

Crypto Map IPSec Manual Configuration Mode Commands

The Crypto IPSec Map Manual Configuration Mode is used to configure static IPSec tunnel properties.

Modification(s) to an existing crypto map manual configuration will not take effect until the related security association has been cleared. Refer to the description of the **clear crypto security-association** command in the *Exec Mode Commands* chapter for more information.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, they only be used for testing purposes.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

- end, on page 2
- exit, on page 2
- match address, on page 2
- set control-dont-fragment, on page 4
- set ip mtu, on page 5
- set ipv6 mtu, on page 6
- set peer, on page 7
- set session-key, on page 8
- set transform-set, on page 11

end

Exits the current configuration mode and returns to the Exec mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `end`

Usage Guidelines Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product All

Privilege Security Administrator, Administrator

Syntax Description `exit`

Usage Guidelines Use this command to return to the parent configuration mode.

match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

[no] match address *acl_name* **[** *priority* **]**

no

Removes a previously matched ACL.

match address *acl_name*

Specifies the name of the ACL with which the crypto map is to be matched. *acl_name* is an alphanumeric string of 1 through 47 characters that is case sensitive.

priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. *priority* is an integer from 0 through 4294967295. 0 is the highest priority. Default: 0

Important The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage Guidelines

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named *ACLlist1* and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```

set control-dont-fragment

Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

`[ default ] set control-dont-fragment { clear-bit | copy-bit | set-bit }`

default

Sets or restores default value assigned to a specified parameter.

clear-bit

Clears the DF bit from the outer IP header (sets it to 0).

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage Guidelines

Use this command to clear, copy, or set the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Example

The following command sets the DF bit in the outer IP header.

```
set control-dont-fragment set-bit
```

set ip mtu

Configures the IPv4 Maximum Transmission Unit (MTU) in bytes.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

ip mtu *bytes*

ip mtu *bytes*

Specifies the IPv4 MTU in bytes as an integer from 576 to 2048. Default is 1438.

Usage Guidelines

Use this command to set the IPv4 MTU in bytes

Example

The following command configures an IPv4 MTU of 1024 bytes.

```
set ip mtu 1024
```

set ipv6 mtu

Configures the IPv6 Maximum Transmission Unit (MTU) in bytes.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

ipv6 mtu *bytes*

ip mtu *bytes*

Specifies the IPv6 MTU in bytes as an integer from 576 to 2048. Default is 1438.

Usage Guidelines

Use this command to set the IPv6 MTU in bytes

Example

The following command configures an IPv6 MTU of 1024 bytes.

```
set ip mtu 1024
```

set peer

Configures the IP address of the peer security gateway that the system will establish the IPSec tunnel with.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-manual-map)#`

Syntax Description

[no] set peer *gw_address*

no

Removes a previously configured peer address.

set peer *gw_address*

Specifies the IP address of the peer security gateway with which the IPSec tunnel will be established. The IP address can be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage Guidelines

Once the manual crypto map is fully configured and applied to an interface, the system will establish an IPSec tunnel with the security gateway specified by this command.

Because the tunnel relies on statically configured parameters, once created, it never expires; it exists until its configuration is deleted.

Example

The following command configures a security gateway address of *192.51.1.100* for the crypto map with which to establish a tunnel.

```
set peer 192.51.1.100
```

set session-key

Configures session key parameters for the manual crypto map.

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

set session-key { inbound | outbound } { ah *ah_spi* **[encrypted] key** *ah_key* **| esp** *esp_spi* **[encrypted] cipher** *encryption_key* **[encrypted] authenticator** *auth_key* **}**

no set session-key { inbound | outbound }

no

Removes previously configured session key information.

inbound

Specifies that the key(s) will be used for tunnels carrying data sent by the security gateway.

outbound

Specifies that the key(s) will be used for tunnels carrying data sent by the system.

ah *ah_spi*

Configures the Security Parameter Index (SPI) for the Authentication Header (AH) protocol. The SPI is used to identify the AH security association (SA) between the system and the security gateway. *ah_spi* is an integer from 256 through 4294967295.

encrypted

Indicates the key provided is encrypted.

The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key**, **cipher**, and/or **authenticator** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

key *ah_key*

Configures the key used by the system to de/encapsulate IP packets using Authentication Header (AH) protocol. *ah_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

esp *esp_spi*

Configures SPI for the Encapsulating Security Payload (ESP) protocol. The SPI is used to identify the ESP security association (SA) between the system and the security gateway. *esp_spi* is an integer from 256 through 4294967295.

The length of the configured key must match the configured algorithm.

cipher *encryption_key*

Specifies the key used by the system to de/encrypt the payloads of IP packets using the ESP protocol. *encryption_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

authenticator *auth_key*

Specifies the key used by the system to authenticate the IP packets once encryption has been performed. *auth_key* must be entered as either an alphanumeric string or a hexadecimal number beginning with "0x".

The length of the configured key must match the configured algorithm.

Usage Guidelines

Manual crypto maps rely on the use of statically configured keys to establish IPSec tunnels. This command allows the configuration of the static keys.

Identical keys must be configured on both the system and the security gateway in order for the tunnel to be established.

The length of the configured key must match the configured algorithm.

This command can be entered up to two time for the same crypto map: once to configure inbound key properties, and once to configure outbound key properties.

Example

The following command configures a manual crypto map with the following session key properties:

- Keys are for tunnels initiated by the system to the security gateway.
- ESP will be used with an SPI of *310*.
- Encryption key is *sd23r9skd0fi3as*.
- Authentication key is *sfd23408imi9yn*.

```
set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator
sfd23408imi9yn
```

set transform-set

Configures the name of a transform set that the crypto map is associated with.



Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. This command must not be used for HNBGW and HeNBGW in these releases. For more information, contact your Cisco account representative.

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context *context_name* **> crypto map** *map_name* **ipsec-manual**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

Syntax Description

`[ no ] set transform-set` *`transform_name`*

no

Removes a previously configured transform set association.

set transform-set *transform_name*

Specifies the name of the transform set expressed as an alphanumeric string of 1 through 127 characters that is case sensitive.

Usage Guidelines

System transform sets contain the IPSec policy definitions for crypto maps. Refer to the **crypto ipsec transform-set** command for information on creating transform sets.

Important Transform sets must be configured prior to configuring session key information for the crypto map.

Example

The following command associates a transform set named *esp_tset* with the crypto map:

```
set transform-set esp_tset
```