# Session Initiation Protocol トリガー VPN

Session Initiation Protocol トリガー VPN（SIP トリガー VPN または VPN SIP）は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。VPN SIP 機能は、2 つの SIP ユーザ エージェントが相互の IP アドレスを解決し、自己署名証明書、サードパーティ証明書、または事前共有キーのフィンガープリントを安全に交換して、IPsec ベース VPN の確立に同意するプロセスを定義します（訳注：NTT東日本及び西日本の提供する「ひかり電話データコネクト」サービスに接続するための機能です）。

サービス プロバイダーは、銀行の ATM や支店など、SIP ベースのサービスを必要とする顧客に VPN SIP サービスを提供します。この VPN SIP サービスは、バックアップ ネットワーク機能の ISDN 接続に代わるものです。プライマリのブロードバンド サービス リンクがダウンした場合、これらの銀行の ATM や支店は VPN SIP サービスを介して中央ヘッドエンドまたはデータ センターに接続します。

サービス プロバイダーの SIP サーバは、VPN SIP サービスの調整に加えて、サービスの使用時間を基にしたサービス料金の請求にも使用されます。

# VPN SIP の機能情報

表 *1 : VPN SIP* の機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Session Initiation Protocol トリガー VPN | | VPN SIP は、サービス プロバイダーが提供するサービスで、Session Initiation Protocol（SIP）を使用して、オンデマンド メディアやピア間のアプリケーション共有に必要な VPN が設定されます。<br>次のコマンドが導入されました：**nat force-encap, show vpn-sip session, show vpn-sip sip, show vpn-sip registration-status, vpn-sip local-number, vpn-sip logging, vpn-sip tunnel source** |

# VPN SIP の情報

## VPN SIP ソリューションのコンポーネント

VPN SIP は、IPSec 静的仮想トンネル インターフェイス（SVTI）を使用します。IPSec SVTI は、IPSec セキュリティ アソシエーション（SA）がトンネル インターフェイスと SVTI ピア間でまったく確立されていない場合でも、アクティブ（UP）な状態のままになります。

VPN SIP ソリューションの 3 つのコンポーネントを次に示します。

- SIP
- VPN SIP
- 暗号（IP Security（IPsec）、インターネットキーエクスチェンジ（IKE）、トンネル保護（TP）、暗号内の Public Key Infrastructure（PKI）モジュール）

## Session Initiation Protocol

SIP は、IKE セッションを開始するための名前解決メカニズムとして使用されます。VPN SIP は、SIP サービスを使用して、固定 IP アドレスを持たないホーム ルータまたはスモール ビジネス ルータに VPN 接続を確立します。この接続は、自己署名証明書か事前共有キーを使用し

て実現されます。SIP は、Session Description Protocol（SDP）オファー/アンサー モデルでのメディア セッションに必要な IKE の使用をネゴシエートします。

SIP は静的に設定されています。リモート SIP 番号それぞれに対して、1 つのトンネル インターフェイスを設定する必要があります。

SIP は、VPN SIP サービスの使用料を SIP 番号に基づいて顧客に請求する課金機能もサービス プロバイダーに提供します。SIP 番号に基づく請求は、サービス プロバイダー ネットワーク内で発生するものであり、Cisco VPN SIP ルータのようなエンド デバイスとは無関係です。

# VPN SIP のソリューション

VPN SIP は、SIP モジュールと暗号モジュールを連携し、両者の間を抽象化する中央ブロックです。

SIP 番号の背後にあるリモート ネットワークへ向けられたトラフィックがトンネル インターフェイスにルーティングされると、そのピアには IPSEC SA が設定されていないため、IPSec コントロール プレーンはパケット スイッチング パスからのトリガーを受け取ります。このトンネルは VPN SIP 用に設定されているため、IPsec コントロール プレーンは VPN SIP にトリガーを渡します。

（注） その SIP 番号のリモート ネットワークの静的ルートは、このトンネル インターフェイスを指すように設定される必要があります。

VPN SIP サービスがトリガーされると、SIP は SIP 電話番号のペアを使用してコールを設定します。SIP は VPN SIP に着信コールの詳細も渡し、ローカルの自己署名証明書または事前共有キーのローカル アドレスとフィンガープリント情報を使用して、IKE メディア セッションをネゴシエートします。SIP は VPN SIP にリモート アドレスとフィンガープリント情報も渡します。

VPN SIP サービスはトンネル ステータスの更新をリッスンし、SIP を呼び出して、SIP セッションを切断します。VPN SIP サービスは、現在のアクティブなセッションを表示する手段も提供します。

# 機能一覧

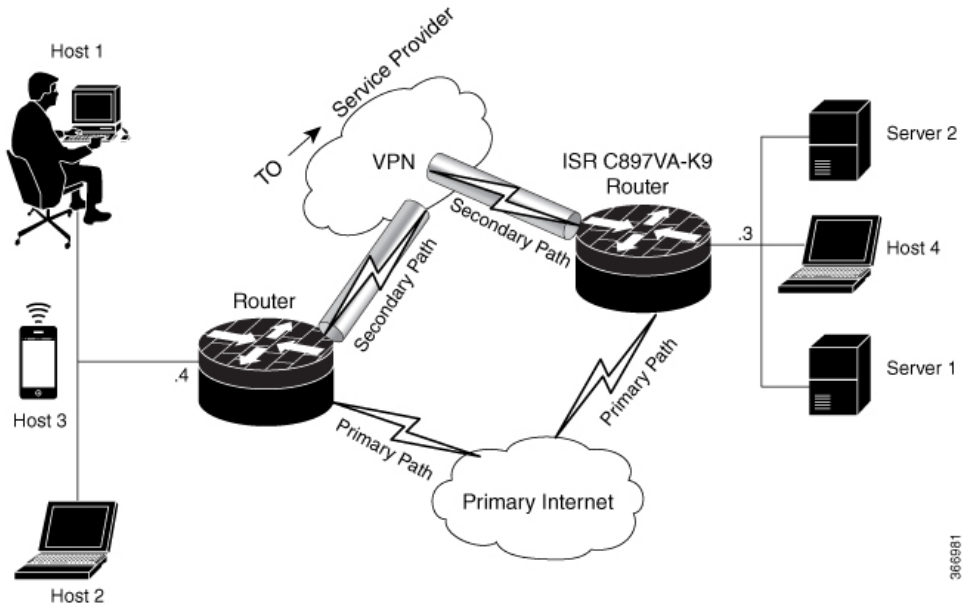
次に、VPN SIP 機能の概略を示します。

- IP SLA は、ルート トラッキングを使用してプライマリ リンクをモニタリングします。プライマリ リンクが失敗すると、IP SLA はこの障害を検出します。
- プライマリ パスが失敗すると、IP SLA はルーターに設定されているメトリックがさらに高いルートにデフォルト ルートを切り替えます。
- 関連するトラフィックがセカンダリ リンクを使用してフローを試みると、SIP は SIP サーバに招待メッセージを送信し、VPN ピア情報を取得します。

- ルータは VPN ピア情報（IP アドレス、ローカル SIP 番号とリモート SIP 番号、IKE ポート、およびフィンガープリント）を受け取って、VPN SIP トンネルを確立します。
- プライマリ パスが復帰すると、IP SLA はプライマリ パスを検出し、ルートが元のパスに戻ります。アイドル タイマーの有効期限が切れると、IPSec は破棄され、SIP コールは切断されます。

