FlexVPNソリューションの設定と確認

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

背景説明

- IKEv2とIKEv1
- 拡張性
- 主な特長
- ルーティング
- 認可ポリシー
- FlexVPNと他のテクノロジーの比較

ネットワーク図

設定

- サイト間FlexVPNの設定
  - ステップ1：ルータAの設定
  - ステップ2：ルータBの設定
  - 確認
- ハブアンドスポークFlexVPN
  - ステップ1：ハブの設定
  - ステップ2：スポークの設定
  - 確認
- スポーク間FlexVPN
  - ステップ1：ハブの設定
  - ステップ2：スポークAの設定
  - ステップ3：スポークBの設定
  - 確認

トラブルシューティング

はじめに

このドキュメントでは、Flex Virtual Private Network(VPN)環境について説明し、その機能を紹介して、各FlexVPNトポロジを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco IOSおよびCisco IOS XE
- インターネットキーエクスチェンジ(IKE)バージョン2
- IPSec（Internet Protocol Security）
- FlexVPN

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco IOS XEアムステルダム–17.3.6

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FlexVPNは、シスコが提供する多用途で包括的なVPNソリューションで、さまざまなタイプのVPN接続に対して統合フレームワークを提供するように設計されています。IKEv2(Internet Key Exchange version 2)プロトコルを基盤とするFlexVPNは、VPNの設定、管理、および導入を簡素化するように設計されており、一貫したツールセットを利用します。同じコマンドと設定手順をさまざまなVPNタイプ（サイト間、リモートアクセスなど）で適用できます。 この一貫性により、エラーが減少し、導入プロセスがより直感的になります。

IKEv2とIKEv1

FlexVPNは、AES(Advanced Encryption Standard)やSHA-256(Secure Hash Algorithm)などの最新の暗号化アルゴリズムをサポートするIKEv2を利用します。 これらのアルゴリズムは、強力な暗号化とデータ整合性を提供し、VPN経由で送信されるデータが傍受されたり改ざんされたりするのを防ぎます。

IKEv2は、IKEv1よりも多くの認証方式を提供します。事前共有キー(PSK)と証明書ベースの認証タイプおよびハイブリッド認証タイプに加えて、IKEv2では応答側がクライアント認証に拡張認証プロトコル(EAP)を使用できます。

FlexVPNでは、クライアント認証にEAPが使用され、ルータはリレーとして動作し、クライアントとバックエンドEAPサーバ（通常はRADIUSサーバ）の間でEAPメッセージを渡します。FlexVPNは、認証プロセスを保護するために、EAP-TLS、EAP-PEAP、EAP-PSKなどのさまざまなEAP方式をサポートしています。

次の表に、IKEv1機能とIKEv2機能の違いを示します。

	IKEv2	IKEv1
プロトコル確立メッセージ	4メッセージ	6メッセージ
EAPサポート	はい（2通の追加メッセージ）	いいえ

セキュリティアソシエーションのネゴシエーション	2通の追加メッセージ	3通の追加メッセージ
UDP 500/4500上で実行	Yes	Yes
NATトラバーサル(NAT-T)	Yes	Yes
再送信と確認応答の機能	Yes	Yes
ID保護、DoS保護メカニズム、およびPFS（完全転送秘密）を提供	Yes	Yes
次世代暗号のサポート	Yes	いいえ

拡張性

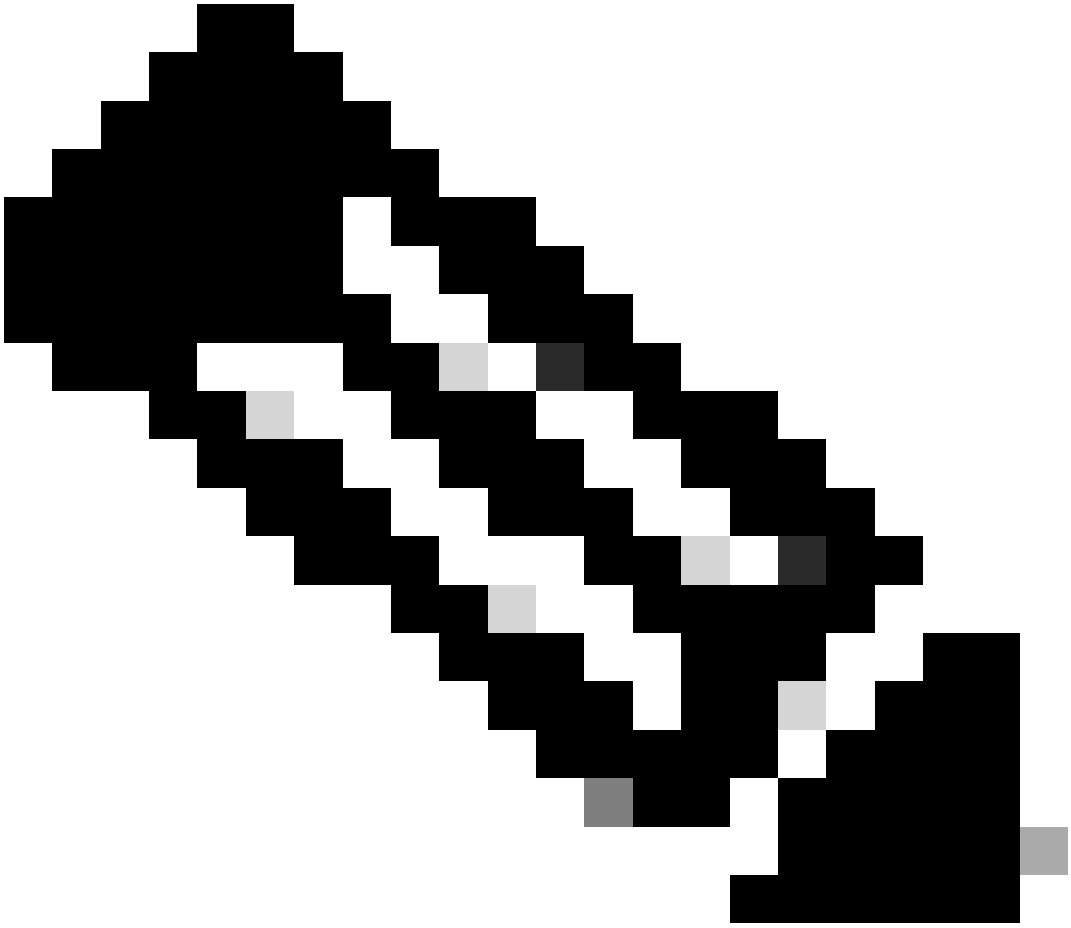
FlexVPNは、小規模なオフィスから大規模なビジネスネットワークまで簡単に拡張できます。これは、安全で信頼性の高いネットワークアクセスを必要とする、多数のリモートユーザを抱える組織にとって理想的な選択肢です。

