IPSec Network Security Commands on Cisco IOS XR Software

This module describes the commands used to configure IP Security (IPSec) network security on the Cisco IOS XR software.

For detailed information about IPSec concepts, configuration tasks, and examples, see the *Implementing IPSec Network Security on Cisco IOS XR software* configuration module.

clear cryptoengine statistics

To clear the statistics for the crypto engine, use the **clear crypto engine statistics** command in EXEC mode.

clear crypto engine statistics location *node-id*

Syntax Description

location *node-id*	Specifies the crypto engine subslot location.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

You must provide a location. For example, the location specifies a bay for a shared port adapter (SPA), which is either 0/1/0 or 0/1/1.

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how to clear the statistics for the crypto engine for location 0/1/1:

```
RP/0/0/CPU0:router# clear crypto engine statistics location 0/1/1
```

Related Commands

Command	Description
show crypto engine statistics	Displays information for the hardware data path counters that are gathered from the crypto engine statistics.

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 in EXEC mode.

clear crypto ipsec sa {*sa-id* | **all**}

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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	The range for the *sa-id* argument increased to 16500 sessions.
Release 3.5.0	No modification.
Release 3.6.0	The upper limit for the *sa-id* argument range was increased to 64,500 sessions.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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	Displays the settings used by current SAs.

clear crypto ipsec sa interface

To clear all the security associations (SAs) under the specified the interface, use the **clear crypto ipsec sa interface** command in EXEC mode.

clear crypto ipsec sa interface {**service_ipsec** *number* | **service_gre** *number* |**tunnel-ipsec** *number*}

Syntax Description

tunnel-ipsec *number*	Specifies IPSec Tunnel interfaces. The range is from 0 to 4294967295.
service_ipsec *number*	Specifies IPSec Service interfaces. The range is from 1 to 65535.
service_gre *number*	Specifies GRE Service interfaces. The range is from 1 to 65535.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Task ID

Task ID	Operations
crypto	execute

Examples

The following example shows how clear all the SAs for a tunnel-ipsec interface:

```
RP/0/0/CPU0:router# clear crypto ipsec sa interface tunnel-ipsec 1
```

Related Commands

Command	Description
show crypto ipsec sa	Displays specific security associations (SAs), or all SAs in the IP Security (IPSec) security associations database (SADB).
show crypto ipsec interface	Displays the crypto IPSec interface.

crypto ipsec df-bit (global)

To set the DF bit for the encapsulating header in tunnel mode to all interfaces, use the **crypto ipsec df-bit** command in global configuration mode.

crypto ipsec df-bit {**clear** | **set** | **copy**}

Syntax Description

clear	Specifies that the outer IP header has the DF bit cleared and the router can fragment the packet to add the IP Security (IPSec) encapsulation.
set	Specifies that the outer IP header has the DF bit set; however, the router can fragment the packet if the original packet had the DF bit cleared.
copy	Specifies that the router looks in the original packet for the outer DF bit setting. The **copy** keyword is the default setting.

Defaults

The default is the **copy** keyword.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **crypto ipsec df-bit** command in global configuration mode to configure your router to specify the DF bit in an encapsulated header.

You can use the clear setting for the DF bit when encapsulating tunnel mode IPSec traffic so that you can send packets larger than the available maximum transmission unit (MTU) size, even if you do not know the available MTU size.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to clear the DF bit on all interfaces:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec df-bit clear
```

Related Commands

Command	Description
crypto ipsec df-bit (interface)	Sets the DF bit for the encapsulating header in tunnel mode to a specific interface.
interface service-ipsec	Creates a static IPSec virtual interface.
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.

crypto ipsec df-bit (interface)

To set the DF bit for the encapsulating header in tunnel mode to a specific interface, use the **crypto ipsec df-bit** command in service-ipsec interface configuration mode.

crypto ipsec df-bit {**clear** | **set** | **copy**}

Syntax Description

clear	Specifies that the outer IP header can have the DF bit cleared and the router may fragment the packet to add the IP Security (IPSec) encapsulation.
set	Specifies that the outer IP header can have the DF bit set; however, the router may fragment the packet if the original packet had the DF bit cleared.
copy	Specifies that the router looks in the original packet for the outer DF bit setting. The **copy** keyword is the default setting.

Defaults

The default is taken from the global configuration.

Command Modes

service-ipsec interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **crypto ipsec df-bit** command in interface configuration mode to configure your router to specify the DF bit in an encapsulated header. This command overrides any existing DF bit global settings.

You can use the clear setting for the DF bit when encapsulating tunnel mode IPSec traffic so that you can send packets larger than the available maximum transmission unit (MTU) size, even if you do not know the available MTU size.

Task ID

Task ID	Operations
crypto	read, write

Examples

In following example, the router is configured to globally clear the setting for the DF bit and copy the bit from the interface named service-ipsec 5. Thus, all interfaces except service-ipsec 5 allow the router to send packets larger than the available MTU size; service-ipsec 5 allows the router to fragment the packet:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface service-ipsec 5
RP/0/0/CPU0:router(config-if)# crypto ipsec df-bit clear
```

Related Commands

Command	Description
crypto ipsec df-bit (global)	Sets the DF bit for the encapsulating header in tunnel mode to all interfaces.
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface service-ipsec	Creates a static IPSec virtual interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.

crypto mib ipsec flowmib history failure size

To set the size of the IP Security (IPSec) MIB failure history table, use the **crypto mib ipsec flowmib history failure size** command in global configuration mode.

crypto mib ipsec flowmib history failure size *number*

Syntax Description

number	Size of the failure history table. The range is from 2 to 16000. The default value is 16000.

Defaults

The default value is 16000.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

A failure history table stores the reason for tunnel failure and the time that the failure occurred. A failure history table is used as a simple method to distinguish between a normal and an abnormal tunnel termination. That is, if a tunnel entry in the tunnel history table has no associated failure record, the tunnel must have terminated normally. However, every failure does not correspond to a tunnel. Supported setup failures are recorded in the failure table, but a history table is not associated because a tunnel was never set up.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the size of a failure history table is configured to be 140:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto mib ipsec flowmib history failure size 140
```

crypto ipsec pmtu

To specify the default path maximum transmission unit (MTU) for the SAs that is created under the interface, use the **crypto ipsec pmtu** command in service-ipsec interface configuration mode. To disable this feature, use the **no** form of this command.

crypto ipsec pmtu *pmtu*

no crypto ipsec pmtu *pmtu*

Syntax Description

pmtu	Value of MTU in bytes. The range is from 68 to 9216.

Defaults

If you do not specifically set the **crypto ipsec pmtu** command, the default value is 9000.

Command Modes

Service-ipsec interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

The **crypto ipsec pmtu** command is supported under service-ipsec interfaces only. The service-gre interfaces are not supported.

The PMTU must be set with the MTU value on the WAN (encrypted) side.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the **crypto ipsec pmtu** command is set to 1500 for the service-ipsec interface:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface service-ipsec 5
```

```
RP/0/0/CPU0:router(config-if)# crypto ipsec pmtu 1500
```

Related Commands

Command	Description
interface service-ipsec	Creates a static IPSec virtual interface.

crypto ipsec pre-fragmentation disable

To specify the handling of fragmentation for the near-MTU-sized packets, use the **crypto ipsec pre-fragmentation disable** command in global configuration mode or service-ipsec interface configuration mode. To disable this feature, use the **no** form of this command.

crypto ipsec pre-fragmentation disable

no crypto ipsec pre-fragmentation disable

Syntax Description(

disable	Disables fragmentation of large packets before IPSec encapsulation.

