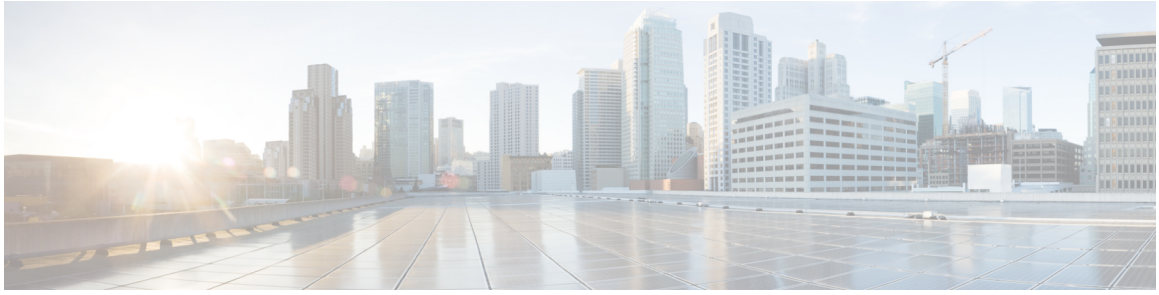


本書は、『Japanese translation of "Session Initiation Protocol Triggered VPN"』の章の翻訳のみ提供しております。
全文は英語版ドキュメントを参照してください。

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/15-mt/sec-sec-for-vpns-w-ipsec-15-mt-book.html

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。

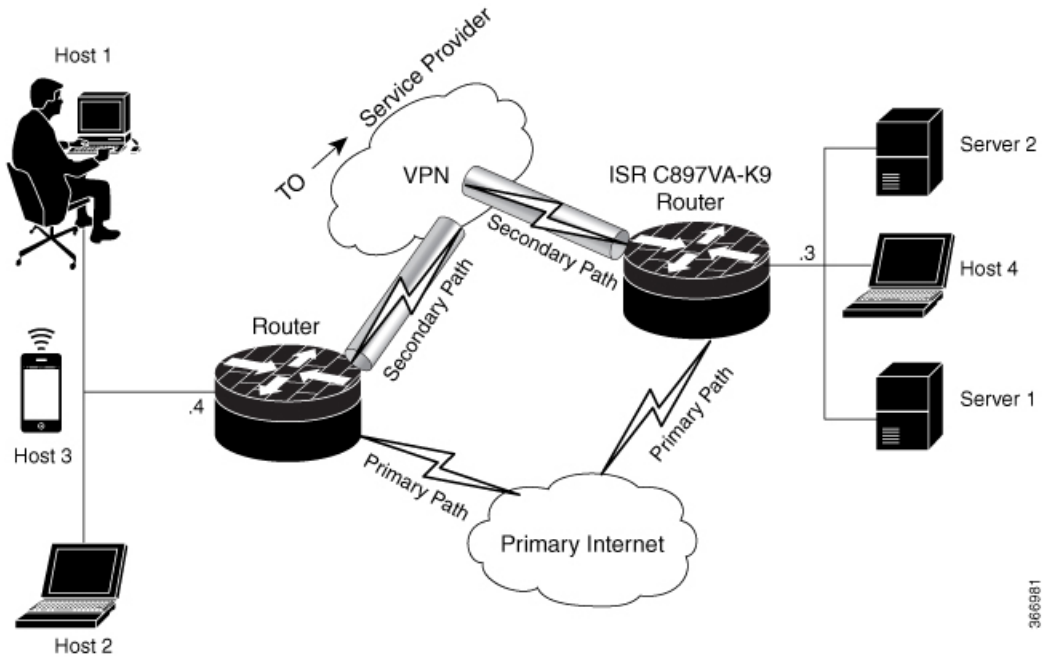
機能一覧

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。

サポートされるプラットフォーム

VPN SIP 機能は次のプラットフォームでサポートされています。

第 2 世代 Cisco サービス統合型ルータ（ISR G2）800 シリーズ プラットフォーム

- C819H-K9
-
- C841M-8X-JAIS/K9
- C881-K9
-
- C891FJ-K9
- C891-24X/K9
- C892FSP-K9
- C897VA-K9
- C899G-LTE-JP-K9
- C899G-LTE-LA-K9
- C819G-LTE-LA-K9
- C819GW-LTE-LA-QK9

