services ipsec-vpn ipsec security associations extensive on page 481

Output Fields Table 30 on page 478 lists the output fields for the **show services ipsec-vpn ipsec security-associations** command. Output fields are listed in the approximate order in which they appear.

Table 30: show services ipsec-vpn ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec security associations are defined. If appropriate, includes the outside service interface VRF name.	All levels
Rule	Name of the rule set applied to the security association.	**detail extensive**
Term	Name of the IPsec term applied to the security association.	**detail extensive**
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	**detail extensive**
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
IPsec inside interface	Name of the logical interface hosting the IPsec tunnels.	All levels
Tunnel MTU	MTU of the IPsec tunnel.	All levels

Table 30: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Local identity	Protocol, address or prefix, and port number of the local entity of the IPsec association. The format is **id-type-name (proto-name:port-number,[0..*id-data-len*] = *iddata-presentation*)**. The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the ***id-data-len*** parameter can be one of the following, depending on the address configured in the IPsec rule: • For an IPv4 address, the length is 4 and the value displayed is 3. • For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. • For a range of IPv4 addresses, the length is 8 and the value displayed is 7. • For an IPv6 address prefix, the length is 16 and the value displayed is 15. • For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. • For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. The value of the ***id-data-presentation*** field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the local peer of the IPsec association, it is displayed instead of the address details.	All levels
Remote identity	Protocol, address or prefix, and port number of the remote entity of the IPsec association. The format is **id-type-name (proto-name:port-number,[0..*id-data-len*] = *iddata-presentation*)**. The protocol is always displayed as any because it is not user-configurable in the IPsec rule. Similarly, the port number field in the output is always displayed as 0 because it is not user-configurable in the IPsec rule. The value of the ***id-data-len*** parameter can be one of the following, depending on the address configured in the IPsec rule: • For an IPv4 address, the length is 4 and the value displayed is 3. • For a subnet mask of an IPv4 address, the length is 8 and the value displayed is 7. • For a range of IPv4 addresses, the length is 8 and the value displayed is 7. • For an IPv6 address prefix, the length is 16 and the value displayed is 15. • For a subnet mask of an IPv6 address prefix, the length is 32 and the value displayed is 31. • For a range of IPv6 address prefixes, the length is 32 and the value displayed is 31. The value of the ***id-data-presentation*** field denotes the IPv4 address or IPv6 prefix details. If the fully qualified domain name (FQDN) is specified instead of the address for the remote peer of the IPsec association, it is displayed instead of the address details.	All levels
Primary remote gateway	IP address of the configured primary remote peer.	All levels
Backup remote gateway	IP address of the configured backup remote peer.	All levels

Table 30: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
State	State of the primary or backup interface: **Active**, **Offline**, or **Standby**. Both ES PICs are initialized to **Offline**. For primary and backup peers, **State** can be **Active** or **Standby**. If both peers are in a state of **Standby**, no connection exists yet between the two peers.	All levels
Failover counter	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.	All levels
Direction	Direction of the security association: **inbound** or **outbound**.	All levels
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index. • When the value of **Protocol** is **AH** or **ESP**, **AUX-SPI** is always **0**. • When the value of **Protocol** is **AH+ESP**, **AUX-SPI** is always a positive integer.	All levels
Mode	Mode of the security association: • **transport**—Protects single host-to-host protections. • **tunnel**—Protects connections between security gateways.	**detail extensive**
Type	Type of security association: • **manual**—Security parameters require no negotiation. They are static, and are configured by the user. • **dynamic**—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode.	**detail extensive**
State	Status of the security association: • **Installed**—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) • **Not installed**—The security association is not installed in the security association database.	**detail extensive**
Protocol	Protocol supported: • **transport** mode supports Encapsulation Security Protocol (**ESP**) or Authentication Header (**AH**). • **tunnel** mode supports **ESP** or **AH+ESP**.	All levels
Authentication	Type of authentication used: **hmac-md5-96**, **hmac-sha1-96**, or **none**.	**detail extensive**
Encryption	Type of encryption algorithm used: can be **aes-cbc (128 bits)**, **aes-cbc (192 bits)**, **aes-cbc (256 bits)**, **des-cbc**, **3des-cbc**, or **None**.	**detail**