次に、VPN SIP ソリューションのトポロジを示します。

**図 *1 : VPN SIP* のトポロジ**




# SIP コール フロー

SIP コール フローは、ローカル ピアでの開始とリモート ピアでのコールの受信に分かれます。

### SIP コールの開始

データ プレーン内の SVTI インターフェイスにパケットがルーティングされると、そのアドレスを解決するためにピア SIP 番号に対して SIP コールを発呼する必要があります。これにより、VPN トンネルがアクティブになります。

- ローカル認証タイプが PSK の場合、IKEv2 はピア SIP 番号と一致するキーを検索します。IKEv2 キーリングは、各 SIP ピアの SIP 番号として id_key_id 型（文字列）で設定する必要があります。IKEv2 は検索されたキーのフィンガープリントを計算し、VPN SIP に渡します。
- ローカル認証タイプが自己署名証明書やサード パーティ証明書の場合、IKEv2 は IKEv2 プロファイルに設定されているローカルの証明書のフィンガープリントを計算し、VPN SIP に渡します。

VPN SIP モジュールは、ピアに SIP コールを設定するために SIP と対話します。コールが成功すると、VPN SIP は解決された IP アドレスを SVTI のトンネル接続先として設定し、SVTI に対して VPN トンネルを開始するように要求します。

（注） ワイルドカード キーが必要な場合は、IKEv2 プロファイルで、authentication local pre-share key コマンドと authentication remote pre-share key コマンドを使用します。

### リモート ピアでの SIP コールの受信

ピアから SIP コールを受信すると、さまざまな暗号モジュールが以下のように相関して動作します。

- トンネル保護は、VPN SIP モジュールによるトンネルの宛先アドレスの設定に協力します。
- IKEv2 は、ローカル認証タイプ（PSK または PKI）とローカル フィンガープリントを VPN SIP モジュールに返します。ローカル認証タイプが PSK の場合、IKEv2 は対応する SIP 番号と一致するキーを検索します。

（注） IKEv2 は SIP 番号によってのみピアを識別できます。

ピア間で SIP コール ネゴシエーションが行われている間に、各ピアは SDP 上で交換される一意のローカル IKEv2 ポート番号を選択する必要があります。セッションごとに異なるポート番号をサポートするため、VPN SIP モジュールは IP ポート アドレス変換（PAT）をプログラムにより自動的に設定します。PAT は、IKEv2 ポート（4500）と、SDP 上で交換されるポート番号との変換を担います。変換には、セカンダリ リンク上に IP NAT が設定され、ループバック インターフェイスが VPN SIP トンネルの送信元として設定される必要があります。変換の有効期間は、VPN SIP セッションの有効期間で決まります。

### SDP オファーとアンサー

RFC 6193 で定義されている、SIP コールでネゴシエートされる SDP オファーとアンサーの例を次に示します。

```
offer SDP
      ...
      m=application 50001 udp ike-esp-udpencap
      c=IN IP4 10.6.6.49
      a=ike-setup:active
      a=fingerprint:SHA-1 \
      b=AS:512
      4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
      ...

   answer SDP
      ...
      m=application 50002 udp ike-esp-udpencap
      c=IN IP4 10.6.6.50
```

```
a=ike-setup:passive
a=fingerprint:SHA-1 \
b=AS:512
D2:9F:6F:1E:CD:D3:09:E8:70:65:1A:51:7C:9D:30:4F:21:E4:4A:8E
```

SDP ネゴシエーションの一環として、両方のピアが「b=AS :number」という SDP 属性を使用し、VPN SIP セッションの最大帯域幅のレートをネゴシエートします。SDP に表示されるピア双方の帯域幅が異なる場合、小さい方の値が最大帯域幅として使用される必要があります。「b=AS :number」SDP 属性がオファーかアンサーに含まれていない場合、SIP コールは正常に設定されていません。

ネゴシエートされた最大帯域幅は、プログラムによって設定される出力方向の QoS ポリシーを介して SVTI トンネル インターフェイスに適用されます。静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。

SIP コールが完了し、ピアのアドレスが解決されると、VPN SIP は SVTI のトンネル接続先を設定し、トンネルを開始する要求を送信します。

# IKEv2 ネゴシエーション

次に、IKEv2 セキュリティ セッション（SA）ネゴシエーションのプロセスを示します。

- セッションの開始前に、IKEv2 は VPN SIP を使用して、そのセッションが VPN SIP セッションであるかどうかを確認します。
- セッションが VPN SIP セッションで、ローカル認証タイプが PSK の場合、IKEv2 はピアの IP アドレスの代わりにピアの SIP 番号を使用して、PSK キー ペアを検索します。
- 自己署名証明書を検証する場合、IKEv2 はその証明書が自己署名されたものかを確認して、証明書を検証します。
  - IKEv2 プロトコルの一部である既存の AUTH ペイロード検証に加えて、IKEv2 は受信した証明書または検索された PSK のハッシュを計算して、IKEv2 が VPN SIP モジュールからクエリする SIP ネゴシエーションのフィンガープリントと比較します。フィンガープリントが一致する場合のみ、IKEv2 はピアの認証が有効であると見なします。一致しない場合、IKEv2 はそのピアが認証に失敗したことを宣言し、VPN セッションを終了します。

VPN SIP ソリューションは、バックアップ VPN でトラフィックをルーティングする必要がなくなったことを、IPSEC アイドル タイマーに基づいて検出します。トラフィックがない時にセッションが切断されるようにするには、IPSec プロファイルにアイドル時間を設定する必要があります。推奨設定は 120 秒です。

VPN SIP と SIP は、連係して SIP コールを切断します。

IPsec アイドル時間の有効期限が切れると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知します。VPN SIP は、SIP モジュールに対して、IKEv2 からの確認を待機せずに SIP コールを切断するように要求します。

SIP コールの切断をピアから受信すると、VPN SIP モジュールは IPsec トンネルをダウンするように IKEv2 に通知し、SIP に対して SIP コールの切断を許可します。

# VPN SIP の前提条件

- セキュリティ K9 ライセンスをルータで有効にする必要があります。
- ルータには最低 1 GB のメモリが必要です。
- SIP ユーザ エージェントの SIP 登録要求が成功するには、VPN SIP ルータが SIP レジストラを使用できる必要があります。
- DHCP サーバは、SIP サーバ アドレスを取得するためにオプション 120 と 125 をサポートする必要があります。SIP サーバ アドレスは、SIP セッションの登録と確立に必要になります。
- プライマリ パスがダウンしたときにバックアップ WAN パスが使用される ようにするには、ルーティングを適切に設定しておく必要があります。
- トンネル インターフェイスの最大伝送ユニット（MTU）は、セカンダリ WAN インターフェイスの MTU よりも小さくなければなりません。
- IKEv2 認証に自己署名証明書やサード パーティ証明書を使用する場合は、IP 層のフラグメンテーションを避けるために、VPN SIP ルータに IKEv2 フラグメンテーションを設定します。
- NAT SIP ALG は無効にする必要があります。
- 発信者ID通知サービス（訳注：「ナンバー・ディスプレイ」）が該当の加入者契約において、ネットワーク側で設定されている必要があります。

