IPSec Commands

This module describes the IPSec commands.

Note The following IPSec commands are available only if the <platform>-k9sec.pie is installed.

clear crypto ipsec sa

To delete specific security associations (SAs), or all SAs in the IP Security (IPSec) security associations database (SADB), use the **clear crypto ipsec sa** command.

clear crypto ipsec sa {*sa-id*| **all**| **counters** | {*sa-id*| **all**}| **interface tunnel-ipsec**}

Syntax Description

sa-id	Identifier for the SA. IPSec supports from 1 to 64,500 sessions.
all	Deletes all IPSec SAs in the IPSec SADB.
counters	Clears the counters in the IPSec SADB.
interface	Clears the interfaces in the IPSec SADB.
tunnel-ipsec	The range of tunnel-ipsec is <0-4294967295>.

Command Default

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.4.0	The range for the *sa-id* argument increased to 16500 sessions.
Release 3.6.0	The upper limit for the *sa-id* argument range was increased to 64,500 sessions.

Usage Guidelines

SAs are established to secure data flows in IPSec. Use the **clear crypto ipsec sa** command to delete active IPSec sessions or force IPSec to reestablish new SAs. Usually, the establishment of SAs is negotiated between peers through Internet Key Exchange (IKE) on behalf of IPSec.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to remove the SA with ID 100 from the SADB:

```
RP/0/0/CPU0:router# clear crypto ipsec sa 100
```

Related Commands

Command	Description
show crypto ipsec sa, on page 5	Displays the settings used by current SAs.

description (IPSec profile)

To create a description of an IPSec profile, use the **description** command in profile configuration mode. To delete a profile description, use the **no** form of this command.

description *string*

no description

Syntax Description

string	Character string describing the IPSec profile.

Command Default

None

Command Modes

Crypto IPSec profile

Command History

Release	Modification
Release 3.2	This command was introduced.

Usage Guidelines

Use the **description** command inside the profile configuration submode to create a description for an IPSec profile.

Task ID

Task ID	Operations
profile configuration	read, write

Examples

The following example shows the creation of a profile description:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/0/CPU0:router(config-newprofile)# description this is a sample profile
```

show crypto ipsec sa

To display security association (SA) information based on the rack/slot/module location, use the **show crypto ipsec sa** command.

show crypto ipsec sa [*sa-id*| **peer** *ip-address*| **profile** *profile-name*| **detail**| **count**| **fvrf** *fvrf-name*| **ivrf** *ivrf-name*| **location** *node-id*]

Syntax Description

sa-id	(Optional) Identifier for the SA. The range is from 1 to 64500.
peer *ip-address*	(Optional) IP address used on the remote (PC) side. Invalid IP addresses are not accepted.
profile *profile-name*	(Optional) Specifies the alphanumeric name for a security profile. The character range is from 1 to 64. Profile names cannot be duplicated.
detail	(Optional) Provides additional dynamic SA information.
count	(Optional) Provides SA count.
fvrf *fvrf-name*	(Optional) Specifies that all existing SAs for front door virtual routing and forwarding (FVRF) is the same as the fvrf-name.
ivrf *ivrf-name*	(Optional) Specifies that all existing SAs for inside virtual routing and forwarding (IVRF) is the same as the ivrf-name.
location *node-id*	(Optional) Specifies that the SAs are configured on a specified location.

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.4.0	The range for the *sa-id* argument increased to 16500 sessions. Support was added for the following keywords: • fvrf • ivrf • location
Release 3.6.0	The upper limit for the *sa-id* argument range was increased to 64,500 sessions.

Usage Guidelines

If no optional argument or keyword is used, all SAs are displayed within a flow. Within a flow, the SAs are listed by protocol (Encapsulating Security Payload [ESP] or Authentication Header [AH]) and direction (inbound or outbound).

The **detail** keyword provides additional information only for SAs that are configured in a software crypto engine. The SAs are configured by using tunnel-ipsec and transport.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec sa** command:

```
RP/0/0/CPU0:router# show crypto ipsec sa

SSA id:          510
Node id:        0/1/0
SA Type:        MANUAL
interface:      service-ipsec22
profile  :      p7
local  ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.255/512/0)
remote ident (addr/mask/prot/port) : (0.0.0.0/0.0.0.0/512/0)
local crypto endpt: 0.0.0.0, remote crypto endpt: 0.0.0.0, vrf default

 #pkts tx         :0                     #pkts rx         :0
 #bytes tx        :0                     #bytes rx        :0
 #pkts encrypt    :0                     #pkts decrypt    :0
 #pkts digest     :0                     #pkts verify     :0
 #pkts encrpt fail:0                     #pkts decrpt fail:0
 #pkts digest fail:0                     #pkts verify fail:0
 #pkts replay fail:0
 #pkts tx errors  :0                     #pkts rx errors  :0

outbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
inbound esp sas:
        spi: 0x322(802)
        transform: esp-3des-md5
        in use settings = Tunnel
        sa agreed lifetime: 3600s, 4194303kb
        sa timing: remaining key lifetime: 3142303931sec/0kb
        sa DPD: disable, mode none, timeout 0s
        sa idle timeout: disable, 0s
        sa anti-replay (HW accel): enable, window 64
```

This table describes the significant fields shown in the display.

Table 1: show crypto ipsec sa Field Descriptions

Field	Description
SA id	Identifier for the SA.
interface	Identifier for the interface.
profile	String of alphanumeric characters that specify the name of a security profile.
local ident	IP address, mask, protocol, and port of the local peer.
remote ident	IP address, mask, protocol and port of the remote peer.
outbound esp sas	Outbound ESP SAs.
inbound esp sas	Inbound ESP SAs.
transform	The transform being used in the SA.
sa lifetime	The lifetime value used in the SA.

The following sample output is from the **show crypto ipsec sa** command for the **profile** keyword for a profile named pn1:

```
RP/0/0/CPU0:router# show crypto ipsec sa profile pn1

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

The following sample output is from the **show crypto ipsec sa** command for the **peer** keyword:

```
RP/0/0/CPU0:router# show crypto ipsec sa peer 172.19.72.120

SA id: 2
interface: tunnel0
```

```
profile: pn1
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

SA id: 2
interface: tunnel0
profile: pn1
local ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
local crypto endpt: 172.19.72.120, remote crypto endpt: 172.19.70.92
inbound esp sas:
spi: 0x2777997c (662149500)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb
```

show crypto ipsec statistics

To display global statistics for all inside virtual routing and forwarding (IVRF), use the **show crypto ipsec statistics** command in EXEC mode.

show crypto ipsec statistics [**ivrf** [*vrf name*]]

Syntax Description

ivrf *vrf name*	(Optional) Specifies that all existing SAs whose inside virtual routing and forwarding (IVRF) is the same as the ivrf-name.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.

Usage Guidelines

You can use the **show crypto ipsec statistics** command with the following results:

- Displays the statistics of all the VRFs that are associated with IPSec.
- Using the **ivrf** keyword, displays the statistics of the default VRF.
- Using the **ivrf** keyword and *vrf name* argument, displays the statistics of the specified VRF.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output displays the statistics of all the VRFs that are associated to IPSec from the **show crypto ipsec statistics** command:

```
RP/0/0/CPU0:router# show crypto ipsec statistics

 VRF: default  (VRF ID: 60000000)

 Active Tunnels :  1
 Expired Tunnels:  0

 pkts tx         :0                      pkts rx         :0
```

```
bytes tx        :0                      bytes rx        :0
pkts encrypt    :0                      pkts decrypt    :0
pkts digest    :0                      pkts verify     :0
pkts encrpt fail:0                      pkts decrpt fail:0
pkts digest fail:0                      pkts verify fail:0
pkts replay fail:0
pkts No SA fails:0
pkts sys cap fails:0
pkts tx errors  :0                      pkts rx errors  :0
```

This table describes the significant fields shown in the display.

