



IPSec Network Security Commands on Cisco IOS XR Software

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

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

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	
<i>sa-id</i>	Identifier for the SA. IPSec supports from 1 to 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 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

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

```
RP/0/RP0/CPU0:router# clear crypto ipsec sa 100
```

Related Commands	Command	Description
	show crypto ipsec sa	Displays the settings used by current SAs.

client authentication list

To apply extended authentication (Xauth) for Internet Key Exchange (IKE) interaction, use the **client authentication list** command in profile configuration mode. To remove Xauth, use the **no** form of this command.

client authentication list *authen-list-name*

no client authentication list *authen-list-name*

Syntax Description

authen-list-name Username and password storage location (local or remote server) as defined in the **aaa authentication login** command.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Xauth allows all Cisco IOS XR software authentication, authorization, and accounting (AAA) authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list name must match the Xauth configuration list name for user authentication to occur.

Examples

In the following example, AAA username and password storage location information is applied from the list0 authentication list to a profile named sample:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec profile sample
RP/0/RP0/CPU0:router(config-sample)# client authentication list list0
```

Related Commands

Command	Description
isakmp authorization list	Applies mode configuration for IKE interaction.

crypto ipsec chkpt-disabled

To disable IP Security (IPSec) checkpointing, use the **crypto ipsec chkpt-disabled** command in global configuration mode. To reenable checkpointing, use the **no** form of this command.

crypto ipsec chkpt-disabled

no crypto ipsec chkpt-disabled

Syntax Description This command has no arguments or keywords.

Defaults IPSec checkpointing is enabled by default.

Command Modes Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

IPSec checkpoints security associations (SAs) in the local database. If an IPSec process restarts, SAs are retrieved from the local database and need not be reestablished with remote peers.

An SA describes how two or more entities use security services to communicate securely. For example, an IPSec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPSec connection.

IPSec checkpointing is enabled by default. To disable IPSec checkpointing, use the **crypto ipsec chkpt-disabled** command in global configuration mode.

Examples

The following example shows how to disable IPSec checkpointing:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec chkpt-disabled
```

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 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 tunnel modes, including the keying mechanism to be used, how the traffic is protected, and so on.

The following commands are available in profile configuration mode:

- **client authentication list** *authen-list-name* and **no client authentication list**
The *authen-list-name* argument specifies the authentication name that Internet Key Exchange (IKE) uses for extended authentication (Xauth) support.
- **isakmp authorization list** *author-list-name* and **no isakmp authorization list** *author-list-name*
The *author-list-name* argument specifies the authorization list that IKE will use for mode configuration.
- **match** *acl-name* **transform-set** *transform-set-name*
This command 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. You cannot use the same ACL name more than once.

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

This command 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 type** {*static* | *dynamic* [*discover*]} and **no set type**

This command sets or resets the profile mode. Default is *static*. *Dynamic* mode 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). The *discover* argument enables IKE tunnel endpoint discovery (TED) protocol handling.

Examples

The following example shows how to create a crypto profile named *newprofile*, set the PFS to *group2*, and configure *newprofile* as a dynamic profile with IKE TED protocol handling:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec profile newprofile
RP/0/RP0/CPU0:router(config-newprofile)# set pfs group2
RP/0/RP0/CPU0:router(config-newprofile)# set type dynamic discover
RP/0/RP0/CPU0:router(config-newprofile) match myacl transform-set mytransformset
```

Related Commands

Command	Description
client authentication list	Applies Xauth for IKE interaction.
isakmp authorization list	Applies mode configuration for IKE interaction.
match transform-set	Configures an ACL to use for packet classification and the transform set to use for IPsec processing.
set pfs	Sets PFS for IKE to handle Diffie-Hellman negotiation.
set type	Sets the profile mode type.

crypto ipsec security-association lifetime

To change 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 <i>seconds</i>	Number of seconds an SA lives before expiring. The range is from 120 to 86400 seconds.
kilobytes <i>kilobytes</i>	Volume of traffic (in KB) that can pass between IPSec peers using a given SA before that SA expires. The range is from 2560 to 4194303 KB.

Defaults

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

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 (and corresponding 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 256 KB less than the **kilobytes** lifetime (whichever occurs first).

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.

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/RP0/CPU0:router(config)# crypto ipsec security-association lifetime seconds 2700
RP/0/RP0/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.

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 transform-set-name transform1 [transform2 [transform3]]
```

```
no crypto ipsec transform-set transform-set-name
```

