FlexVPN スポークツースポークの設定

最新版発行日：2014 年 3 月 28 日

FlexVPN スポークツースポーク機能によって、FlexVPN クライアントは、仮想トンネル インターフェイス（VTI）、インターネット キー エクスチェンジ バージョン 2（IKEv2）、および Next Hop Resolution Protocol（NHRP）を活用して別の FlexVPN クライアントと直接の暗号トンネルを確立し、スポークツースポーク接続を構築することができます。

FlexVPN スポーク間の前提条件

IKEv2、FlexVPN サーバー、および FlexVPN スポークを設定する必要があります。

FlexVPN スポーク間に関する情報

FlexVPN および NHRP

FlexVPN は、シスコによる IKEv2 標準の実装であり、サイトツーサイト、リモートアクセス、ハブ アンド スポーク トポロジ、および部分メッシュ（スポークツースポーク ダイレクト）を組み合わせたユニファイド パラダイムと CLI を備えています。FlexVPN は、トンネル インターフェイス パラダイムを広範に使用し、かつ暗号マップを使用してレガシー VPN 実装との互換性を維持するシンプルなモジュラ フレームワークを提供します。

FlexVPN サーバーは、FlexVPN のサーバー側機能を提供します。FlexVPN クライアントは、FlexVPN クライアントと別の FlexVPN サーバーの間にセキュアな IPsec VPN トンネルを確立します。

NHRP は、Address Resolution Protocol（ARP）のようなプロトコルで、ノンブロードキャストマルチアクセス（NBMA）ネットワークの問題を軽減します。NHRP を使用すると、NBMA ネットワークに接続されている NHRP は、ネットワークの一部である他のエンティティの NBMA アドレスを動的に学習します。このため、これらのエンティティは、トラフィックに中間ホップを使用せずに直接通信できるようになります。

FlexVPN スポークツースポーク機能は、NHRP と FlexVPN クライアント（スポーク）を統合して、既存の FlexVPN ネットワークにある別のクライアントとの直接の暗号化チャネルを確立します。接続は、仮想トンネル インターフェイス（VTI）、IKEv2、および NHRP を使用して構築されます。ここで、NHRP はネットワーク内の FlexVPN クライアントの解決に使用されます。

FlexVPN では、次のことが推奨されます。

- ルーティング エントリは、スポーク間で交換されません。
- 異なるプロファイルがスポークに使用され、**config-exchange** コマンドはスポーク用に設定されません。

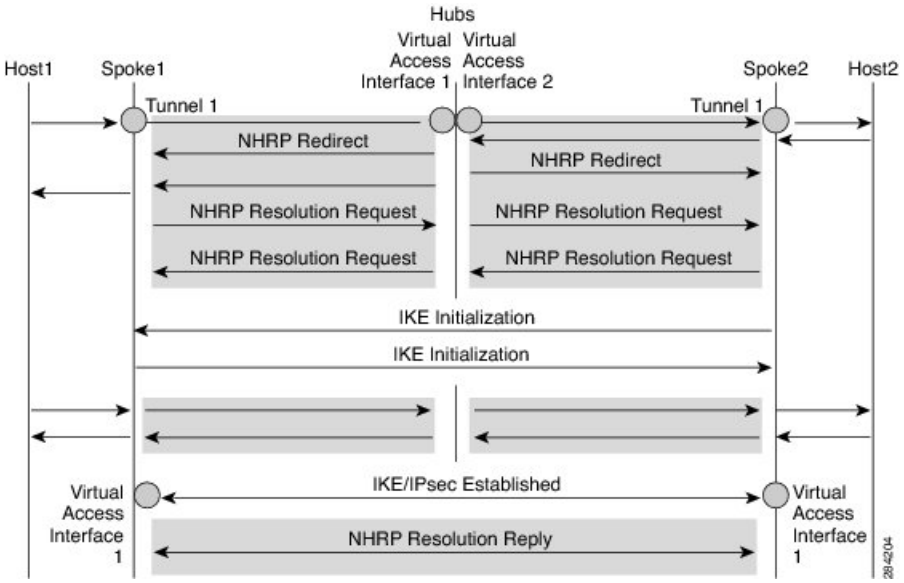
FlexVPN IPv6 ダイレクト スポーク間機能は、FlexVPN スポークに対する IPv6 アドレスの使用をサポートします。IPv6 アドレスのサポートにより、IPv6 over IPv4、IPv4 over IPv6、および IPv6 over IPv6 の転送がサポートされます。