Defaults

Prefragmentation is enabled.

Command Modes

Global configuration
Service-ipsec interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

The prefragmentation feature allows an encrypting router to predetermine the encapsulated packet size from information available in transform sets, which are configured as part of the IPSec security association (SA). If it is predetermined that the packet exceeds the MTU of the interface, the packet is fragmented before encryption. This function avoids process-level reassembly before decryption and helps improve decryption performance and overall IPSec traffic throughput.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **crypto ipsec pre-fragmentation disable** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec pre-fragmentation disable
```

crypto ipsec profile

To configure the IP Security (IPSec) profile and enter profile configuration mode, use the **crypto ipsec profile** command in global configuration mode. To remove the IPSec profile, use the **no** form of this command.

crypto ipsec profile *name*

no crypto ipsec profile *name*

Syntax Description

name	Name of an IPSec profile to create or modify. The maximum length is 32 characters.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introducd on the .
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	An argument was added to **reverse-route** command profile entry and other commands.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **crypto ipsec profile** command to create a new crypto profile or modify an existing crypto profile.

Crypto profiles configure cryptographic behavior for IPSec transport and IPSec-enabled interfaces (service-ipsec, service-gre, and tunnel-ipsec).

The following commands are available in profile configuration mode:

- **match transform-set** —Configures the access control list (ACL) to use for packet classification and the transform set to use for IPSec processing. Multiples of this command are supported under the same profile.
- **reverse-route**—Enables reverse-route injection (RRI) metrics, allowing configuration of an administrative distance from 1 to 255 as a precedence for dynamic routing.

- **set pfs**—Sets or resets the perfect forward secrecy (PFS) setting for IKE to handle Diffie-Hellman negotiation.

  The default is group1, which corresponds to 768-bit Diffie-Hellman prime modulus group; group2 corresponds to 1024-bit Diffie-Hellman prime modulus group; and group5 corresponds to 1536-bit Diffie-Hellman prime modulus group.

  PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised because subsequent keys are not derived from previous keys.
- **set security-association replay disable**—Disables replay checking for a particular crypto profile.
- **set security-association idle-time**—Specifies the maximum amount of time in which the current peer can be idle before the default peer is used.
- **set security-association lifetime**—Overrides (for a particular crypto map entry) the global lifetime value.
- **set session-key inbound ah**—Specifies the IP Security session keys to set the inbound IPSec session key for the Authentication Header (AH) protocol.
- **set session-key inbound esp**—Specifies the IP Security session key to set the inbound IPSec session key for Encapsulation Security Protocol (ESP).
- **set session-key outbound ah**—Specifies the IP Security session key to set the outbound IPSec session key for the AH protocol.
- **set session-key outbound esp**—Specifies the IP Security session key to set the outbound IPSec session key for ESP.
- **set transform-set**—Specifies a list of transform sets in priority order.
- **set type**—Sets or resets the profile mode. The default is the **static** keyword. The **dynamic** keyword lets the profile handle Dynamic Crypto Profile (DCP), which means security association (SA) negotiation from any authenticated peer is allowed. Static mode lets the peer be identified in the configuration (tunnel mode).

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to create a crypto profile named “newprofile,” set the PFS to group2, and configure the profile as a dynamic profile:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/0/CPU0:router(config-newprofile)# set pfs group2
RP/0/0/CPU0:router(config-newprofile)# set type dynamic
RP/0/0/CPU0:router(config-newprofile) match myacl transform-set mytransformset
```

Related Commands

Command	Description
match transform-set	Configures an ACL to use for packet classification, and if the packets need protecting, the transform set to use for IPSec processing.
set pfs	Sets PFS for IKE to handle Diffie-Hellman negotiation.

Command	Description
set security-association idle-time	Specifies the maximum amount of time in which the current peer can be idle before the default peer is used.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value.
set security-association replay disable	Disables replay checking for a particular crypto profile.
set session-key inbound ah	Specifies the IP Security session keys to set the inbound IPSec session key for the AH protocol.
set session-key inbound esp	Specifies the IP Security session key to set the inbound IPSec session key for ESP.
set session-key outbound ah	Specifies the IP Security session key to set the outbound IPSec session key for the AH protocol.
set session-key outbound esp	Specifies the IP Security session key to set the outbound IPSec session key for ESP.
set transform-set	Specifies a list of transform sets in priority order.
set type	Sets the profile mode type.
show crypto ipsec profile	Displays the crypto profiles that are defined on a router.

crypto ipsec nat-transparency disable

To disable security parameter index (SPI) matching or User Datagram Protocol (UDP) encapsulation between two Virtual Private Network (VPN) devices, use the **crypto ipsec nat-transparency** command on both devices in global configuration mode. To enable back this feature, use the **no** form of this command.

crypto ipsec nat-transparency disable

no crypto ipsec nat-transparency disable

Syntax Description

disable	Disables NAT transparency capability.

Defaults

The NAT transparency feature is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **cryto ipsec nat-transparency** command to resolve issues that arise when Network Address Translation (NAT) is configured in an IP Security (IPsec)-aware network.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **crypto ipsec nat-transparency** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec nat-transparency disable
```

crypto ipsec security-association idle-time

To configure the IP Security (IPSec) security association (SA) idle timer, use the **crypto ipsec security-association idle-time** command in global configuration mode. To inactivate the IPSec SA idle timer, use the **no** form of this command.

crypto ipsec security-association idle-time *seconds*

no crypto ipsec security-association idle-time

Syntax Description

seconds	Time, in seconds, that the idle timer allows an inactive peer to maintain an SA. Valid values for the *seconds* argument range from 600 to 86400.

Defaults

IPSec SA idle timers are disabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **crypto ipsec security-association idle-time** command to configure the IPSec SA idle timer. The timer controls the amount of time that an SA is maintained for an idle peer.

The IPSec SA idle timers are different from the global lifetimes for IPSec SAs. The expiration of the global lifetimes is independent of peer activity. The IPSec SA idle timer allows SAs associated with inactive peers to be deleted before the global lifetime has expired.

Note If the last IPSec SA to a given peer is deleted due to idle timer expiration, the Internet Key Exchange (IKE) SA to that peer is also deleted.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to configure the IPSec SA idle timer to drop SAs for inactive peers after 600 seconds:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec security-association idle-time 600
```

Related Commands

Command	Description
clear crypto ipsec sa	Deletes specific SAs.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating IPSec SAs.
set security-association idle-time	Specifies the maximum time in which the current peer can be idle before the default peer is used.

crypto ipsec security-association lifetime

To change the global lifetime values used when negotiating IP Security (IPSec) security associations (SAs), use the **crypto ipsec security-association lifetime** command in global configuration mode. To reset an SA lifetime to the default value, use the **no** form of this command.

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** | **kilobytes**}

Syntax Description

seconds *seconds*	Number of seconds an SA lives before expiring. The range is from 120 to 86400 seconds.
kilobytes *kilobytes*	Volume of traffic (in KB) that can pass between IPSec peers using a given SA before that SA expires. Range is from 2560 to 536870912 KB.

