

Crypto Map IPSec IKEv1 Configuration Mode Commands

Modification(s) to an existing IKEv1 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 IKEv1 Configuration Mode is used to configure properties for IPSec tunnels that will be created using the Internet Key Exchange (IKE) that operates within the framework of the Internet Key Exchange version 1 (IKEv1).

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-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
- ipsec-on-demux, on page 2
- match address, on page 3
- match crypto group, on page 4
- match ip pool, on page 6
- set, on page 7

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.

ipsec-on-demux

Enable spawning of IPSec manager for this Crypto map on Demux Card.

Product IPSec (IKEv1/IKEv2 ACL Mode)

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

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

Syntax Description `[ no ] ipsec-on-demux`

no

Disables the spawning of IPSec manager for Crypto map on Demux Card.

ipsec-on-demux

Enables the spawning of IPSec manager for this Crypto map on Demux Card.



Important If the configuration is removed using no option, then this Crypto map must be removed and added again for this configuration to work.

Example

The following configuration enables spawning of IPSec manager for this Crypto map on Demux Card.

```
ipsec-on-demux
```

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 IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-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 as an alphanumeric string of 1 through 79 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.

The preference is an integer value from 0 to 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
```

match crypto group

Matches or associates the crypto map a crypto group 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 IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] match crypto group` *`group_name`* **`{ primary | secondary }`**

no

Deletes a previously configured crypto group association.

match crypto group *group_name*

Specifies the name of the crypto group entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

primary

Specifies that the policies configured as part of this crypto map will be used for the primary tunnel in the Redundant IPSec Tunnel Failover feature.

secondary

Specifies that the policies configured as part of this crypto map will be used for the secondary tunnel in the Redundant IPSec Tunnel Failover feature.

Usage Guidelines

Use this command to dictate the primary and secondary tunnel policies used for the Redundant IPSec Tunnel Failover feature.

At least two policies must be configured to use this feature. One policy must be configured as the primary, the other as the secondary.

Example

The following command associates the crypto map to a crypto group called *group1* and dictates that it will serve as the primary tunnel policy:

```
match crypto group group1 primary
```

match ip pool

Matches the specified IP pool to the current IKEv1 crypto map. This command can be used multiple times to change more than one IP pool.

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.

Important The **match ip pool** command is not supported on the ASR 5500 platform.

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 IPSec IKEv1 Configuration

configure > **context** *context_name* > **crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] match ip pool pool-name *pool_name* **[destination-network** *ip_address* **[/***mask* **]**

no

Delete the matching statement for the specified IP pool from the crypto map.

match ip pool pool-name *pool_name*

Specifies the name of an existing IP poolthat should be matched as an alphanumeric string of 1 through 31 characters.

destination-network *ip_address* [*/mask*]

Specifies the IP address of the destination network in IPv4 dotted-decimal or IPV6 colon-separated-hexadecimal notation.

/mask specifies the subnet mask bits (representing the subnet mask). This variable must be entered in IPv4 dotted-decimal or !Pv6 colon-separated-hexadecimal CIDR notation.

An IP pool attached to the crypto map can have multiple IPSec tunnels according to the destination of the packet being forwarded to internet.



Important Each invocation of this command will add another destination network to the IP pool, with a maximum of eight destination networks per crypto map.

Usage Guidelines

Use this command to set the names of IP pools that should be matched in the current crypto map.



Important If an IP address pool that is matched to a IKEv1 crypto map is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the **clear crypto** command in the Exec mode for information on clearing security associations.

Example

The following command sets a rule for the current crypto map that will match an IP pool named *ippool1*:

```
match ip pool pool-name ippool1
```

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

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context *context_name* **> crypto map** *policy_name* **ipsec-ikev1**

Entering the above command sequence results in the following prompt:

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

Syntax Description

set { bgp *peer_address* **| control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [keepalive** *sec* **] | ip mtu** *bytes* **| ipv6 mtu** *bytes* **| mode { aggressive | main } | peer** *peer_address* **| pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id | ipv4-address [mode { aggressive | main }] | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes** *kbytes* **| seconds** *secs* **} transform-set** *transform_name* **[transform-set** *transform_name2 ...* **transform-set** *transform_name6* **]**

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

bgp *peer_address*

Specifies the IP address of the BGP peer in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

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 *time*]



Important NAT Traversal (NATT) for IKEv1 IPSec session is not supported.

Specifies IKE parameters.

natt: Enables IPSec NAT Traversal.

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

ip mtu *bytes*

Specifies the IPv4 Maximum Transmission Unit (MTU) in bytes as an integer from 576 to 2048.

ipv6 mtu *bytes*

Specifies the IPv6 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.

peer *peer_address*

Specifies the peer IP address of a remote gateway in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

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: id-key-id

id-key-id: ID KEY ID

ipv4-address: ID IPV4 Address

- **mode**: Configures IKE mode
- **aggressive**: IKE negotiation mode: AGGRESSIVE
- **main**: IKE negotiation mode: MAIN

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 { disable-phase2-rekey | keepalive | kilo-bytes *kbytes* | seconds *secs* }

Defaults:

- **disable-phase2-rekey**: Rekeying is enabled by default
- **keepalive**: Disabled
- **kilo-bytes:** 4608000 kbytes
- **seconds:** 28800 seconds

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.

- **disable-phase2-rekey**: If this keyword is specified, the Phase2 SA is not rekeyed when the lifetime expires.
- **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 (n kilobytes) to allow through the tunnel before the SA lifetime expires. *kbytes* must be an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires. *secs* must be 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.

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

no

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

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
```