主な特長

- 動的構成およびオンデマンドトンネル：
  - FlexVPN接続が開始されると、システムは事前設定されたテンプレートに基づいて仮想アクセスインターフェイスを生成します。このインターフェイスは、接続が確立されている間、トンネルエンドポイントとして機能します。トンネルが不要になると、仮想アクセスインターフェイスが切断され、システムリソースが解放されます。

- 柔軟な導入：
  - ハブアンドスポークモデル：中央のハブが複数のブランチオフィスに接続します。FlexVPNは、単一のフレームワークでこれらの接続のセットアップを簡素化し、大規模なネットワークに最適です。
  - フルメッシュおよび部分メッシュトポロジ：すべてのサイトが中央ハブを経由せずに直接通信できるため、遅延が減少し、パフォーマンスが向上します。

- 高可用性と冗長性：
  - 冗長ハブ：バックアップ用に複数のハブをサポートします。1つのハブに障害が発生すると、ブランチは別のハブに接続して、接続を継続できます。
  - ロードバランシング：複数のデバイスにVPN接続を分散し、1つのデバイスが過負荷になるのを防ぎます。これは、大規模な展開でパフォーマンスを維持するために不可欠です。



注：ハブ接続のロードバランシングの設定の詳細については、次のガイドを参照してください。

IKEv2ロードバランサの設定

- スケーラブルな認証と認可：
  - AAA統合：Cisco ISEやRADIUSなどのAAAサーバと連携して、大規模な使用に不可欠なユーザクレデンシャルとポリシーの一元管理を行います。
  - PKIと証明書：安全な認証のために公開キーインフラストラクチャ(PKI)とデジタル証明書をサポートします。これは、特に大規模な環境において、事前共有キーを使用するよりもスケーラブルです。

ルーティング

FlexVPNのルーティング機能は、拡張性を強化し、複数のVPN接続を効率的に管理し、それぞれの接続にトラフィックを動的にルーティングできるように設計されています。FlexVPNのルーティングを効率化する次の主要なコンポーネントとメカニズムは次のとおりです。

- バーチャルテンプレートインターフェイス：IPアドレスの割り当て、トンネルの送信元、IPsecの設定など、VPN接続に必要なすべての設定が含まれた設定テンプレートです。このインターフェイスでは、特定のIPアドレスをトンネルの送信元として設定する代わりに、通常はループバックからIPアドレスを「借りる」ようにip unnumberedコマンドを設定します。これにより、各スポークが同じテンプレートを使用できるようになり、各スポークが独自の送信元IPアドレスを使用できるようになります。

- バーチャルアクセスインターフェイス：バーチャルテンプレートインターフェイスから設定を継承する、動的に作成されたインターフェイスです。新しいVPN接続が確立されるたびに、仮想テンプレートに基づいて新しい仮想アクセスインターフェイスが作成されます。これは、各VPNセッションに固有のインターフェイスがあることを意味し、これにより管理と拡張が簡素化されます。

- ダイナミックルーティングプロトコル：OSPF、EIGRP、BGP over VPNトンネルなどのルーティングプロトコルと連携して動作します。これにより、ルーティング情報が自動的に更新されます。これは、大規模で動的なネットワークにとって重要です。