（注） スポーク間 FlexVPN は、ダイナミック AAA 認証をサポートしていません。

NHRP 解決要求と FlexVPN の応答

次の図は、NHRP 解決要求と FlexVPN の応答を示します。

図 *1 : NHRP* 解決要求と応答



双方向のトラフィックにより、同様のイベントが、Spoke1、Spoke2、およびハブの両方向で発生します。明確にするために、Host1 から Host2 へのイベントについて説明します。Spoke1 と Spoke2 の背後にある別のネットワーク N2（192.168.2.0/24）の後に、ネットワーク N1（192.168.1.0/24）があると仮定します。2つのスポーク間のネットワークは、アクセス コントロール リスト（ACL）によって照合されます。これは、両方のスポークの IKEv2 ポリシーに ACL が適用されるためです。

両方のスポークからのプレフィックス情報と共に、ネットワークはIKEv2情報のペイロード交換によってハブに伝達されます。ハブの IKEv2 によるルーティング テーブルへのルート追加が、次のように発生します。

- 192.168.1.0/24：Virtual Access Interface1 から接続される
- 192.168.2.0/24：Virtual Access Interface2 から接続される

このハブは IKEv2 から両方のスポークへ集約ルートをプッシュし、スポークはそれらのルーティング テーブルにこのルートをインストールします。次のようになります。

- 192.168.0.0/16：ネクスト ホップ <ハブのトンネル アドレス> - Interface Tunnel 1

（注） また、ルーティング プロトコルは、ルーティング テーブルにルートを追加できます。

N1 から N2 へトラフィックが移動すると仮定すると、トラフィック フローは次のとおりです。

1. Host1 は、Host2 宛てのトラフィックを送信します。トラフィックは Spoke1 の LAN インターフェイスに到達し、ルートを検索し、集約ルートを見つけて、パケットを Interface Tunnel 1 にルーティングします。
2. トラフィックがハブの Virtual Access Interface1 に到達すると、トラフィックは、Virtual Access Interface2 から直接接続するか、ポイントツーポイントのトンネル インターフェイスを使用する、N2 のルート エントリ用のルート テーブルを検索します。
3. Host1 から Host2 へのトラフィックは、Virtual Access Interface1 と Virtual Access Interface2 を経由してハブを通過します。このハブは、入力インターフェイスおよび出力インターフェイス（Virtual Access Interface1 と Virtual Access Interface2）が同じ NHRP ネットワーク（両方のインターフェイスで設定されたネットワーク D）に属することを判断します。ハブは NHRP リダイレクト メッセージを Virtual Access Interface1 の Spoke1 に送信します。
4. リダイレクトを受信すると、Spoke1 は Host2 への解決要求をポイントツーポイント トンネル インターフェイス（リダイレクトを受信したのと同じインターフェイス）を経由して開始します。解決要求は、ルーティング パス（Spoke1-hub-spoke2）を通過します。解決要求を受信すると、Spoke2 は、それが出力点であり、その解決要求に応答する必要があることを判断します。
5. Spoke2 はトンネル インターフェイスの解決要求を受信し、トンネル インターフェイスから仮想テンプレート番号を取得します。仮想テンプレート番号を使用して、仮想アクセス インターフェイスを作成し、暗号チャネルを開始し、IKEv2 と IPSec のセキュリティ アソシエーション（SA）を確立します。2 つのスポーク間に暗号 SA が確立されると、Spoke2

は Spoke1 に必要な NHRP キャッシュ エントリとそのネットワークを、新しく作成した仮想アクセス インターフェイス以下に設置し、その仮想アクセス インターフェイスを介して解決の応答を送信します。