Table 2: show crypto ipsec statistics Field Descriptions

Field	Description
VRF	VRF name and ID.
Active Tunnels	Number of active tunnels associated with the VRF. The VRF is the IVRF for these tunnels.
Expired Tunnels	Number of tunnels that are expired on the VRF. The VRF is the IVRF for these tunnels.
pkts tx	Aggregated number of outgoing packets on all the active tunnels associated to the VRF. The packets are from the trusted network.
bytes tx	Aggregated number of outgoing bytes on all the active tunnels associated to the VRF.
pkts encrypt	Aggregated number of encrypted packets on all the active tunnels associated to the VRF.
pkts digest	Aggregated number of authenticated packets on all the active tunnels associated to the VRF.
pkts encrypt fail	Aggregated number of packets that are dropped due to failing encryption on all the active tunnels associated to the VRF.
pkts digest fail	Aggregated number of packets that are dropped due to failing authentication on all the active tunnels associated to the VRF.
pkts replay fail	Aggregated number of packets that are dropped due to anti-replay check on all the active tunnels associated to the VRF.
pkts No SA fails	Aggregated number of incoming packets that failed because no SA was found in the context of the VRF.
pkts sys cap fails	Aggregated number of packets that failed due to lack of resources in the Cisco IPSec VPN SPA in the context of the VRF.

Field	Description
pkts tx errors	Number of outgoing packets that are dropped for any reason.
pkts rx	Aggregated number of incoming packets on all the active tunnels associated to the VRF. The packets are coming from the untrusted network.
bytes rx	Aggregated number of incoming bytes on all the active tunnels associated to the VRF.
pkts decrypt	Aggregated number of decrypted packets on all the active tunnels associated to the VRF.
pkts verify	Aggregated number of authenticated packets on all the active tunnels associated to the VRF.
pkts decrypt fail	Aggregated number of packets that are dropped due to failing decryption on all the active tunnels associated to the VRF.
pkts verify fail	Aggregated number of packets that are dropped due to failing authentication on all the active tunnels associated to the VRF.
pkts rx errors	Number of incoming packets that are dropped for any reason.

show crypto ipsec summary

To display IP Security (IPSec) summary information, use the **show crypto ipsec summary** command.

show crypto ipsec summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.5.0	Sample output was modified to display port number to the local peer and remote peer fields.

Usage Guidelines

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec summary** command:

```
RP/0/0/CPU0:router# show crypto ipsec summary

# * Attached to a transform indicates a bundle

# Active IPSec Sessions: 1

SA  Interface       Local Peer/Port   Remote Peer/Port  FVRF    Profile  Transform Lifetime
------------------------------------------------------------------------------------------
502 service-ipsec100 70.70.70.2/500    60.60.60.2/500    default ipsec1   esp-3des  esp
3600/100000000
```

This table describes the significant fields shown in the display.

Table 3: show crypto ipsec summary Field Descriptions

Field	Description
SA	Identifier for the security association.

Field	Description
Node	Identifier for the node.
Local Peer	IP address of the local peer.
Remote Peer	IP address of the remote peer.
FVRF	The front door virtual routing and forwarding (FVRF) of the SA. If the FVRF is global, the output shows f_vrf as an empty field
Mode	Profile mode type.
Profile	Crypto profile in use.
Transform	Transform in use.
Lifetime	Lifetime value, displayed in seconds followed by kilobytes.

show crypto ipsec transform-set

To display the configured transform sets, use the **show crypto ipsec transform-set** command.

show crypto ipsec transform-set [*transform-set-name*]

Syntax Description

transform-set-name	(Optional) IPSec transform set with the specified value for the *transform-set-name* argument are displayed.

Command Default

No default values. The default behavior is to print all the available transform-sets.

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.

Usage Guidelines

If no transform is specified, all transforms are displayed.

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is from the **show crypto ipsec transform-set** command:

```
RP/0/0/CPU0:router# show crypto ipsec transform-set

Transform set combined-des-sha: {esp-des esp-sha-hmac}
Transform set tsfm2: {esp-md5-hmac esp-3des }
        Mode: Transport
Transform set tsfm1: {esp-md5-hmac esp-3des }
        Mode: Tunnel
Transform set ts1: {esp-des  }
        Mode: Tunnel
```