- IKEv2は、FlexVPNサーバがネットワーク属性をクライアントにプッシュできるようにすることで、ルートをアドバタイズします。クライアントは、トンネルインターフェイスにこれらのルートをインストールします。また、クライアントはコンフィギュレーションモードの交換時に自身のネットワークをサーバと通信し、両端でルートの更新を行うことができます。

- NHRP(Next Hop Resolution Protocol)は、パブリックIPアドレスをプライベートVPNエンドポイントにマッピングするためにハブアンドスポークトポロジで使用されるダイナミックアドレス解決プロトコルです。スポークが直接通信する他のスポークIPを検出できるようにする

認可ポリシー

FlexVPNのIKEv2許可ポリシーは、VPN接続のさまざまな側面を制御するように設定できます。IKEv2認可ポリシーは、ローカル認可ポリシーを定義し、ローカル属性とリモート属性の両方またはいずれかを含みます。

- VPNルーティングおよび転送(VRF)やQOSポリシーなどのローカル属性は、ローカルに適用されます。
- ルートなどのリモート属性は、コンフィギュレーションモードを介してピアにプッシュされます。
- ローカルポリシーを定義するには、crypto ikev2 authorization policyコマンドを使用します。
- IKEv2認可ポリシーは、IKEv2プロファイルからAAA authorizationコマンドを介して参照されます。

次の表に、IKEv2認可ポリシーで設定できる主要なパラメータの概要を示します。

項目	説明
[AAA]	AAAサーバとの統合により、ユーザクレデンシャルの検証、アクセスの許可、使用のアカウント

	設定を行います。ポリシーでは、検証をルータ上でローカルに実行するか、RADIUSサーバなどを介してリモートで実行するかを指定できます。
クライアントの設定	アイドルタイムアウト値、キープアライブ、DNSおよびWINSサーバの割り当てなどの構成設定をクライアントにプッシュします。
クライアント固有の設定	IDまたはグループメンバーシップに基づいて、異なるクライアントに異なる設定を許可します。
ルートセット	この設定では、特定のトラフィックがVPNトンネルを通過できます。これにより、接続が成功した場合にVPN Clientにプッシュされるルートインジェクションが実行されます。

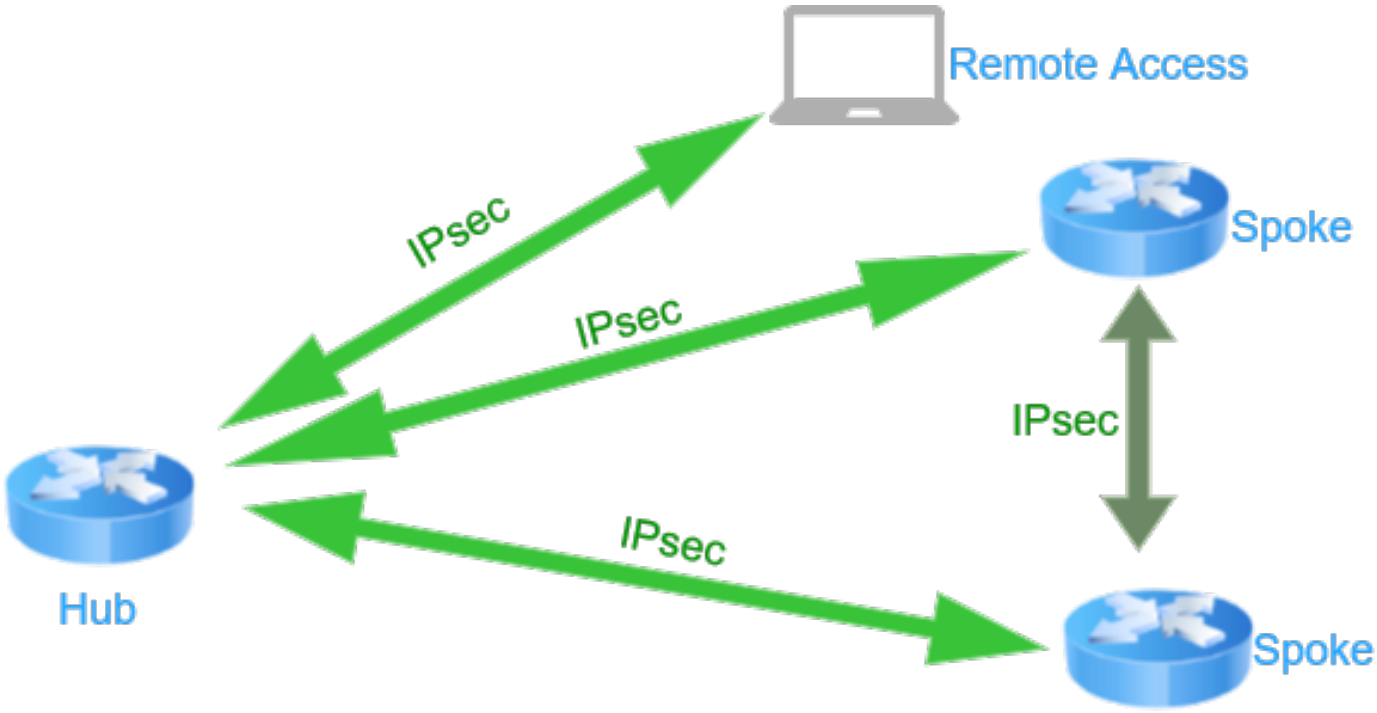
FlexVPNと他のテクノロジーの比較

FlexVPNは、現代のネットワーク環境にとって魅力的な選択肢となる幅広い利点を提供します。FlexVPNは、統合フレームワークを提供することで、設定と管理の簡素化、セキュリティの強化、拡張性のサポート、相互運用性の確保、および複雑さの軽減を実現します。

