



# 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](#), on page 2
- [description \(IPSec profile\)](#), on page 4
- [interface tunnel-ip \(GRE\)](#), on page 5
- [show crypto ipsec sa](#), on page 6
- [show crypto ipsec summary](#), on page 10
- [show crypto ipsec transform-set](#), on page 12
- [tunnel mode \(IP\)](#), on page 13
- [tunnel tos \(IP\)](#), on page 14
- [tunnel ttl \(IP\)](#), on page 15
- [tunnel dfbit disable \(IP\)](#), on page 16

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

**Command Default** No default behavior or values

**Command Modes** EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced.
	Release 3.4.0	The range for the <i>sa-id</i> argument increased to 16500 sessions.
	Release 3.6.0	The upper limit for the <i>sa-id</i> argument range was increased to 64,500 sessions.

**Usage Guidelines** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/CPU0:router# clear crypto ipsec sa 100
```

**Related Commands**

Command	Description
<a href="#">show crypto ipsec sa, on page 6</a>	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**

<b>Syntax Description</b>	<i>string</i> Character string describing the IPSec profile.
---------------------------	--

<b>Command Default</b>	None
------------------------	------

<b>Command Modes</b>	Crypto IPSec profile
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 2.0	This command was introduced.

<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
-------------------------	---

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

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	profile configuration	read, write

### Examples

The following example shows the creation of a profile description:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/RP0/CPU0:router(config-newprofile)# description this is a sample profile
```

## interface tunnel-ip (GRE)

To configure a tunnel interface for generic routing encapsulation (GRE), use the **interface tunnel-ip** command in global configuration mode. To delete the IP tunnel interface, use the **no** form of this command.

```
interface tunnel-ip number
no interface tunnel-ip number
```

### Syntax Description

*number* Instance number of the interface. The range is from 0 to 65535.

### Command Default

None

### Command Modes

Global configuration

### Command History

Release	Modification
Release 3.9.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### Task ID

Task ID	Operations
interface	read, write

### Examples

The following example shows how to use the **interface tunnel-ip** command:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 50000
RP/0/RP0/CPU0:router(config-if)#
```

## 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

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

### Command Modes

EXEC

### Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.4.0	The range for the <i>sa-id</i> argument increased to 16500 sessions. Support was added for the following keywords: <ul style="list-style-type: none"> <li>• fvrf</li> <li>• ivrf</li> <li>• location</li> </ul>
Release 3.6.0	The upper limit for the <i>sa-id</i> argument range was increased to 64,500 sessions.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

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/RP0/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.

Field	Description
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/RP0/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/RP0/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: pml  
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 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 2.0	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** To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Task ID	Task ID	Operations
	crypto	read

## Examples

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

```
RP/0/RP0/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 2: show crypto ipsec summary Field Descriptions**

Field	Description
SA	Identifier for the security association.
Node	Identifier for the node.
Local Peer	IP address of the local peer.

Field	Description
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*]

<b>Syntax Description</b>	<i>transform-set-name</i> (Optional) IPSec transform set with the specified value for the <i>transform-set-name</i> argument are displayed.
---------------------------	---

<b>Command Default</b>	No default values. The default behavior is to print all the available transform-sets.
------------------------	---

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.5.0	This command was introduced.

<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
-------------------------	---

If no transform is specified, all transforms are displayed.

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	crypto	read

<b>Examples</b>	The following sample output is from the <b>show crypto ipsec transform-set</b> command:
-----------------	---

```
RP/0/RP0/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
```

## tunnel mode (IP)

To set the encapsulation mode of the tunnel interface, use the **tunnel mode** in interface configuration mode. To delete the encapsulation mode, use the **no** form of this command.

```
tunnel mode gre ipv4
no tunnel mode
```

### Syntax Description

**gre** Generic Routing Encapsulation tunnel component.

*ipv4* IPv4 address of the tunnel interface.

### Command Default

The default tunnel mode is **gre ipv4**.

### Command Modes

Interface configuration

### Command History

Release	Modification
Release 3.9.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The tunnel is not operational until one of the modes is specified. Only one mode can be specified for a tunnel instance at any given time.

### Task ID

Task ID	Operations
tunnel	read, write
interface	read, write

### Examples

The following example shows how to set the encapsulation mode of the tunnel interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 1
RP/0/RP0/CPU0:router(config-if)# tunnel mode gre ipv4
```

## tunnel tos (IP)

To specify a TOS value in the tunnel encapsulating packet, use the **tunnel tos** command in the interface configuration mode. To return to the default TOS value, use the **no** form of this command.

**tunnel tos** *tos number*  
**no tunnel tos**

<b>Syntax Description</b>	<i>tos</i> TOS value in numbers. Range is from 0 to 255 <i>number</i>
---------------------------	--

<b>Command Default</b>	The system copies the TOS and COS bits of the internal IP header to the GRE IP header.
------------------------	--

<b>Command Modes</b>	Interface configuration
----------------------	-------------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	Release 3.9.0	This command was introduced.

<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
-------------------------	---

<b>Task ID</b>	<b>Task ID</b>	<b>Operations</b>
	tunnel	read, write
	interface	read, write

### Examples

The following example shows how to set the encapsulation mode of the tunnel interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 1
RP/0/RP0/CPU0:router(config-if)# tunnel tos 134
```

## tunnel ttl (IP)

To configure the time-to-live (TTL) value for the packets entering the tunnel, use the **tunnel ttl** command in the interface configuration mode. To return to the default TTL value, use the **no** form of this command.

```
tunnel ttl ttl number
no tunnel ttl
```

### Syntax Description

*ttl*      TTL value in numbers. Range is from 1 to 255  
*number*

### Command Default

The default value is 255.

### Command Modes

Interface configuration

### Command History

Release	Modification
Release 3.9.0	This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

### Task ID

Task ID	Operations
tunnel	read, write
interface	read, write

### Examples

The following example shows how to set the encapsulation mode of the tunnel interface:

```
RP/0/RP0/CPU0:router# configure
RP/0/RP0/CPU0:router(config)# interface tunnel-ip 1
RP/0/RP0/CPU0:router(config-if)# tunnel ttl 100
```

## tunnel dfbit disable (IP)

To allow fragmentation by configuring the DF bit setting in the tunnel transport header, use the **tunnel dfbit disable** command in the interface configuration mode. To return to the default DF bit setting, use the **no** form of this command.

**tunnel dfbit disable**  
**no tunnel dfbit disable**

<b>Syntax Description</b>	This command has no keywords or arguments.						
<b>Command Default</b>	The tunnel transport header is encapsulated with the DF bit set.						
<b>Command Modes</b>	Interface configuration						
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>Release 3.9.0</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	Release 3.9.0	This command was introduced.		
Release	Modification						
Release 3.9.0	This command was introduced.						
<b>Usage Guidelines</b>	To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.						
<b>Task ID</b>	<table border="1"> <thead> <tr> <th>Task ID</th> <th>Operations</th> </tr> </thead> <tbody> <tr> <td>tunnel</td> <td>read, write</td> </tr> <tr> <td>interface</td> <td>read, write</td> </tr> </tbody> </table>	Task ID	Operations	tunnel	read, write	interface	read, write
Task ID	Operations						
tunnel	read, write						
interface	read, write						
<b>Examples</b>	<p>The following example shows how to set the encapsulation mode of the tunnel interface:</p> <pre>RP/0/RP0/CPU0:router# <b>configure</b> RP/0/RP0/CPU0:router(config)# <b>interface tunnel-ip 1</b> RP/0/RP0/CPU0:router(config-if)# <b>tunnel dfbit disable</b></pre>						