Syntax Description

<i>transform-set-name</i>	Name of the transform set to create or modify. Maximum is 32 characters in length.
<i>transform1</i> <i>transform2</i> <i>transform3</i>	Specifies up to three transforms. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform set values are described in the “Usage Guidelines” section. At least one transform is required.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 ES 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 may 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 that 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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# crypto ipsec transform-set new esp-sha-hmac
```

Related Commands

Command	Description
clear crypto ipsec sa	Deletes specific SAs or all SAs in the IPSec SADB.
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.

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 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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 has to be configured in the `crypto ipsec transport` mode.

Examples

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

```
RP/0/RP0/CPU0:router(config)# crypto ipsec transport  
RP/0/RP0/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	<i>string</i>	Character string describing the IPSec profile.
--------------------	---------------	--

Defaults	The default description is blank.
----------	-----------------------------------

Command Modes	Profile configuration
---------------	-----------------------

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
------------------	--

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

Examples	The following example shows the creation of a profile description:
----------	--

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

isakmp authorization list

To apply mode configuration for Internet Key Exchange (IKE) interaction, use the **isakmp authorization list** command in profile configuration mode. To remove mode configuration, use the **no** form of this command.

isakmp authorization list *author-list-name*

no isakmp authorization list *author-list-name*

Syntax Description

<i>author-list-name</i>	Storage source used to find the policy as defined in the aaa authorization network command.
-------------------------	--

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Mode configuration allows a gateway to download an IP address (and other network level configuration) to the client as part of an IKE negotiation. Using this exchange, the gateway gives IP addresses to the IKE client to be used as an “inner” IP address encapsulated under IP Security (IPSec). This method provides a known IP address for the client that can be matched against IPSec policy.

Use the **isakmp authorization list** command with the **client authentication list** command, which applies extended authentication (Xauth) for IKE interaction.

Examples

In the following example, mode configuration is applied to a crypto profile named new:

```
RP/0/RP0/CPU0:router(config-new)# isakmp authorization list list2
```

Related Commands

Command	Description
client authentication list	Applies Xauth for IKE interaction.

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

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

Syntax Description

<i>acl-name</i>	ACL number used for packet classification. Range is from 1 to 65535.
<i>transform-set-name</i>	Name of a transform set. Maximum is 32 characters in length.

Defaults

No default behavior or values

Command Modes

Profile configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples

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

```
RP/0/RP0/CPU0:router(config-profile)# match 101 transform-set tset1
```

Related Commands

Command	Description
crypto ipsec profile	Configures the IPSec profile and enters profile configuration mode.
crypto ipsec transform-set	Defines a transform set (an acceptable combination of security protocols and algorithms).

profile

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

profile *profile-name*

no profile *profile-name*

Syntax Description

<i>profile-name</i>	The previously defined crypto profile to use. This crypto profile cannot be shared within the same IPSec mode or across different IPSec modes. The character range is from 1 to 32 characters.
---------------------	--

Defaults

No default behavior or values

Command Modes

Transport configuration
Interface tunnel configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

The same crypto profile cannot be shared in different IPSec modes. Multiple commands can be specified for different types of traffic.

Examples

The following example shows a crypto profile being configured:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec transport
RP/0/RP0/CPU0:router(config-transport)# profile pn1
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec0
RP/0/RP0/CPU0:router(config-if)# profile pn1
```

Related Commands

Command	Description
crypto ipsec transport	Enters IPSec transport configuration mode.

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

group1

Command Modes

Profile configuration

Command History

Release	Modification
Release 2.0	This command was introduced on the Cisco CRS-1.
Release 3.0	No modification.
Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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.

Examples

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

```
RP/0/RP0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/RP0/CPU0:router(config-myprofile)# set pfs group2
```

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 [discover]}
```

```
no set type
```

Syntax Description	static	Identifies the peer in the configuration (tunnel mode).
	dynamic	Lets the profile handle Dynamic Crypto Profile (DCP), which means security association (SA) negotiation from any authenticated peer is allowed.
	discover	(Optional) Used in dynamic mode, enables Internet Key Exchange (IKE) tunnel endpoint discovery (TED) handling.

Defaults static

Command Modes Profile configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

Examples In the following example, the profile mode type is set to dynamic and IKE TED handling is enabled:

```
RP/0/RP0/CPU0:router(config)# crypto ipsec profile myprofile
RP/0/RP0/CPU0:router(config-myprofile)# set type dynamic discover
```

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**]

Syntax Description	
<i>sa-id</i>	(Optional) Identifier for the SA. The range is from 1 to 500.
peer <i>ip-address</i>	(Optional) IP address used on the remote (PC) side. Invalid IP addresses are not accepted.
profile <i>profile-name</i>	(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.