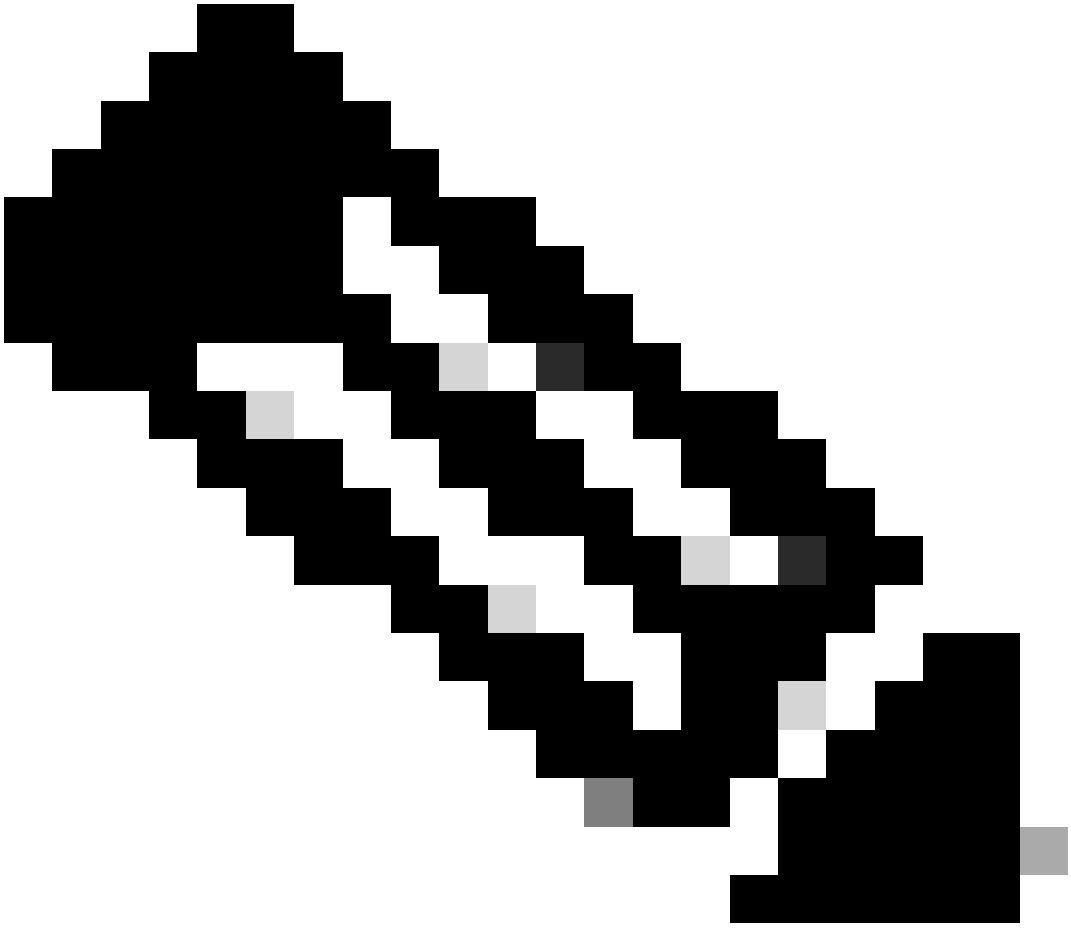
	Crypto Map	DMVPN	FlexVPN
ダイナミックルーティング	いいえ	Yes	Yes
動的なスポーク間ダイレクト	いいえ	Yes	Yes
リモート アクセス VPN	Yes	いいえ	Yes
設定のプッシュ	いいえ	いいえ	Yes
ピアツーピアの設定	いいえ	いいえ	Yes
ピアツーピアQos	いいえ	Yes	Yes
AAAサーバの統合	いいえ	いいえ	Yes

ネットワーク図

FlexVPNでは、デバイス間にトンネルを作成し、ハブとスポーク間の通信を確立できます。また、図に示すように、リモートアクセスVPNユーザのスポークと接続の間で直接通信するためのトンネルを作成することもできます。



