Crypto Template Configuration Mode Commands

The Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Important Available commands or keywords/variables vary based on platform type, product version, and installed license(s).

- allow-cert-enc cert-hash-url, on page 2
- allow-custom-fqdn-idr, on page 2
- authentication, on page 3
- blockedlist, on page 5
- ca-certificate list, on page 6
- ca-crl list, on page 6
- certificate, on page 7
- configuration-payload, on page 8
- control-dont-fragment, on page 9
- dns-handling, on page 9
- dos cookie-challenge notify-payload, on page 11
- ecn, on page 12
- end, on page 12
- exit, on page 13
- identity local, on page 13
- ikev2-ikesa, on page 14
- ikev2-ikesa ddos, on page 18
- ikev2-ikesa dscp, on page 20
- ip, on page 21

- ipv6, on page 22
- keepalive, on page 23
- max-childsa, on page 24
- nai, on page 25
- natt, on page 26
- notify-payload, on page 27
- ocsp, on page 28
- payload, on page 29
- peer network, on page 30
- remote-secret-list, on page 31
- server certificate, on page 32
- timeout, on page 32
- vendor-policy, on page 33
- permitlist, on page 34

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
```

allow-custom-fqdn-idr

Allows non-standard FQDN (Fully Qualified Domain Name) strings in the IDr (Identification - Responder) payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

Product

All services using IKEv2 IPSec

Privilege

Security Administrator

Syntax Description **[default | no] allow-custom-fqdn-idr**

no

Does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

default

Restores the default setting, which does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

You can chain multiple CA-CRLs in a single command instance.

Usage Guidelines Use this command to configure the system to skip the syntax check for the IDr payload in IKE_AUTH messages received from the UE with the payload type as FQDN. This allows non-standard FQDN strings such as APN names in the IDr payload.

Example

The following command configures the system to allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN:

allow-custom-fqdn-idr

authentication

Configures the gateway and subscriber authentication methods to be used by this crypto template.

Product All IPSec-related services

Privilege Security Administrator

Syntax Description

authentication { **eap-profile** *name* [**second-phase eap-profile** *name*] | **local** { **certificate** | **pre-shared-key** { **encrypted key** *value* | **key** *clear_text* } } | **min-key-size** *min_key_size* | **pre-shared-key** { **encrypted key** *value* | **key** *clear_text* [**second-phase eap-profile** *name*] } | **remote** { **certificate** | **eap-profile** *name* [**second-phase eap-profile** *name*] | **pre-shared-key** { **encrypted key** *value* | **key** *clear_text* [**second-phase eap-profile** *name*] } } }
no authentication local { certificate | min-key-size | pre-shared-key }
default authentication min-key-size

default

Returns the command to its default setting.

no

Removes the authentication parameters from the configuration.

eap-profile *name* [second-phase eap-profile *name*]

Specifies that authentication is to be performed using a named Extensible Authentication Protocol (EAP) profile. *name* is an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.

The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.

local { certificate | pre-shared-key { encrypted key *value* | key *clear_text* }

Specifies the local authentication method required for services using the crypto template.

certificate: Specifies that the certificate method of authentication must be used for services using the crypto template.

min-key-size: Sets minimum certificate key size. *min_key_size* must be an integer between 255 to 8192. Default is 255.

pre-shared-key { encrypted key *value* **| key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 16 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. **key** *clear_text* configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255 characters.

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

Specifies that a pre-shared key is to be used for services using the crypto template.

encrypted key *value*: Specifies that the pre-shared key used for authentication is encrypted. *value* must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher.

key *clear_text*: Specifies that the pre-shared key used for authentication is clear text. *clear_text* must be an alphanumeric string of 1 through 255 characters.

remote { certificate | eap-profile *name* [second-phase eap-profile *name*] | pre-shared-key { encrypted key *value* | key *clear_text* }

Specifies the remote authentication method required for services using the crypto template.

certificate: Specifies that the certificate method of remote authentication must be used for services using the crypto template.

eap-profile *name* **[second-phase eap-profile** *name* **]**: Specifies that remote authentication is to be performed using a named EAP profile. *name* must be an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.

The **second-phase eap-profile** *name* is only required for installations using multiple authentications. *name* must be an alphanumeric string of 1 through 127 characters.

pre-shared-key { encrypted key *value* **| key** *clear_text* **}**: Specifies that a pre-shared key is to be used for services using the crypto template. **encrypted key** *value* configures an encrypted pre-shared key used for authentication. *value* must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. **key** *value* configures a clear text pre-shared key used for authentication. *clear_text* must be an alphanumeric string of 1 through 255 characters.

Usage Guidelines

Use this command to specify the type of authentication performed for subscribers or gateways attempting to access the service using this crypto template.

Entering the **authentication eap-profile** command results in the following prompt:

