IPSec Pairwise Keys Overview

Table 1: Feature History

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco IOS XE SD-WAN Release 16.12.1b	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

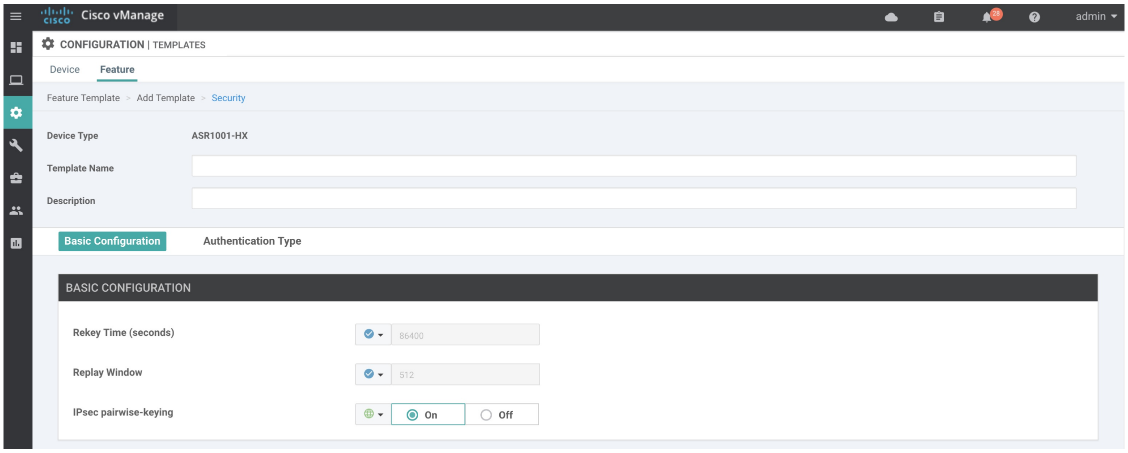
Configure IPSec Pairwise Keys

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.

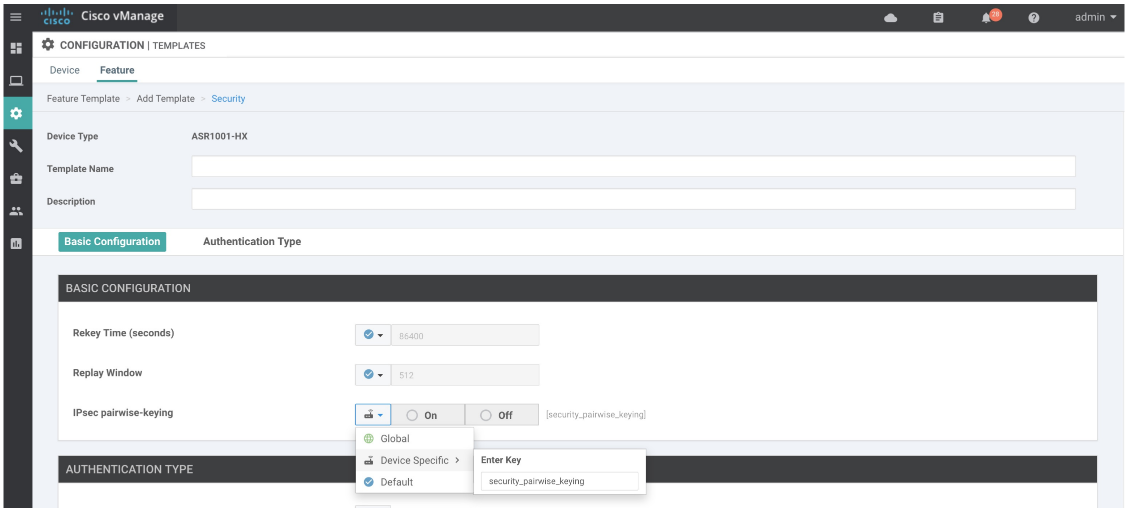
5. From theBasic Configuration tab, select On or Off from the IPsec Pairwise-Keying field..

