

Crypto Group Configuration Mode Commands

The Crypto Group Configuration Mode is used to configure crypto (tunnel) groups that provide fail-over redundancy for IPSec tunnels to packet data networks (PDNs).

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

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

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
- match address, on page 2
- match ip pool, on page 3
- switchover, on page 5

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

Associates an access control list (ACL) with the crypto group.



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 Group Configuration

configure > **context** *context_name* > **crypto group** *group_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] match address` *`acl_name`* **`[`** *`preference`* **`]`**

no

Deletes a previously configured ACL association.

match address *acl_name*

Specifies the name of the ACL being matched to the crypto group entered as an alphanumeric string of 1 through 47 characters.

preference

The priority of the ACL.

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

If multiple ACLs are assigned the same priority, the last one entered will be used first.

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

Usage Guidelines

IP ACLs are associated with crypto groups using this command. Both the crypto group and the ACLs must be configured in the same context.

ISAKMP crypto maps can then be associated with the crypto group. This allows user traffic matching the rules of the ACL to be handled according to the policies configured as part of the crypto map.

Example

The following command associates an ACL called *corporate_acl* to the crypto group:

```
match address corporate_acl
```

match ip pool

Matches the specified IP pool to the current crypto group. This command can be used multiple times to match 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 within a crypto group 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, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] match ip pool pool-name *pool_name*

no

Deletes the matching statement for the specified IP pool from the crypto group.

match ip pool pool-name *pool_name*

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

Usage Guidelines

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

Example

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

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

switchover

Configures the fail-over properties for the crypto group as part of the Redundant IPSec Fail-Over feature.

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 Group Configuration

configure > context *context_name* **> crypto group** *group_name*

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
[ no ] switchover auto [ do-not-revert ]
```

no

Disables the automatic switchover of tunnels. This applies to switching primary-to-secondary and secondary-to-primary.

switchover auto

Allows the automatic switchover of tunnels. Default: Enabled

do-not-revert

Disables the automatic switchover of secondary tunnels to primary tunnels. Default: Disabled

Usage Guidelines

This command configures the fail-over options for the Redundant IPSec Fail-over feature.

If the automatic fail-over options are disabled, tunneled traffic must be manually switched to the alternate tunnel (or manually activated if no alternate tunnel is configured and available) using the following command in the Exec Mode:

```
crypto-group group_name activate { primary | secondary }
```

For a definition of this command, see the **crypto-group** section of the Exec Mode Commands chapter of this guide.

Example

The following command disables the automatic secondary-to-primary switchover:

```
switchover auto do-not-revert
```