```
[context_name]hostname(cfg-crypto-tmpl-eap-key)#
```

EAP Authentication Configuration Mode commands are defined in the *EAP Authentication Configuration Mode Commands* chapter.

Example

The following command enables authentication via an EAP profile named *eap23* for subscribers using the service with this crypto template:

```
authentication eap-profile eap23
```

blockedlist

Enables the use of a blockedlist (access denied) file to be used by a security gateway.

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 the use of a blacklist.

Usage Guidelines

Enable the use of a previously created blockedlist to deny access to prohibited peers via a security gateway.

A blockedlist is a list or register of entities that are being 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.

Each entry in the blockedlist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

Example

In releases prior to StarOS 21.26:

The following command enables use of a blacklist:

blacklist

ca-certificate list

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

Product

All IPSec-related services

Privilege

Security Administrator, Administrator

Syntax Description

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

no

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

ca-cert-name *name*

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

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

Usage Guidelines

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

Example

Use the following example to add a CA certificate named *CA_list1* to a list:

ca-certificate list CA_list1

ca-crl list

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

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

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

no

Removes the CA-CRL configuration from this template.

ca-crl-name *name*

Specifies the CA-CRL to associate with this crypto template. *name* must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists (maximum 4) can be configured for a crypto template.

You can chain multiple CA-CRLs in a single command instance.

Usage Guidelines

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

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 template:

```
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 template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
certificate name [ validate ]
no certificate [ validate ]
```

no

Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

name

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

validate

Enable validations for the self-certificate.

Usage Guidelines Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

Example

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

```
no certificate
```

configuration-payload

This command is used to configure mapping of the configuration payload attributes.

Product All IPSec-related services

Privilege Security Administrator

Syntax Description

```
configuration-payload private-attribute-type { imei integer | p-cscf-v4
v4_value | p-cscf-v6 v6_value }
[ no | default ] configuration-payload private-attribute-type { imei |
p-cscf-v4 | p-cscf-v6 }
```

no

Removes mapping of the configuration payload attributes.

default

Restores the defuat value for mapping of the configuration payload attributes.

private-attribute-type

Defines the private payload attribute.

imei *integer*

Defines an International Mobile Equipemnt Identity number as an integer from 16384 to 32767.

p-cscf-v4 *v4_value*

Defines the IPv4 pcscf payload attribute value. Default value is 16384.

v4_value is an integer from 16384 to 32767.

p-cscf-v6 *v6_value*

Defines IPv6 pcscf payload attribute value. Default value is 16390.

v6_value is an integer from 16384 to 32767.

Usage Guidelines Use this command to configure mapping of the configuration payload attributes.

Example

The following command configures the mapping of the configuration payload attributes p-cscf-v6 to 17001.

configuration-payload private-attribute-type p-cscf-v6 *17001*

control-dont-fragment

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

Product

All IPSec-related services

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

dns-handling

Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.

Product

PDIF

Privilege

Security Administrator

Syntax Description

