Crypto Template IKEv2-Vendor Configuration Mode Commands

The Crypto Template IKEv2-Vendor Configuration Mode is used to configure an IKEv2 IPSec policy for a vendor. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

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

- configuration-payload, on page 1
- do show, on page 2
- end, on page 3
- exit, on page 3
- ikev2-ikesa, on page 3
- keepalive, on page 5
- payload, on page 6

configuration-payload

This command is used to configure mapping of the configuration payload attributes for a crypto vendor template.

Product

All IPSec-related services

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description

configuration-payload private-attribute-type { imei *integer* **| p-cscf-v4** *v4_value* **| p-cscf-v6** *v6_value* **}**
remove configuration-payload private-attribute-type { imei | p-cscf-v4 | p-cscf-v6 }

remove

Removes mapping of the configuration payload attributes.

private-attribute-type

Defines the private payload attribute.

imei *integer*

Defines an International Mobile Equipemnt Identity number. Default value is 16391.

integer must be 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 for a crypto vendor template.

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*

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description `do show`

Usage Guidelines Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

Caution There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

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 vendor template.

Product All IPSec-related services

Privilege Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description

```
ikev2-ikesa { fragmentation | ignore-rekeying-requests | mobike [
cookie-challenge ] | rekey [ disallow-param-change ] | transform-set list
 name1 [ name2 [ name3 [ name4 [ name5 [ name6 ] ] ] ] ] }
remove ikev2-ikesa { fragmentation | ignore-rekeying-requests | mobike |
 rekey | transform-set list }
```

remove

Disables a previously enabled ikev2-ikesa configuration.

fragmentation

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

Default: IKESA fragmentation and re-assembly is allowed.

ignore-rekeying-requests

Ignores received IKE_SA Rekeying Requests.

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

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.

transform-set list

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set.

name1 through *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 vendor template.

Example

The following command enables IKESA fragmentation and re-assembly:

```
ikev2-ikesa fragmentation
```

The following command configures the IKEv2 IKESA list, consisting of transform sets named *ikesa43* and *ikesa326*:

```
ikev2-ikesa transform-set list ikesa43 ikesa326
```

keepalive

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

Product All products supporting IPSec

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description

keepalive [interval *seconds* **[timeout** *timeout_seconds* **[num-retry** *retry_seconds* **]]]**

{ no | remove } keepalive

no

Disables keepalive messaging.

remove

Removes previously configured keepalive messaging.

interval *sec*

Specifies the duration (in seconds) after which the next keepalive request is sent.

sec must be an integer from 10 through 3600.

Default: 3600 seconds

timeout *timeout_seconds*

Specifies the duration (in seconds) after which keepalive times out.

timeout_seconds must be an integer from 10 through 3600. Default: 10

num-retry *retry_seconds*

Specifies the total number of times to resend the keepalive request after timing out.

retry_seconds 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) with a timeout value of 1 minute (**60** seconds):

```
keepalive interval 180 timeout 60
```

payload

Creates a new, or specifies an existing, crypto template vendor payload, and enters the Crypto Template IKEv2 Vendor Payload Configuration Mode.

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template IKEv2-Vendor Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmp1-ikev2-vendor)#
```

Syntax Description **[remove] payload** *payload_name*

no

Removes a previously configured crypto template IKEv2 vendor payload.

vendor_payload

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

Usage Guidelines Use this command to create a new or enter an existing crypto template IKEv2 vendor payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated.

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

Example

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

```
payload payload5
```