6. 仮想アクセス インターフェイスから解決要求を受信した後、Spoke1 は Spoke2 に必要なキャッシュ エントリとそのネットワークを設置します。また、Spoke1 は、ハブを示す一時キャッシュ エントリを削除し、Tunnel Interface1 以下のネットワークを解決します。
7. NHRP は、ネクスト ホップ上書き（NHO）または H ルートとしてショートカット ルートを追加します。ショートカット スイッチングの詳細については、「DMVPN ネットワークにおける NHRP のショートカット スイッチング拡張」を参照してください。

FlexVPN スポークツースポークの設定方法

FlexVPN サーバーの仮想トンネル インターフェイスの設定

始める前に

FlexVPN サーバーとクライアントを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered loopback** *number*
5. 次のいずれかを実行します。
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. **ip nhrp redirect** [**timeout** *seconds*]
7. **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** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 1 type tunnel`	仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレートインターフェイスを作成します。
ステップ 4	**ip unnumbered loopback** *number* 例： `Device(config-if)# ip unnumbered loopback 0`	既存インターフェイス（通常はループバック インターフェイス）の IP アドレスを仮想トンネル インターフェイスに割り当てます。

ステップ 5	次のいずれかを実行します。
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	例：
	`Device(config-if)# ip nhrp network-id 1`
	例：
	`Device(config-if)# ipv6 nhrp network-id 1`
		インターフェイスで NHRP を有効にします。

ステップ 6	**ip nhrp redirect** [**timeout** *seconds*] 例： `Device(config-if)# ip nhrp redirect`	トラフィックが NHRP ネットワークで転送されている場合、リダイレクト トラフィック通知を有効にします。重複するリダイレクトを送信しないようにするには、**timeout** キーワードと *seconds* 引数を使用して、作成したリダイレクト エントリの有効期限を指定します。
ステップ 7	**exit** 例： `Device(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、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポークの NHRP ショートカットの設定

このタスクを実行して、FlexVPN スポークのトンネル インターフェイスで NHRP ショートカットを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. 次のいずれかを実行します。
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*
5. **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** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface tunnel** *number* 例： `Device(config)# interface tunnel 1`	FlexVPN クライアント 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。

ステップ 4	次のいずれかを実行します。
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	例：
	`Device(config-if)# ip nhrp shortcut 1`
	例：
	`Device(config-if)# ipv6 nhrp shortcut 1`
		FlexVPN クライアントのトンネル インターフェイスで NHRP ショートカットを有効にします。これは、スポーク間トンネルの確立に必要です。この設定で指定する仮想テンプレート番号と、「FlexVPN スポークの仮想トンネル インターフェイスの設定 （6 ページ）」タスクで指定する仮想テンプレート番号は同じにする必要があります。

ステップ 5	**exit** 例： `Device(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、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポークの仮想トンネル インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type tunnel**
4. **ip unnumbered tunnel** *number*
5. 次のいずれかを実行します。
   - **ip nhrp network-id** *number*
   - **ipv6 nhrp network-id** *number*
6. 次のいずれかを実行します。
   - **ip nhrp shortcut** *virtual-template-number*
   - **ipv6 nhrp shortcut** *virtual-template-number*

7. **ip nhrp redirect** [**timeout** *seconds*]
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** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface virtual-template** *number* **type tunnel** 例： `Device(config)# interface virtual-template 1 type tunnel`	仮想アクセス インターフェイスの作成時にダイナミックに設定および適用される仮想テンプレート インターフェイスを作成します。
ステップ 4	**ip unnumbered tunnel** *number* 例： `Device(config-if)# ip unnumbered tunnel 1`	FlexVPN トンネル インターフェイスの IPv4 アドレスを仮想トンネル インターフェイスに割り当てます。

ステップ 5	次のいずれかを実行します。
	• **ip nhrp network-id** *number*
	• **ipv6 nhrp network-id** *number*
	例：
	`Device(config-if)# ip nhrp network-id 1`
	例：
	`Device(config-if)# ipv6 nhrp network-id 1`
		インターフェイスで NHRP を有効にします。