```
[ default ] dns-handling { custom | normal }
```

default

Configures the default condition as **normal**. By default, PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

dns-handling custom

Configures the PDIF to behave as described in the Usage section below.

dns-handling normal

This is the default action. The service always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

Usage Guidelines

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.

In **normal** mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

In **custom** mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the following behaviors:

- If MS includes no INTERNAL_IP4_DNS in Config Payload: PDIF does not return any INTERNAL_IP4_DNS option to MS, whether or not PDIF has received one in DNS NVSE from HA or from local configurations.
- If MS requests one or more INTERNAL_IP4_DNS(s) in Config Payload, and if P-MIP NVSE doesn't contain any DNS address or DNS address not present in any config, PDIF omits INTERNAL_IP4_DNS option to MS in the Config Payload.
- And if P-MIP NVSE includes one DNS address (a.a.a.a / 0.0.0.0), then PDIF sends one INTERNAL_IP4_DNS option in Config Payload back to the MS.
- If the Primary DNS is a.a.a.a and the Secondary DNS is 0.0.0.0, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload).
- If the Primary DNS is 0.0.0.0 and the Secondary DNS is a.a.a.a, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload). PDIF does not take 0.0.0.0 as a valid DNS address that can be assigned to the MS.
- And if P-MIP NVSE includes two DNS addresses (a.a.a.a and b.b.b.b) or configurations exists for these two addresses, then PDIF sends two INTERNAL_IP4_DNSs in the CP for the MS (typically known as primary and secondary DNS addresses).

Example

The following configuration applies the **custom** dns-handling mode:

```
dns-handling custom
```

dos cookie-challenge notify-payload

Configure the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
dos cookie-challenge notify-payload [ half-open-sess-count start integer
stop integer]
[ default | no ] cookie-challenge detect-dos-attack
```

default

Default is to disabled condition.

no

Prevents Denial of Service cookie transmission. This is the default condition.

half-open-sess-count start *integer* stop *integer*

The **half-open-sess-count** is the number of half-open sessions per IPSec manager.

A session is considered half-open if a PDIF has responded to an IKEv2 INIT Request with an IKEv2 INIT Response, but no further message was received on that particular IKE SA.

- **start** *integer*: Starts when the current half-open-sess-count exceeds the start count. The start count is an integer from 0 to 100000.
- **stop** *integer*: Stops when the current half-open-sess-count drops below the stop count. The stop count number is an integer from 0 to 100000. It is always less than or equal to the start count number

Important The start count value 0 is a special case whereby this feature is always enabled. In this event, both **start** and **stop** must be 0.

Usage Guidelines

This feature (which is disabled by default) helps prevent malicious Denial of Service attacks against the server by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.

Example

The following example configures the cookie challenge to begin when the half-open-sess-count reaches 50000 and stops when it drops below 20000:

```
dos cookie-challenge notify-payload half-open-sess-count start 50000 stop
 20000
```

ecn

This command enables explicit congestion notification (ECN) in normal mode or compatible mode for the IPsec tunnel over the SWu interface.

Product

ePDG

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#`

Syntax Description

[no] ecn

no

Enables ECN in compatible mode for IPsec tunnel over SWu interface. The default mode is the compatible mode, supported for backward compatibility.

ecn

Specifies ECN over IPsec tunnel in normal mode.

Usage Guidelines

Use this command to enable ECN in normal mode or compatible mode for the IPsec tunnel over SWu interface.

Example

The following command enables ECN in normal mode for the IPsec tunnel:

ecn

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.

identity local

Configures the identity of the local IPSec Client (IKE ID).

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

```
identity local id-type type id name
no identity local
```

no

Resets the ID to the IP address of the interface to which the crypto template is associated (type = IPv4 or IPv6).

id-type *type*

Configures the IKE identity that the local client uses when authenticating to the gateway. Valid values are:

- **der-ans1-dn**: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
- **fqdn**: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- **ip-addr**: configures NAI Type ID_IP_ADDR (IP Address).
- **key-id**: configures NAI Type ID_KEY_ID (opaque octet string).
- **rfc822-addr**: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

id *name*

Specifies the identifier for the local IKE client as an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to configure the identity of the local IPSec Client.