Table 30: show services ipsec-vpn ipsec security-associations Output Fields *(continued)*

Field Name	Field Description	Level of Output
Soft lifetime **Hard lifetime**	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 hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This information allows the key management system to negotiate a new SA before the hard lifetime expires. • **Expires in** *seconds* **seconds**—Number of seconds left until the security association expires. • **Expires in** *kilobytes* **kilobytes**—Number of kilobytes left until the security association expires.	**detail extensive**
Anti-replay service	State of the service that prevents packets from being replayed: **Enabled** or **Disabled**.	**detail extensive**
Replay window size	Configured size, in packets, of the antireplay service window: **32** or **64**. The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is **0**, antireplay service is disabled.	**detail**

Sample Output

show services ipsec-vpn ipsec security associations extensive

```
user@host> show services ipsec-vpn ipsec security-associations extensive
Service set: service-set-1
  Rule: _junos_, Term: term-1, Tunnel index: 1
  Local gateway: 192.0.2.2, Remote gateway: 198.51.100.4
  IPSec inside interface: sp-2/0/0.1  Local identity:
ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
  Primary remote gateway: 192.0.2.1, State: Standby
  Backup remote gateway: 198.51.100.4, State: Active
  Failover counter: 1

   Direction: inbound, SPI: 3743521590, AUX-SPI: 0
   Mode: tunnel, Type: dynamic, State: Installed
   Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
   Soft lifetime: Expires in 23043 seconds
   Hard lifetime: Expires in 23178 seconds
   Anti-replay service: Enabled, Replay window size: 64

   Direction: outbound, SPI: 2551045240, AUX-SPI: 0
   Mode: tunnel, Type: dynamic, State: Installed
   Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
   Soft lifetime: Expires in 23043 seconds
   Hard lifetime: Expires in 23178 seconds
   Anti-replay service: Enabled, Replay window size: 64
```

show services ipsec-vpn ipsec statistics

Syntax
show services ipsec-vpn ipsec statistics
<brief | detail>
<remote-gw *remote-peer-address*>
<service-set *service-set-name*>

Release Information
Command introduced before Junos OS Release 7.4.
New fields added in Junos OS Release 10.0.

Description
(Adaptive services interface only) Display IPsec statistics for the specified service set. If no service set is specified, the statistics for all service sets are displayed.

Options
none—Display standard IPsec statistics for all service sets.

brief | detail—(Optional) Display the specified level of output.

remote-gw *remote-peer-address*—(Optional) Display IPsec statistics for an individual IPsec tunnel and an individual remote host.

service-set *service-set-name*—(Optional) Display information about a particular service set.

Required Privilege Level
view

List of Sample Output
show services ipsec-vpn ipsec statistics detail on page 484
show services ipsec-vpn ipsec statistics remote-gw on page 484

Output Fields
Table 31 on page 482 lists the output fields for the **show services ipsec-vpn ipsec statistics** command. Output fields are listed in the approximate order in which they appear.

Table 31: show services ipsec-vpn ipsec statistics Output Fields

Field Name	Field Description	Level of Output
PIC	The physical interface on which the IPsec tunnel is configured.	All levels
Service set	Name of the service set for which the IPsec tunnel is defined.	All levels
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	All levels

