IPSec Pairwise Keys Overview

Table 1: Feature History

Feature Name	Release Number	Feature Description
Secure Communication Using Pairwise IPsec Keys	Cisco SD-WAN Release 19.2.1	This feature allows private pairwise IPSec session keys to be created and installed for secure communication between IPSec devices and its peers.

IPSec Pairwise Keys feature implements controller-based key exchange protocol between device and controller.

Controller-based key exchange protocol is used to create a Gateway-to-Gateway VPN (RFC7018) in either a Full-Mesh Topology or Dynamic Full-Mesh Topology.

The network devices set up a protected control-plane connection to the controller. The controller distributes policies to network devices, which enables the network devices to communicate with each other through a secure data plane.

A pair of IPSec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

Supported Platforms

The following platforms are supported for IPSec Pairwise Keys feature:

- Cisco IOS XE SD-WAN devices
- Cisco vEdge devices

Pairwise Keys

Key exchange method combined with authentication policies facilitate pairwise key creation between two network devices. A controller is used to distribute keying material and policies between network devices, resulting in the devices generating private pairwise keys with each other.

IPSec devices share public values from Diffie-Hellman (DH) algorithm with the controllers. The controllers relay the DH public values to authorized peers of the IPsec, device as defined by a centralized policy.

Network devices n create and install private pairwise IPsec session keys to be used to secure communications with their peers.

IPsec Security Association Rekey

Every rekeying IPsec device generates a new DH pair and generates new IPsec security association pairs for each peer with which it is communicating. The new security association pairs are generated as a combination of the new DH private value and the DH public value of each each peer. The IPsec device distributes the new DH public value to the Controller, which forwards it to its authorized peers. Each peer continues to transmit on the existing security association until that peer starts transmitting on the new security associations.

During a simultaneous rekey up to four pairs of IPsec SAs may be temporarily created, and they converge on a single new set of IPsec SAs.

Any IPsec device may initiate a rekey due to reasons such as a local time or volume-based policy, or the counter result of a cipher counter mode Initialization Vector (IV) nearing completion.

When you configure a rekey on a local inbound security association, it triggers peer outbound and inbound security association rekey. The local outbound security association rekey is initiated after the IPSec device recieves the first packet with new Security Parameter Index (SPI) from peer.

Note A pairwise key edge device can form IPSec sessions with both pairwise and non-pairwise edge devices

Note The rekeying process requires higher control plane CPU usage, resulting in lower session scaling