Example

The following command configures the local IPSec Client.

identity local id-type der-asn1-dn id system14

ikev2-ikesa

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

Product

All IPSec-related services

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(crf-crypto-tmp1-ikev2-tunnel)#

Syntax Description

ikev2-ikesa { allow-empty-ikesa | cert-sign { pkcs1.5 | pkcs2.0 } | configuration-attribute p-cscf-v6 { iana | private } length { 16 | 17 } | emergency { keepalive [interval *interval* **] timeout** *seconds* **num-retry** *val* **} | fragmentation | idi** *peer_idi_value* **{ common-id | request-eap-identity } | imsi-privacy auth-imsi| ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | max-retransmissions** *number* **| mobike [cookie-challenge] | policy { congestion-rejection { notify-status-value** *value* **| notify-error-value** *value* **} | 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* **| setup-timer** *sec* **| transform-set list** *name1 name2 name3 name4 name5 name6* **}**

default ikev2-ikesa { allow-empty-ikesa | cert-sign | configuration-attribute p-cscf-v6 { iana | private } length | fragmentation | ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | max-retransmissions | mobike | policy error-notification | rekey [disallow-param-change] | retransmission-timeout | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | auth-method-set | fragmentation | idi *peer_idi_value* **| ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | list** *name* **| mobike | policy error-notification | rekey }| imsi-privacy auth-imsi**

default

Restores the configuration to its default value.

no

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.

cert-sign { pkcs1.5 | pkcs2.0 }

Specifies the certificate sign to be used. Default: pkcs1.5

pkcs1.5: Use the Public-Key Cryptography Standards (PKCS) version 1.5, RSA Encryption Standard.

pkcs2.0:: Use the PKCS version 2.0, RSA Encryption Standard.

configuration-attribute p-cscf-v6 { iana | private } length { 16 | 17 }

Specifies the P-CSCF IPv6 configuration attribute length for both IANA and private attribute values. As per RFC 7651, the configuration attribute length for IANA is 16 bytes.

Default (iana): 16 bytes

Default (private): 17 bytes

emergency { keepalive [interval *interval*] timeout *seconds* num-retry *val* }

Configures emergency call related parameters.

Keepalive : Configures Keepalive Functionality (Dead Peer Detection) to be enabled for all emergency Security Associations derived from this Crypto Template and this will override generic keep alive configuration for emergency calls.

interval : The number of seconds which must elapse during which no traffic is received from the given IKE_SA peer or any CHILD_SAs derived from the IKE_SA for Dead Peer Detection to be initiated (Default: 3). - integer 2..3600

timeout : Configures the Keepalive (Dead Peer Detection) Timeout in seconds. This value configures the number of seconds which must elapse after a Keepalive has been sent, and no response has been received before another keepalive is sent.

seconds : The number of seconds which must elapse after a Keepalive has been sent, and no response has been received, before another Keepalive is send. Default is 3 seconds and the Interval should be between 2 and 3600 seconds.

num-retry : Configure the number of Keepalive (Dead Peer Detection) Retry attempts. If Keepalive (Dead Peer Detection) has been initiated this value configures the number of retry attempts which will be made if no response is received from the peer, before the peer is declared dead.

val : The number of retry attempts which will be made if no response is received from the peer before the peer is declared dead Default is 2 seconds and the Interval should be between 1 and 30 seconds.

fragmentation

Enables IKESA fragmentation (Tx) and re-assembly (Rx).

Default: IKESA fragmentation and re-assembly is allowed.

idi *peer_idi_value* { common-id | request-eap-identity }

Specifies the IDI related configuration to match IDI from peer which enables the ePDG to request the real identity using EAP-Identity Request. *peer_idi_value* is a string of 1 through 127 characters.

request-eap-identity: Requests the EAP-Identity from peer.

common-id: Requests the Common IDi from peer.

imsi-privacy

Configures IMSI Privacy related parameters.

auth-imsi

Enables IKESA to use IMSI for AUTH calculation for IMSI Privacy.

.

ignore-notify-protocol-id

Ignores IKEv2 Informational Exchange Notify Payload Protocol-ID values for strict RFC 4306 compliance.

ignore-rekeying-requests

Ignores received IKE_SA Rekeying Requests.

keepalive-user-activity

Default is no keepalive-user-activity. Activate to reset the user inactivity timer when keepalive messages are received from peer.

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

mobike [cookie-challenge]

IKEv2 Mobility and Multihoming Protocol (MOBIKE) allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations to change. A mobile Virtual Private Network (VPN) client could use MOBIKE to keep the connection with the VPN gateway active while moving from one address to another. Similarly, a multi-homed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working.