# VPN SIP の制約事項

- VPN SIP と CUBE/SIP ゲートウェイを同一デバイス上で設定することはできません。CUBE ライセンスがデバイス上でアクティブな場合、CUBE のみが有効になります。
- トランスポートとメディア（SIP 登録、SIP シグナリング、および IPv4 トランスポートを介して暗号化された IPv4 パケットの IPv4 トランスポート）では、IPv4 のみがサポートされています。
- NAT の背後にあるピア デバイスを使用した SIP シグナリングはサポートされていません（ICE および STUN はサポートされていません）。
- SIP ネゴシエーションは、グローバル VRF でのみサポートされています。
- プライベート アドレスの割り当て、設定モード交換（CP ペイロード）、ルート交換などのリモート アクセス VPN 機能はサポートされていません。

- VPN SIP セッションでのルーティング プロトコルはサポートされていません。
- Rivest-Shamir-Addleman（RSA）サーバ自己署名証明書のみがサポートされています。
- 認証、認可、およびアカウンティング（AAA）を使用した事前共有キーの検索機能は、サポートされていません。
- IPSec アイドル タイマーは、ipsec-profile コマンドを使用して IPSec プロファイルごとに設定します。アイドル時間は、特定の IPSec プロファイルを使用するすべての VPN SIP セッションで同じです。
- IPSLA のモニタリングに使用されるトラック オブジェクトは、Cisco IOS ソフトウェアで最大 1000 オブジェクトまでに制限されています。1 つのトラック オブジェクトを使用して 1 台のピア ルーターを追跡する場合、1 台の IOS デバイスが処理できる VPN SIP セッションの最大数は、トラック オブジェクトの最大数で決まります。
- Cisco IOS ソフトウェアでは、ローカル SIP 番号は 1 つのみサポートされています。
- 静的に設定されたポリシーが既に存在する場合は、プログラムによって設定される QoS ポリシーは適用されず、セッションは失敗します。SVTI インターフェイス上に静的に設定された QoS ポリシーは、すべて削除してください。
- シスコ以外のベンダーによって実装された VPN SIP との相互運用性は、サポートされていません。
- VPN-SIP トンネルに付加されたポリシーマップに含まれるクラスポリシーについては、プライオリティキューイングとクラスベース重み付け均等化キューイング（CBWFQ）のみがサポートされます。
- CBWFQ の設定でサポートされているのは、`bandwidth percent` *`percent`* コマンドのみです。VPN-SIP セッションの帯域幅はピアルータとのネゴシエーションによって変わるため、`bandwidth` *`bandwidth`* コマンドはサポートされていません。
- VPN-SIP の設定は IPv6 ではサポートされていません。
- VPN-SIP の設定は、自律モードでのみサポートされます。
- 参照、フォークなどの複雑な SIP コールシナリオは、VPN-SIP の設定ではサポートされていません。

# VPN SIP の設定方法

## VPN SIP の設定

VPN SIP を設定する手順は次のとおりです。

1. サードパーティ証明書、自己署名証明書、または事前共有キーを使用してトンネル認証を設定します。

1. 証明書を使用するトンネル認証

   顧客のネットワーク内にある証明機関（CA）サーバから証明書を取得するためのトラストポイントを設定します。これはトンネル認証で必要です。次の設定を使用します。

```
peer1(config)# crypto pki trustpoint CA
 enrollment url http://10.45.18.132/
 serial-number none
 subject-name CN=peer2
 revocation-check crl
 rsakeypair peer2

peer2(config)# crypto pki authenticate CA
Certificate has the following attributes:
       Fingerprint MD5: F38A9B4C 2D80490C F8E7581B BABE7CBD
      Fingerprint SHA1: 4907CC36 B1957258 5DFE23B2 649E7DDA 99BDB7C3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

peer2(config)#crypto pki enroll CA
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=peer2
% The subject name in the certificate will include: peer2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA' command will show the fingerprint.
Certificate map for Trustpoint
crypto pki certificate map data 1
issuer-name co cn = orange
```

2. 自己署名証明書を使用するトンネル認証

   自己署名証明書を使用して認証を行う場合、そのデバイス上に自己署名証明書を生成する PKI トラストポイントを設定します。次の設定を使用します。

```
peer4(config)#crypto pki trustpoint Self
    enrollment selfsigned
    revocation-check none
    rsakeypair myRSA
    exit
crypto pki enroll Self

Do you want to continue generating a new Self Signed Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

3. 事前共有キーを使用してトンネル認証を設定します。

```
crypto ikev2 keyring keys
peer peer1
```

```
identity key-id 1234
pre-shared-key key123
```

2. 1. 証明書の IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match certificate data
identity local key-id 5678
authentication remote rsa-sig
authentication local rsa-sig
keyring local keys
pki trustpoint self
nat force-encap
```

2. 事前共有キーの IKEv2 プロファイルを設定します。

```
crypto ikev2 profile IPROF
match identity remote any
identity local key-id 5678
authentication remote pre-share
authentication local pre-share
keyring local keys
nat force-encap
```

（注） IKEv2 SA を設定するには、両方のピアで **nat force-encap** コマンドを設定する必要があります。UDP のカプセル化が SDP でネゴシエートされるので、IKEv2 はポート 4500 で開始し続行される必要があります。

3. IPsec プロファイルを設定します。

```
crypto ipsec profile IPROF
set security-association idle-time 2000
```

4. LAN 側インタ フェースを設定します。

```
interface Vlan101
         ip address 10.3.3.3 255.255.255.0
         no shutdown
!
     interface GigabitEthernet2
         switchport access vlan 101
         no ip address
```

5. ループバック インターフェイスを設定します。

   ループバック インターフェイスは、セカンダリ VPN トンネルの送信元インターフェイスとして使用されます。

```
interface loopback 1
    ip address 10.11.1.1 255.0.0.0
    ip nat inside
```

6. セカンダリ インターフェイスを設定します。

（注） セカンダリ インターフェイスは、IP アドレス、SIP サーバ アドレス、およびベンダー固有の情報を DHCP 経由で受信するように設定する必要があります。

```
interface GigabitEthernet8
     ip dhcp client request sip-server-address
     ip dhcp client request vendor-identifying-specific
     ip address dhcp
    ip nat outside
```

**7.** トンネル インターフェイスを設定します。

```
interface Tunnel1
     ip address 10.3.2.1 255.255.255.255
     load-interval 30
     tunnel source Loopback1
     tunnel mode ipsec ipv4
     tunnel destination dynamic
     tunnel protection ipsec profile IPROF ikev2-profile IPROF
     vpn-sip local-number 5678 remote-number 1234 bandwidth 1000
```

**vpn-sip local-number** *local-number* **remote-number** *remote-number* **bandwidth** *bw-number* コマンドを使用して、SVTI インターフェイスに VPN-SIP を設定します。帯域幅とは、このピアとネゴシエートされる必要のある最大データ伝送速度のことで、ネゴシエートされた値がトンネル インターフェイスに設定されます。使用できる値は 64 Kbps、128 Kbps、256 Kbps、512 Kbps、および 1000 Kbps です。

VPN SIP 用に SVTI を設定した後で、トンネル モード、トンネルの接続先、トンネルの送信元、およびトンネル保護を変更することはできません。モード、送信元、接続先、またはトンネル保護を変更するには、その SVTI インターフェイスから VPN SIP 設定を削除する必要があります。