FlexVPNダイアグラム



注：リモートアクセスVPNの設定は、このガイドでは取り上げていません。この設定の詳細については、次のガイドを参照してください。

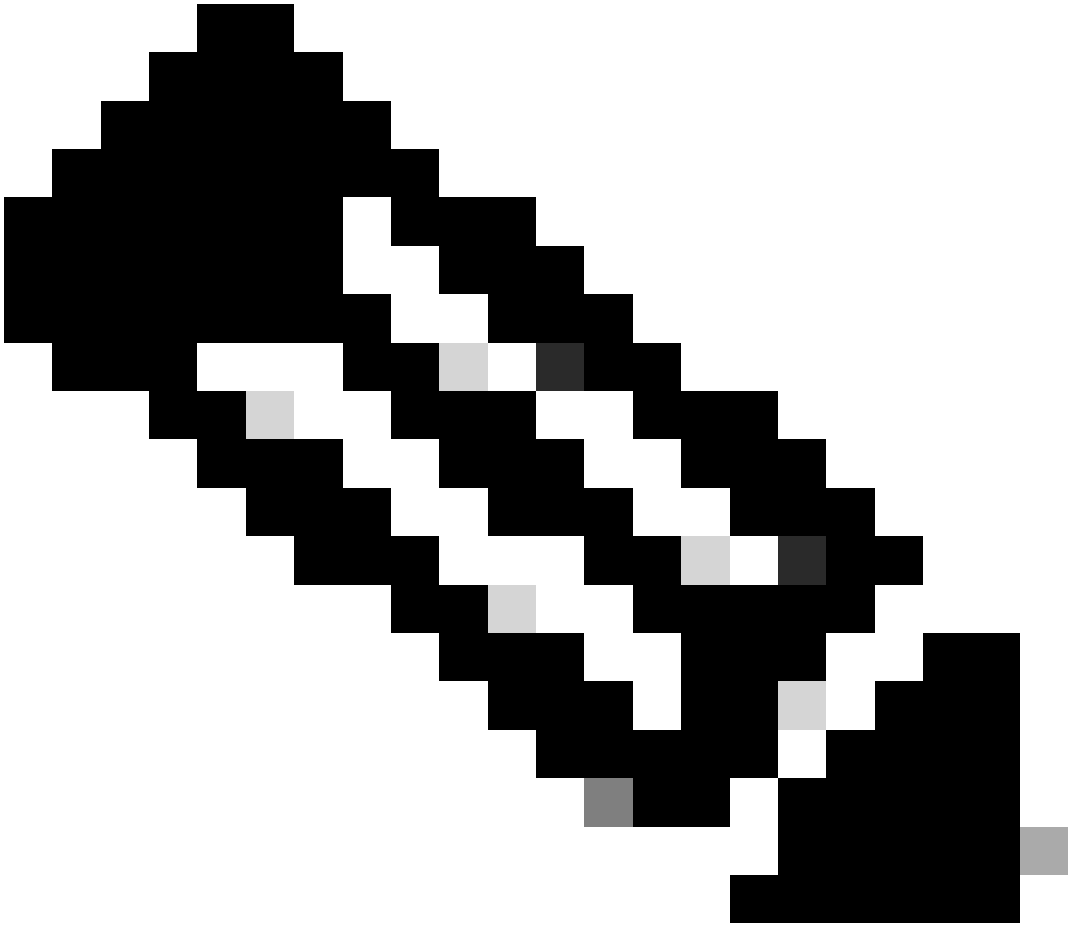
ローカルユーザデータベースを使用したセキュアクライアント(AnyConnect)IKEv2リモートアクセスのためのFlexVPNヘッドエンドの設定

設定

FlexVPNの特徴は、設定が簡単なことにあります。この単純さは、さまざまなタイプのVPNで使用される一貫した設定ブロックで明らかです。FlexVPNは、一般的に適用可能な単純な設定ブロックを提供し、トポロジの特定の機能または要件に応じてオプションの設定または追加の手順を使用できます。

- IKEv2プロポーザル：IKEv2セキュリティアソシエーション(SA)のネゴシエーションで使用されるアルゴリズムを定義します。 作成したら、ネゴシエーション中に選択されるように、このプロポーザルをIKEv2ポリシーに添付します。