Default: Disabled

cookie-challenge: Use this keyword to enable the return routability check. The Gateway performs a return routability check when MOBIKE is enabled along with this keyword. A return routability check ensures that the other party can receive packets at the claimed address. Default: Disabled

policy { congestion-rejection { notify-status-value *value* | notify-error-value *value* } | 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.

congestion-rejection: Sends an Error Notify Message to the MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established.

notify-status-value *value*: Notify Message will be sent to MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established. *value* is RFC 4306 IKEv2 Private Use Status Range - integer 40960 through 65535.

notify-error-value *value*: Notify Message will be sent to MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established. *value* is RFC 4306 IKEv2 Private Use Error Range - integer 8192 through 16383.

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: Enable sending and receive processing for RFC 5996 notifications - TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND

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 prevents 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

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.

no ikev2-ikesa imsi-privacy auth-imsi

Reverts to default of IKESA to use IDI for AUTH calculation for IMSI Privacy.

Usage Guidelines

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

Example

The following command enables IKESA fragmentation and re-assembly:

```
ikev2-ikesa fragmentation
```

The following command configures the maximum number of IKEv2 IKESA request re-transmissions to *7*:

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

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

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

The following command configures the IKEv2 IKESA list, consisting of a transform set named as *ikesa43*:

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

ikev2-ikesa ddos

Configures distributed denial of service (DDoS) mitigation parameters for the IKEv2 IKE Security Associations within this crypto template.

Product

ePDG

HeNBGW

HNBGW

WSG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ikev2-ikesa ddos { decrypt-fail-count *failure_count* **| half-open-sa-timer** *half_open_timer_duration* **| ikev2-req-rate** *ikev2_req_rate_count* **[interval** *interval* **]| max-cert-size** *cert_size* **| message-queue-size** *queue_size* **| rekey-rate** *rekey_rate_value* **}**

```
{ default | no } ikev2-ikesa ddos { decrypt-fail-count | half-open-sa-timer
 | ikev2-req-rate | max-cert-size | message-queue-size | rekey-rate }
```

default

Restores the configuration to its default value.

no

Disables a previously enabled configuration.

decrypt-fail-count *failure_count*

Specifies the maximum tolerable consecutive IKE_AUTH message decryption failure count. During session establishment, if IKE_AUTH decryption failure exceeds the configured threshold, the IKEv2 IKE SA tunnel is cleared. If IKE_AUTH decryption failure exceeds the configured threshold after the session is established, alarms are triggered.

Default: 30

failure_count must be an integer between 1 and 100.

half-open-sa-timer *half_open_timer_duration*

Specifies the half-open IKE SA timeout duration. The half-open IKE SA timer starts when an IKE_SA_INIT request is received. If an IKE_AUTH message is not received before the timer expires, the half-open IKEv2 IKE SA is cleared.

Default: 60

half_open_timer_duration must be an integer between 1 and 1800.

ikev2-req-rate *ikev2_req_rate_count* [interval *interval*]

ikev2-req-rate *ikev2_req_rate_count*: Configures the maximum number of IKEv2 requests allowed per configured interval. *ikev2_req_rate_count* must be an integer from 1 to 3000.

Default: 10

interval *interval* : Configures the interval for monitoring IKEv2 requests. *interval* must be an integer from 1 to 300.

Default: 1 second

max-cert-size *cert_size*

Specifies the maximum certificate size for IKE SA. Use this keyword to detect bad certificates from illegitimate URLs in earlier stages, and thus avoid downloading large certificates.

Default: 2048 bytes

cert_size must be an integer between 512 and 8192.

message-queue-size *queue_size*

Specifies the queue size for incoming IKE messages per IKE SA. When the incoming queued IKE messages (per IKE SA) exceeds the specified limit, the IKE messages exceeding the limit are dropped.

Default: 20

queue_size must be an integer between 1 and 50.

rekey-rate *rekey_rate_value*

Specifies the rate at which the rekey request will be processed per second. When the specified number of Child SA rekey requests per second is exceeded, a TEMPORARY_FAILURE notification will be sent to the peer to indicate that the peer must slow down their requests.

Default: 5

rekey_rate_value must be an integer between 1 and 50.

