IKEv2 and IPSec Parameter Setting Per Device Type

- Feature Information, on page 1
- Feature Description, on page 2
- How IKEv2/IPSec Parameter Setting Per Device Type Works, on page 2
- Configuring IKEv2 and IPSec Parameter Per Device Type, on page 4
- Monitoring and Troubleshooting IKEv2 and IPSec Parameter Setting Per Device Type, on page 5

Feature Information

Summary Data

Status	New Feature
Introduced-In Release	21.2
Modified-In Release(s)	Not Applicable
Applicable Product(s)	ePDG
Applicable Platform(s)	ASR 5500 VPC-SI VPC-DI
Default Setting	Disabled
Related CDETS ID(s)	CSCvc38683
Related Changes in This Release	Not Applicable
Related Documentation	IPSec Reference Guide Command Line Interface Reference Guide

Revision History

Revision Details	Release	Release Date
New in this release.	21.2	April 27, 2017

Feature Description

Overview

This feature provides an IKEv2 and IPSec framework for operators to configure the system where different peer devices can establish an IKEv2/IPSec tunnel with different set of capabilities and features. Vendor-specific crypto templates which are a subset of the IKEv2 dynamic template can be configured for each device separately. Multiple vendor templates can be grouped under a vendor policy and associated to the parent IKEv2 dynamic template. A single Gateway service (supporting IPSec) can serve different peers with different IKEv2/IPSec (pre-defined) requirements.

How IKEv2/IPSec Parameter Setting Per Device Type Works

Feature Components

Vendor Template

A vendor template is a subset of the IKEv2 dynamic crypto template. The available subset of features and configurations for vendor template remain the same as that of the IKEv2 dynamic crypto template.

The following functions/configurations are currently available for the vendor template:

- DPD timer
- IKESA transform-set list
- IPSec transform-set list
- IKE features like Mobike and Fragmentation
- Private numbers for PCSCF/IMEI payloads
- IPSec rekey related configurations
- IKE rekey related configurations

Important It is recommended to use one vendor template to configure each IKEv2 or IPSec functionality as required for the device.

For configuration information, refer the configuration section of this chapter.

Vendor Policy

A vendor policy is used to group multiple vendor templates to a single policy using a vendor ID and the vendor template name. This vendor ID will be used to make updated configuration while comparing vendor ID value received in the IKE SA packet. The vendor policy is associated to the main crypto (service) template. When similar configurations exist under the vendor template and the main crypto (service) template, the configuration under the vendor template takes priority if the vendor ID matches the vendor ID payload from IKE_SA_INIT during tunnel exchange (based on precedence).

A maximum of 32 vendor policies can be configured. Each vendor policy can be associated with a maximum of 64 vendor templates.

For configuration information, refer the configuration section of this chapter.

Associating Vendor Policy to a Crypto (Service) Template

Only one vendor policy can be attached to a crypto (service) template.

Architecture

During IKE_SA_INIT exchange, on receiving the vendor ID payload, allocated IKE SA is updated with the configuration from both the main crypto (service) template and the vendor templates. Configuration values are then taken from IKE SA during tunnel negotiation. The priority of the configuration in the vendor template over the main crypto (service) template is decided by matching the vendor ID string associated to the vendor template (in the vendor policy) with the received vendor ID in the IKE_SA_INIT message.

If the IKE_SA_INIT message contains more than one vendor ID, all the vendor IDs will be matched with the configuration under the vendor policy. For all successful matches, the configuration parameters are taken from the vendor template and the rest of the configuration is taken from the main crypto (service) template. Matching is performed based on the precedence associated with the vendor template. When a configuration is available in more than one vendor template, the configuration is chosen based on the highest precedence in the vendor policy. A precedence value of 1 indicates the highest priority with the vendor policy for a set of associated vendor templates.

Limitations

Architectural Limitations

- In a downgrade scenario for Inter-chassis session recovery, as this feature will not be available in the stand-by chassis, the IKE SA updated with the vendor template configuration will not be synced to the stand-by chassis.