**8.** 接続先ネットワークにスタティックルートを追加します。

メトリックが高いセカンダリ ルートを追加します。

```
ip route 192.168.10.0 255.255.255.0 Tunnel0 track 1
ip route 192.168.10.0 255.255.255.0 Tunnel1 254
```

**9.** IP SLA を設定します。

```
ip sla 1
         icmp-echo 10.11.11.1
         threshold 500
         timeout 500
         frequency 2
        ip sla schedule 1 life forever start-time now
```

**10.** ルート トラッキングを設定します。

```
track 1 ip sla 1 reachability
```

**11.** VPN SIP を有効化します。

```
vpn-sip enable
vpn-sip local-number 5678 address ipv4 GigabitEthernet8
vpn-sip tunnel source Loopback1
vpn-sip logging
```

VPN SIP を設定するには、ローカルの SIP 番号とローカル アドレスを設定する必要があります。**vpn-sip local-number** *SIP-number* **address ipv4** *WAN-interface-name* コマンドを使用して、SIP コールに使用するローカル SIP 番号と、関連づけられた IPv4 アドレスを設定します。

（注） IPv4 アドレスのみ設定できます。暗号モジュールはデュアル スタックをサポートしていません。

- バックアップ WAN インターフェイスのアドレスは、DHCP 割り当てに基づいて変わることがあります。

プライマリ WAN インタ フェースが機能している場合、VPN SIP トンネルの接続先はバックアップ WAN インターフェイスに設定され、トンネル インターフェイスが有効になります。トラフィックがトンネルインターフェイスにルーティングされる場合、接続先は SIP ネゴシエーションの SDP から学習されるピアの IP アドレスに設定されます。プライマリ WAN インターフェイスが失敗した場合、バック ルートがアクティブ化されていれば、パケットはバックアップを介して sVTI にルーティングされます。

（注） ループバック インターフェイスのアドレスにはルーティング不可能な未使用のアドレスを使用し、そのループバック インターフェイスは他のいかなる目的にも使用しないようにお勧めします。ループバック インターフェイスを設定すると、VPN SIP はこのインターフェイスに対するすべての更新プログラムをリッスンし、それらをブロックします。**vpn-sip logging** コマンドにより、セッションの開始、終了、障害発生などのイベントに関する VPN-SIP モジュールのシステムロギングが有効になります。

# ローカル ルータの VPN SIP の確認

### 登録スターテスの確認

```
Peer1# show vpn-sip registration-status
 SIP registration of local number 0388881001 : registered 10.6.6.50
```

### SIP レジストラの確認

```
Peer1#show vpn-sip sip registrar

Line          destination      expires(sec)  contact   transport     call-id
=============================================================================================
0388881001    example.com         2359        10.6.6.50  UDP
3176F988-9EAA11E7-8002AFA0-8EF41435
```

### VPN SIP ステータスの確認

```
Peer1#show vpn-sip session detail
VPN-SIP session current status
```

```
Interface: Tunnel1
   Session status: SESSION_UP (I)
   Uptime         : 00:00:42
   Remote number : 0388881001 =====> This is the Remote Router's SIP number
   Local number  : 0388882001 =====> Local router's SIP number
   Remote address:port: 10.6.6.49:50002
   Local address:port : 10.6.6.50:50001
   Crypto conn handle: 0x8000017D
   SIP Handle         : 0x800000C7
   SIP callID         : 1554
   Configured/Negotiated bandwidth: 64/64 kbps
```

### 暗号化セッションの確認

```
Peer1# show crypto session detail
Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP Vpn-sip

Interface: Tunnel1
Profile: IPROF
Uptime: 00:03:53
Session status: UP-ACTIVE
Peer: 10.6.6.49 port 4500 fvrf: (none) ivrf: (none)
      Phase1_id: 10.6.6.49
      Desc: (none)
  Session ID: 43
  IKEv2 SA: local 10.11.1.1/4500 remote 10.6.6.49/50002 Active
          Capabilities:S connid:1 lifetime:23:56:07 ====> Capabilities:S indicates this
 is a  SIP VPN_SIP Session
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 6 drop 0 life (KB/Sec) 4222536/3366
        Outbound: #pkts enc'ed 4 drop 0 life (KB/Sec) 4222537/3366
```

### IP NAT 変換の確認

```
Peer1#sh ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 2.2.2.2:4500       10.6.6.50:50001    10.6.6.49:50002    10.6.6.49:50002
```

### DHCP SIP 設定の確認

```
Peer9#show vpn-sip sip dhcp
SIP DHCP Info

SIP-DHCP interface:  GigabitEthernet8

SIP server address:
Domain name:         dns:example.com
```

# VPN SIP の設定例

### 認証用自己署名証明書の使用

認証用の自己署名証明書を使用して VPN SIP を設定する例を次に示します。VPN SIP では、イニシエータとレスポンダのロールに違いはありません。ピア ノード上の設定は、変更されたローカルの SIP 番号と同一になります。

```
// Self-signed certificate
crypto pki trustpoint selfCert
  rsakeypair myRSA
  enrollment selfsigned
  revocation-check none
!
crypto ikev2 profile vpn-sip-profile
 match identity remote any
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint selfCert // Use same self-signed trustpoint for sign and verify
 nat force-encap
!
crypto ipsec profile vpn-sip-ipsec
 set security-association idle-time 120
!
vpn-sip enable
vpn-sip local-number 0388883001 address ipv4 GigabitEthernet1
vpn-sip tunnel source Loopback11
vpn-sip logging
!
// one tunnel per peer - configuration is for peer with a SIP-number of 0388884001
int tunnel0
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile vpn-sip-profile
 vpn-sip local-number 0388883001 remote-number 0388884001 bandwidth 1000
!
// ip unnumbered of tunnel interfaces
int loopback 0
  ip address 10.21.1.1 255.255.255.255
!
int loopback11
ip address 10.9.9.9 255.255.255.255
ip nat inside
!
// one tunnel per peer - this is for peer with SIP-number 0388885001
int tunnel1
 ip unnumbered loopback 0
 tunnel source loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile vpn-sip-ipsec ikev2-profile iprof
 vpn-sip sip-local 0388883001 sip-remote 0388885001 bandwidth 1000
!
interface GigabitEthernet8
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp
```

```
ip nat outside


// backup routes configured with higher AD so that these routes will be activated only
when primary path goes down. AD need to be chosen to be greater than that of primary
route.
ip route 10.0.0.0 255.0.0.0 tunnel 0 250
ip route 10.1.0.0 255.0.0.0 tunnel 0 250
ip route 10.2.0.0 255.0.0.0 tunnel 0 250
ip route 10.3.0.0 255.0.0.0 tunnel 0 250
```

# VPN SIP の DHCP の設定

## ホームゲートウェイ配下での接続

Cisco IOS XE リリース 17.11.1a から、ホームゲートウェイ（HGW）の背後に VPN-SIP 対応ルータをインストールできます。このインストールでは、HGWは、固定電話番号の代わりにDynamic Host Configuration Protocol（DHCP）を介してトンネルインターフェイスに内線番号を割り当てます。これにより、ネットワーク上のデータと音声を集約できます。これは、アナログデータとデジタルデータの両方で同じ物理加入者回線を共有する必要があるシナリオで役立ちます。

さらに、HGW のネットワーク仕様に準拠するために、VPN-SIP の DHCP には、vendor-class-data DHCP オプションを介して、HGW ネットワークへ接続する WAN 側インターフェイスの MAC アドレスが必要です。この設定では、デバイスは DHCP 要求の vendor-class-data オプションを介して、自身の WAN インターフェイスの MAC アドレスをホームゲートウェイネットワークに通知します。