VPN SIP の前提条件

- 第 2 世代 Cisco サービス統合型ルータ（ISR G2）800 シリーズ ルータには、Cisco IOS 15.7(3)M1 ソフトウェアをインストールする必要があります。
- 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。
- Cisco ISR G2 ルータでサポートされている VPN SIP 機能のスケールは、8 セッションです。
- 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 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。

   a 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
```

b 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
```

c 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 **a** 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
```

b 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 の設定を完了するには、 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。

（注） LAN 側インタ フェースは、ルーターの ISRG2 インターフェイスに接続されます。

```
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、VPN SIP 用の sVTI 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、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 静的デフォルト 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 0.0.0.0 0.0.0.0 Tunnel0 track 1
ip route 0.0.0.0 0.0.0.0 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* コマンドにより、SIP コールに使用されるローカルの SIP 番号、および関連付けられる IPv4 アドレスが設定されます。

（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** コマンドを使用すると、セッションの開始、ダウン、失敗などのイベントに関する VPN SIP モジュールのシステム ロギングを有効化できます。

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
```

リモート ルータの VPN SIP の確認

リモート ルータの VPN SIP 登録ステータスの確認

```
Peer2# show vpn-sip registration-status
 SIP registration of local number 0388882001 : registered 10.6.6.49
```

リモート ルータの VPN SIP レジストラの確認

```
Peer2# show vpn-sip sip registrar
Line          destination      expires(sec)  contact    transport    call-id
==========================================================================================
0388882001    example.com    2478         10.6.6.49   UDP
E6F23809-9EAB11E7-80029279-40B97F59
```

リモート ルータの VPN SIP セッションに関する詳細の確認

```
Peer2# show vpn-sip session detail
VPN-SIP session current status
Interface: Tunnel1
   Session status: SESSION_UP (R)
   Uptime        : 00:00:21
   Remote number : 0388882001 =====> This is the Peer1 Router's SIP number
   Local number  : 0388881001 =====> Local router's SIP number
   Remote address:port: 10.6.6.50:50001
   Local address:port : 10.6.6.49:50002
   Crypto conn handle: 0x8000017E
   SIP Handle        : 0x800000BE
   SIP callID        : 1556
   Configured/Negotiated bandwidth: 1000/64 kbps
```

リモート ルータの暗号化セッションに関する詳細の確認

```
Peer2 #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: 00:02:32
Session status: UP-ACTIVE
Peer: 10.6.6.50 port 50001 fvrf: (none) ivrf: (none)
      Phase1_id: 10.6.6.50
      Desc: (none)
  Session ID: 147
  IKEv2 SA: local 10.17.1.1/4500 remote 10.6.6.50/50001 Active
          Capabilities:S connid:1 lifetime:23:57:28 ====> 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 4 drop 0 life (KB/Sec) 4293728/3448
        Outbound: #pkts enc'ed 6 drop 0 life (KB/Sec) 4293728/3448
```

リモート ルータの IP NAT 変換の確認

```
Peer2#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 3.3.3.3:4500       10.6.6.49:50002    10.6.6.50:50001    10.6.6.50:50001
```

VPN SIP の設定例

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 アドレスを設定します。

```
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 *1*：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。

コマンド名	説明
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。
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。

コマンド名	説明
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

関連資料

関連項目	参照先
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

標準および RFC

標準/RFC	役職（Title）
RFC 6193（制約事項付き）	Session Description Protocol（SDP）でのインターネットキーエクスチェンジ プロトコル（IKE）に関するメディアの説明

VPN SIP の機能情報

表 *2*：*VPN SIP* の機能情報

機能名（**Feature Name**）	リリース	機能情報
Session Initiation Protocol トリガー VPN	Cisco IOS リリース 15.7(3)M1	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。 **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** の各コマンドが導入されました。