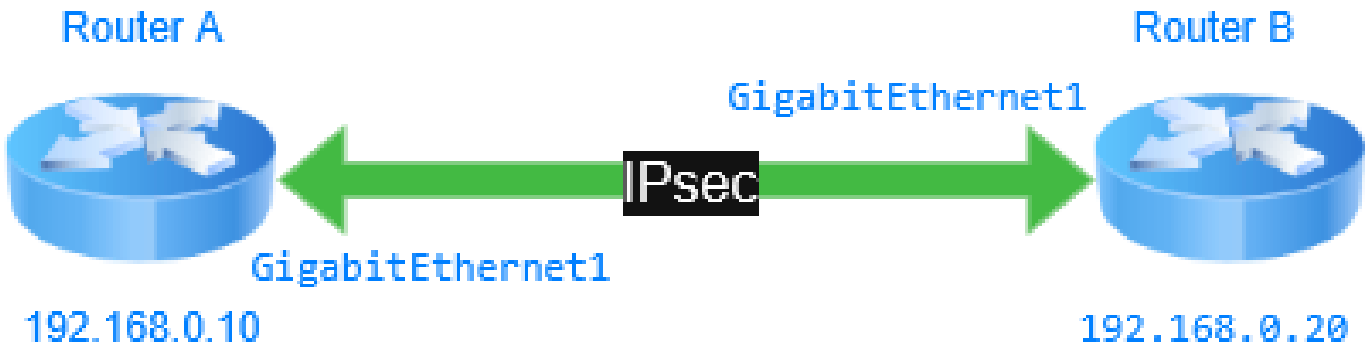
- IKEv2ポリシー：Virtual Routing and Forwarding(VRF)インスタンスまたはローカルIPアドレスにプロポーザルをリンクします。IKEv2プロポーザルへのポリシーリンク。
- IKEv2キーリング：事前共有キー(PSK)を指定します。ピア認証に使用する場合は非対称にできます。
- トラストポイント（オプション）：認証方式として公開キーインフラストラクチャ(PKI)を使用する場合、ピア認証のID属性と認証局(CA)属性を設定します。
- AAA統合（オプション）:FlexVPNは、Cisco ISE(Identity Services Engine)サーバやRADIUSサーバなどのAAAサーバを認証方式として統合します。
- IKEv2プロファイル：VPNピアアドレスや認証方式など、IKE SAのネゴシエートできないパラメータを格納します。デフォルトのIKEv2プロファイルがないため、IKEv2プロファイルを設定し、イニシエータのIPsecプロファイルに接続する必要があります。PSK認証が使用される場合、IKEv2プロファイルはIKEv2キーリングを参照します。PKI認証またはAAA認証方式が使用される場合、ここで参照されます。
- IPSecトランスフォームセット：IPSec SAで受け入れ可能なアルゴリズムの組み合わせを指定します。
- IPsecプロファイル：FlexVPNの設定を単一のプロファイルに統合し、インターフェイスに適用できます。このプロファイルは、IPsecトランスフォームセットとIKEv2プロファイルを参照します。



注：設定例では、事前共有キーを使用して、FlexVPNの設定と簡素化を簡単に示しています。事前共有キーは導入が簡単でトポロジが小さい場合に使用できますが、AAAまたはPKI方式はトポロジが大きい場合に適しています。

サイト間FlexVPNの設定

FlexVPNサイト間トポロジは、2つのサイト間の直接VPN接続用に設計されています。各サイトには、トラフィックが通過できるセキュアなチャネルを確立するトンネルインターフェイスが装備されています。この設定では、図に示すように、2つのサイト間で直接VPN接続を確立する方法について説明します。