### サポートされている PID とファームウェア

次の表は、テストされた HGW の PID とファームウェアバージョンを示しています。シスコは、お客様の拠点に設置されている HGW または HGW の操作についてはサポートを提供していません。（訳注：ホームゲートウェイはNTTの資産としてお客様宅内に設置されるものであるためです）この機能を使用する前に、環境を確認することをお勧めします。

| HGW PID | ファームウェア バージョン |
|---|---|
| RT-400NE | 8.06 |
| RT-400MI | 09.00.0015 |
| RT-400KI | 08.00.0040 |
| RT-500MI | 08.00.0004 |
| RT-500KI | 08.00.0020 |
| RX-600MI | 01.00.0001 |
| RX-600KI | 01.00.0001 |

| HGW PID | ファームウェア バージョン |
|---|---|
| OG410Xi | 2.32 |
| OG410Xa | 2.32 |

# ホームゲートウェイ配下での接続

DHCP ローカル番号を設定すると、デバイスは DHCP 応答を受信するまで SIP 登録を遅延させます。デバイスは、DHCP サーバーが内線番号を提供することを想定しています。この内線番号は、SIP サーバーへの登録に使用されます。登録が成功し、デバイスが SIP サーバーとのセッションを開始すると、200 OK 応答を通じて、内線番号、外線番号、およびその他の使用可能な番号を受信します。

（注） 外線番号は、ルータをグローバルに識別する番号です。この外線番号は、データ接続を確立するためにも必要です。

DHCP 拡張により、データ接続には SIP シグナリングチャンネルと IPsec データ接続の 2 つのチャンネルがあります。データパケットにトンネル保護が必要な場合、SIP コールが開始されます。

VPN-SIP の DHCP を設定するには、次の手順を実行します。

# DHCP クライアントの有効化

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip dhcp client request sip-server-address**
5. **ip dhcp client request vendor-identifying-specific**
6. **ip address dhcp**
7. **ip dhcp client vendor-class mac-address**
8. **ip nat outside**
9. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。プロンプトが表示されたらパスワードを入力します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 2 | **configure terminal**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface type number**<br>例：<br>`Router(config)# interface gigabitethernet 0/0` | インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **ip dhcp client request sip-server-address**<br>例：<br>`Router(config-if)# ip dhcp client request sip-server-address` | DHCP サーバーに SIP サーバーアドレスを要求するように DHCP クライアントを設定します。 |
| ステップ 5 | **ip dhcp client request vendor-identifying-specific**<br>例：<br>`Router(config-if)# ip dhcp client request vendor-identifying-specific` | DHCP サーバーにベンダー固有の情報を要求するように DHCP クライアントを設定します。 |
| ステップ 6 | **ip address dhcp**<br>例：<br>`Router(config-if)# ip address dhcp` | インターフェイス上で DHCP から IP アドレスを取得します。 |
| ステップ 7 | **ip dhcp client vendor-class mac-address**<br>例：<br>`Router(config-if)# ip dhcp client vendor-class mac-address` | HGW の DHCP 仕様に準拠します。 |
| ステップ 8 | **ip nat outside**<br>例：<br>`Router(config-if)# ip nat outside` | 外部ネットワークにインターフェイスを接続します。 |
| ステップ 9 | **exit**<br>例：<br>`Router(config-if)# end` | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# DHCP クライアントを有効にする設定例

次に、DHCP クライアントを有効にするためのサンプルコードを示します。

```
interface GigabitEthernet 0/0/0
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp
 ip dhcp client vendor-class mac-address
 ip nat outside
```

# トンネリング認証の設定

サードパーティ証明書、自己署名証明書、または事前共有キー（PSK）を使用してトンネル認証を設定できます。トンネル認証を設定するには、次のいずれかのタスクを実行します。

## 証明書を使用したトンネル認証の設定

顧客のネットワーク内にある証明機関（CA）サーバから証明書を取得するためのトラストポイントを設定します。これはトンネル認証で必要です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** name
4. **enrollment url** `url`
5. **serial-number**
6. **subject-name** `[subject-name]`
7. **revocation-check crl**
8. **rsakeypair**
9. **crypto pki authenticate CA**
10. **crypto pki enroll CA** `name`
11. **exit**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **crypto pki trustpoint** name<br>例：<br>`Router(config)# crypto pki trustpoint CA` | トラストポイントおよび設定された名前を指定して、CA トラストポイントコンフィギュレーションモードを開始します。 |
| ステップ 4 | **enrollment url** `url`<br>例：<br>`Router(ca-trustpoint)# enrollment url http://10.45.18.132/` | ルータが証明書要求を送信する CA の URL を指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 5 | **serial-number**<br>例：<br>`Router(ca-trustpoint)# serial-number` | **none** キーワードを指定した場合を除き、証明書要求でルータのシリアル番号を指定します。<br>証明書要求にシリアル番号を含めない場合は、**none** キーワードを使用します。 |
| ステップ 6 | **subject-name [subject-name]**<br>例：<br>`Router(ca-trustpoint)# subject-name CN=peer2` | 証明書要求で使用される要求された情報カテゴリ名を指定します。情報カテゴリ名が指定されていない場合は、デフォルトの情報カテゴリ名である完全修飾ドメイン名（FQDN）が使用されます。 |
| ステップ 7 | **revocation-check crl**<br>例：<br>`Router(ca-trustpoint)# revocation-check crl` | 証明書失効リスト（CRL）メカニズムを使用して証明書の有効性を確認します。 |
| ステップ 8 | **rsakeypair**<br>例：<br>`Router (ca-trustoint)# rsakeypair peer2` | トラストポイントのキーペアを提供します。 |
| ステップ 9 | **crypto pki authenticate CA**<br>例：<br>`Router(config)# crypto pki authenticate CA` | CA の公開キーが含まれている CA の自己署名証明書を取得して、CA をルータに対して認証します。 |
| ステップ 10 | **crypto pki enroll CA name**<br>例：<br>`Router(config)# crypto pki enroll CA` | 証明書要求を生成し、コピーして証明書サーバーに貼り付けるために要求を表示します。<br>証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に証明書要求を表示するかについても選択できます。 |
| ステップ 11 | **exit**<br>例：<br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

## 例：証明書を使用したトンネル認証の設定

これは、証明書を使用してトンネル認証を設定するためのサンプルコードです。

```
peer1(config)# crypto pki trustpoint CA
 enrollment url http://10.45.18.132/
 serial-number none
 subject-name CN=peer2
 revocation-check crl
 rsakeypair peer2

peer2(config)# crypto pki authenticate CA
Certificate has the following attributes:
```

```
Fingerprint MD5: F38A9B4C 2D80490C F8E7581B BABE7CBD
Fingerprint SHA1: 4907CC36 B1957258 5DFE23B2 649E7DDA 99BDB7C3
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.

peer2(config)#crypto pki enroll CA
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the
CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration. Please make
a note of it.
Password:
Re-enter password:
% The subject name in the certificate will include: CN=peer2
% The subject name in the certificate will include: peer2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose CA' command will show the fingerprint.
Certificate map for Trustpoint
crypto pki certificate map data 1
issuer-name co cn = orange
```