ステップ 6	次のいずれかを実行します。
	• **ip nhrp shortcut** *virtual-template-number*
	• **ipv6 nhrp shortcut** *virtual-template-number*
	例：
	`Device(config-if)# ip nhrp shortcut 1`
	例：
	`Device(config-if)# ipv6 nhrp shortcut 1`
		インターフェイスでNHRP ショートカット スイッチングを有効にします。
		（注） 現在の仮想テンプレート番号を指定する必要があります。仮想テンプレート番号は、FlexVPN クライアント トンネル インターフェイスの設定と同じにする必要があります。

ステップ 7	**ip nhrp redirect** [**timeout** *seconds*] 例： `Device(config-if)# ip nhrp redirect`	仮想トンネルインターフェイスでNHRP のリダイレクトを有効化します。ネットワークがあるスポークから別のスポークに移動する場合は、これが便利です。

	コマンドまたはアクション	目的
		• 重複するリダイレクトを送信しないようにするには、**timeout** キーワードと *seconds* 引数を使用して、作成したリダイレクトエントリの有効期限を指定します。
ステップ 8	**exit** 例： `Device(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、グローバル コンフィギュレーション モードに戻ります。

FlexVPN スポーク設定の確認

FlexVPN スポークの設定を確認するには、次のコマンドを使用します。

手順の概要

1. **show crypto ikev2 client flexvpn**
2. **show ipv6 route**
3. **show ipv6 nhrp**

手順の詳細

ステップ 1 show crypto ikev2 client flexvpn

例：

```
Device# show crypto ikev2 client flexvpn

  Profile : flexblk
  Current state:ACTIVE
  Peer : 4001::2000:1
  Source : Ethernet0/0
  ivrf : IP DEFAULT
  fvrf : IP DEFAULT
  Backup group: None
  Tunnel interface : Tunnel0
```

FlexVPN サーバーおよびクライアント間の FlexVPN 接続ステータスが表示されます。

ステップ 2 show ipv6 route

例：

```
Device# show ipv6 route

IPv6 Routing Table - default - 15 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       l - LISP
```

```
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   3001::/112 [0/0]
     via Tunnel0, directly connected
S   3001::1/128 [2/0], tag 1
     via 3001::1, Virtual-Access1 [Shortcut]
     via Virtual-Access1, directly connected
L   3001::2/128 [0/0]
     via Tunnel0, receive
S   3001::3/128 [2/0], tag 1
     via Tunnel0, directly connected
C   4001::2000:0/112 [0/0]
     via Ethernet0/0, directly connected
L   4001::2000:3/128 [0/0]
     via Ethernet0/0, receive
S   5001::/64 [2/0], tag 1
     via Tunnel0, directly connected
C   5001::2000:0/112 [0/0]
     via Loopback0, directly connected
L   5001::2000:1/128 [0/0]
     via Loopback0, receive
D   5001::3000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
D   5001::4000:0/112 [90/28288000]
     via FE80::A8BB:CCFF:FE01:F400, Tunnel0
H   5001::4000:1/128 [250/1]
     via 3001::1, Virtual-Access1
C   5001::5000:0/112 [0/0]
     via Loopback1, directly connected
L   5001::5000:1/128 [0/0]
     via Loopback1, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

IPv6 ルートと Next Hop Resolution Protocol（NHRP）のマッピング情報が表示されます。

ステップ 3 show ipv6 nhrp

例：

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 172.17.1.9
    (Claimed NBMA address: 172.16.2.1)
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 172.17.2.10
```

例：

```
Device# show ipv6 nhrp

3001::1/128 via 3001::1
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router implicit rib nho
```

```
   NBMA address: 4001::2000:2
5001::4000:1/128 via 3001::1
   Virtual-Access1 created 00:00:56, expire 01:59:03
   Type: dynamic, Flags: router rib
   NBMA address: 4001::2000:2
5001::5000:1/128 via 3001::2
   Virtual-Access1 created 00:01:52, expire 01:58:14
   Type: dynamic, Flags: router unique local
   NBMA address: 4001::2000:3
```

