セキュリティ機能

通信の暗号化

米国連邦政府は、保管中および転送中のすべてのデータを暗号化することを要求しています。

この要件を満たすために、シスコは次の形式の暗号化を使用します。

- Transport Layer Security（TLS）1.2 による暗号化。
- FIPS オブジェクトモジュール：FIPS 140-2 の要件を満たし、FIPS 承認の暗号化機能を実行し、Cisco SSL ディストリビューションと組み合わせて使用するように設計されています。官公庁向け Cisco SD-WAN では、FIPS モードはデフォルトで有効になっています。

  詳細については、「Cisco FIPS オブジェクトモジュール」を参照してください。
- Cisco SSL は、シスコが拡張したバージョンの OpenSSL であり、製品の FIPS 準拠を可能にします。

  詳細については、「暗号モジュール認定制度（CMVP）」を参照してください。

（注） 官公庁向け Cisco SD-WAN の境界内にあるすべての仮想マシンは、7.x バージョンの Cisco SSL ライブラリを使用します。これは FIPS モードで動作するため、保管中および転送中のすべてのデータが暗号化されます。

IPsec ペアワイズキー

表 *1:* 機能の履歴

機能名	リリース情報	説明
IPsec ペアワイズキーを使用したセキュアな通信	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能を使用すると、IPsecデバイスとそのピアの間でのセキュアな通信のために、IPsec秘密ペアワイズセッションキーを作成してインストールすることができます。

IPsec ペアワイズキー機能により、デバイスとコントローラの間にコントローラベースのキー交換プロトコルが実装されます。

コントローラベースのキー交換プロトコルは、フルメッシュトポロジまたはダイナミック フルメッシュ トポロジのいずれかでゲートウェイ間 VPN（RFC7018）を作成するために使用されます。

ネットワークデバイスは、コントローラへの保護されたコントロールプレーン接続をセットアップします。コントローラは、ネットワークデバイスにポリシーを配信します。その後、ネットワークデバイスは、セキュアなデータプレーンを介して相互に通信します。

ローカルおよびリモートのトランスポートロケーション（TLOC）のペアごとに、IPsec セッションキーのペア（1 つの暗号キーと 1 つの復号キー）が設定されます。

ペアワイズキー

キー交換方式と認証ポリシーの組み合わせにより、2 つのネットワークデバイス間でのペアワイズキー作成が容易になります。ネットワークデバイス間でのキー関連情報とポリシーの配信には、コントローラを使用します。デバイスは、相互に秘密ペアワイズキーを生成します。

IPsecデバイスは、Diffie-Hellman（DH）アルゴリズムからの公開キーをコントローラと共有します。コントローラは、一元化されたポリシーの定義に従って、DH 公開キーを IPsec デバイスの許可されたピアにリレーします。

ネットワークデバイスは、ピアとのセキュアな通信のために IPsec 秘密ペアワイズセッションキーを作成してインストールします。

IPSec セキュリティ アソシエーション キーの再生成

キーを再生成するすべての IPsec デバイスは、通信している各ピアに対して、新しい Diffie-Hellman（DH）ペアと新しい IPsec セキュリティア ソシエーション ペアを生成します。新しいセキュリティ アソシエーション ペアは、各ピアの新しい DH 秘密キーと DH 公開キーを組み合わせて生成されます。IPsec デバイスは新しい DH 公開値をコントローラに配信し、コントローラはその値を許可されたピアに転送します。各ピアは、引き続き既存のセキュリ

ティ アソシエーションに送信し、その後に新しいセキュリティ アソシエーションにも送信します。

同時キー再生成時に、最大 4 ペアの IPsec セキュリティ アソシエーション（SA）を一時的に作成できます。これらの 4 つのペアは、デバイスの 1 つのキー再生成に収束します。

IPsec デバイスは、現地時間またはボリュームベースのポリシーや、完了に近づいた暗号カウンタモード初期化ベクトルのカウンタ結果といった理由により、キー再生成を開始できます。

ローカル インバウンド セキュリティ アソシエーションでキー再生成を設定する場合、それによってピアのアウトバウンドおよびインバウンド セキュリティ アソシエーションのキー再生成がトリガーされます。ローカル アウトバウンド セキュリティ アソシエーションのキー再生成は、IPsec デバイスがピアから新しいセキュリティ パラメータ インデックス（SPI）が指定された最初のパケットを受信した後に開始されます。

（注）
- ペアワイズキーデバイスは、ペアワイズデバイスと非ペアワイズデバイスの両方と IPsec セッションを形成できます。
- キー再生成プロセスでは、コントロールプレーンの CPU 使用率が高くなるため、セッションのスケーリングが低くなります。

Cisco vManage を使用した IPsec ペアワイズキーの設定

1. Cisco vManage のホームページで、**[Configuration]** > **[Templates]** を選択します。
2. [Feature] タブで、[Add Template] をクリックします。
3. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
4. [Basic Information] タブで、[Cisco Security] 機能テンプレートをクリックします。
5. [Basic Configuration] タブで、[IPsec pairwise-keying] フィールドの [On] または [Off] オプションボタンを選択します。
6. または、[Enter Key] フィールドにデバイス固有のペアワイズキーを入力します。
7. [保存（Save）] をクリックします。

CLI でのペアワイズキーの設定とキー再生成の有効化

ローカルおよびリモートのトランスポートロケーションのペアごとに、IPsec セッションキーのペアが設定されます。

これらのキーでは、AES-GCM-256（マルチキャストの場合は AES_256_CBC）暗号を使用して暗号化が実行されます。デフォルトでは、キーは 3600 秒間有効です。

ペアワイズキーの設定

ペアワイズキーを設定するには、次のコマンドを使用します。

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

（注） 秘密キーの設定を有効にするには、Cisco IOS XE SD-WAN デバイスを再起動する必要があります。

IPsec ペアワイズキーのキー再生成の設定

ペアワイズキーのキー再生成を設定するには、次のコマンドを使用します。

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

Cisco IOS XE SD-WAN デバイス での IPsec ペアワイズキーの確認

ペアワイズキーのアウトバウンド接続を確認するには、次のコマンドを使用します。

```
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
```

IPsec ペアワイズキーのインバウンド接続を確認するには、次のコマンドを使用します。

```
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    10.1.0.2          lte              10.1.0.1          private1
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          private1
```

```
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                                  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-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
```

Cisco IOS XE SD-WAN デバイス に関する IPsec ペアワイズキー情報を表示するには、次のコマンドを使用します。

```
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
```

Cisco IOS XE SD-WAN デバイス での debug コマンド

IPsecペアワイズキーに関連する問題をデバッグするには、次の **debug** コマンドを使用します。

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