Usage Guidelines

Use this command to configure parameters for Distributed Denial of Service (DDoS) mitigation for the IKEv2 IKE Security Associations within this crypto template.

Example

The following command configures the half-open IKE SA timeout duration to *300* seconds:

```
ikev2-ikesa ddos half-open-sa-timer 300
```

ikev2-ikesa dscp

Configures the Differentiated Services Code Point (DSCP) value in the IPv4 and IPv6 headers of the IKEv2 packets sent to the peer for this crypto template.

Product

ePDG

HeNBGW

HNBGW

SecGW

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

ikev2-ikesa dscp *dscp_hex_value*

default ikev2-ikesa dscp

default

Restores the configuration to its default value.

dscp *dscp_hex_value*

Specifies the DSCP value in the IKEv2 packets sent to the peer.

Default: 0x00

dscp_hex_value must be an hexa-decimal value between 0x00 and 0x3F.

Usage Guidelines

Use this command to configure the Differentiated Services Code Point (DSCP) value in the IPv4 and IPv6 headers of the IKEv2 packets sent to the peer for this crypto template.

Example

The following command configures the DSCP value to *0x2A*:

```
ikev2-ikesa dscp 0x2A
```

ip

Configures IPv4 related information.

Product

All IPSec-related services

ePDG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

```
ip { fragment { inner | outer } | ikev2-mtu mtu_size | mtu size }
default ip { fragment | ikev2-mtu | mtu }
```

default

Sets / Restores default value assigned for IPv4 related information. The default value for fragment is outer. The default value for ikev2-mtu is 1384. The default value for mtu is 1438.

fragment { inner | outer }

Configures the fragment type when User Payload is IPv4 type and DF bit not set.

Default: outer

inner: Fragments the IPv4 payload and encapsulate in the IPSec tunnel.

outer: Fragment to happen after the IPSec encapsulation.

ikev2-mtu *mtu_size*

Configures MTU size of the IKEv2 Payload for IPv4 tunnel.

mtu_size is an integer between 460 and 1932.

mtu *size*

Configures MTU of the User Payload for IPv4 tunnel.

size is an integer between 576 and 2048.

Usage Guidelines

Use this command to configure IPv4 related information for given ePDG services configured on this system.

For IPSec, use this command to set the Maximum Transmission Unit (MTU) size for the IKEv2 payload over IPv4 tunnels.

Example

The following command sets the IKEv2 MTU size to 1500:

```
ip ikev2-mtu 1500
```

The following command sets the MTU size to 1500:

```
ip mtu 1500
```

ipv6

Configures the MTU (Maximum Transmission Unit) of the user payload for IPv6 tunnels in bytes.

Product

All IPSec-related services

ePDG

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

For ePDG:

```
ipv6 mtu size
default ipv6 mtu
```

For IPSec:

```
ipv6 ikev2-mtu mtu-size
default ipv6 ikev2-mtu
```

default

Sets the IPv6 tunnel MTU to its default size.

mtu *size*

Specifies the MTU size of a packet to accommodate IPSec headers added to a packet.

Default:1422

size must be an integer from 1280 through 2048.

ikev2-mtu *mtu_size*

Configures MTU size of the IKEV2 Payload for IPv6 tunnel.

Default: 1364

mtu_size must be an integer from 1144 through 1912.

Usage Guidelines

For ePDG, use this command to increase the MTU size of a packet to accommodate IPSec headers added to a packet and thus avoid sending an ICMP Fragmentation Needed packet.

For IPSec, use this command to set the Maximum Transmission Unit (MTU) size for the IKEv2 payload over IPv6 tunnels.

Example

The following command sets the IKEv2 MTU size to 1500:

```
ipv6 ikev2-mtu 1500
```

The following command sets the MTU size to 1800:

```
ipv6 mtu 1800
```

keepalive

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

Product

All products supporting IPSec

Privilege

Security Administrator

Syntax Description

```
keepalive [ interval sec ]
default keepalive [ interval ]
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

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
```

max-childsa

Defines a soft limit for the number of child Security Associations (SAs) per IKEv2 policy.