NHRP キャッシュ エントリが表示されます。最初の例では、出力に、転送が IPv4（NBMA アドレス）であることが示されます。リモート スポークは、要求された NBMA アドレス フィールドが示すとおり、ネットワーク アドレス変換（NAT）下にあります。このアドレスはリモート スポークの NAT 前アドレスです。また、キャッシュ エントリには、各スポークと関連付けられたフラグが表示され、ルーティング テーブルで各エントリに挿入されたルートの種類が示されます。ネクストホップ上書き（NHO）は、ショートカット ルートを示します。*rib* フラグは、そのキャッシュ エントリに追加された NHRP H ルートを示します。2 番目の例は、転送が IPv6（NBMA アドレス）であることを示します。要求されたアドレスが出力にないため、リモート スポークは NAT 下にはありません。

FlexVPN スポーク設定のトラブルシューティングのヒント

FlexVPN スポーク設定をトラブルシューティングするいくつかのヒントを示します。

1. スポーク間の接続を確認します。
2. クライアント（スポーク）とサーバーの設定を確認します。
3. スポークの背後にあるリモート ホストの到達可能性を確認します。
4. ルートをアドバタイズするために使用される、ルーティング プロトコル設定を確認します。
5. IKEv2 と IPSec が正しく設定されていることを確認します。
6. スポークの NHRP ショートカット設定と、サーバー（ハブ）のリダイレクト設定を確認します。

問題	トラブルシューティングのヒント
スポークからハブへの接続は作成されません。	ハブで作成された仮想アクセス インターフェイスがないことが原因で、接続が作成されない場合があります。 • ハブとスポークの間の接続を確認します。 • **show crypto session** コマンドを使用して、ハブとスポークのセキュリティ アソシエーション（SA）の状態を確認します。 • SA がアクティブ（**show crypto session** コマンドで表示される）の場合、スポークの FlexVPN の状態を、 **show crypto ikev2 client flexvpn** コマンドの出力で確認します。

問題	トラブルシューティングのヒント
スポーク間トンネルは作成されません。	

問題	トラブルシューティングのヒント
	トラフィックは、スポーク間トンネルを開始するため、ハブ経由でスポークからスポークに送られる必要があります。 • ハブの設定で、NHRP リダイレクトが有効かどうかを確認します。 • スポークの設定で、NHRP ショートカットが有効になっているかどうかを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドを使用して、FlexVPN サーバー（ハブ）の設定で、ハブがトラフィック間接参照をスポークに送信するかどうかを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドを使用して、スポークがトラフィックを受信して、解決要求を送信したことを確認します。 • **show ip** [**ipv6**] **nhrp** コマンドを使用して、いずれかのスポークにリモート ホストとスポークの NHRP キャッシュ エントリがあることを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドをリモート スポークで使用して、解決要求を受信したことを確認します。 • **show crypto ikev2 sa** コマンドと **show crypto session** コマンドを使用して、スポークが解決要求を受信し、暗号セッションを開始したことを確認します。 • **show ip** [**ipv6**] **interface brief** コマンドを使用して、仮想アクセス インターフェイスが両方のスポークにあることを確認します。 • **show ip** [**ipv6**] **nhrp traffic** コマンドをスポークで使用して、解決応答が送信され、仮想アクセス インターフェイスのピアによって受信されたことを確認します。 • **show ip** [**ipv6**] **nhrp** コマンドを使用して、リモート ホストのための完全な NHRP キャッシュ エントリがすべてのスポークに存在することを確認します。 • **show ip** [**ipv6**] **route** コマンドを使用して、Hルートやネクストホップ上書き（NHO）ルートがあることを確認します。

FlexVPN スポークツースポークの設定例

例：FlexVPN スポーク間のスタティック ルーティングの設定

次の例では、FlexVPN サーバーおよび FlexVPN クライアントで IKE 伝播されるスタティック ルーティングを使用して、FlexVPN スポーク間を設定する方法を示します。次は、FlexVPN サーバーの設定です。

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
ip access-list standard flex-route
 permit any
```

次は、最初の FlexVPN クライアントの設定です。

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
```

```
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.110.0 0.0.0.255
```

