Crypto Map IPSec Dynamic Configuration Mode Commands

Modification(s) to an existing dynamic crypto map 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.

Command Modes

The Crypto Map IPSec Dynamic Configuration Mode is used to configure IPSec tunnels that are created as needed to facilitate subscriber sessions using Mobile IP or L2TP.

Exec > Global Configuration > Context Configuration > Crypto Map Dynamic Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-dynamic**

Entering the above command sequence results in the following prompt:

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

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

- end, on page 1
- exit, on page 2
- set, on page 2

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.

set

Configures parameters for the dynamic 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 Dynamic Configuration

configure > **context** *context_name* > **crypto map** *policy_name* **ipsec-dynamic**

Entering the above command sequence results in the following prompt:

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

Syntax Description

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [keepalive *sec* **] | ip mtu** *bytes* **| pfs { group1 | group2 | group5} | phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet} | security-association lifetime { keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} | transform-set** *transform_name* **[transform-set** *transform_name2...* **transform-set** *transform_name6* **] }**

no set { ikev1 natt | pfs | security-association lifetime {keepalive | kilo-bytes | seconds } | phase1-idtype | phase2-idtype | transform-set *transform_name* **[transform-set** *transform_name2...* **transform-set** *transform_name6* **] }**

no

Deletes the specified parameter or resets the specified parameter to the default value.

control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don't fragment (DF) bit in the outer IP header of the IPSec tunnel data packet. Options are:

- **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).

ikev1 natt [keepalive *sec*]

Enables IPSec NAT Traversal.

keepalive *sec*: The time to keep the NAT connection alive in seconds. *sec* must be an integer of from 1 through 3600.

ip mtu *bytes*

Specifies the IP Maximum Transmission Unit (MTU) in bytes as an integer from 576 to 2048.

mode { aggressive | main }

Configures the IKE negotiation mode as AGRESSIVE or MAIN.

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).

- **group1**: Diffie-Hellman Group1 (768-bit modp)
- **group2**:- Diffie-Hellman Group2 (1024-bit modp)
- **group5**:- Diffie-Hellman Group5 (1536-bit modp)

phase1-idtype { id-key-id | ipv4-address } [mode { aggressive | main }]

Sets the IKE negotiations Phase 1 payload identifier.

Default: ipv4-address

id-key-id: Use ID_KEY_ID as the Phase 1 payload identifier.

ipv4-address: Use IPV4_ADDR as the Phase 1 payload identifier.

mode { aggressive | main }: Specify the IKE mode.

phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.

Default: ipv4-address-subnet

ipv4-address: Use IPV4_ADDR as the Phase 2 payload identifier.

ipv4-address-subnet: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

security-association lifetime { keepalive | kilo-bytes *kbytes* | seconds *secs* }

Defaults:

- **keepalive**: Disabled
- **kilo-bytes**: 4608000 kbytes
- **seconds**: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.

- **keepalive**: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- **kilo-bytes**: This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires; entered as an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires; entered as an integer from 1200 through 86400.

Important If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map's SA lifetime (either in terms of kilobytes or seconds), then the **keepalive** parameter **must** be configured.

transform-set *transform_name* [transform-set *transform_name2 ...* transform-set *transform_name6*]

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command **crypto ipsec transform-set** for information on creating transform sets.

You can repeat this keyword up to 6 times on the command line to specify multiple transform sets.

trasnform_name is the name of the transform set entered as an alphanumeric string from 1 through 127 characters that is case sensitive.

Usage Guidelines

Use this command to set parameters for a dynamic crypto map.

Example

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to *50000* KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to *10000* seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets *tset1* and *tset2*:

```
set transform-set tset1 transform-set tset2
```