## 自己署名証明書を使用したトンネル認証の設定

自己署名証明書を使用してトンネル認証を設定するには、**crypto pki trustpoint self** コマンドを実行します。このコマンドにより、デバイスで自己署名証明書を生成するためのPKIトラストポイントを設定できます。

```
Router(config)# crypto pki trustpoint self
enrollment self signed
revocation-check none
rsakeypair myRSA
exit

crypto pki enroll self
Do you want to continue generating a new Self Signed Certificate? [yes/no]: yes
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

## 事前共有キーを使用したトンネル認証の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring keyring-name**
4. **peer name**
5. **address {ipv4-address [mask] | ipv6-addressprefix}**
6. **identity {address { ipv4-address | ipv6-address} | fqdn name | email email-id | key-id key-id}**
7. **pre-shared-key {local| remote} {0| 6| line}**
8. **exit**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **crypto ikev2 keyring keyring-name**<br>例：<br>`Router(config)# crypto ikev2 keyring kyr1` | IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。 |
| ステップ 4 | **peer name**<br>例：<br>`Router(config-ikev2-keyring)# peer peer1` | ピアまたはピアグループを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。 |
| ステップ 5 | **address {ipv4-address [mask] \| ipv6-addressprefix}**<br>例：<br>`Router(config-ikev2-keyring-peer)# address 10.0.0.1 255.255.255.0` | IP アドレスまたはピアの範囲を指定します。この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。 |
| ステップ 6 | **identity {address { ipv4-address \| ipv6-address} \| fqdn name \| email email-id \| key-id key-id}**<br>例：<br>`Router(config-ikev2-keyring-peer)# identity key-id 1234` | 次の ID を使用して IKEv2 ピアを特定します。<br>• 電子メール<br>• [FQDN]<br>• IPv4 アドレス<br>• キー ID<br>ID は IKEv2 レスポンダ上のキー ルックアップにしか使用できません。 |
| ステップ 7 | **pre-shared-key {local\| remote} {0\| 6\| line}**<br>例：<br>`Router(config-ikev2-keyring-peer)# pre-shared-key key123` | ピアの PSK を指定します。**local** キーワードまたは **remote** キーワードを入力し、非対称 PSK を指定します。デフォルトでは、PSK は対称です。 |
| ステップ 8 | **exit**<br>例：<br>`Router(config-ikev2-keyring-peer)# end` | キーリング ピア コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。 |

## 例：事前共有キーを使用したトンネル認証の設定

これは、事前共有キーを使用してトンネル認証を設定するためのサンプルコードです

```
crypto ikev2 keyring keys
 peer p1
 identity key-id 0388881001
 pre-shared-key cisco
 !
 peer p2
 identity key-id 0388882002
 pre-shared-key cisco
!
crypto ikev2 keyring HUB-KEY
peer SPOKES
address 0.0.0.0 0.0.0.0
pre-shared-key cisco
```

# 証明書の IKEv2 プロファイルの設定

IKEv2 プロファイルの証明書を設定するには、**crypto ikev2 profile IPROF** コマンドを実行します。次に、証明書の IKEv2 プロファイルを設定するためのサンプルコードを示します。

```
Router(config)# crypto ikev2 profile IPROF-psk
 match identity remote any
 identity local key-id dhcp
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 nat force-encap
```

# IPsec プロファイルの設定

IPSec プロファイルを設定するには、**crypto ipsec profile IPROF** コマンドを実行します。次に、IPSec プロファイルを設定するためのサンプルコードを示します。

```
Router(config)# crypto ipsec profile IPROF
 set security-association idle-time 300
```

# VPN SIP を有効化します。

VPN-SIP 機能を有効にするには、**vpn-sip enable** コマンドを実行します。次に、VPN-SIP を有効にするサンプルコードを示します。

```
Router(config)# vpn-sip enable
vpn-sip local-number dhcp address ipv4 GigabitEthernet0/0/0
vpn-sip tunnel source Loopback1
```

# LAN 側インターフェイスの設定

LAN 側のインターフェースを設定するには、**interface VLAN <interface>** コマンドを実行します。次に、LAN 側インターフェイスを設定するためのサンプルコードを示します。

```
Router(config)# interface GigabitEthernet2
ip address 192.0.2.3 255.255.255.0
no shutdown
```

# ループバック インターフェイスの設定

ループバック インターフェイスを設定するには、**interface loopback <number>** コマンドを実行します。次に、ループバック インターフェイスを設定するためのサンプルコードを示します。

```
Router(config)# interface Loopback1
 ip address 10.255.255.3 255.255.255.0
 ip nat inside
```

# トンネルインターフェイスの設定

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel source** {*ip-address* | *interface-type number*}
5. **tunnel destination**
6. **tunnel protection IPsec profile** *name*
7. **vpn-sip local-number dhcp remote-number bandwidth**
8. **exit**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`Router> enable` | 特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。 |
| ステップ 2 | **configure terminal**<br>例：<br>`Router# configure terminal` | グローバル設定モードを開始します。 |
| ステップ 3 | **interface tunnel** *number*<br>例：<br>`Router(config)# interface tunnel1` | トンネルインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。*number* 引数には、作成または設定するトンネル インターフェイスの数を指定します。作成可能なトンネル インターフェイスの数に制限はありません。 |
| ステップ 4 | **tunnel source** {*ip-address* \| *interface-type number*}<br>例： | トンネルインターフェイスの送信元 IP アドレスまたは送信元インターフェイスタイプ番号を設定します。この手順では、**tunnel protection IPsec profile** コ |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | `Router(config-if)# ip address 12.12.12.12 255.255.255.255`<br>`tunnel source Loopback1` | マンドも使用するため、トンネル送信元として、IP アドレスではなくインターフェイスを指定する必要があります。 |
| ステップ 5 | **tunnel destination**<br>例：<br>`Router(config-if)# tunnel destination destination dynamic` | トンネルの宛先を指定します。 |
| ステップ 6 | **tunnel protection IPsec profile** *name*<br>例：<br>`Router(config-if)# tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk` | トンネル インターフェイスを IPsec プロファイルに関連付けます。*name* 引数には、IPsec プロファイルの名前を指定します。この値は、**crypto IPsec profile** <*name*> コマンドで指定した値と同じである必要があります。 |
| ステップ 7 | **vpn-sip local-number dhcp remote-number bandwidth**<br>例：<br>`Router(config-if)# vpn-sip local-number dhcp remote-number 0388881001 bandwidth 1000` | VPN-SIP のインターフェイスを設定します。帯域幅とは、このピアとネゴシエートされる必要のある最大データ伝送速度のことで、ネゴシエートされた値がトンネルインターフェイスに設定されます。使用できる値は、64 kbps、128 kbps、256 kbps、512 kbps、および 1000 kbps です。<br>（注） VPN SIP 用にインターフェイスを設定した後で、トンネルモード、トンネルの接続先、トンネルの送信元、およびトンネル保護を変更することはできません。モード、送信元、接続先、またはトンネル保護を変更するには、そのインターフェイスから VPN SIP 設定を削除する必要があります。 |
| ステップ 8 | **exit**<br>例：<br>`Router(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# 例：トンネルインターフェイスの設定

これは、トンネルインターフェイスを設定するためのサンプルコードです。

```
Router(config)# interface Tunnel1
 ip address 10.12.12.12 255.255.255.255
 tunnel source Loopback1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk
 vpn-sip local-number dhcp remote-number 0388881001 bandwidth 1000
!
```