Product All products supporting IPSEcv2

Privilege Security Administrator

Syntax Description

```
max-childsa integer [ overload-action { ignore | terminate } ]
```

max-childsa *integer*

Specifies a soft limit for the maximum number of Child SAs per IKEv2 policy as an integer from 1 to 4 for releases prior to 15.0, or 1 to 5 for 15.0 and higher. Default = 2.

overload-action { ignore | terminate }

Specifies the action to be taken when the specified soft limit for the maximum number of Child SAs is reached. The options are:

- **ignore**: The IKEv2 stack ignores the specified soft limit for Child SAs.
- **terminate**: The IKEv2 stack rejects any new Child SAs if the specified soft limit is reached.

Usage Guidelines Two maximum Child SA values are maintained per IKEv2 policy. The first is a system-enforced maximum value, which is four Child SAs per IKEv2 policy. The second is a configurable soft maximum value, which can be a value between one and four. This command defines the soft limit for the maximum number of Child SAs per IKEv2 policy.

Example

The following command specifies a soft limit of four Child SAs with the overload action of terminate.

```
max-childsa 4 overload-action terminate
```

nai

Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr (recipient's identity).

Product

Important This command is deprecated from 15.0 and later releases.

All Security Gateway products

Privilege

Security Administrator

Syntax Description

```
nai { idr name [ id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr |
key-id | rfc822-addr } ] | use-received-idr }
default nai idr
no nai { idr | use-received-idr }
```

default

Configures the default command **no nai idr**. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value of type ID_IP_ADDR.

no

no nai idr configures the value whereby the service IP address is sent as the IDr value with the type ID_IP_ADDR. This is the default condition.

idr *name*

Specifies the name of the IDr crypto template as an alphanumeric string of 1 through 79 characters.

id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr | key-id | rfc822-addr }

Configures the NAI IDr type parameter. If no id-type is specified, then **rfc822-addr** is assumed.

- **der-asn1-dn**: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
- **der-asn1-gn**: configures NAI Type DER_ASN1_GN (Distinguished Encoding Rules, ASN.1 encoding, General Name)
- **fqdn**: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- **ip-addr**: configures NAI Type ID_IP_ADDR (IP Address).
- **key-id**: configures NAI Type ID_KEY_ID (opaque octet string).
- **rfc822-addr**: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

use-received-idr

Specifies that the received IDr be used in the crypto template.

Usage Guidelines The configured IDr is sent to the MS in the first IKEv2 AUTH response.

Example

The following command configures the NAI IDr to the default condition.

```
default naiidr idr
```

natt

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

Important IKEv2 ACL with NAT-T is not supported.

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 60 to 86400. Default: 240.

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
```

notify-payload

This command configures the parameters to be sent in NOTIFY payload.

Product

All products supporting IPSec OCSP

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

```
notify-payload { device-id | error-message-type { network-permanent |
network-transient-major | network-transient-minor | ue }| pdn-type-allowed
 | base value }

default notify-payload { device-id | error-message-type { network-permanent
 | network-transient-major | network-transient-minor | ue } base }

no notify-payload device-id
```

default

Sets / restores default value assigned for the parameters to be sent in NOTIFY payload.

no

If previously configured, removes the configuration.

device-id

Enables ePDG to request for the IMEI or IMEI SV information using the DEVICE_IDENTITY notify payload in the IKE_AUTH_RESP message from the UE, if the UE does not share this information in the first IKE_AUTH_REQ message in the configuration attributes.

Default: Enabled

error-message-type

This command configures the type of notify error message.

Error Categories:

- **network-permanent**: Configures the value for permanent network errors. Default is 11000.

- **network-transient-major**: Configures the value for major transient network errors. Default is 10500.
- **network-transient-minor**: Configures the value for minor transient network errors. Default is 10000.
- **ue**: Configures the value for UE related errors. Default is 9000.

pdn-type-allowed

This command enables the IP type notification.

base *value*: Configures the base value for the chosen error category. Only private range supported 8192-16383.

value must be an integer between 8192 and 16383.

Usage Guidelines

Use this command to configure the parameters to be sent in NOTIFY payload.

Example

The following command configures the notify payload parameter **error-message-type network-transient-minor base** to value 10000.