Defaults

seconds: 3600 seconds (1 hour)
kilobytes: 4194303 kilobytes (10 MBps for 1 hour)

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.4.1	The range for the **kilobytes** keyword was modified.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

IPSec SAs use shared secret keys. These keys and their SAs time out together.

Assuming that the particular crypto profile entry does not have lifetime values configured, when the router requests new SAs during SA negotiation, it specifies its global lifetime value in the request to the peer; it uses this value as the lifetime of the new SAs. When the router receives a negotiation request from the peer, it uses either the smaller of the lifetime value proposed by the peer or the locally configured lifetime value as the lifetime of the new SAs.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The SA expires after the first of these lifetimes is reached.

If you change a global lifetime, the change is not applied to existing SAs, but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, clear all or part of the SA database by using the **clear crypto ipsec sa** command.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** form of the command. The timed lifetime causes the SA to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** form of the command. The traffic-volume lifetime causes the SA to time out after the specified amount of traffic (in KB) has been protected by the key of the SAs.

Shorter lifetimes can make mounting a successful key recovery attack more difficult because the attacker has less data encrypted under the same key with which to work. However, shorter lifetimes require more CPU processing time for establishing new SAs.

How These Lifetimes Work

The SA keys expire according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in KB has passed (specified by the **kilobytes** keyword).

A new SA is negotiated *before* the lifetime threshold of the existing SA is reached to ensure that a new SA is ready for use when the old one expires. The new SA is negotiated approximately 30 seconds before the **seconds** lifetime expires or when the volume of traffic through the tunnel reaches around 90percent of the **kilobytes** lifetime (whichever occurs first). The final values of the seconds and kilobytes lifetimes are determined per SA during the SA negotiation and are agreed on by both sides. Each side offers the configured lifetime and the shortest lifetime is then chosen.

If no traffic has passed through the tunnel during the entire life of the SA, a new SA is not negotiated when the lifetime expires. Instead, a new SA is negotiated only when IPSec identifies another packet that should be protected.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to shorten lifetimes to reduce the risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2304000 KB (10 MBps for 30 minutes).

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec security-association lifetime seconds 2700
RP/0/0/CPU0:router(config)# crypto ipsec security-association lifetime kilobytes 2304000
```

Related Commands

Command	Description
clear crypto ipsec sa	Deletes a specific SA or all SAs in the IPSec SADB.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations.

crypto ipsec security-association replay disable

To disable antireplay checking globally, use the **crypto ipsec security-association replay disable** command in global configuration mode. To reset the configuration to enable antireplay checking, use the **no** form of this command.

crypto ipsec security-association replay disable

Syntax Description

This command has no arguments or keywords.

Defaults

Antireplay checking is enabled.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that antireplay checking has been disabled globally:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec security-association replay disable
```

Related Commands

Command	Description
crypto ipsec security-association replay window-size	Sets the size of the security association (SA) antireplay window globally.
crypto ipsec nat-transparency disable	Configures the IPSec SA idle timer.

crypto ipsec security-association replay window-size

To set the size of the security association (SA) antireplay window globally, use the **crypto ipsec security-association replay window-size** command in global configuration mode. To reset the window size to the default of 64, use the **no** form of this command.

crypto ipsec security-association replay window-size {*N*}

no crypto ipsec security-association replay window-size

Syntax Description

N	Size of the window. Values are 64, 128, 256, 512, and 1024. This value becomes the default value. **Note** The window size is significant only if antireplay checking is enabled.

Defaults

If a window size is not entered, the default is 64.

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the size of the SA antireplay window is set globally to 128:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec security-association replay window-size 128
```

Related Commands

Command	Description
crypto ipsec security-association replay disable	Disables antireplay checking globally.

crypto ipsec transform-set

To define a transform set (an acceptable combination of security protocols and algorithms), use the **crypto ipsec transform-set** command in global configuration mode. To delete a transform set, use the **no** form of this command.

crypto ipsec transform-set *name*
transform-set submode **transform** *protocol*
transform-set submode **mode** {t**ransport** | **tunnel**}

no crypto ipsec transform-set *name*

Syntax Description

name	Name of the transform set to create or modify. Maximum is 32 characters in length.
transform	(Optional) Defines transforms (protocols) for the transform set.
mode	(Optional) Changes the mode for a transform set.
transport	(Optional) Specifies the transport mode for a transform set.
tunnel	(Optional) Specifies the tunnel mode for a transform set. The default value is the **tunnel** keyword.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced.
Release 3.0	No modification.
Release 3.2	No modification.
Release 3.3.0	No modification.
Release 3.4.0	The **mode**, **transform**, **transport**, and **tunnel** keywords were added.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

The syntax for the **crypto ipsec transform-set** command is similar to the **crypto ipsec profile** command.

Use transform sets to define the IPSec security protocols and algorithms for Authentication Header (AH), Encapsulating Security Payload (ESP), or both.

For AH, use either of the following authentication algorithms:

- ah-md5-hmac: AH-HMAC-Message Digest 5 (MD5) transform
- ah-sha-hmac: AH-HMAC-SHA transform

For ESP, use any of the following cipher algorithms:

- esp-3des: ESP transform using 3DES(EDE) cipher (168 bits)
- esp-des: ESP transform using Digital Encryption Standard (DES) cipher (56 bits)
- esp-aes: ESP transform using Advanced Encryption Standard (AES) cipher (128 bits)
- esp-192-aes: ESP transform using AES cipher (192 bits)
- esp-256-aes: ESP transform using AES cipher (256 bits)

For an optional ESP, use either of the following authentication algorithms:

- esp-md5-hmac: ESP transform using Hashed Message Authentication Code-Message Digest 5 (HMAC-MD5) auth
- esp-sha-hmac: ESP transform using HMAC-SHA auth

Verification of valid transform combinations is done during command-line interface (CLI) configuration. Multiple transform sets can be configured, and then one or more of these transform sets are specified in the crypto profile. The transform set defined in the crypto profile is used in the IPSec service affecting negotiation to protect the data flows specified by that crypto profile access list. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of the IPSec SAs for both peers. Changes to an existing transform set affects subsequent SA negotiations.

Examples of acceptable transform combinations to define the IPSec security protocols and algorithms for AH, ESP, or both follow:

- **ah-md5-hmac**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

The CLI parser prevents you from entering invalid combinations; for example, after you specify an AH transform, you cannot specify another AH transform for the current transform set.

IPSec Protocols: Encapsulation Security Protocol and Authentication Header

Both the ESP and AH protocols implement security services for IPSec.

ESP provides packet encryption and optional data authentication and antireplay services. ESP encapsulates the protected data—either a full IP datagram or only the payload—with an ESP header and ESP trailer.

AH provides data authentication and antireplay services. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload.

Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram; transport mode encapsulates and protects the payload of an IP datagram.

Tip The following tips can help you select transform sets that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.
- If you want to ensure data authentication for the outer IP header and the data, include an AH transform. (The benefits of outer IP header data integrity are debatable.)
- If you use an ESP encryption transform, also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH), you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slower.

Note Some transforms might not be supported by the IPSec peer.

Suggested transform combinations follow:

- **esp-des** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

Changing Existing Transforms

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transform replaces the existing transform for that transform set.

Any change to a transform set definition is applied only to crypto profile entries that reference the transform set. The changes are not applied to existing SAs, but are used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, clear all or part of the security association database (SADB) by using the **clear crypto ipsec sa** command.

You can change the mode that is specified for the transform. This setting is used only when the traffic to be protected has the same IP address as the IPSec peers. (This traffic can be encapsulated either in tunnel or transport mode.) This setting is ignored for all other traffic. (All other traffic is encapsulated in tunnel mode.)

After you define a transform set, you are put into the transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you use this command to change the mode, the change affects only the negotiation of subsequent IPSec security associations that specify the transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. For more information, see the clear crypto ipsec sa command.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol [ESP] header and trailer, an Authentication Header [AH], or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic and for service-gre interfaces. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) in which hosts on one protected network send packets to hosts on a different protected network through a pair of IPSec peers. With VPNs, the IPSec peers "tunnel" the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to define the transform set with an IPSec peer that supports esp-sha-hmac:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec transform-set new
RP/0/0/CPU0:router(config-transform-set new)# transform esp-sha-hmac
```

