

Chapter 26

IPSec Monitoring and Troubleshooting

Table 63 summarizes the command-line interface (CLI) commands you can use to monitor and troubleshoot security. In the table, the commands are grouped by functionality. In the remainder of this chapter, they are explained alphabetically.

Table 63: Commands for Monitoring Security

Task Category	Task or Information to Monitor	Command
IKE	Clear IKE security associations.	clear ike security-associations on page 367
	IKE security association information.	show ike security-associations on page 370
IPSec Security Associations	Clear IPSec security associations.	clear ipsec security-associations on page 368
	IPSec security association information.	show ipsec security-associations on page 376
IPSec Redundancy	Switch between primary and backup interfaces and tunnels.	request ipsec switch on page 369
	Primary and backup interface and tunnel information.	show ipsec redundancy on page 375
IPSec Certificates	Display IPSec certificate database.	show ipsec certificates on page 373

clear ike security-associations

Syntax clear ike security-associations < *destination ip-address*>

Description Clear information about the current IKE security association. This command is valid for dynamic type security associations only.

Options none—Clear all IKE security associations.

destination ip-address—(Optional) Clear a particular IKE security association to this destination address.

Required Privilege Level view

clear ipsec security-associations

Syntax clear ipsec security-associations < *sa-name*>

Description Clear information about the current IPsec security association. A new security association is then created. This command is valid for dynamic type security associations only.

Options none—Clear all IPsec security associations.

sa-name—(Optional) Clear a particular security association.

Required Privilege Level view

Sample Output: clear ipsec security-associations (detail)

```

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

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

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

user@host> clear ipsec security-associations

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

Direction: inbound, SPI: 1031597683, State: Installed
Mode: tunnel, Type: dynamic
Protocol: ESP, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expires in 23037 seconds
Hard lifetime: Expires in 28797 seconds

Direction: outbound, SPI: 1618419878, State: Installed
Mode: tunnel, Type: dynamic
Protocol: ESP, Authentication: hmac-md5-96, Encryption: None
Soft lifetime: Expires in 23037 seconds
Hard lifetime: Expires in 28797 seconds

```

request ipsec switch

Syntax request ipsec switch <interface> <security-associations>

Description Manually switch between primary and backup interfaces or security associations. To view the status of the interfaces and security associations, see *show ipsec redundancy* on page 375.

Options interface—(Optional) Switch to the backup encryption PIC.
security-associations—(Optional) Switch to the backup tunnel.

Required Privilege Level view

show ike security-associations

Syntax show ike security-associations <peer-address> <brief | detail>

Description Display information about the Internet Key Exchange (IKE) security associations (sa).

Options brief—(Optional) Display brief IKE security association information.

detail—(Optional) Display detailed IKE security association information.

peer-address—(Optional) The remote end of the IKE negotiation.

Default: brief

Required Privilege Level view

Output Fields IKE peer—The remote end of the IKE negotiation.

Role—Part played in the IKE session. If you are triggering the IKE negotiation, then you are the initiator. If you are accepting the first IKE exchange packets, then you are the responder.

Remote Address—(standard) Responder's address.

State—State of the IKE security association. If the state is mature, the IKE security association is established. If the state is not matured, the IKE security association is in the process of negotiation.

Initiator cookie—When triggering the IKE negotiation, a random number is sent to the remote node.

Responder cookie—Remote mode generates its own random number and sends it back to the initiator as a verification that the packets were received.



Note

Of the numerous security services available, protection against denial of service 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 denial-of-service attempts (such as simple flooding with invalid IP source addresses).

Exchange type—Specifies the number of messages in a 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 software supports two types of exchanges:

Main—The exchange is done with 6 messages. Main encrypts the payload, protecting the identity of the neighbor.

Aggressive—The exchange is done with 3 messages. Aggressive does not encrypt the payload, leaving the identity of the neighbor unprotected.

Authentication method—Type of authentication determines which payloads are exchanged and when they are exchanged. pre-shared keys is the only authentication method supported at this time.

Local—Prefix and port number of the local end.

Remote—Prefix and port number of the remote end.

Lifetime—Number of seconds remaining until the IKE security association expires.

Algorithms—Header for the IKE algorithms output.