Figure 1: IPSec Pairwise Keying



Device Type ASR1001-HX
Template Name
Description
Rekey Time (seconds) 86400
Replay Window 512
IPsec pairwise-keying ● On ○ Off

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



Device Type ASR1001-HX
Template Name
Description
Rekey Time (seconds) 86400
Replay Window 512
IPsec pairwise-keying ○ On ○ Off [security_pairwise_keying]
Enter Key security_pairwise_keying

7. Click **Save**.

Configure Pairways Keys and Rekeying

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

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 Pairwse Keys

Use the following command to configure pairways keys:

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

Note On Cisco IOS XE SD-WAN Devices, You must reboot the device for the pairwise keys 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 XE SD-WAN Routers

Use the following command to verify outboutnd connections for Pairwise Keys:

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

                                     REMOTE                  SA    PKEY  NONCE   PKEY
SS   E-KEY   AH
 SOURCE IP    Source Port  SOURCE IP   DEST Port LOCAL TLOC ADDRESS  REMOTE TLOC COLOR
REMOTE TLOC ADDRESS   REMOTE TLOC COLOR     PWK-SPI  INDEX      ID      HASH   HASH   HASH
   HASH  AUTH
─────────────────┼──┼────────────────┼──┼──────┼──────┼──────┼──────┼──┼──┼──┼──┼──┼──┼──┼─
10.168.11.3   12346    192.168.90.3      12346    10.1.0.2                 lte
  10.1.0.1          private1          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          private1          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 inbound connection on IPSec Pairways Keys

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

                                          SOURCE
   DEST        LOCAL            LOCAL            REMOTE           REMOTE
SA    PKEY  NONCE   PKEY    SS   D-KEY   AH
               SOURCE IP                   PORT                   DEST IP
   PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS      TLOC COLOR     PWK-SPI
INDEX    ID    HASH   HASH   HASH   HASH  AUTH
─────────────────┼──┼────────────────┼──┼──────┼──────┼──────┼──────┼──┼──┼──┼──┼──┼──┼──┼─
192.168.90.3                             12346    10.168.11.3
 12346    5.1.0.2          lte              5.1.0.1          private1          000000   2
     1       5605   70C7   17B0   F5A5  true
192.168.92.6                             12346    10.168.11.3
 12346    5.1.0.2          lte              5.1.0.6          default           00100B   52
     1       5605   70C7   CCC2   C9E1  true
192.168.90.3                             12346    10.168.12.3
 12346    5.1.0.2          blue             5.1.0.1          private1          000000   5
     1       B9F9   5C75   17B0   F5A5  true
192.168.92.6                             12346    10.168.12.3
 12346    5.1.0.2          blue             5.1.0.6          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
------------+------------+--------------------------------+------+-----+----+----+---+----
5.1.0.2         lte             10.168.11.3    12346           257     6     1     5605
70C7
5.1.0.2         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                                sport  dest IP
                                dport  SA ptr      spi/old                crypto_hdl/old
-----+---+-----+-----------------+--+------------------+---+---+---------+----------------
1541        3       11          192.168.90.3                          12346  192.168.92.6
                             12346  0x312b84f0  0x00000115/0x00000114
0x0000000031fbfa80/0x0000000031fbd520
6661        131     36          10.168.12.3                           12346  192.168.92.6
                             12346  0x312b9990  0x0000b001/0x0000a001
0x0000000031fbe380/0x0000000031fbc9a0
7429        117     6           10.168.11.3                           12346  192.168.92.6
                             12346  0x312b9300  0x0000b001/0x0000a001
0x0000000031fbd970/0x0000000031fbb580


           System id    Wan int Wan ip
Yubei-cedge     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-1ng       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 Cisco IOS XE SD-WAN devices:

```
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 XE SD-WAN Devices

Use the following debug commands for debugging issues related to IPSec Pairwise Keys feature:

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