Crypto Map IKEv2-IPv4 Configuration Mode Commands

Command Modes

The Crypto Map IKEv2-IPv4 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv4 Configuration

configure > **context** *context_name* > **crypto map** *template_name* **ikev2-ipv4**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv4-map)#
```

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

allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product

Security gateway products

Privilege

Security Administrator

Syntax Description

```
[ no ] allow-cert-enc cert-hash-url
```

no

Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

Usage Guidelines

Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example

The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```

authentication

Configures the subscriber authentication method used for this 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

Syntax Description

```
authentication { local { certificate | pre-shared-key } { encrypted key value | key value } | min-key-sizemin_key_size | remote { certificate | pre-shared-key } { encrypted key value| keyvalue }
[ no | default ] authentication  min-key-size
```

local | remote

Specifies which authentication method will be used by the crypto map – local or remote.

[no | default] authentication min-key-size

no Disables minimum key size validation feature.

default Sets default key size. Default is 255.

min-key-size*min_key_size*

Specifies Minimum Cert Key size. Default is 255.

min_key_size must be an integer between 255 and 8192.

certificate

Specifies that a certificate will be used by this crypto map for authentication.

pre-shared-key { encrypted key *value* | key *value* }

Specifies that a pre-shared key will be used by this crypto map for authentication.

encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 16 to 496 characters for release 15.0 and higher.

key *value*: Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 32 characters for releases prior to 14.0 or 1 through 255 characters for release 14.0 and higher.

Usage Guidelines

Use this command to specify the type of authentication performed for IPSEC peers attempting to access the system via this crypto map.

Example

The following command sets the authentication method to an open key value of *6d7970617373776f7264*:

```
authentication pre-shared-key key 6d7970617373776f7264
```

blockedlist

Enables or disables a blockedlist (access denied) for this map.

Product

All products supporting IPSec blockedlisting

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

In releases prior to StarOS 21.26:

```
[ no ] blacklist
```

From StarOS 21.26 and later releases:

```
[ no ] blockedlist
```

no

Disables blockedlisting for this crypto map. By default blockedlisting is disabled.

Usage Guidelines

Use this command to enable blockedlisting for this crypto map. A blockedlist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blockedlisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blockedlisting, refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

The following command enables blacklisting:

```
blacklist
```

From StarOS 21.26 and later releases:

The following command enables blockedlisting:

```
blockedist
```

ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate to a 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

Syntax Description

```
ca-certificate list ca-cert-name name [ ca-cert-name  name ]
no ca-certificate
```

no

Unbinds the ca-certificate(s) bound to the crypto map.

ca-cert-name *name*

Binds the named X.509 Certificate Authority (CA) certificate to a crypto map. *name* is an alphanumeric string of 1 through 129 characters.

You can chain multiple(max 4) certificates in a single command instance.

Usage Guidelines

Used to bind an X.509 CA certificate to a map.

Example

Use the following example to add a CA certificate to a list:

```
ca-certificate list ca-cert-name CA_list1
```

ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this 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

Syntax Description

```
ca-crl list ca-crl-name name [ ca-crl-name name ] +
no ca-crl
```

no

Removes the CA-CRL configuration from this map.

ca-crl-name *name*

Specifies the CA-CRL to associate with this crypto map. *name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters.

+ indicates that a list of multiple CA-CRLs can be configured for a crypto map. You can chain multiple (max four) CA-CRLs in a single command instance.

Usage Guidelines

Use this command to associate a CA-CRL name with this crypto map.

CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

Example

The following example binds CA-CRLs named *CRL-5* and *CRL-7* to this crypto map:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```

certificate

Used to bind a single X.509 trusted certificate to a 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

Syntax Description

