



Security Features



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, Cisco vSmart to Cisco Catalyst 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.

- [Encrypt Communications, on page 1](#)
- [IPsec Pairwise Keys, on page 2](#)

Encrypt Communications

The U.S. federal government requires that all data at rest and in transit be encrypted.

To satisfy this requirement, Cisco uses the following forms of encryption:

- Transport Layer Security (TLS) 1.2 encryption.
- FIPS Object Module - meets the FIPS 140-2 requirements, performs the FIPS-approved cryptographic functions, and is designed for use in conjunction with Cisco SSL distributions. FIPS mode is enabled by default in Cisco Catalyst SD-WAN for government.

For more information, see [Cisco FIPS Object Module](#).

- Cisco SSL is a Cisco-enhanced version of OpenSSL, which enables products to achieve FIPS compliance.

For more information, see [Cryptographic Module Validation Program CMVP](#).



Note All the virtual machines within the Cisco Catalyst SD-WAN for government boundary use the 7.x version of the Cisco SSL library, which runs in FIPS mode, thereby ensuring that all the data at rest and in transit are encrypted.

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**, **Cisco vSmart** to **Cisco Catalyst 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 IOS XE Catalyst SD-WAN Release 16.12.1b	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).

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 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 a Cisco IOS XE Catalyst SD-WAN Device

Use the following command to verify the outbound connections for pairwise keys:

```
Device# show sdwan ipsec pwk outbound-connections
```

SS	E-KEY	AH	REMOTE	SA	PKEY	NONCE	PKEY	REMOTE TLOC COLOR	TLOC	INDEX	ADDRESS	REMOTE TLOC COLOR	HASH	HASH	HASH	
SOURCE IP	Source	Port	SOURCE IP	DEST	Port	LOCAL	TLOC	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR
REMOTE TLOC ADDRESS	REMOTE	TLOC	COLOR	PWK-SPI	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS
HASH	AUTH	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX
10.168.11.3	12346	192.168.90.3	12346	10.1.0.2				lte								
10.1.0.1	privatel		000000	202	0	6668		17B0	F5A5							
true																
10.168.11.3	12346	192.168.92.6	12346	10.1.0.2				lte								
10.1.0.6	default		00A001	52	10	0ED6	AF12	0A09	8030							
true																
10.168.12.3	12346	192.168.90.3	12346	10.1.0.2				blue								
10.1.0.1	privatel		000000	205	0	6668		17B0	F5A5							
true																
10.168.12.3	12346	192.168.92.6	12346	10.1.0.2				blue								
10.1.0.6	default		00A001	55	10	0ED6	AF12	B9B7	BE29							
true																

Use the following command to verify the inbound connections on IPsec pairwise keys:

```
Device# show sdwan ipsec pwk inbound-connections
```

DEST	LOCAL	LOCAL	SOURCE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE	REMOTE
SA	PKEY	NONCE	PKEY	SS	D-KEY	AH	PORT	TLOC	ADDRESS	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	PWK-SPI
INDEX	ID	TLOC	ADDRESS	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS	REMOTE	TLOC	COLOR	INDEX	ADDRESS
192.168.90.3							12346	10.168.11.3									
12346	10.1.0.2			lte			10.1.0.1	privatel									000000
2	1	5605	70C7	17B0	F5A5	true											
192.168.92.6							12346	10.168.11.3									
12346	10.1.0.2			lte			10.1.0.6	default									00100B
52	1	5605	70C7	CCC2	C9E1	true											
192.168.90.3							12346	10.168.12.3									
12346	10.1.0.2			blue			10.1.0.1	privatel									000000
5	1	B9F9	5C75	17B0	F5A5	true											
192.168.92.6							12346	10.168.12.3									
12346	10.1.0.2			blue			10.1.0.6	default									00100B

```
55      1      B9F9  5C75  A0F8  7B6B  true
```

```
Device# show sdwan ipsec pwk local-sa
```

```

                                     SA
PKEY  NONCE  PKEY
TLOC-ADDRESS  TLOC-COLOR  SOURCE-IP  SOURCE PORT  SPI  INDEX  ID
-----+-----+-----+-----+-----+-----+-----
10.1.0.2      lte          10.168.11.3  12346        257  6      1  5605
70C7
10.1.0.2      blue        10.168.12.3  12346        257  3      1  B9F9
5C75
```

```
Device# show platform hardware qfp active feature ipsec da spi
```

```

g_hash_idx  Flow id  QFP SA hdl  source IP  spi/old  sport  dest IP
-----+-----+-----+-----+-----+-----+-----+-----
1541        3        11        192.168.90.3  12346 0x312b84f0 0x00000115/0x00000114
0x0000000031fbfa80/0x0000000031fbd520
6661        131       36        10.168.12.3  12346 0x312b9990 0x0000b001/0x0000a001
0x0000000031fbc380/0x0000000031fbc9a0
7429        117       6         10.168.11.3  12346 0x312b9300 0x0000b001/0x0000a001
0x0000000031fbd970/0x0000000031fbb580
```

```

System id  Wan int  Wan ip
Yubei-ledge  5102   Gi2.xxx  Sub 10.168.xxx
Yubei-tsn    5108   Gi0/0/1  192.168.92.8
Yubei-ovld   5106   Gi0/0/0  192.168.92.6
Yubei-lng    5107   Gi0/0/0  192.168.92.7
Yubei-utah   5104   Gi0/0/0  192.168.92.4
Yubei-vedge  5101   ge0/0    192.168.90.3
```

Use the following command to display IPsec pairwise keys information on a Cisco IOS XE Catalyst SD-WAN device:

```
Device# show sdwan 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
```

Debug Commands on Cisco IOS XE Catalyst SD-WAN Devices

Use the following **debug** commands for debugging issues related to IPsec pairwise keys:

```

debug plat soft sdwan ftm pwk [dump | log]
debug plat soft sdwan ttm pwk [dump | log]
debug plat soft sdwan vdaemon pwk [dump | log]
```