```
interface Tunnel10
 ip address 10.20.20.21 255.255.255.255
 tunnel source Loopback1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPROF ikev2-profile IPROF-psk
 vpn-sip local-number dhcp remote-number 0388882002 bandwidth 100
```

# VPN-SIP での DHCP 設定の確認

次の show コマンドの出力は、VPN-SIP の DHCP が HGW の背後にある Cisco IOS XE ルータで正常に設定されているかどうかを確認する方法を示しています。

```
Router_behind_HGW# show vpn-sip sip dhcp
SIP DHCP Info
SIP-DHCP interface:  GigabitEthernet 0/0/0
SIP server address:  ipv4:192.168.1.1
Domain name:         dns:ntt-east.ne.jp
```

```
Router_behind_HGW# show vpn-sip registration-status
  SIP registration of local number dhcp : registered 192.168.1.200
  Local dynamic number via dhcp[3], via SIP[0398765432]
```

```
Router_behind_HGW# show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================
3             ntt-east.ne.jp   2439          192.168.1.20
UDP           FFFFFFFFCCE6C415-5D8611ED-FFFFFFFF810AE9D4-FFFFFFFFD
```

```
Router_behind_HGW# show vpn-sip session detail
VPN-SIP session current status
Interface: Tunnel0
    Session status: SESSION_UP (I)
    Uptime        : 00:00:37
    Remote number : 0387654321
    Local number  : dhcp
    Remote address:port: aaa.bbb.ccc.ddd:27129
    Local address:port : 192.168.1.200:50026
    Crypto conn handle: 0x4000003D
    SIP Handle        : 0x4000001B
    SIP callID        : 301
    Configured/Negotiated bandwidth: 256/256 kbps
    Applied service policy:
```

```
Router_behind_HGW# show crypto session
Crypto session current status
Interface: Tunnel0
Profile: IPROF
Session status: UP-ACTIVE
Peer: aaa.bbb.ccc.ddd port 27129
   Session ID: 26
   IKEv2 SA: local 10.255.255.1/4500 remote aaa.bbb.ccc.ddd/27129 Active
   IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
   Active SAs: 2, origin: crypto map
```

```
Router_behind_HGW# show crypto ikev2 sa
  IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf
   Status
1         10.255.255.1/4500     aaa.bbb.ccc.ddd/27129  none/none
    READY
       Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH
```

```
       Grp:19, Auth sign: PSK, Auth verify: PSK
       Life/Active Time: 86400/86 sec
       CE id: 1022, Session-id: 22
       Local spi: 59E8EED28441BC32
       Remote spi: B5487716A19873BE
       IPv6 Crypto IKEv2  SA

Router_behind_HGW# show crypto ipsec sa

interface: Tunnel0
Crypto map tag: Tunnel0-head-0, local addr 10.255.255.1
protected vrf: (none)
local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer aaa.bbb.ccc.ddd port 27129
PERMIT, flags={origin_is_acl,}
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 0, #recv errors 0

local crypto endpt.: 10.255.255.1, remote crypto endpt.:
aaa.bbb.ccc.ddd
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb
GigabitEthernet0/0/0
current outbound spi: 0xE0F51D37(3774160183)
PFS (Y/N): N, DH group: none

inbound esp sas:
      spi: 0x493D896(76798102)
      transform: esp-aes esp-sha-hmac ,
      in use settings ={Tunnel UDP-Encaps, }
      conn id: 2044, flow_id: ESG:44, sibling_flags FFFFFFFF80004048,
crypto map: Tunnel0-head-0, initiator : True
       sa timing: remaining key lifetime (k/sec): (4607999/3509)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: 0xE0F51D37(3774160183)
         transform: esp-aes esp-sha-hmac ,
         in use settings ={Tunnel UDP-Encaps, }
         conn id: 2043, flow_id: ESG:43, sibling_flags FFFFFFFF80004048,
crypto map: Tunnel0-head-0, initiator : True
         sa timing: remaining key lifetime (k/sec): (4607999/3509)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)
      outbound ah sas:
      outbound pcp sas:


Router_behind_HGW# show ip nat translations
Pro  Inside global         Inside local          Outside local
Outside global
udp  192.168.1.200:50269   10.255.255.1:4500     aaa.bbb.ccc.ddd:23060
aaa.bbb.ccc.ddd:23060
Total number of translations: 1
```

# VPN SIP のトラブルシューティング

### show コマンドの出力にトンネル インターフェイスを表示する

症状

Show VPN-SIP セッションにトンネルインタ フェースの情報が表示されません。次の例では、トンネル インターフェイスである tunnel1 の情報が表示されていません。

```
Peer5-F#show vpn-sip session
VPN-SIP session current status

Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 192.30.18.22:0

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
```

考えられる原因

そのトンネル インターフェイスに VPN SIP が設定されていません。

```
Peer5-F#sh run int tun1
Building configuration...

Current configuration : 201 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.0.0.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
end
```

推奨処置

そのトンネル インターフェイスに VPN SIP を設定します。

```
:

Peer5-F#show running interface tunnel 1
Building configuration...

Current configuration : 278 bytes
!
interface Tunnel1
 ip address 10.5.5.5 255.255.255.255
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 vpn-sip local-number 0623458888 remote-number 0312341111 bandwidth 1000
end
```

次に、上記のシナリオを実行した出力を示します。

```
Peer5-F#show vpn-sip session detail
VPN-SIP session current status

Interface: Tunnel1
   Session status: READY_TO_CONNECT
   Remote number : 0312341111
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0

   Crypto conn handle: 0x8000002C
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps

Interface: Tunnel2
   Session status: READY_TO_CONNECT
   Remote number : 0334563333
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000012
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel3
   Session status: READY_TO_CONNECT
   Remote number : 0323452222
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000031
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 512/0 kbps

Interface: Tunnel4
   Session status: READY_TO_CONNECT
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x8000002F
   SIP Handle        : 0x0
   SIP callID        : --
```

```
   Configured/Negotiated bandwidth: 1000/0 kbps

Interface: Tunnel6
   Session status: READY_TO_CONNECT
   Remote number : 0634567777
   Local number  : 0623458888
   Remote address:port: 0.0.0.0:0
   Local address:port : 172.30.18.22:0
   Crypto conn handle: 0x80000026
   SIP Handle        : 0x0
   SIP callID        : --
   Configured/Negotiated bandwidth: 1000/0 kbps
```

### SIP 登録ステータスのトラブルシューティング

症状

SIP 登録ステータスが登録されていません。

```
Peer5#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : not registered
```

考えられる原因

その WAN インターフェイスに IP アドレスが設定されていません。

```
Peer5#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         unassigned      YES unset  up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5        YES NVRAM  up                    up
NVI0                       10.1.1.1         YES unset  up                    up
Loopback1                  10.1.1.1         YES NVRAM  up                    up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.5.5.5         YES NVRAM  up                    down
Tunnel2                    10.2.2.2         YES NVRAM  up                    down
Tunnel3                    10.3.3.3         YES NVRAM  up                    down
Tunnel4                    10.4.4.4         YES NVRAM  up                    down
Tunnel6                    10.8.8.8         YES NVRAM  up                    down

Peer5-F#show run interface gigabitEthernet 0/4
Building configuration...