```
[ no ] certificate name
```

no

Unbinds a certificate from crypto map.

name

Specifies the name of a X.509 trusted certificate to bind to a crypto map. *name* is an alphanumeric string of 1 through 129 characters.

Usage Guidelines

Use this command to bind an X.509 certificate to a map.

Example

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```

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.

i

Product

ePDG

FA

GGSN

HA

HeNBGW

HNBGW

HSGW

MME

P-GW

PDSN

S-GW

SAEGW

SCM

SecGW

SGSN

Privilege

Security Administrator

Syntax Description

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

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

A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

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

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

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.

ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

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

Syntax Description

```
ikev2-ikesa { allow-empty-ikesa | max-retransmissions number | policy {
error-notification [ invalid-major-version ] [ invalid-message-id [
invalid-major-version | invalid-syntax ] ] | invalid-syntax [
invalid-major-version ] | use-rfc5996-notification } | rekey [
disallow-param-change ] | retransmission-timeout msec [ exponential ] |
setup-timer sec | transform-set list name1 name2 name3 name4 name5 name6  }
default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy
error-notification | rekey [ disallow-param-change ] | setup-timer }
```

```
no ikev2-ikesa { allow-empty-ikesa name | policy { error-notification |
use-rfc5996-notification } | rekey sec | transform-set list }
```

no ikev2-ikesa

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

max-retransmissions *number*

Specifies the maximum number of retransmissions of an IKEv2 IKE Exchange Request if a response has not been received. *number* must be an integer from 1 through 8. Default: 5

policy { error-notification [invalid-major-version] [invalid-message-id [invalid-major-version | invalid-syntax]] | invalid-syntax [invalid-major-version] | use-rfc5996-notification }

Specifies the default policy for generating an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

error-notification: Sends an Error Notify Message to the MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

[invalid-major-version]: Sends an Error Notify Message for Invalid Major Version

[invalid-message-id]: Sends an Error Notify Message for Invalid IKEv2 Exchange Message ID.

[invalid-syntax]: Sends an Error Notify Message for Invalid IKEv2 Exchange Syntax.

use-rfc5996-notification: Enables support for TEMPORARY_FAILURE and CHILDSA_NOT_FOUND notify payloads.

rekey [disallow-param-change]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The **disallow-param-change** option does not allow changes in negotiation parameters during rekey.

retransmission-timeout *msec*

Specifies the timeout period (in milliseconds) before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). *msec* must be an integer from 300 to 15000. Default: 500

exponential

Specifies that the subsequent retransmission delays are exponentially increased with a maximum limit of 15000ms.

setup-timer *sec*

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. *sec* must be an integer from 1 through 3600. Default: 16

transform-set list *name1*

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set. *name1 ...name6*must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage Guidelines

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the maximum number of IKEv2 IKESA request retransmissions to *7*:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to *400* milliseconds:

```
ikev2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA transform set *ikesa43*:

```
ikev2-ikesa transform-set list ikesa43
```

keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

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

Syntax Description

```
keepalive [ interval sec ] [ timeout sec [ num-retry num ]
no keepalive
```

no

Disables keepalive messaging.

interval *sec*

Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. *sec* must be an integer from 10 through 3600. Default: 10

timeout *sec*

Specifies the amount of time (in seconds) which must elapse during which no traffic is received from the IKE_SA peer or any CHILD_SAs derived from the IKE_SA for Dead Peer Detection to be initiated. *sec* must be an integer from 10 through 3600. Default: 10

num-retry *num*

Specifies the number of times the system will retry a non-responsive peer before defining the peer as off-line or out-of-service. *num* must be an integer from 1 through 100. Default: 2

Usage Guidelines

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (*180* seconds):

```
keepalive interval 180
```

match

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

Syntax Description

```
match address acl_name [ priority ]
no match address acl_name
```

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 79 characters that is case sensitive.

priority

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0

The ACL preference is factored when a single packet matches the criteria of more than one ACL.