Site_to_Site_ダイアグラム

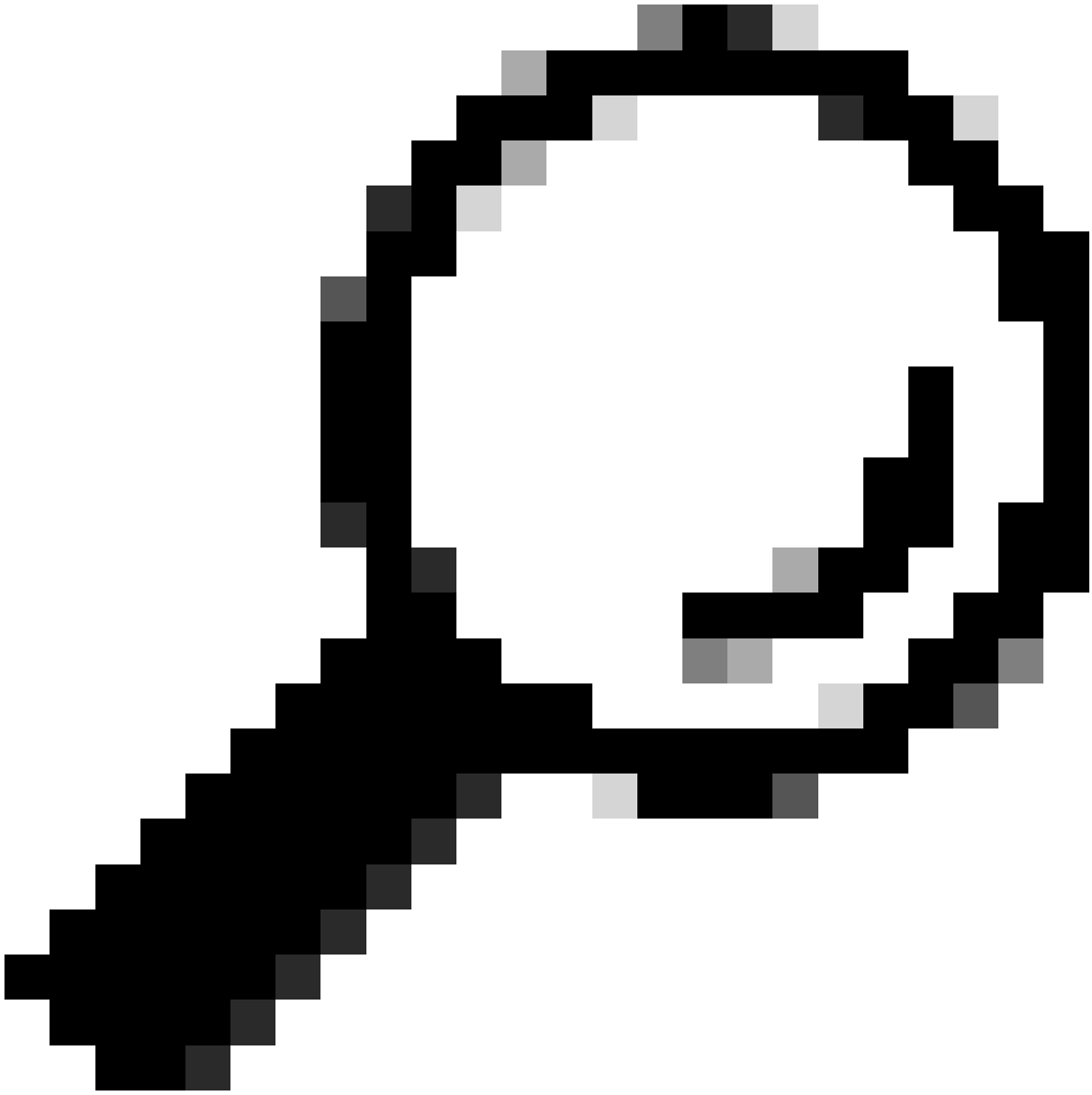
ステップ1：ルータAの設定

a. IKEv2プロポーザルとポリシーを定義します。

b.キーリングを設定し、ピアの認証に使用する事前共有キー(PSK)を入力します。

c. IKEv2プロファイルを作成し、キーリングを割り当てます。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



ヒント:**IKEv2 Smart Defaults**機能では、ほとんどの使用例をカバーしているため、FlexVPNの設定は最小限に抑えられています。**IKEv2**スマートデフォルトは、特定の用途に合わせてカスタマイズできますが、シスコではこの方法を推奨していません。

d. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

e. **IPsec**プロファイルを作成します。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
```

```
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f.トンネルインターフェイスを設定します。

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g.ダイナミックルーティングの設定 トンネルインターフェイスをアドバタイズします。その後、トンネルを通過する必要がある他のネットワークをアドバタイズできます。

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

ステップ2：ルータBの設定

a. IKEv2プロポーザルとポリシーを定義します。

b. キーリングを設定し、ピアの認証に使用する事前共有キーを入力します。

c. IKEv2プロファイルを作成し、キーリングを割り当てます。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

```
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

e. IPsecプロファイルを作成し、前に作成したIKEv2プロファイルとトランスフォームセットを割り当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. トンネルインターフェイスを設定します。

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g.トンネルインターフェイスをアドバタイズするようにダイナミックルーティングを設定します。その後、トンネルを通過する必要がある他のネットワークをアドバタイズできます。

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

確認

- show ip interface briefコマンドを使用してトンネルインターフェイスのステータスを確認し、トンネルがアップ/アップのステータスであることを確認します。

<#root>

RouterB#

show ip interface brief

Interface IP-Address OK? Method Status Protocol
GigabitEthernet1 192.168.0.20 YES NVRAM up up
Tunnel0 10.1.120.11 YES manual

up

up

1. show crypto ikev2 saコマンドを使用して、ルータ間にセキュアな接続が確立されていることを確認します。

<#root>

RouterB#

show crypto ikev2 sa

IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
2 192.168.0.20/500 192.168.0.10/500 none/none

READY

Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK

Life/Active Time: 86400/3139 sec

IPv6 Crypto IKEv2 SA

- show crypto ipsec saコマンドを使用して、encapカウンタとdecapsカウンタが増加していることを確認することにより、トラフィックが暗号化されており、トンネルを通過していることを確認します。

<#root>

```
RouterB#
show crypto ipsec sa


interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #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.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
```

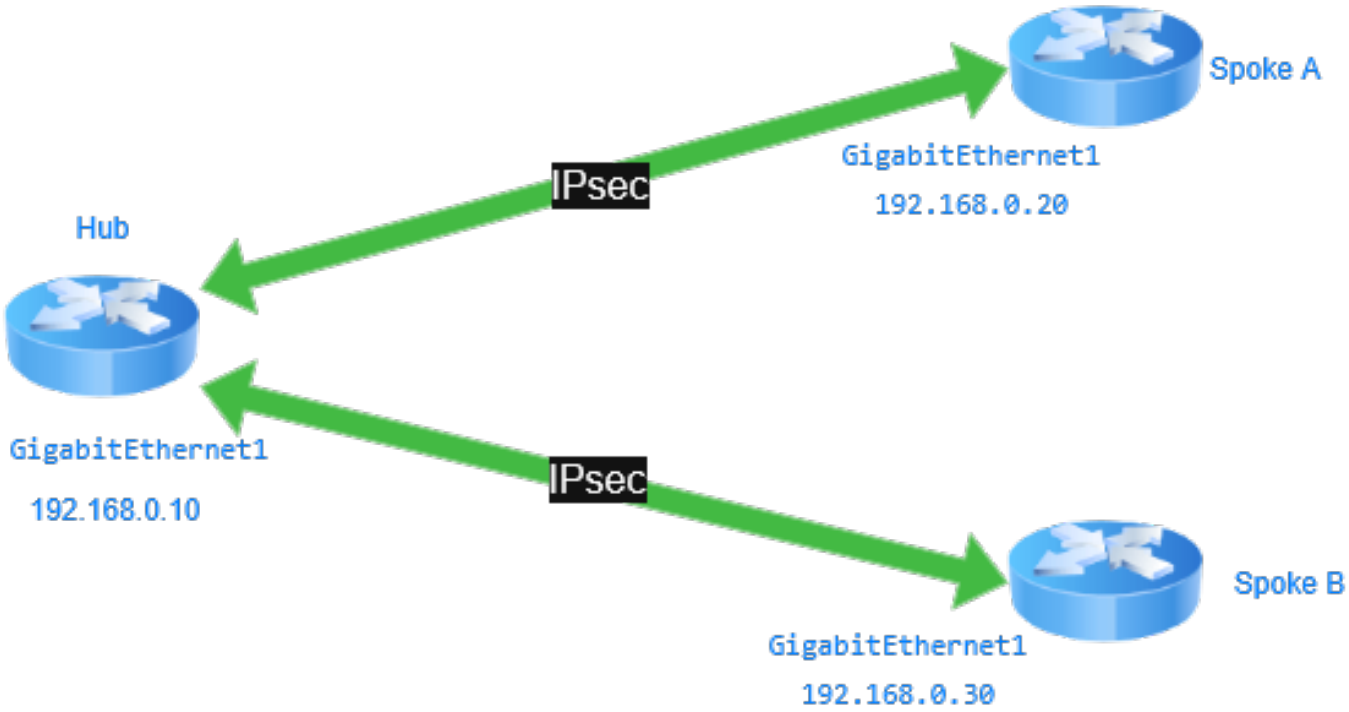
```
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0