Table 31: show services ipsec-vpn ipsec statistics Output Fields *(continued)*

Field Name	Field Description	Level of Output
ESP statistics	Encapsulation Security Payload (ESP) statistics: • **Encrypted bytes**—Total number of bytes encrypted by the local system across the IPsec tunnel. • **Decrypted bytes**—Total number of bytes decrypted by the local system across the IPsec tunnel. • **Encrypted packets**—Total number of packets encrypted by the local system across the IPsec tunnel. • **Decrypted packets**—Total number of packets decrypted by the local system across the IPsec tunnel	All levels
AH Statistics	Authentication Header statistics: • **Input bytes**—Total number of bytes received by the local system across the IPsec tunnel. • **Output bytes**—Total number of bytes transmitted by the local system across the IPsec tunnel. • **Input packets**—Total number of packets received by the local system across the IPsec tunnel. • **Output packets**—Total number of packets transmitted by the local system across the IPsec tunnel.	All levels
Errors	• **AH authentication failures**—Number of authentication header (AH) failures. An AH failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel. • **ESP authentication failures**—Number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets. • **ESP Decryption failures**—Number of ESP decryption failures. • **Bad headers**—Number of invalid headers detected. • **Bad trailers**—Number of invalid trailers detected. • **Replay before window drops**—Number of replay errors. A replay error is generated when a duplicate packet is received within the replay window. • **Replayed pkts**—Number of packets replayed. • **IP integrity errors**—Number of IP integrity errors. • **Exceeds tunnel MTU**—Number of times the tunnel maximum transmission unit (MTU) value was exceeded. • **Rule lookup failures**—Number of rule lookup failures. • **No SA errors**—Number of errors resulting from a missing security association (SA). • **Flow errors**—Number of flow errors. • **Misc errors**—Number of miscellaneous errors.	All levels

Sample Output

show services ipsec-vpn ipsec statistics detail

```
user@host> show services ipsec-vpn ipsec statistics
PIC: sp-0/2/0, Service set: ss0

ESP Statistics:
  Encrypted bytes:                0
  Decrypted bytes:                0
  Encrypted packets:              0
  Decrypted packets:              0
AH Statistics:
  Input bytes:                  168
  Output bytes:                 168
  Input packets:                  2
  Output packets:                 2
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

show services ipsec-vpn ipsec statistics remote-gw

```
user@host> show services ipsec-vpn ipsec statistics remote-gw 192.0.2.1
PIC: sp-3/1/0, Service set: service-set-2
Local gateway: 198.51.100.1, Remote gateway: 192.0.2.1, Tunnel index: 2
ESP Statistics:
 Encrypted bytes:                0
 Decrypted bytes:                0
 Encrypted packets:              0
 Decrypted packets:              0
AH Statistics:
 Input bytes:                    0
 Output bytes:                   0
 Input packets:                  0
 Output packets:                 0
Errors:
  AH authentication failures:     0
  ESP authentication failures:    0
  ESP decryption failures:        0
  Bad headers: 0, Bad trailers: 0
  Replay before window drops: 0, Replayed pkts: 0
  IP integrity errors: 0, Exceeds tunnel MTU: 0
  Rule lookup failures: 0, No SA errors: 0
  Flow errors: 0, Misc errors: 0
```

show system certificate

Syntax
show system certificate
<certificate-id>

Release Information
Command introduced before Junos OS Release 7.4.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description
(Encryption interface on M Series, T Series routers, QFX Series, and OCX Series switches only) Display installed certificates signed by the Juniper Networks certificate authority.

Options
none—Display all installed certificates signed by the Juniper Networks certificate authority.

certificate-id—(Optional) Display the details of a particular certificate.

Required Privilege Level
maintenance

List of Sample Output
show system certificate on page 486
show system certificate (QFX Series) on page 486

Output Fields
Table 32 on page 485 lists the output fields for the **show system certificate** command. Output fields are listed in the approximate order in which they appear.

Table 32: show system certificate Output Fields

Field Name	Field Description
Certificate identifier	Unique identifier associated with a certificate. The certificate identifier is the common name of the subject.
Issuer **Subject**	Information about the certificate issuer and the distinguished name (**DN**) of the issuer, respectively: • **Organization**—Name of the owner's organization. • **Organizational unit**—Name of the owner's department. • **Country**—Two-character country code in which the owner's system is located. • **State**—State in the USA in which the owner is using the certificate. • **Locality**—City in which the owner's system is located. • **Common name**—Name of the owner of the certificate. • **E-mail address**—E-mail address of the owner of the certificate.
Validity	When a certificate is valid.
Signature algorithm	Encryption algorithm applied to the installed certificate.
Public key algorithm	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@example.com
  Subject:
  Organization: Juniper Networks, Organizational unit: Juniper CA,
Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
E-mail address:ca@example.com
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 Series)

```
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@example.com
  Subject:
  Organization: Juniper Networks, Organizational unit: Juniper CA,
Country: US, State: CA, Locality: Sunnyvale, Common name: Dallas-v3,
E-mail address:ca@example.com
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
```