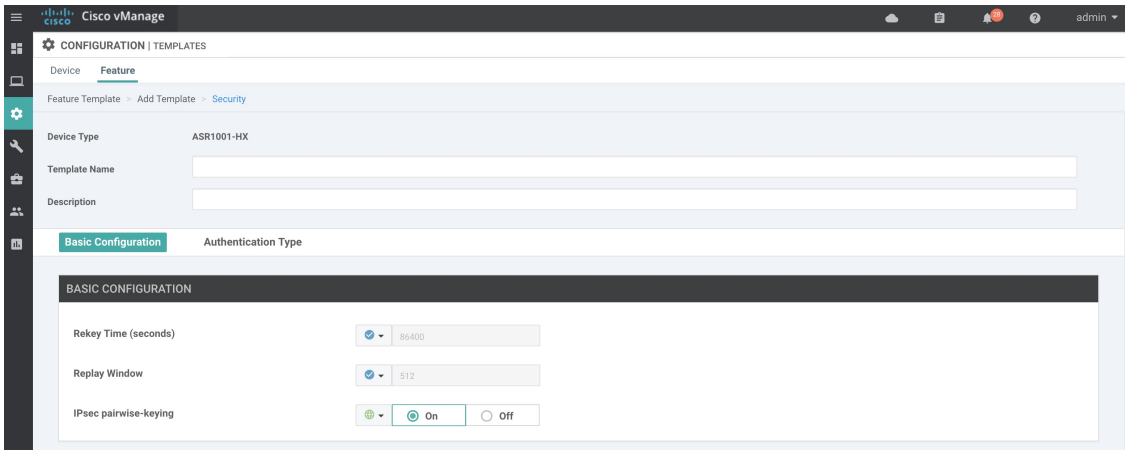
Configure IPSec Pairwise Keys

Configure IPSec Pairwise Keys Using vManage

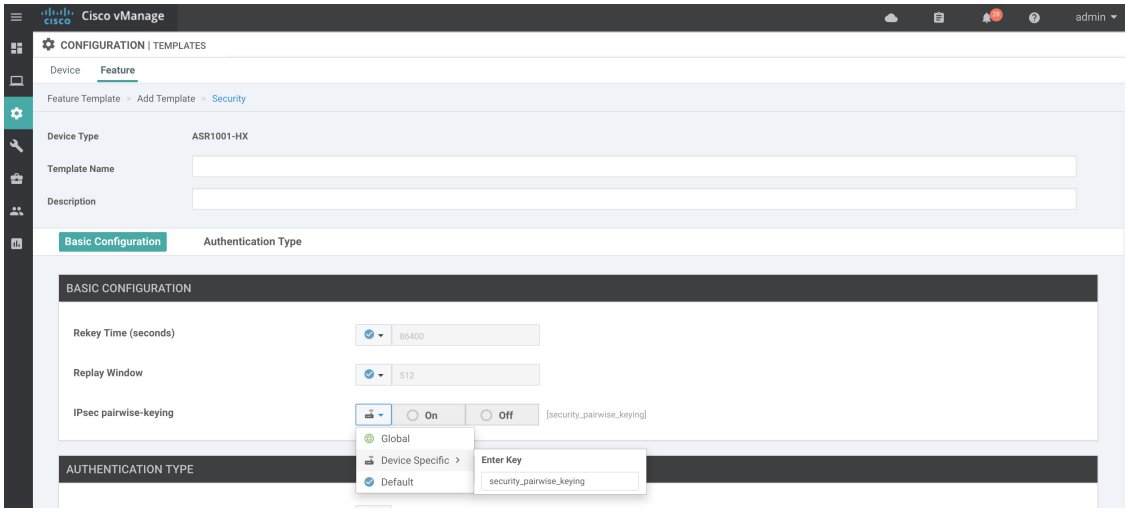
1. In vManage NMS, select the **Configuration ► Templates** screen.
2. In the **Feature** tab, click **Create Template**.
3. From the **Device Model** check box, select the type of device for which you are creating the template.
4. From the **Basic Information** tab, choose **Security** template.

5. From theBasic Configuration tab, select On or Off from the IPsec Pairwise-Keying field..

Figure 1: IPSec Pairwise Keying



6. Alternatively, enter the pairwise key specific to the device in the **EnterKey** field.



7. Click **Save**.

Configure Pairwise Keys and Enable Rekeying on the CLI

A pair of IPsec session keys is configured for each pair of local and remote transport locations.

The keys use AES-GCM-256 (AES_256_CBC for multicast) cipher to perform encryption. By default, a key is valid for 3600 seconds.

Configure Pairwise Keys

Use the following command to configure pairwise keys:

```
Device(config)# security ipsec pairwise-keying
```

Note You must reboot the Cisco IOS XE SD-WAN device for the private-key configuration to take effect.

Configure Rekeying for IPsec Pairwise Keys

Use the following command to configure rekeying for pairwise keys:

```
Device(config)# security ipsec pwk-sym-rekey
```

Verify IPSec Pairwise Keys on Cisco vEdge Routers

Use the following command to display IPSec pairwise keys information on Cisco vEdge Routers:

```
Device# show security-info

security-info authentication-type "AH_SHA1_HMAC SHA1_HMAC"
security-info rekey 86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Enabled
security-info pairwise-keying Enabled
```

Use the following command to verify outbound connection for IPSec pairwise keys:

```
SOURCE SOURCE DEST DEST                                                 REMOTE
REMOTE         AUTHENTICATION                   NEGOTIATED
       PEER          PEER
IP             PORT       IP       PORT      SPI          TUNNEL MTU TLOC ADDRESS TLOC COLOR
 USED                       KEY-HASH ENCRYPTION ALGORITHM TC SPIs KEY-HASH SPI
-------------------------------------------------------------------------------------------------
10.1.16.16 12366 10.1.15.15 12426 260            1441               172.16.255.15      lte
                     AH_SHA1_HMAC *****4aec      AES-GCM-256                       8
       *****d01e 1538
```

Use the following command to verify inboud connection for IPSec pairways keys:

```
Device# show ipsec inbound-connections

SOURCE  SOURCE       DEST    DEST     REMOTE            REMOTE LOCAL LOCAL  NEGOTIATED PEER
  PEER
IP      PORT          IP  PORT       TLOC ADDRESS TLOC   COLOR TLOC  ADDRESS  TLOC
COLOR ENCRYPTION  ALGORITHM  TC SPIs KEY-HASH SPI
-------------------------------------------------------------------------------------------------
10.1.15.15 12426 10.1.16.16 12366     172.16.255.15      lte 172.16.255.16 lte AES-GCM-256
 8 *****d01e 518
```