Configuration Limitations

- **IKE SA rekey configuration** – If some of the **ikev2-ikesa rekey**, **ikev2-ikesa rekey disallow-param-change**, or **ikev2-ikesa ignore rekeying requests** commands exist in the main crypto (service) template configuration, and if any of these commands also exist in the vendor template, all configuration will be taken from the vendor template if the vendor ID matches.
- **IPSec rekey and lifetime configuration** – If any of the **rekey keepalive**, **ignore rekeying requests**, or **lifetime** command exists in the vendor template, all IPSec rekey configurations will be taken from the vendor template.

- Currently, only one payload configuration is effective.

Configuring IKEv2 and IPSec Parameter Per Device Type

Configuring Vendor Template for Vendor-specific Information

Use the following configuration to create a vendor template, and get into the Crypto Template IKEv2 Vendor Configuration Mode:

```
config
   context context_name
      crypto template template_name ikev2-vendor
```

Notes:

- The following commands are available under the Crypto Template IKEv2 Vendor configuration mode to configure IPSec-related parameters. Their functionalities are similar to the commands under the Crypto Template Configuration Mode.
  - configuration-payload
  - ikev2-ikesa
  - keepalive
  - payload

Configuring Vendor Policy and Associating With Vendor Template

Use the following configuration to create a vendor policy, and associate it with the vendor template:

```
config
   context context_name
      crypto vendor-policy vendor_policy_name
         precedence value vendor-id vendor_id vendor-template template_name
         end
```

Notes:

- A maximum of 32 vendor policies can be configured.
- A maximum of 64 vendor templates can be associated with a vendor policy.
- *vendor_id* must be an integer from 1 through 64.
- **template_name** must be an alphanumeric string from 1 to 127 characters.

Associating Vendor Policy to Crypto Template

Use the following configuration to associate the vendor policy to the crypto (services) template:

```
config
   context context_name
      crypto template template_name ikev2-dynamic
         vendor-policy policy_name
         end
```

Notes:

- *policy_name* must be an alphanumeric string from 1 to 127 characters.

Monitoring and Troubleshooting IKEv2 and IPSec Parameter Setting Per Device Type

Show Command(s) and/or Outputs

show crypto statistics ikev2

The following fields are available in the output of the **show crypto statistics ikev2** command in support of this feature:

```
IKEv2 SA_INIT Vendor-ID Matching Statistics:
Total packet rcvd with Vendor ID:  1  Total Vendor-ID's rcvd in IKE_SA_INIT:   4
Rcvd Vendor-ID successful Match:   3  Rcvd Vendor-ID no Match              :   1
```

Table 1: show crypto statistics ikev2 Command Output Descriptions

Field	Description
IKEv2 SA_INIT Vendor-ID Matching Statistics:	
Total packet rcvd with Vendor ID	Total number of packets received with vendor ID.
Total Vendor-ID's rcvd in IKE_SA_INIT	Total number of vendor IDs received in the IKE_SA_INIT message.
Rcvd Vendor-ID successful Match	Total number of matches for the vendor IDs received in the IKE_SA_INIT message.
Rcvd Vendor-ID no Match	Total number of vendor IDs that did not match.

show crypto template

The following fields are available in the output of the **show crypto template** command in support of this feature:

Main (services) template values

```
Attached vendor policy: vp1
```

*Table 2: **show crypto template** Command Output Descriptions*

Field	Description
Attached vendor policy	Specifies the vendor policy associated with the crypto template.

Vendor template configured values

```
Crypto Map Type: IPSEC IKEv2 Vendor Template
```

*Table 3: **show crypto template** Command Output Descriptions*

Field	Description
Crypto Map Type	Specifies that the crypto map type used is from the vendor template.

Important The output also displays those configured parameters applicable to the vendor template. The fields are similar to the configuration available for the IKEv2 dynamic crypto template.

show crypto vendor-policy

The following fields are available in the output of the **show crypto vendor-policy** command in support of this feature:

```
Crypto Vendor Policy Name vp1
  VID IKESA1 vendor template v1 precedence 1
  VID IKESA2 vendor template v2 precedence 2
1 Crypto vendor policy are configured
```

*Table 4: **show crypto vendor-policy** Command Output Descriptions*

Field	Description
Crypto Vendor Policy Name	Specifies the name of the vendor policy.
Example: VID IKESA2 vendor template v2 precedence 2	Specifies the vendor policy, associated vendor template, vendor ID, and Precedence.