```
notify-payload error-message-type network-transient-minor base 10000
```

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 template payload and enters the Crypto Template Payload Configuration Mode.

Product

All Security Gateway products

Privilege

Security Administrator

Syntax Description

```
[ no ] payload name match childsa [ match { any | ipv4 | ipv6 } ]
```

no

Removes a currently configured crypto template payload.

payload *name*

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

match { any | ipv4 | ipv6 }

Filters IPSec Child Security Association creation requests for subscriber calls by applying the following options:

- **any**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 and/or IPv6.

- **ipv4**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 only.
- **ipv6**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv6 only.

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. Omitting the second match parameter for either IPv4 or IPv6 will make the payload applicable to all IP address pools.

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

Example

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

```
payload payload5 match childsa
```

peer network

Configures a list of allowed peer addresses on this crypto template.

Product

All IPSec-related services

Privilege

Security Administrator

Syntax Description

```
peer network ip_address /mask [ encrypted pre-shared-key encrypt_key |
pre-shared-key key ]
no peer network ip_address/ mask
```

no

Removes the specified peer network IP address from this crypto template.

peer network *ip_address* [/*mask*]

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

Maximum of four peer networks can be configured per template.

/*mask* specifies the subnet mask bits. *mask* is an integer value from 1 to 32 for IPv4 addresses and 1 to 128 for IPv6 addresses (CIDR notation).

encrypted pre-shared-key *encrypt_key*

Specifies that an encrypted pre-shared key is to be used for IPSec authentication for the address range. *encrypt_key* must be an alphanumeric string or hexadecimal sequence from 16 to 212.

pre-shared-key *key*

Specifies that a clear text pre-shared key is to be used for IPSec authentication for the address range. *key* must be an alphanumeric string or hexadecimal sequence from 1 to 32.

Usage Guidelines

Use this command to configure a list or range of allowed peer network IP addresses for this template.

Example

The following command configures a set of IP addresses with starting address of 10.2.3.4 and a bit mask of 8:

```
peer network 10.2.3.4/8
```

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

server certificate

Configure server certificate for a given Crypto Template.

Product

ePDG

Privilege

Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(crf-crypto-tmp1-ikev2-tunnel)#

Syntax Description

server-certificate *certificate_name* **ca-certificate-list** *ca_certificate_list_name*

no server-certificate *certificate_name* [**validate**]

certificate_name

configures server certificate for a given Crypto Template, certificate name should a string of size between 1 and 128.

ca_certificate_list_name

configures server certificate list name for a given Crypto Template, certificate name should a string of size between 1 and 128.

Usage Guidelines

Use the below command to configure server certificate for a given Crypto Template:

Example

The following command configures Server Certificate 20 and CA Certificate List 10:

server-certificate *20* **ca-certificate-list** *10*

timeout

Sets the OCSP Certificate Server timeout interval in seconds. This is the interval within which the response from an external OCSP or HASH-url server should be received.

Product ePDG

Privilege Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

```
timeout cert-server timeout_value
 default timeout cert-server
```

default

Sets / Restores default value assigned for Certificate Server timeout in seconds. Default is 20 seconds.

timeout_value

Specifies the timeout value in seconds which is an integer between 1 through 60.

Usage Guidelines Use this command to configure Certificate Server timeout in seconds.

Example

The following command configures Certificate Server timeout as 50 seconds:

```
timeout cert-server 50
```

vendor-policy

Associate a vendor policy to this crypto template.

Product ePDG

HeNBGW

HNBGW

WSG

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(crf-crypto-tmp1-ikev2-tunnel)#
```

Syntax Description

vendor-policy *policy_name*

no vendor-policy

no

Removes association of the vendor policy to this crypto template.

policy_name

policy_name must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to associate a vendor policy to this crypto template.

Example

The following command associates a vendor policy named *atlpcy* to this crypto template:

vendor-policy atlpcy

permitlist

Enables the use of an existing permitlist (access permitted) file by a security gateway.

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 the use of a permitlist.

Usage Guidelines

Enable the use of a previously created permitlist to allow privileged peers access via a security gateway.

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.

Each entry in the permitlist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

Example

In releases prior to StarOS 21.26:

The following command enables the use of a whitelist:

whitelist