Authentication—(Detail output only) Type of authentication algorithm used. It can be md5 or sha1.

Encryption—(Detail output only) Type of encryption algorithm used. It can be des-cbc, 3des-cbc, or None.

Pseudo random function— Function that generates highly unpredictable random numbers. It can be hmac-md5 or hmac-sha1.

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.

Flags—Notification to the key management daemon of the status of the IKE negotiation. It can be one of the following:

caller notification sent—Caller program notified about the completion of the IKE negotiation.

waiting for done—Negotiation is done. The library is waiting the 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.

IPSec security associations—Number of IPSec security associations created and deleted with this IKE security association.

Phase 2 negotiations in progress—Number phase 2 IKE negotiations in progress.

Negotiation type—Type of the phase 2 negotiation. At this time, JUNOS software 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)

Sample Output: show ike security-associations (standard)

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

Sample Output: show ike security-associations detail

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

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

show ipsec certificates

Syntax	show ipsec certificates <cr1>
Description	Display information about the IPsec certificate database.
Options	<p>none—Display information about all of the entries in the IPsec certificate database.</p> <p>cr1—(Optional) Display information about the entries on the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates. The CRL is signed by a Certificate Authority (CA) or CRL issuer and made freely available in a public repository. Each revoked certificate is identified in a CRL by its certificate serial number.</p>
Output Fields	<p>Database—Display information about the IPsec certificate database.</p> <p>Total entries—Number of database entries, including entries that are not trusted or that are in the process of being deleted.</p> <p>Active entries—Number of database entries, excluding entries that are marked as deleted.</p> <p>Locked entries—Number of statically configured database entries that cannot expire, such as Certificate Authority (CA) certificates that are root or trusted.</p> <p>ID—Identification number of the database entry. ID is generated by the internal certificate database.</p> <p>References—Reference number the certificate manager has for the particular entry.</p> <p>Serial—Unique serial number assigned to each certificate by the Certificate Authority.</p> <p>Subject—Distinguished name for the certificate for C, O, CN, as described in the RFC 3280.</p> <p>flags—Describe the state of the certificate.</p> <p>Trusted—Passed validity checks.</p> <p>Not trusted—Failed validity checks.</p> <p>Root—Entry is locked and may have been learned through IKE or a locally configured ca certificate.</p> <p>Non-root—Entry is not locked.</p> <p>Cr1-issuer—Entity issues CRLs.</p> <p>Non-cr1-issuer—Entity does not issue CRLs.</p> <p>Alternative name information—Auxiliary identity for the certificate. It can be dns-name, email-address, ip-address, or uri (uniform resource identifier).</p> <p>Validity period starts—Start time that the certificate is valid, in the format <i>yyyy mon dd, hh:mm:ss</i> GMT.</p>

Validity period ends—End time that the certificate is valid, in the format *yyyy mon dd, hh:mm:ss GMT*.

Issuer—Information about the entity who has signed and issued the CRL as described in RFC 2459.

Sample Output: show ipsec certificates

```
user@host> show ipsec certificates
Database: Total entries: 3 Active entries: 4 Locked entries: 1
ID      Serial      Subject
5       22314868    C=us, O=x
4       22315496    C=us, O=x
1       1538512     C=FI, O=Company-ABC
```

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 redundancy

Syntax	show ipsec redundancy interface <interface-name> security association <sa-name>
Description	Display information about the state of the primary and backup interfaces and tunnels. To switch between primary and backup, use request ipsec switch on page 369.
Options	interface <i>interface-name</i> —(Optional) Display information about a particular encryption interface. security association <sa-name>—(Optional) Display information about a particular security association.
Output Fields	Failure 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. Primary Interface—Name of the interface configured to be the primary interface. Backup interface—Name of the interface configured to be the backup interface. State—State of the primary or backup interface can be Active, Offline, or Standby. Both Encryption Services PICs are initialized to Offline. For primary and remote peers, State can be Active or Standby. Both peers are in a state of Standby by default (there is not yet a connection between the two peers). Security association—Name of the security association. Local IP—Local IP address. Primary remote IP—IP address of the configured primary remote peer. Backup remote IP—IP address of the configured backup remote peer.
Sample Output: show ipsec redundancy interface	<pre> user@host> show ipsec redundancy interface Failure counter: 0 Primary interface: es-1/3/0, State: Active Backup interface : es-1/1/0, State: Standby </pre>
Sample Output: show ipsec redundancy security-associations	<pre> user@host> show ipsec redundancy security-associations sa-dynamic Security association: sa-dynamic, Failure counter: 0 Local IP: 4.4.4.4 Primary remote IP: 4.4.4.5, State: Standby Backup remote IP : 3.3.3.3, State: Standby </pre>