Command Modes EXEC

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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).

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

```
RP/0/RP0/CPU0:router# show crypto ipsec sa

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)
##pkts processed: 0, ##pkts dropped 0, ##total bytes 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: pnl
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)
##pkts processed: 0, ##pkts dropped 0, ##total bytes 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

```

Table 11 describes the significant fields shown in the display.

Table 11 *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 profile** command for a profile named `pnl`:

```

RP/0/RP0/CPU0:router# show crypto ipsec sa profile pnl
SA id: 2
interface: tunnel0
profile: pnl
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: pnl
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 peer** command:

```
RP/0/RP0/CPU0:router# show crypto ipsec sa peer 172.19.72.120
SA id: 2
interface: tunnel0
profile: pml
local ident (addr/mask/prot/port): (172.19.70.92/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.19.72.120/255.255.255.255/0/0)
local crypto endpt: 172.19.70.92, remote crypto endpt: 172.19.72.120
outbound esp sas:
spi: 0x8b0e950f (2332988687)
transform: esp-3des-sha
in use settings = Tunnel
sa lifetime: 3600s, 4194303kb

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

show crypto ipsec summary

To display IP Security (IPSec) summary information, use the **show crypto ipsec summary** command 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 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

```
RP/0/RP0/CPU0:router# show crypto ipsec summary
# * Attached to a transform indicates a bundle
# Active IPSec Sessions:1
SA Node Local Peer Remote Peer      Mode Profile Transform Lifetime
-----
1 0/0/010.0.0.5172.16.0.5      TN   captain  esp-3des  1800/4194303
```

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.
Mode	Profile mode type.
Profile	Crypto profile in use.
Transform	Transform in use.
Lifetime	Lifetime value, displayed in seconds followed by kilobytes.

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	<i>ip-address</i> 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 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines	To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the <i>Configuring AAA Services on Cisco IOS XR Software</i> module of the <i>Cisco IOS XR System Security Configuration Guide</i> .
-------------------------	--

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.

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

```
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec0
RP/0/RP0/CPU0:router(config-if)# tunnel source 172.19.70.92
RP/0/RP0/CPU0:router(config-if)# tunnel destination 172.19.72.120
RP/0/RP0/CPU0:router(config-if)# profile pn1
```

Related Commands	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 interface configuration mode. To remove the source address, use the **no** form of this command.

tunnel source {*ip-address* | *type instance*}

no tunnel source

Syntax Description	
<i>ip-address</i>	IP address to use as the source address for packets in the tunnel.
<i>type</i>	Interface type. For more information, use the question mark (?) online help function.
<i>instance</i>	<p>Either a physical interface instance or a virtual interface instance as follows:</p> <ul style="list-style-type: none"> Physical interface instance. Naming notation is <i>rack/slot/module/port</i> and a slash between values is required as part of the notation. <ul style="list-style-type: none"> <i>rack</i>: Chassis number of the rack. <i>slot</i>: Physical slot number of the modular services card or line card. <i>module</i>: Module number. A physical layer interface module (PLIM) is always 0. <i>port</i>: Physical port number of the interface. <p>Note In references to a Management Ethernet interface located on a route processor card, the physical slot number is alphanumeric (RP0 or RP1) and the module is CPU0. Example: interface MgmtEth0/RP1/CPU0/0.</p> <ul style="list-style-type: none"> Virtual interface instance. Number range varies depending on interface type. <p>For more information about the syntax for the router, use the question mark (?) online help function.</p>

Defaults No tunnel interface source address or interface is specified.

Command Modes Interface configuration

Command History	Release	Modification
	Release 2.0	This command was introduced on the Cisco CRS-1.
	Release 3.0	No modification.
	Release 3.2	This command was supported on the Cisco XR 12000 Series Router.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes the proper task IDs. For detailed information about user groups and task IDs, see the *Configuring AAA Services on Cisco IOS XR Software* module of the *Cisco IOS XR System Security Configuration Guide*.

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

Examples

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

```
RP/0/RP0/CPU0:router(config)# interface tunnel-ipsec0
RP/0/RP0/CPU0:router(config-if)# tunnel source 172.19.72.92
RP/0/RP0/CPU0:router(config-if)# tunnel destination 172.19.72.120
RP/0/RP0/CPU0:router(config-if)# profile pn1
```

Related Commands

Command	Description
tunnel destination (IPSec)	Specifies the destination for a tunnel interface.
