

Chapter 27

IPSec Services Operational Mode Commands

Table 51 summarizes the command-line interface (CLI) commands you can use to monitor and troubleshoot IP Security (IPSec) services interfaces on the Adaptive Services (AS) PIC. In the table, the commands are grouped by functionality. In the remainder of this chapter, they are explained alphabetically.

To monitor and troubleshoot IPSec on the ES PIC, see “IPSec Operational Mode Commands” on page 421.

Table 51: Commands for Monitoring IPSec Services

Task Category	Task or Information to Monitor	Command
IKE Security Associations	Display Internet Key Exchange (IKE) VPN security associations for service sets.	show services ipsec-vpn ike security-associations on page 367
	Clear all IKE VPN security associations.	clear services ipsec-vpn on page 366
IPSec Security Associations	Display IPSec VPN security associations for service sets.	show services ipsec-vpn ipsec security-associations on page 370
	Clear all IPSec VPN security associations.	clear services ipsec-vpn on page 366
IPSec Statistics	Display IPSec VPN statistics for service sets.	show services ipsec-vpn ipsec statistics on page 373

clear services ipsec-vpn

Syntax clear services ipsec-vpn (ike | ipsec) security-associations <peer-address-name>

Description Clear either IKE or IPSec security associations.

Options ike security-associations—Clear all IKE security associations.

ipsec security-associations—Clear all IPSec security associations.

peer-address-name—(Optional) Clear only the IKE or IPSec security association specified by the peer address.

Required Privilege Level view

show services ipsec-vpn ike security-associations

Syntax	show services ipsec-vpn ike security-associations <brief detail> <service-set <i>service-set-name</i> >
Description	Display Internet Key Exchange (IKE) 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 IPsec security associations for all service sets. The display output is in brief mode. brief—Display IKE security association information in brief mode. detail—Display IKE security association information in detailed mode. service-set <i>service-set-name</i> —(Optional) Display information about a particular service set.
Required Privilege Level	view
Output Fields	<p>IKE peer—The remote end of the IKE negotiation.</p> <p>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.</p> <p>Remote Address—(Standard) Responder’s address.</p> <p>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.</p> <p>Initiator cookie—When the IKE negotiation is triggered, a random number is sent to the remote node.</p> <p>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.</p>



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 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 software 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.

Authentication method—The type of authentication determines which payloads are exchanged and when they are exchanged. The JUNOS software currently supports only pre-shared keys.

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 of phase 2 IKE negotiations in progress.

Negotiation type—The type of phase 2 negotiation. The JUNOS software 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)*

Sample Output: show services ipsec-vpn ike security-associations (standard)

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

Sample Output: show services ipsec-vpn ike security-associations detail

```
user@host> show services ipsec-vpn 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 services ipsec-vpn ipsec security-associations

Syntax	show services ipsec-vpn ipsec security-associations <brief detail> <service-set <i>service-set-name</i> >
Description	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	<p>None—Display IPsec security associations for all service sets. The display output is in brief mode.</p> <p>brief—Display IPsec security association information in brief mode.</p> <p>detail—Display IPsec security association information in detailed mode.</p> <p>service-set <i>service-set-name</i>—(Optional) Display information about a particular service set.</p>
Required Privilege Level	view
Output Fields	<p>Service set—Name of the service set for which the IPsec security associations are defined.</p> <p>Rule—(Detail output only) Name of the rule set applied to the security association.</p> <p>Term—(Detail output only) Name of the IPsec term applied to the security association</p> <p>Tunnel index— (Detail output only) Numeric identifier of the specific IPsec tunnel for the security association.</p> <p>Local gateway—Gateway address of the local system.</p> <p>Remote gates—Gateway address of the remote system.</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.</p> <p>When the value of Protocol is AH or ESP, AUX-SPI is always 0.</p> <p>When the value of Protocol is AH+ESP, AUX-SPI is always a positive integer.</p> <p>Mode—(Detail output only) Mode of the security association. Mode can be transport or tunnel.</p> <p>transport—Protects single host-to-host protections.</p> <p>tunnel—Protects connections between security gateways.</p>

Type—(Detail output only) 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.

State—(Detail output only) State has two options, Installed and Not installed.

Installed—The security association is installed in the security association database.

Not installed—The security association is not installed in the security association database.



NOTE: For transport mode security associations, the value of State should always be Installed.

Protocol—Protocol supported.

transport mode supports Encapsulation Security Protocol (ESP) or Authentication Header (AH).

tunnel mode supports ESP or 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 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—(Detail output only) State of the service that prevents packets from being replayed. It can be Enabled or Disabled.

Replay window size—(Detail output only) 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 services ipsec-vpn ipsec security-associations brief

