IPsec Pairwise Keys

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, and **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco Catalyst SD-WAN Release 19.2.1	This feature allows you to create and install private pairwise IPsec session keys for secure communication between an IPsec device and its peers.

The IPsec pairwise keys feature implements controller-based key exchange protocol between a 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. The network devices, in turn, communicate with each other through a secure data plane.

A pair of IPsec session keys (one encryption key and one decryption key) are configured for each pair of local and remote transport locations (TLOC).

Supported Platforms

The following platforms are supported for IPSec Pairwise Keys feature:

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

Pairwise Keys

Key exchange method combined with authentication policies facilitate pairwise key creation between two network devices. You use a controller to distribute keying material and policies between network devices. The devices generate private pairwise keys with each other.

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

Network devices create and install private pairwise IPsec session keys to secure communication with their peers.

IPsec Security Association Rekey

Every rekeying IPsec device generates a new Diffie-Hellman (DH) pair and 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 key and the DH public key of 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 to the existing security association, and subsequently, to new security associations.

During a simultaneous rekey, up to four pairs of IPsec Security Associations (SAs) can be temporarily created. These four pairs converge on a single rekey of a device.

An IPsec device can initiate a rekey due to reasons such as the local time or a volume-based policy, or the counter result of a cipher counter mode initialization vector nearing completion.

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

Note

- A pairwise-key device can form IPsec sessions with both pairwise and nonpairwise devices.
- The rekeying process requires higher control plane CPU usage, resulting in lower session scaling.

Configure IPSec Pairwise Keys

Configure IPsec Pairwise Keys Using Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates** and then click **Add Template**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. From the **Device Model** drop-down menu, choose the type of device for which you are creating the template.
4. From **Basic Information**, click **Cisco Security** feature template.
5. From **Basic Configuration**, click **On** or **Off** from the **IPsec pairwise-keying** field.
6. Alternatively, enter the pairwise key specific to the device in the **Enter Key** 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 Catalyst 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
```