次は、2 番目の FlexVPN クライアントの設定です。

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
```

```
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip access-list standard flex-route
 permit 192.168.120.0 0.0.0.255
```

例：FlexVPN スポーク間の BGP を使用するダイナミック ルーティングの設定

次の例では、FlexVPN サーバーおよび FlexVPN クライアントで BGP を使用する（ダイナミック ネイバー探索により）ダイナミック ルーティングを、FlexVPN スポーク間で設定する方法を示します。次は、FlexVPN サーバーの設定です。

```
hostname hub
!
crypto ikev2 authorization policy default
 pool flex-pool
 def-domain cisco.com
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn hub.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface Ethernet0/0
 ip address 10.0.0.100 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback0
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
ip local pool flex-pool 172.16.0.1 172.16.0.254
!
router bgp 65100
 bgp router-id 10.0.0.100
 bgp log-neighbor-changes
 bgp listen range 172.16.0.0/24 peer-group spokes
```

```
 neighbor spokes peer-group
 neighbor spokes remote-as 65100
 neighbor spokes transport connection-mode passive
 neighbor spokes update-source Loopback0
 !
 address-family ipv4
  neighbor spokes activate
  neighbor spokes default-originate
  neighbor spokes prefix-list no-default in
 exit-address-family
!
ip prefix-list no-default seq 5 deny 0.0.0.0/0
ip prefix-list no-default seq 10 permit 0.0.0.0/0 le 32
```

次は、最初の FlexVPN クライアントの設定です。

```
hostname spoke1
!
crypto ikev2 authorization policy default
 route set interface
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke1.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.110 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.110.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.110
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
```

```
  network 192.168.110.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

次は、2 番目の FlexVPN クライアントの設定です。

```
hostname spoke2
!
crypto ikev2 authorization policy default
 route set interface
 route set access-list flex-route
!
crypto ikev2 profile default
 match identity remote fqdn domain cisco.com
 identity local fqdn spoke2.cisco.com
 authentication local rsa-sig
 authentication remote rsa-sig
 pki trustpoint CA
 aaa authorization group cert list default default
 virtual-template 1
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel source Ethernet0/0
 tunnel destination 10.0.0.100
 tunnel protection ipsec profile default
!
interface Ethernet0/0
 ip address 10.0.0.120 255.255.255.0
!
interface Ethernet1/0
 ip address 192.168.120.1 255.255.255.0
!
interface Virtual-Template1 type tunnel
 ip unnumbered Tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 tunnel protection ipsec profile default
!
router bgp 65100
 bgp router-id 10.0.0.120
 bgp log-neighbor-changes
 neighbor hubs peer-group
 neighbor hubs remote-as 65100
 neighbor hubs update-source Tunnel0
 neighbor 172.16.1.1 peer-group hubs
 !
 address-family ipv4
  network 192.168.120.0
  neighbor 172.16.1.1 activate
 exit-address-family
```

FlexVPN スポーク間の設定に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference Commands A to C*』 • 『*Cisco IOS Security Command Reference Commands D to L*』 • 『*Cisco IOS Security Command Reference Commands M to R*』 • 『*Cisco IOS Security Command Reference Commands S to Z*』
ショートカット スイッチングの強化	『*Shortcut Switching Enhancements for NHRP in DMVPN Networks*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

FlexVPN スポーク間の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : FlexVPN* スポーク間の機能情報

機能名	リリース	機能情報
FlexVPN スポーク間		FlexVPN スポーク間機能では、FlexVPN クライアントは別の FlexVPN クライアントとの直接暗号チャネルを確立できます。この機能はVTI、IKEv2、およびNHRP を利用して、スポーク間接続を構築します。 この機能は、Cisco IOS Release 15.2(2)T で導入されました。 次のコマンドが導入または変更されました。 **ip unnumbered loopback0, tunnel source, tunnel mode gre ip, nhrp network-id, ip nhrp redirect, ip nhrp shortcut.**
FlexVPN IPv6 ダイレクト スポーク間		FlexVPN IPv6 ダイレクト スポーク間機能は、FlexVPN スポークに対する IPv6 アドレスの使用をサポートします。IPv6 アドレスのサポートにより、IPv6 over IPv4、IPv4 over IPv6、および IPv6 over IPv6 の転送がサポートされます。 次のコマンドが導入または変更されました。 **ipv6 nhrp shortcut.**

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。