```

user@host> show services ipsec-vpn ipsec security-associations brief
Service set: ssdynamic0

Rule: rule_dynamic0, Term: term, Tunnel index: 1
Local gateway: 10.27.0.2, Remote gateway: 10.27.0.1
Direction SPI    AUX-SPI  Mode   Type  Protocol
inbound 3113285016 0      tunnel dynamic ESP
outbound 902773313 0      tunnel dynamic ESP
    
```

Sample Output: show services ipsec-vpn ipsec security-associations detail

```

user@host> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-1
Rule: rule-1, Term: term-1, Tunnel index: 1
Local gateway: 21.21.1.1, Remote gateway: 21.21.2.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Direction: inbound, SPI: 1909541182, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Not installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 35 seconds
Hard lifetime: Expires in 125 seconds
Anti-replay service: Disabled
    
```

show services ipsec-vpn ipsec statistics

Syntax	show services ipsec-vpn ipsec statistics <brief detail> <remote-gw <i>remote-peer-address</i> > <service-set <i>service-set-name</i> >
Description	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 IPsec statistics for all service sets. The display output is in brief mode. brief—Display total IPsec statistics for a service set. detail—Display IPsec statistics for all the tunnels within a service set. remote-gw <i>remote-peer-address</i> —Display IPsec statistics for an individual IPsec tunnel and an individual remote host. service-set <i>service-set-name</i> —(Optional) Display information about a particular service set.
Required Privilege Level	view
Output Fields	PIC—The physical interface on which the IPsec tunnel is configured. Service set—Name of the service set for which the IPsec tunnel is defined. Local gateway—Gateway address of the local system. Remote gates—Gateway address of the remote system. Tunnel index— (Detail output only) Numeric identifier of the specific IPsec tunnel for the security association. 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. 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

AH authentication failures—Total number of Authentication Header (AH) failures. An AH authentication failure occurs when there is a mismatch of the authentication header in a packet transmitted across an IPsec tunnel.

Replay errors—Total number of replay errors. A replay error is generated when a duplicate packet is received within the replay window.

ESP authentication failures—Total number of Encapsulation Security Payload (ESP) failures. An ESP failure occurs when there is an authentication mismatch in ESP packets.

Decryption errors—Total number of decryption errors.

Bad headers—Total number of bad headers detected.

Bad trailers—Total number of bad trailers detected.

Sample Output: show services ipsec-vpn ipsec statistics brief

```
user@host> show services ipsec-vpn ipsec statistics brief
PIC: sp-3/1/0, Service set: service-set-1
```

```
ESP Statistics:
Encrypted bytes:      0
Decrypted bytes:     0
Encrypted packets:   0
Decrypted packets:   0
AH Statistics:
Input bytes:         0
Output bytes:        0
Input packets:       0
Output packets:      0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, Decryption errors: 0
Bad headers: 0 Bad trailers: 0
```

Sample Output: show services ipsec-vpn ipsec statistics detail

```
user@host> show services ipsec-vpn ipsec statistics detail
PIC: sp-3/1/0, Service set: service-set-1
```

```
Local gateway: 21.21.1.1, Remote gateway: 21.21.2.1, Tunnel index: 1
ESP Statistics:
Encrypted bytes:      0
Decrypted bytes:     0
Encrypted packets:   0
Decrypted packets:   0
AH Statistics:
Input bytes:         0
Output bytes:        0
Input packets:       0
Output packets:      0
Errors:
AH authentication failures: 0, Replay errors: 0
ESP authentication failures: 0, Decryption errors: 0
Bad headers: 0 Bad trailers: 0
```

Sample Output: show services ipsec-vpn ipsec statistics remote-gw

```
user@host> show services ipsec-vpn ipsec statistics remote-gw 22.22.2.1
PIC: sp-3/1/0, Service set: service-set-2

Local gateway: 22.22.1.1, Remote gateway: 22.22.2.1, 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, Replay errors: 0
  ESP authentication failures: 0, Decryption errors: 0
  Bad headers: 0 Bad trailers: 0
```

