Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands

The Crypto Template IKEv2-Dynamic Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for *ip-address-allocation*.

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

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

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.

ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product All Security Gateway products

Privilege Security Administrator

Command Modes Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description **`ignore-rekeying-requests`**

Usage Guidelines Prevents creation of a CHILD SA based on this crypto template.

Example

The following command prevents creation of a CHILD SA based on this crypto template:

`ignore-rekeying-requests`

ip-address-allocation

Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a tunnel inner address (TIA) to the ChildSA. The second payload is configured after a successful MAnaged IP (MIP) initiation and can use the default Home Address (HoA) option.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#`

Syntax Description

`ip-address-allocation { dynamic | home-address }`
`default ip-address-allocation`

default

Sets IP address allocation to the home-address.

ip-address-allocation dynamic

Specifies that the IP address for the subscriber is allocated from a dynamic IP pool.

ip-address-allocation home-address

The IP address for the subscriber is allocated by the Home Agent. This is the default setting for this command.

Usage Guidelines

Use this command to configure how ChildSA payloads are allocated IP addresses for this crypto template.

Example

The following command is for the first ChildSA and will ensure that it gets a TIA address from an IP address pool:

`ip-address-allocation dynamic`

The following command is for the second ChildSA and will ensure that it gets a HoA address from the HA:

`default ip-address-allocation`

ipsec transform-set

Configures the IPSec transform set to be used for this crypto template payload.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

[no] ipsec transform-set list *name* **[***name2* **] [***name3* **] [***name4* **]**

no

Specifies the IPSec transform set to be deleted. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

name

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. *name* must be an alphanumeric string of 1 through 127 characters.

Usage Guidelines

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example

The following command configures IPSec transform sets named *ipset1* and *ipset2* to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2
```

lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

```
lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes }
default lifetime
```

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. *sec* must be an integer from 60 through 604800. Default: 86400

kilo-bytes *kbytes*

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this crypto template payload. *kbytes* must be an integer from 1 through 2147483647.

default lifetime

Sets the lifetime to its default value of 86400 seconds.

Usage Guidelines

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be *120* seconds:

```
lifetime 120
```

maximum-child-sa

Configures the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

maximum-child-sa *num*
default maximum-child-sa

maximum-child-sa *num*

Specifies the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association. *num* must be 1. Default: 1

default maximum-child-sa

Sets the maximum number of Child SAs to its default value of 1.

Usage Guidelines

Use this command to configure the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

Example

The following command configures the maximum number of child SAs to 1:

```
maximum-child-sa 1
```

rekey

Configures IPSec Child Security Association rekeying.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

[no] rekey [keepalive]

no

Disables this feature.

keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage Guidelines

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying

means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

```
no rekey
```

tsi

Configures the IKEv2 Traffic Selector-Initiator (TSi) payload address options.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

tsi start-address { any end-address any | endpoint end-address endpoint }

any end-address any

Configures the TSi payload to allow all IP addresses.

endpoint end-address endpoint

Configures the TSi payload to allow only the Mobile endpoint address. (Default)

Usage Guidelines

On receiving a successful IKE_SA_INIT Response from PDIF, the MS sends an IKE_ AUTH Request for the first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it includes the MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes an IDi payload containing the NAI, SA, TSi, TSr, and CP (requesting IP address and DNS address) payloads.

Example

Use the following example to configure a TSi payload that allows all addresses:

```
tsi start-address any end-address any
```

tsr

Configures the IKEv2 Traffic Selector-Responder (TSr) payload address options.

Product

All Security Gateway products

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context *context_name* **> crypto template** *template_name* **ikev2-dynamic > payload** *payload_name* **match childsa match { any | ipv4 | ipv6 }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax Description

[no] tsr start-address *ip address* **end-address** *ip address*

no

Disables the specified tsr address range.

start-address *ip address*

Specifies the starting IP address of the TSr payload in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

See the limitations listed in the *Usage* section.

end-address *ipv4 address*

Specifies the ending IP address of the TSr payload in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

See the limitations listed in the *Usage* section.

Usage Guidelines

This command is used to specify an IP address range in the single TSr payload that the PDG/TTG returns in the last IKE_AUTH message. This TSr is Child SA-specific.

This command is subject to the following limitations:

- The configuration is restricted to a maximum of four TSrs per payload and per childsa.
- Overlapping TSrs are not allowed either inside the same payload or across different payloads.
- When a TSr is configured via this command, only the configured TSr will be considered for narrowing-down. For example, if one IPv4 TSr is configured, and the gateway receives an IPv6 TSr, the gateway will reject the call with a TS_UNACCEPTABLE notification.
- The UE/PEER must send both INTERNAL_IP4_ADDRESS and INTERNAL_IP6_ADDRESS in the Configuration Payload, whenever it needs both IPv4 and IPv6 addresses in TSrs. Otherwise, the gateway will respond back with only one type depending upon the type of address received in the Configuration Payload. For example,.if the gateway receives only INTERNAL_IP4_ADDRESS in the Configuration Payload but both IPv4 and IPv6 addresses are in the TSrs, the GW will narrow down only the IPv4 address, and ignore the IPv6 TSrs.

- IPv4 TSrs are not allowed inside IPv6 payloads.
- IPv6 TSrs are not allowed inside IPv4 payloads.

Example

Use the following example to configure a TSr payload that specifies an IPv4 address range for the payload:

```
tsr start-address 10.2.3.4 end-address 10.2.3.155
```

tsr