The following example shows how to change the mode to transport for a transform set:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec transform-set new
RP/0/0/CPU0:router(config-transform-set new)# mode transport
```

Related Commands

Command	Description
clear crypto ipsec sa	Deletes specific SAs or all SAs in the IPSec SADB.
set transform-set	Specifies a list of transform sets in priority order.
match transform-set	Configures an ACL to use for packet classification, and if the packets need protecting, the transform set to use for IPSec processing.
show crypto ipsec transform-set	Displays the configured transform sets.

crypto ipsec transport

To enter IPSec transport configuration mode, use the **crypto ipsec transport** command in global configuration mode. To exit IPSec transport configuration mode, use the **no** form of this command.

crypto ipsec transport

no crypto ipsec transport

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Authentication Header (AH) and Encapsulating Security Payload (ESP) operate in two IPSec modes, transport and tunnel.

In the transport mode, IP Security (IPSec) protects the Upper Layer Protocol (ULP) header and the payload. IPSec transport mode is used when security is desired end-to-end, that is, security endpoints are the same as host endpoints.

In the tunnel mode, the entire IP datagram is protected, which includes the IP header, the ULP header, and the payload. Tunnel mode is used when security endpoints are not the same as host endpoints. IPSec tunnels can be nested.

All transport mode IPSec traffic must be configured in the crypto ipsec transport mode.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that IPSec transport configuration mode is entered and then a crypto profile is configured in this mode:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec transport
RP/0/0/CPU0:router(config-transport)# profile pn1
```

Related Commands

Command	Description
profile	Specifies the crypto profile to use in IPSec processing.

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.

Defaults

No default behavior or values.

Command Modes

Crypto IPSec profile

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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
```

Related Commands

Command	Description
reverse-route	Configures reverse-route injection (RRI) metrics for a crypto profile.

interface service-ipsec

To create a static IPSec-protected virtual interface, use the **interface service-ipsec** command in global configuration mode. To delete the static IPSec virtual interface, use the **no** form of this command.

interface service-ipsec *number*

no interface service-ipsec *number*

Syntax Description

number	Identifies a static IPSec-protected virtual interface. The range is from 1 to 65535.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **interface service-ipsec** command to enter service-ipsec interface configuration mode.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **interface service-ipsec** command:

```
RP/0/RSP00/CPU0:router# configure
RP/0/RSP00/CPU0:router(config)# interface service-ipsec 200
RP/0/RSP00/CPU0:router(config-if)#
```

Related Commands

Command	Description
crypto ipsec nat-transparency disable	Specifies the default path maximum transmission unit (MTU) for the SAs that is created under the interface.
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.
profile	Specifies which crypto profile to use for IP Security (IPSec) processing.
service-location (IPSec)	Specifies both active and standby locations for the interface.
show services redundancy	Displays all configured services with their active and standby physical locations, as configured by the **services-location** command. For information, see *Cisco IOS XR System Management Command Reference*.

interface service-gre

To create a static IPSec-protected generic routing encapsulation (GRE) interface, use the **interface service-gre** command in global configuration mode. To delete a static IPSec-protected GRE interface, use the **no** form of this command.

interface service-gre *number*

no interface service-gre *number*

Syntax Description

number	Identifies a static IPSec-protected GRE interface. The range is from 1 to 65535.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **interface service-gre** command to enter service-gre interface configuration mode.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **interface service-gre** command:

```
RP/0/RSP00/CPU0:router# configure
RP/0/RSP00/CPU0:router(config)# interface service-gre 500
RP/0/RSP00/CPU0:router(config-if)#
```

Related Commands

Command	Description
interface service-ipsec	Creates a static IPSec virtual interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.
profile	Specifies which crypto profile to use for IP Security (IPSec) processing.
service-location (IPSec)	Specifies both active and standby locations for the interface.

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

interface tunnel-ipsec

To create a virtual IPSec-protected tunnel interface, use the **interface tunnel-ipsec** command in global configuration mode. To delete the IPSec tunnel interface, use the **no** form of this command.

interface tunnel-ipsec *number*

no interface tunnel-ipsec *number*

Syntax Description

number	Identifies a virtual IPSec-protected tunnel interface. The range is from 0 to 4294967295.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

The **interface tunnel-ipsec** command is used for virtual tunnel interfaces, which are not implemented on a service card.

Use the **interface tunnel-ipsec** command to enter tunnel-ipsec interface configuration mode.

Task ID

Task ID	Operations
interface	read, write

Examples

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

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

Related Commands

Command	Description
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface service-ipsec	Creates a static IPSec virtual interface.
profile	Specifies which crypto profile to use for IP Security (IPSec) processing.
service-location (IPSec)	Specifies both active and standby locations for the interface.

match transform-set

To configure an access control list (ACL) to use for packet classification, and if the packet needs protecting, the transform set to use for IP Security (IPSec) processing, use the **match transform-set** command in profile configuration mode. To remove the configuration, use the **no** form of this command.

match *acl-name* **transform-set** *transform-set-name*

no match *acl-name* **transform-set** *transform-set-name*

Syntax Description

acl-name	ACL name used for packet classification. Range is from 1 to 65535.
transform-set-name	Name of a transform set. You can configure up to five transform sets in priority order. Maximum is 32 characters in length.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

For the Cisco IPSec VPN SPA, the crypto IPSec profiles that use this syntax are attached only to the tunnel-ipsec interfaces and service-ipsec interfaces and not to the service-gre interfaces.

You can configure a few lines of the **match transform-set** command under one profile. The following example shows that acl1 and acl2 can match different traffic patterns:

```
crypto ipsec profile p1
    match acl1 transform-set ts1
    match acl2 transform-set ts2
```

We do not recommend configuring ACLs that match the same traffic pattern under the same profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to specify 101 as the ACL and tset1 as the transform set:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/0/CPU0:router(config-newprofile)# match 101 transform-set tset1
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
crypto ipsec transform-set	Defines a transform set (an acceptable combination of security protocols and algorithms).
set transform-set	Specifies a list of transform sets in priority order.

profile

To specify which crypto profile to use for IP Security (IPSec) processing, use the **profile** command in the appropriate configuration mode. To remove a crypto profile name, use the **no** form of this command.

profile *profile-name*

no profile *profile-name*

Syntax Description

profile-name	Previously defined crypto profile to use. Profiles cannot be shared on different tunnel-ipsec interfaces, transport modes, or both within the same IPSec mode or across different IPSec modes. The character range is from 1 to 32 characters. **Note** You can share profiles between different service-ipsec interfaces and service-gre interfaces. However, you cannot share a profile between a service-ipsec and a service-gre interfaces.

Defaults

No default behavior or values

Command Modes

Transport configuration
Tunnel-ipsec interface configuration
Service-ipsec interface configuration
Service-gre interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	Support was added for the service-ipsec interface and service-gre interface configuration modes.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **profile** command to specify the profile to use in IPSec processing, and then determine which traffic is protected and how the traffic is protected.

The same profile cannot be shared in different IPSec modes.

The following conditions are listed:

- The profile cannot be shared in different tunnel-ipsec interfaces and in transport configuration mode; however, the profile is shared between different service-ipsec and service-gre interfaces.
- You can configure a few profiles under transport and tunnel interfaces. Service-ipsec and service-gre interfaces each have only one profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows a crypto profile being configured:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec transport
RP/0/0/CPU0:router(config-transport)# profile pn1
RP/0/0/CPU0:router(config-transport)# exit
```

Related Commands

Command	Description
crypto ipsec transport	Enters IPSec transport configuration mode.
interface service-ipsec	Creates a static IPSec virtual interface.
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.

reverse-route

To enable configuration of reverse-route injection (RRI) metrics for a crypto profile entry, based on a routing preference for either statically or dynamically learned routes, use the **reverse-route** command in profile configuration mode. To cancel RRI metric configuration or revert to a crypto profile, use the **no** form of this command.

reverse-route {[distance *distance value* **| tag** *tag value*]}

no reverse-route

Syntax Description

distance *distance value*	Administrative distance from 1 to 255 sets a precedence for dynamic routing. Static route always takes precedence. The default is 0.
tag *tag value*	Tag can be from 1 to 497777. When you add a tag to a route, you associate a value with a predefined group that allows you to manipulate the routing policy on all the routes that share the same tag value.

Defaults

Default distance is 0, indicating a static route. Statically learned routes take precedence by default.

Command Default

IPSec profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	The key words **distance** and **tag** were added to enhance configuration of an administrative distance in the reverse-route profile.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

You may configure either the **distance** or **tag** keyword, or both, in any order, as desired.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **reverse-route** command:

```
RP/0/0/CPU0:router# crypto ipsec profile myprofile
RP/0/0/CPU0:router(config-myprofile)# reverse-route distance 1 tag 11
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.

service-location (IPSec)

To specify both active and standby locations for the interface, use the **service-location** command in the appropriate configuration mode. To remove the service location from the interface, use the **no** form of this command.

service-location preferred-active *node-id* [**preferred-standby** *node-id* [**auto-revert**]]

no service-location preferred-active *node-id* [**preferred-standby** *node-id* [**auto-revert**]]

Syntax Description

preferred-active *node-id*	Specifies that the SPA in this location serves all traffic going through the interface. The *node-id* argument is expressed in *rack/slot/module* notation.
preferred-standby *node-id*	(Optional) Specifies which location is used in case of a SPA failure or a line card failure. The *node-id* argument is expressed in *rack/slot/module* notation.
auto-revert	(Optional) Reverts back to the active location once the active location is ready to process traffic. **Note** The **auto-revert** keyword is specified only if the **preferred-standby** keyword with the *node-id* argument is configured.

Defaults

No default behavior or values

Command Modes

service-ipsec interface configuration
service-gre interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

By using the **no** form of this command, the features and the interface are removed from the specified location.

The **service-location** (IPSec) command is configured only under the service-ipsec and service-gre interfaces.

When the **service-location** command is specified, features of the interface are created on the specified locations. When removing the **service-location** command, all of the features, such as QoS and IPSec SAs are removed from the location.

A virtual interface must be associated with an IPSec service SPA. All interfaces that share the same, for example, tunnel source and front door virtual routing and forwarding (FVRF) number of objects, must be associated with the same service location.

If a location is specified and there is no Cisco IPSec VPN SPA in this location, the features are not configured on the interface.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to use the **service-location** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface service-ipsec 500RP/0/0/CPU0:router(config-if)#
service-location preferred-active 0/0/0 preferred-standby 0/1/0
```

Related Commands

Command	Description
interface service-ipsec	Creates a static IPSec virtual interface.
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
profile	Specifies which crypto profile to use for IPSec processing.
show services redundancy	Displays all configured services with their active and standby physical locations, as configured by the **services-location** command. For information, see *Cisco IOS XR System Management Command Reference*.
tunnel destination (IPSec)	Specifies the destination for a tunnel interface.
tunnel source (IPSec)	Specifies the source address for a tunnel interface.
tunnel vrf (IPSec)	Associates a VRF instance with a specific tunnel destination, interface, or subinterface.

set pfs

To set or reset the perfect forward secrecy (PFS) setting for Internet Key Exchange (IKE) to handle Diffie-Hellman negotiation, use the **set pfs** command in profile configuration mode. To reset the PFS setting, use the **no** form of this command.

set pfs {**group1** | **group2** | **group5**}

no set pfs {**group1** | **group2** | **group5**}

Syntax Description

group1	Corresponds to the 768-bit Diffie-Hellman prime modulus group.
group2	Corresponds to the 1024-bit Diffie-Hellman prime modulus group.
group5	Corresponds to the 1536-bit Diffie-Hellman prime modulus group.

Defaults

The default is 768-bit Diffie-Hellman (group 1).

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

PFS is a cryptographic characteristic associated with a derived shared secret value. With PFS, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys.