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 *acl-list1* and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```

natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

Product All Security Gateway products

Privilege Security Administrator

Syntax Description

```
[ default | no ] natt [ include-header ] [ send-keepalive [ idle-interval
 idle_secs ] [ interval interval_secs ] ]
```

default

Disables NAT-T for all security associations associated with this crypto template.

no

Disables NAT-T for all security associations associated with this crypto template.

include-header

Includes the NAT-T header in IPSec packets.

send-keepalive [idle-interval *idle_secs*] [interval *interval_secs*]

Sends NAT-Traversal keepalive messages.

idle-interval *idle_secs*: Specifies the number of seconds that can elapse without sending NAT keepalive packets before sending NAT keepalive packets is started. *idle_secs* is an integer from 20 to 86400. Default: 60.

interval *interval_secs*: Specifies the number of seconds between the sending of NAT keepalive packets. *interval_secs* is an integer from 20 to 86400. Default: 60.

Usage Guidelines

Use this command to configure NAT-T for security associations within this crypto template.

Example

The following command disables NAT-T for this crypto template:

```
no natt
```

ocsp

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

Product

All products supporting IPSec

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Syntax Description

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

no

Disables the use of OCSP.

default

Restores the default value assigned for ocsp nonce.

nonce

Enables sending nonce (unique identifier) in OCSP requests.

responder-address *ipv4_address*

Configures the OCSP responder address that is used when absent in the peer (device) certificate.

ipv4_address is an IPv4 address specified in dotted decimal format.

port *port_value*

Configures the port for OCSP responder.

port_value is an integer value between 1 and 65535. The default port is 8889.

Usage Guidelines

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate.

OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

Example

The following command enables OSCP:

```
ocsp
```

payload

Creates a new, or specifies an existing, crypto map payload and enters the Crypto Map Payload Configuration Mode.

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

Syntax Description

```
payload name match ipv4
no payload name
```

payload *name*

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match ipv4

Filters IPSec IPv4 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

Usage Guidelines

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the *ip-address-allocation* then no MIP call can be established, just a Simple IP call.

Currently, the only available match is for ChildSA, although other matches are planned for future releases.

Entering this command results in the following prompt:

[*ctxt_name*]*hostname*(cfg-crypto-<*name*>-ikev2-tunnel-payload)#

Crypto Template IKEv2-IPv4 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv4 Payload Configuration Mode Commands chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv4
```

peer

Configures the IP address of a peer IPSec.

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

Syntax Description

```
peer ip_address
no peer
```

no

Removes the configured peer IP address.

peer *ip_address*

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

Usage Guidelines

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of *fe80::200:f8ff:fe21:67cf*:

```
peer fe80::200:f8ff:fe21:67cf
```

remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product

All Security Gateway products

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Syntax Description

```
remote-secret-list list_name
no remote-secret-list
```

no

Disables use of a Remote Secret List.

list_name

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through127 characters.

Usage Guidelines Enable the use of a Remote Secret List containing up to 1000 pre-shared keys.

Only one active remote-secret-list is supported per system.

For additional information, refer to the *Remote Secret List Configuration Commands* chapter of the *Command Line Interface Reference* and the *System Administration Guide*.

Example

The following command enables a remote-secret-list named *rs-list*:

```
remote-secret-list rs-list
```

permitlist

Enables or disables a permitlist (access granted) for this crypto map.

Product All products supporting IPSec permitlisting .

Important This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege Security Administrator

Syntax Description In releases prior to StarOS 21.26:

```
[ no ] whitelist
```

From StarOS 21.26 and later releases:

```
[ no ] permitlist
```

no

Disables permitlisting for this crypto map. By default permitlisting is disabled.

Usage Guidelines

Use this command to enable permitlisting for this crypto map. A permitlist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With permitlisting , no peer is allowed to connect unless it appears in the list. For additional information on permitlisting , refer to the *System Administration Guide.*

Example

In releases prior to StarOS 21.26:

The following command enables whitelisting:

```
whitelist
```

From StarOS 21.26 and later releases:

The following command enables permitlisting:

```
permitlist
```