Current configuration : 213 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 no ip address           ====> no IP address
 ip nat outside
 ip virtual-reassembly in
 duplex auto
```

```
 speed auto
end
```

推奨処置

**ip address dhcp** コマンドを使用してインターフェイスの IP アドレスを設定する。

```
Peer5-F#show running-config interface gigabitEthernet 0/4
Building configuration...

Current configuration : 215 bytes
!
interface GigabitEthernet0/4
 ip dhcp client request sip-server-address
 ip dhcp client request vendor-identifying-specific
 ip address dhcp         ====> configure IP address DHCP
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
end


Peer5-F#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  down                  down
GigabitEthernet0/1         unassigned      YES unset  up                    up
GigabitEthernet0/2         unassigned      YES unset  down                  down
GigabitEthernet0/3         unassigned      YES unset  down                  down
GigabitEthernet0/4         172.30.18.22    YES DHCP   up                    up
GigabitEthernet0/5         10.5.5.5        YES manual up                    up
Vlan1                      10.45.1.5        YES NVRAM  up                     up
NVI0                       10.1.1.1         YES unset  up                     up
Loopback1                  10.1.1.1         YES NVRAM  up                     up
Loopback5                  10.5.5.5        YES NVRAM  administratively down down
Loopback11                 10.11.11.11     YES NVRAM  up                    up
Tunnel1                    10.6.5.5         YES NVRAM  up                     down
Tunnel2                    10.2.2.2         YES NVRAM  up                     down
Tunnel3                    10.3.3.3         YES NVRAM  up                     down
Tunnel4                    10.4.4.4         YES NVRAM  up                     down
Tunnel6                    10.8.8.8         YES NVRAM  up                     down

Peer5-F#show vpn-sip sip registrar
Line          destination      expires(sec)  contact
transport     call-id
============================================================
0623458888    example.com   2863          172.30.18.22
UDP           1E83ECF0-AF0611E7-802B8FCF-594EB9E7@122.50.18.22

Peer5-F#show vpn-sip registration-status

 SIP registration of local number 0623458888 : registered 172.30.18.22
```

### Negotiating IKE 状態でのセッション停止

症状

Negotiating IKE 状態で VPN SIP セッションが停止します。

```
Peer5#show vpn-sip session remote-number 0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
```

```
   Session status: NEGOTIATING_IKE (R)
   Uptime        : 00:00:58
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 172.30.168.3:24825
   Local address:port : 172.30.18.22:50012
   Crypto conn handle: 0x8000002E
   SIP Handle        : 0x8000000C
   SIP callID        : 16
   Configured/Negotiated bandwidth: 1000/1000 kbps
```

考えられる原因

IKEv2 関連の設定が不適切です。

次の例では、キーリングで設定されているキー ID が、リモート ピアの SIP 番号と一致していません。

```
Peer5-F#show running-config interface tunnel 4
Building configuration...

Current configuration : 276 bytes
!
interface Tunnel4
 ip address 10.4.4.4 255.0.0.0
 tunnel source Loopback11
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile test-prof ikev2-profile test
 VPN-SIP local-number 0623458888 remote-number 0612349999 bandwidth 1000  ====> Remote
number mentioned here doesn’t match the remote number in the keyring
end

IKEv2 Keyring configs:
!
crypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk10337101690
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key cisco123
 !
 peer peer3
  identity key-id 0323452222
  pre-shared-key cisco123
 !
 peer peer4
  identity key-id 0645676666
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
```

```
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
```

推奨処置

キーリングの設定を修正します。

```
rypto ikev2 keyring keys
 peer peer1
  identity key-id 0312341111
  pre-shared-key psk1
 !
 peer abc
  identity key-id 0345674444
  pre-shared-key psk1
 !
 peer peer2
  identity key-id 0334563333
  pre-shared-key psk1
 !
 peer peer6
  identity key-id 0634567777
  pre-shared-key psk1
 !
 peer peer3
  identity key-id 0323452222
  pre-shared-key psk1
 !
 peer peer4
  identity key-id 0612349999
  pre-shared-key psk1
 !
 peer NONID
  identity fqdn example.com
  pre-shared-key psk1
 !
!
!
crypto ikev2 profile test
 match identity remote any
 identity local key-id 0623458888
 authentication remote pre-share
 authentication local pre-share
 keyring local keys
 dpd 10 6 periodic
 nat force-encap
!

Peer5-F#show vpn-sip session remote-number  0612349999 detail
VPN-SIP session current status

Interface: Tunnel4
   Session status: SESSION_UP (R)
   Uptime        : 00:02:04
   Remote number : 0612349999
   Local number  : 0623458888
   Remote address:port: 172.30.168.3:24845
```

```
Local address:port : 172.30.18.22:50020
Crypto conn handle: 0x8000004E
SIP Handle         : 0x80000014
SIP callID         : 24
Configured/Negotiated bandwidth: 1000/1000 kbps
```

### セッション開始のトラブルシューティング

症状

セッションが開始せず、Negotiating IKE 状態で停止します。

考えられる原因

大きな PKI 証明書が IKE 認証メッセージに含まれている状況で、IKE パケットがフラグメンテーションを起こしています。

推奨処置

ルータに IKEv2 フラグメンテーションを設定します。

### debug コマンド

次のデバッグ コマンドを VPN SIP 設定のデバッグに使用できます。

**表 *2:* デバッグ コマンド**

| コマンド名 | 説明 |
|---|---|
| **debug vpn-sip event** | VPN SIP を使用した SVTI 登録、SIP 登録、コールセットアップなどのデバッグ メッセージを出力します。 |
| **debug vpn-sip errors** | 初期化、登録、コール セットアップなどの最中にエラーが発生した場合にのみ、エラーメッセージを出力します。 |
| **debug vpn-sip sip all** | すべての SIP デバッグ トレースを有効化します。 |
| **debug vpn-sip sip calls** | SIP SPI コールのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip dhcp** | SIP DHCP デバッグ トレースを有効化します。 |
| **debug vpn-sip sip error** | SIP エラーのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip events** | SIP イベントのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip feature** | 機能レベルでのデバッグを有効化します。 |

| コマンド名 | 説明 |
|---|---|
| **debug vpn-sip sip function** | SIP機能のデバッグ トレースを有効化します。 |
| **debug vpn-sip sip info** | SIP情報のデバッグ トレースを有効化します。 |
| **debug vpn-sip sip level** | 情報レベルでのデバッグを有効化します。 |
| **debug vpn-sip sip media** | SIP メディアのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip messages** | SIP SPI メッセージのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip non-call** | コール コンテキスト以外のトレース（OPTIONS、SUBSCRIBE など）を有効化します。 |
| **debug vpn-sip sip preauth** | SIP 事前認証のデバッグ トレースを有効化します。 |
| **debug vpn-sip sip states** | SIP SPI状態のデバッグ トレースを有効化します。 |
| **debug vpn-sip sip translate** | SIP変換のデバッグ トレースを有効化します。 |
| **debug vpn-sip sip transport** | SIP トランスポートのデバッグ トレースを有効化します。 |
| **debug vpn-sip sip verbose** | デバッグ モードを有効化します。 |

# VPN SIP に関する追加情報

### 標準および RFC

| 標準/RFC | タイトル |
|---|---|
| RFC 6193（制約事項付き） | セッション記述プロトコル（SDP）におけるIKEのメディア記述 |

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。