show ipsec security-associations

Syntax	show ipsec security-associations <sa-name> <brief detail>
Description	Display information about the IPsec security associations applied to the local or transit traffic stream.
Options	brief—(Optional) Display brief IPsec security association information. detail—(Optional) Display detailed IPsec security association information. sa-name—(Optional) Display a particular security association. Default: brief
Required Privilege Level	view
Sample Output	Sample Output: show ipsec security-associations brief (with manual SA) on page 377 Sample Output: show ipsec security-associations detail (with manual SA) on page 378 Sample Output: show ipsec security-associations brief (with dynamic SA) on page 378 Sample Output: show ipsec security-associations detail (with dynamic SA) on page 378
Output Fields	<p>Security association—Name and interface family of the security association. If the interface family field is absent, it is a transport mode security association. The interface family can have one of three options:</p> <p>Up—The security association is referenced in the interface family and the interface family is up.</p> <p>Down—The security association is referenced in the interface family and the interface family is down.</p> <p>No reference—The security association is not referenced in the interface family.</p> <p>Direction—Direction of the security association; it can be inbound or outbound.</p> <p>SPI—Value of the security parameter index.</p> <p>AUX-SPI—Value of the auxiliary security parameter index. AUX-SPI is always 0 for a Protocol value AH or ESP. It has a positive integer value for Protocol AH+ESP.</p> <p>State—(Detail output only) State has two options, installed and not installed.</p> <p>Installed—The security association is installed in the security association database.</p> <p>Not installed—The security association is not installed in the security association database.</p>

**Note**

For transport mode security associations, state should always be installed.

Mode—Mode of the security association. Mode can be transport or tunnel.

transport—Protects single host-to-host protections.

tunnel—Protects connections between security gateways.

Type—Type of the security association. Type can be manual or dynamic.

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.

Protocol—Protocol supported. transport mode supports Encapsulation Security Protocol (ESP) or Authentication Header (AH). tunnel mode supports ESP and AH+ ESP.

Authentication—(Detail output only) Type of authentication used. It can be hmac-md5-96, hmac-sha1-96, or none.

Encryption—(Detail output only) Type of encryption used. It can be des-cbc, 3des-cbc, or None.

Soft lifetime, Hard lifetime—(Detail and 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—The number of seconds left until the security association expires.

Expires in *kilobytes* kilobytes—The number of kilobytes left until the security association expires.

Anti-replay service—State of the service that prevents packets from being replayed. It can be Enabled or Disabled.

Replay window size—The configured size of the anti-replay service window. The anti-replay window size protects the receiver against replay attacks by rejecting old or duplicate packets. It can be 32 or 64 packets. If the replay window size is 0, then the anti-replay service is disabled.

Sample Output: show ipsec security-associations brief (with manual SA)

```
user@host> show ipsec security-associations sa-manual brief
Security association: sa-manual, Interface family: Up
Direction SPI      AUX-SPI    Mode      Type      Protocol
inbound  2908734119  0          tunnel    manual    AH
outbound 3494029335  0          tunnel    manual    AH
```

Sample Output: show ipsec security-associations detail (with manual SA)

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

Direction: inbound, SPI: 2908734119, AUX-SPI: 0, State: Installed
Mode: tunnel, Type: dynamic
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
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
Anti-replay service: Disabled
```

Sample Output: show ipsec security-associations brief (with dynamic SA)

```
user@host> show ipsec security-associations sa-dynamic brief
Security association: sa-dynamic, Interface family: Up
Direction SPI      AUX-SPI  Mode   Type   Protocol
inbound  2908734119  0      tunnel dynamic AH
outbound  3494029335  0      tunnel dynamic AH
```

Sample Output: show ipsec security-associations detail (with dynamic SA)

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

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
```