Task IDd

Task ID	Operations
crypto	read, write

Examples

In the following example, an IP Security (IPSec) profile named myprofile is created and PFS is set to group2:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/0/CPU0:router(config-myprofile)# set pfs group2
```

set security-association idle-time

To specify the maximum time in which the current peer can be idle before the default peer is used and to override the global configuration, use the **set security-association idle-time** command in profile configuration mode. To disable this feature, use the **no** form of this command.

set security-association idle-time *seconds*

no set security-association idle-time *seconds*

Syntax Description

seconds	Number of seconds for which the current peer can be idle before the default peer is used. The valid values are 600 to 86400.

Defaults

If none is specified, the global settings are used.

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **set security-association idle-time** command if you want the default peer when the current peer times out. If there is a timeout to the current peer, the connection to that peer is closed.

For more usage information, see the **crypto ipsec security-association idle-time** command.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to use the **set security-association idle-time** command:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile myprofile
```

```
RP/0/0/CPU0:router(config-myprofile)# set security-association idle-time 800
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
crypto ipsec security-association idle-time	Configures the IP Security (IPSec) security association (SA) idle timer.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value.

set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security security associations, use the **set security-association lifetime** command in profile configuration mode. To reset an SA lifetime to the default value, use the **no** form of this command.

set security-association lifetime seconds *seconds* **kilobytes** *kilobytes*

no set security-association lifetime seconds *seconds* **kilobytes** *kilobytes*

Syntax Description

seconds *seconds*	Specifies the number of seconds a security association lives before expiring. The range is from 120 to 86400.
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before that security association expires. The range is from 2560 to 536870912. The default value is 100000000 KB (220 MBps for 1 hour).

Defaults

Default is taken from global configuration.

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.4.1	The maximum value for the **kilobytes** keyword changed to 536870912. The default value changed from 4194303 to 100000000 KB (220 MBps for 1 hour).
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

For more usage information, see the **crypto ipsec security-association lifetime** command.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to shorten lifetimes to reduce the risk that the keys could be compromised. The timed lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 KB (10 MBps for 30 minutes).

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/0/CPU0:router(config-myprofile)# set security-association lifetime seconds 2700
RP/0/0/CPU0:router(config-myprofile)# set security-association lifetime kilobytes 2304000
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
crypto ipsec security-association lifetime	Changes the global lifetime values that are used when negotiating IPSec SAs.
set security-association idle-time	Specifies the maximum time in which the current peer can be idle before the default peer is used.

set security-association replay disable

To disable replay checking for a particular crypto profile, use the **set security-association replay disable** command in profile configuration mode.

set security-association replay disable

Syntax Description

This command has no arguments or keywords.

Defaults

Antireplay checking is enabled.

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

You must set the inbound keys.

The **set security-association replay disable** command overrides the global setting. For more usage information, see the **crypto ipsec security-association replay disable** command.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to disable replay checking for a particular crypto profile:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/0/CPU0:router(config-myprofile)# set security-association replay disable
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
crypto ipsec security-association replay disable	Disables antireplay checking globally.

set session-key inbound ah

To manually specify the IP Security session keys to set the inbound IPSec session key for the Authentication Header (AH) protocol, use the **set session-key inbound ah** command in profile configuration mode. To remove IPSec session keys, use the **no** form of this command.

set session-key inbound ah *spi hex-key-data*

no set session-key inbound ah

Syntax Description

spi	Security parameter index (SPI), a number that uniquely identifies a security association. The SPI is an arbitrary number you assign in the range of 256 to 4294967295 (FFFF FFFF). You can assign the same SPI to both directions. When using a hardware crypto engine, you cannot use the same inbound SPI twice in different protocols and profiles.
hex-key-data	Session key; enter in hexadecimal format. This argument is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto transform set includes a DES algorithm, you must specify at least 8 bytes per key. If the crypto transform set includes an MD5 algorithm, you must specify at least 16 bytes per key. If the crypto transform set includes an SHA algorithm, you must specify 20 bytes per key. Keys longer than the preceding sizes are truncated.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

To create a manual SA, both inbound and outbound keys must be configured. The keys must match the specified transform-set under the profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually establish security associations and include an AH protocol:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile map-p1
RP/0/0/CPU0:router(config-map-p1)# set pfs group1
RP/0/0/CPU0:router(config-map-p1)# set type static
RP/0/0/CPU0:router(config-map-p1)# match acl transform-set ts10
RP/0/0/CPU0:router(config-map-p1)# set session-key inbound ah 1631532061
74353698822494650663329589937693
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
set session-key outbound ah	Specifies the IP Security session key to set the outbound IPSec session key for the Authentication Header (AH) protocol manually.

set session-key inbound esp

To manually specify the IP Security session key to set the inbound IPSec session key for Encapsulation Security Protocol (ESP), use the **set session-key inbound esp** command in profile configuration mode. To remove IPSec session keys, use the **no** form of this command.

set session-key inbound esp *spi* {**cipher** *hex-key-data* | **authentication** *hex-key-data*}

no set session-key inbound esp

Syntax Description

spi	Security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4294967295 (FFFF FFFF). You can assign the same SPI to both directions. When using a hardware crypto engine, you cannot use the same inbound SPI twice in different protocols and profiles.
cipher	Specifies that the key string is used with the ESP encryption transform.
hex-key-data	Session key; enter in hexadecimal format. This argument is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto transform set includes a DES algorithm, you must specify at least 8 bytes per key. If the crypto transform set includes an MD5 algorithm, you must specify at least 16 bytes per key. If the crypto transform set includes an SHA algorithm, you must specify 20 bytes per key. Keys longer than the preceding sizes are simply truncated.
authentication	Indicates that the key string is used with the ESP authentication transform. The **authentication** keyword is required only when the transform set includes an ESP authentication transform.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Release	Modification
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

If the transform set includes an ESP encryption protocol, you must define IPSec keys for ESP encryption for inbound traffic. If the transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound traffic.

To create a manual SA, both inbound and outbound keys must be configured. The keys match the specified transform-set under the profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually establish security associations and include an ESP protocol for inbound traffic; session keys are created by using the **cipher** keyword:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile map-p1
RP/0/0/CPU0:router(config-map-p1)# set pfs group1
RP/0/0/CPU0:router(config-map-p1)# set type static
RP/0/0/CPU0:router(config-map-p1)# match acl transform-set ts10
RP/0/0/CPU0:router(config-map-p1)# set session-key inbound esp 1771900421 cipher
799479494599315713206965743872311481573994372323
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
set session-key outbound esp	Specifies the IP Security session key to set the outbound IPSec session key for ESP manually.

set session-key outbound ah

To manually specify the IP Security session key to set the outbound IPSec session key for the Authentication Header (AH) protocol, use the **set session-key outbound ah** command in profile configuration mode. To remove IPSec session keys, use the **no** form of this command.

set session-key outbound ah *spi hex-key-data*

no set session-key outbound ah *spi hex-key-data*

Syntax Description

spi	Security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4294967295 (FFFF FFFF). You can assign the same SPI to both directions. When using a hardware crypto engine, you cannot use the same inbound SPI twice in different protocols and profiles.
hex-key-data	Session key; enter in hexadecimal format. This argument is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto transform set includes a DES algorithm, you must specify at least 8 bytes per key. If the crypto transform set includes an MD5 algorithm, you must specify at least 16 bytes per key. If the crypto transform set includes an SHA algorithm, you must specify 20 bytes per key. Keys longer than the preceding sizes are simply truncated.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

To create a manual SA, both inbound and outbound keys must be configured. The keys must match the specified transform set under the profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually establish security associations and include an AH protocol for outbound traffic:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile map-p1
RP/0/0/CPU0:router(config-map-p1)# set pfs group1
RP/0/0/CPU0:router(config-map-p1)# set type static
RP/0/0/CPU0:router(config-map-p1)# match acl transform-set ts10
RP/0/0/CPU0:router(config-map-p1)# set session-key outbound ah 1913957174
44556535898960895859936813538982
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
set session-key inbound ah	Specifies the IP Security session keys to set the inbound IPSec session key for the Authentication Header (AH) protocol manually.

set session-key outbound esp

To manually specify the IP Security session key to set the outbound IPSec session key for ESP, use the **set session-key outbound esp** command in profile configuration mode. To remove IPSec session keys, use the **no** form of this command.

set session-key outbound esp *spi* {**cipher** *hex-key-data*| **authentication** *hex-key-data*}

no set session-key outbound esp

Syntax Description

spi	Security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4294967295 (FFFF FFFF). You can assign the same SPI to both directions. When using a hardware crypto engine, you cannot use the same inbound SPI twice in different protocols and profiles.
cipher	Specifies that the key string is used with the ESP encryption transform.
hex-key-data	Session key; enter in hexadecimal format. This argument is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto transform set includes a DES algorithm, you must specify at least 8 bytes per key. If the crypto transform set includes an MD5 algorithm, you must specify at least 16 bytes per key. If the crypto transform set includes an SHA algorithm, you must specify 20 bytes per key. Keys longer than the preceding sizes are simply truncated.
authentication	Indicates that the key string is used with the ESP authentication transform. The **authentication** keyword is required only when the transform set includes an ESP authentication transform.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.

Release	Modification
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

To create a manual SA, both inbound and outbound keys must be configured. The keys must match the specified transform-set under the profile.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows how to manually establish security associations and include an ESP protocol for outbound traffic; session keys are created by using the **cipher** and **authentication** keywords:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile map-p1
RP/0/0/CPU0:router(config-map-p1)# set pfs group1
RP/0/0/CPU0:router(config-map-p1)# set type static
RP/0/0/CPU0:router(config-map-p1)# match acl transform-set ts10
RP/0/0/CPU0:router(config-map-p1)#set session-key outbound esp 1658435903 cipher
91219335358535731180639597833438815579384999280 3
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
set session-key inbound esp	Specifies the IP Security session key to set the inbound IPSec session key for Encapsulation Security Protocol (ESP) manually.

set transform-set

To specify a list of transform sets in priority order, use the **set transform-set** command in profile configuration mode. To disable this feature, use the **no** form of this command.

set transform-set *transform-set-name*

no set transform-set *transform-set-name*

Syntax Description

transform-set-name	Name of the transform set. You can configure up to five transform sets in priority order. The maximum number of characters is 32.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Profiles that use the **set transform-set** command are attached only to service-gre interfaces.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the transform set is named ts1:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/0/CPU0:router(config-myprofile)# set transform-set ts1
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.
crypto ipsec transform-set	Defines a transform set (an acceptable combination of security protocols and algorithms)
match transform-set	Configures an ACL to use for packet classification, and if the packets need protecting, the transform set to use for IPSec processing.

set type

To set the profile mode type, use the **set type** command in profile configuration mode. To reset the mode type, use the **no** form of this command.

set type {**static** | **dynamic**}

no set type

Syntax Description

static	Identifies the peer in the configuration.
dynamic	Lets the profile handle Dynamic Crypto Profile (DCP), which means security association (SA) negotiation from any authenticated peer is allowed.

Defaults

The profile mode type is static by default.

Command Modes

Profile configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

When configuring a dynamic profile, the interface in which the profile is attached to should not be configured with a tunnel destination.

Task ID

Task ID	Operations
crypto	read, write

Examples

The following example shows that the profile mode type is set to dynamic and IKE TED handling is enabled:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# configurecrypto ipsec profile myprofile
set type dynamic
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.

show crypto engine statistics

To display information for the hardware data path counters that are gathered from the Cisco IPSec VPN SPA, use the **show crypto engine statistics** command in EXEC mode.

show crypto engine statistics [**inbound**| **outbound**] [**detail**] **location** *node-id*

Syntax Description

inbound	(Optional) Specifies the decryption side for the data path statistics.
outbound	(Optional) Specifies the encryption side for the data path statistics.
detail	(Optional) Displays the encryption side for the detailed data path statistics. The detail keyword displays the SPI4.2 controller counters.
location *node-id*	Specifies the crypto engine subslot location.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Task ID

Task ID	Operations
crypto	read

Examples

The following example displays sample output from the **show crypto engine statistics** command:

```
RP/0/0/CPU0:router# show crypto engine statistics detail location 0/3/1

Decryption Side Data Path Statistics

====================================
Packets RX.................:                        0
Packets TX.................:                        0
IPSec Transport Mode.......:                        0
```

```
IPSec Tunnel Mode..........:                        0
AH Packets.................:                        0
ESP Packets................:                        0
NAT-T Decapsulations.......:                        0
Clear......................:                        0
ICMP.......................:                        0
Packets Drop...............:                        0
Authentication Errors......:                        0
Decryption Errors..........:                        0
Decryption Errors..........:                        0
Replay Check Failed........:                        0
Policy Check Failed........:                        0
Illegal CLear Packet.......:                        0
SPD Errors.................:                        0
Hard Life Drop.............:                        0
Invalid SA.................:                        0
SPI No Match...............:                        0
Destination No Match.......:                        0
Protocol No Match..........:                        0
Reassembly Frag RX.........:                        0
IPSec Fragments............:                        0
IPSec Reasm Done...........:                        0
Clear Fragments............:                        0
Clear Reasm Done...........:                        0
Reasm Datagrams Drop.......:                        0
Fragments Drop.............:                        0

Decryption Side Controller Statistics

====================================
Frames RX..................:                        0
Bytes RX...................:                        0
Mcast/Bcast Frames RX......:                        0
RX Less 128Bytes...........:                        0
RX Less 512Bytes...........:                        0
RX Less 1KBytes............:                        0
RX Less 9KBytes............:                        0
RX Frames Drop.............:                        0
Frames TX..................:                       18
Bytes TX...................:                     1486
Mcast/Bcast Frames TX......:                        0
TX Less 128Bytes...........:                       15
TX Less 512Bytes...........:                        3
TX Less 1KBytes............:                        0
TX Less 9KBytes............:                        0

Encryption Side Data Path Statistics

====================================
Packets RX.................:                        0
Packets TX.................:                        0
IPSec Transport Mode.......:                        0
IPSec Tunnel Mode..........:                        0
NAT-T Encapsulations.......:                        0
LAF prefragmented..........:                        0
Fragmented.................:                        0
Clear......................:                        0
ICMP.......................:                        0
Packets Drop...............:                        0
IKE/TED Drop...............:                        0
Authentication Errors......:                        0
Encryption Errors..........:                        0
Fragmentation Failure......:                        0
Hard life Drop.............:                        0
```

```
Invalid SA.................:                        0
Reassembly Frag RX.........:                        0
Clear Fragments............:                        0
Clear Reasm Done...........:                        0
Datagrams Drop.............:                        0
Fragments Drop.............:                        0

Encryption Side Controller Statistics

====================================
Frames RX..................:                       11
Bytes RX...................:                     1072
Mcast/Bcast Frames RX......:                        0
RX Less 128Bytes...........:                        8
RX Less 512Bytes...........:                        3
RX Less 1KBytes............:                        0
RX Less 9KBytes............:                        0
RX Frames Drop.............:                        0
Frames TX..................:                        0
Bytes TX...................:                        0
Mcast/Bcast Frames TX......:                        0
TX Less 128Bytes...........:                        0
TX Less 512Bytes...........:                        0
TX Less 1KBytes............:                        0
TX Less 9KBytes............:                        0
```

Related Commands

Command	Description
clear cryptoengine statistics	Clears the statistics for the crypto engine.

show crypto ipsec interface

To display the crypto IPSec interface, use the **show crypto ipsec interface** command in EXEC mode.

show crypto ipsec interface {**service-gre** *number* | **service-ipsec** *number* **tunnel-ipsec** *number*}

Syntax Description

service-gre *number*	Specifies a service-gre interface. The *number* argument is the number of service-gre interfaces. Range is from 1-65535.
service-ipsec *number*	Specifies a service-ipsec interface. The *number* argument is the number of service-ipsec interfaces. Range is from 1-65535.
tunnel-ipsec *number*	Specifies a tunnel-ipsec interface. The *number* argument is the number of tunnel-ipsec interfaces. Range is from 0-4294967295.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Task ID

Task ID	Operations
crypto	read

Examples

The following sample output is for the service-ipsec interface:

```
RP/0/0/CPU0:router# show crypto ipsec interface service-ipsec 1

--------------- IPSec interface ---------------
Interface service-ipsec1, mode Tunnel, intf_handle 0x5000180
Locations 0/1/1, 0/2/0 VRF default (60000000)
Number of profiles 0, number of flows 0
Tunnel: source 0.0.0.0, destination 0.0.0.0, tunnel VRF default
```

```
DF-bit: copy, pre-fragmentation enable
default pmtu: 9216
No flows on this interface.
```

Table 9 describes the significant fields shown in the display.

Related Commands

Table 9 show crypto ipsec interface Field Descriptions

Field	Description
Tunnel	The interface tunnel source, destination, and tunnel VRF configuration.
DF-bit	The DF bit mode is specified under the interface. If none is configured, the mode is specified in the global configuration.
default pmtu	The path MTU of the interface.

Command	Description
interface service-gre	Creates a static IPSec-protected generic routing encapsulation (GRE) interface.
interface service-ipsec	Creates a static IPSec virtual interface.
interface tunnel-ipsec	Creates a virtual IPSec tunnel interface.

show crypto ipsec profile

To display crypto profiles that are defined on a router, use the **show crypto ipsec profile** command in EXEC mode.

show crypto ipsec profile [*profile name*]

Syntax Description

profile name	(Optional) Name of the IPSec profile.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.5.0	This command was introduced.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

If no profile is specified, all profiles are displayed.

Task ID

Task ID	Operations
crypto	read

Examples

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

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

Crypto Profile: ipsec1
        Profile is Static
        Anti Replay Enable
        Interfaces using this profile:(service-ipsec/gre)
                service-ipsec100
        ACLs matched by this profile:
                acl-1 :Transform-sets:tsfm1,

Crypto Profile: gre
        Profile is Static
```

```
Anti Replay Enable
Interfaces using this profile:(service-ipsec/gre)
        service-gre1
ACLs matched by this profile:
        Transform-sets:tsfm2,
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IP Security (IPSec) profile and enters profile configuration mode.

show crypto ipsec sa

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

show crypto ipsec sa [*sa-id* | **peer** *ip-address* | **profile** *profile-name* | **detail** | **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.
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 3.3.0	No modification.
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 3.5.0	No modification.
Release 3.6.0	The upper limit for the *sa-id* argument range was increased to 64,500 sessions.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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
```

Table 10 describes the significant fields shown in the display.

Table 10 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.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.4.0	This command was introduced.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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
```

Table 11 describes the significant fields shown in the display.

Table 11 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.

Table 11 show crypto ipsec statistics Field Descriptions (continued)

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 in EXEC mode.

show crypto ipsec summary

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	Sample output was modified to display port number to the local peer and remote peer fields.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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
```

Table 12 describes the significant fields shown in the display.

Table 12 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.
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 in EXEC mode.

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.

Defaults

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.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

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
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set (an acceptable combination of security protocols and algorithms).
match transform-set	Configures an ACL to use for packet classification, and if the packets need protecting, the transform set to use for IPSec processing.
set transform-set	Specifies a list of transform sets in priority order.

tunnel destination (IPSec)

To specify the destination for a tunnel interface, use the **tunnel destination** command in interface configuration mode. To remove the destination, use the **no** form of this command.

tunnel destination *ip-address*

no tunnel destination *ip-address*

Syntax Description

ip-address	IP address of the host destination expressed in four-part dotted-decimal notation.

Defaults

No tunnel interface destination is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **tunnel destination** command to configure the destination address for an IP Security (IPSec) tunnel.

You should not have two tunnels using the same encapsulation mode with the same source and destination address.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the tunnel destination 172.19.72.120:

```
RP/0/0/CPU0:router# configure
```

```
RP/0/0/CPU0:router(config)# interface tunnel-ip 25
RP/0/0/CPU0:router(config-if)# tunnel source 172.19.70.92
RP/0/0/CPU0:router(config-if)# tunnel destination 172.19.72.120
RP/0/0/CPU0:router(config-if)# profile pn1
```

Related Commands

Command	Description
tunnel source (IPSec)	Specifies a source address for a tunnel interface.

Command	Description
tunnel source (IPSec)	Specifies a source address for a tunnel interface.

Command	Description
tunnel source (IPSec)	Specifies a source address for a tunnel interface.

Command	Description
tunnel source (IPSec)	Specifies a source address for a tunnel interface.

Command	Description
tunnel source (IPSec)	Specifies a source address for a tunnel interface.

tunnel source (IPSec)

To specify the source address for a tunnel interface, use the **tunnel source** command in IPSEC interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address*| *type interface-path-id*}

no tunnel source

Syntax Description

ip-address	IP address to use as the source address for packets in the tunnel.
type	Interface type. For more information, use the question mark (**?**) online help function.
interface-path-id	Physical interface or virtual interface. **Note** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (**?**) online help function.

Defaults

No tunnel interface source address or interface is specified.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.2	This command was introduced.
Release 3.3.0	No modification.
Release 3.4.0	No modification.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

Use the **tunnel source** command to configure the source address or interface type and instance for an IP Security tunnel.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to configure the tunnel source 172.19.72.92:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface tunnel-ip 25
RP/0/0/CPU0:router(config-if)# tunnel source 172.19.72.92
RP/0/0/CPU0:router(config-if)# tunnel destination 172.19.72.120
RP/0/0/CPU0:router(config-if)# profile pn1
```

Related Commands

Command	Description
service-location (IPSec)	Specifies both active and standby locations for the interface.
tunnel destination (IPSec)	Specifies the destination for a tunnel interface.
tunnel vrf (IPSec)	Associates a VRF instance with a specific tunnel destination.

tunnel vrf (IPSec)

To associate a VRF instance with a specific tunnel destination, interface, or subinterface, use the **tunnel vrf** command in interface configuration mode. To disassociate a VRF from the tunnel destination, use the **no** form of this command.

tunnel vrf *vrf-name*

no tunnel vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Defaults

The default destination is determined by the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
Release 3.4.0	This command was introduced on the Cisco XR 12000 Series Router IPSec VPN SPA.
Release 3.5.0	No modification.
Release 3.6.0	No modification.
Release 3.7.0	No modification.
Release 3.8.0	No modification.
Release 3.9.0	No modification.

Usage Guidelines

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

The tunnel source and destination must be in the same VRF.

Either the IP VRF or the tunnel VRF can be set to the global routing table (using the **no vrf forwarding** command or the **no tunnel vrf** command).

The tunnel is disabled if no route to the tunnel destination is defined. If the tunnel VRF is set, there must be a route to that destination in the VRF.

Task ID

Task ID	Operations
interface	read, write

Examples

The following example shows how to associate VRF forwarding with either tunnel destination or tunnel source:

```
RP/0/0/CPU0:router# configure
RP/0/0/CPU0:router(config)# interface service-ipsec 1
RP/0/0/CPU0:router(config-if)# tunnel vrf forwarding
RP/0/0/CPU0:router(config-if)# tunnel source 172.19.72.92
RP/0/0/CPU0:router(config-if)# tunnel destination 172.19.62.82
RP/0/0/CPU0:router(config-if)# service-location preferred-active 0/0/0 preferred-standby
0/1/0
```

Related Commands

Command	Description
service-location (IPSec)	Specifies both active and standby locations for the interface.
tunnel destination (IPSec)	Specifies the destination for a tunnel interface.
tunnel source (IPSec)	Specifies the source address for a tunnel interface.