sa timing: remaining key lifetime (k/sec): (4607991/3137)

         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)

      outbound ah sas:

      outbound pcp sas:
```

- show ip eigrp neighborsコマンドを使用して、EIGRPアジャセンシー関係が他のサイトと確立されていることを確認します。

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

ハブアンドスポークFlexVPN

ハブアンドスポークトポロジでは、複数のスポークルータが中央のハブルータに接続します。この設定は、スポークが主にハブと通信するシナリオに最適です。FlexVPNでは、通信効率を高めるためにダイナミックトンネルを設定できます。ハブはIKEv2ルーティングを使用してスポークルータにルートを配布し、シームレスな接続を確保します。 図に示すように、この設定では、ハブとスポークの間のVPN接続、および複数のスポークとの動的接続を確立するようにハブを設定する方法、さらにスポークを追加する機能について説明します。



Hub_and_Spoke_Diagram（ハブアンドスポーク図）

ステップ1：ハブの設定

a. IKEv2プロポーザルとポリシーを定義します。

b. キーリングを設定し、スポークの認証に使用する事前共有キー(PSK)を入力します。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.ハブルータでAAAサービスを有効にし、ローカルデバイス設定からのポリシーを指定するFlexAuthという名前のネットワーク認証リストを定義します。

```
!
aaa new-model
```

```
 aaa authorization network FlexAuth local
!
```

d. 10.1.1.2 ~ 10.1.1.254のアドレスを含むFlexPoolという名前のIPアドレスプールを定義します。このプールは、スポークのトンネルインターフェイスにIPアドレスを自動的に割り当てるために使用されます。

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. FlexTrafficという名前の標準IPアクセスリストを定義して、ネットワーク10.10.1.0/24を許可します。このACLは、トンネル経由でFlexVPNスポークに到達するために、スポークにプッシュされるネットワークを定義します。

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

アクセスリストとIPアドレスプールは、**IKEv2許可ポリシー**で参照されます。

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. IKEv2プロファイルを作成し、キーリングとAAA許可グループを割り当てます。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

h. IPsecプロファイルを作成し、IKEv2プロファイルと作成済みのトランスポートセットを割り当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. **virtual-template 1**を**type tunnel**として設定します。インターフェイスをIPアンナンバードアドレスとして参照し、**IPsec**プロファイルを

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

ステップ2：スポークの設定

a. IKEv2プロポーザルとポリシーを定義します。

b.キーリングを設定し、ハブに対する認証に使用される事前共有キー(PSK)を入力します。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.ハブルータでAAAサービスを有効にし、ローカルデバイス設定からのポリシーを指定する**FlexAuth**という名前のネットワーク認証リストを定義します。次に、IPアドレスとルートをFlexVPNスポークにプッシュするようにモードコンフィギュレーションポリシーを設定します。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. **FlexTraffic**という名前の標準IPアクセスリストを定義して、ネットワーク10.20.2.0/24を許可します。 このACLは、トンネルを通過するためにこのスポークによって共有されるネットワークを定義します。

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

アクセスリストは**IKEv2許可ポリシー**で割り当てられます。

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. IKEv2プロファイルを作成し、キーリングとAAA許可グループを割り当てます。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f.トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

g. IPsecプロファイルを作成し、前に作成したIKEv2プロファイルとトランスポートセットを割り

当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h.ネゴシエートされたIPアドレスのプロパティを使用してトンネルインターフェイスを設定します。このプロパティは、ハブ上で設定されたプールから取得されます。

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

確認

show ip interface briefコマンドを使用して、トンネル、バーチャルテンプレート、バーチャルアクセスのステータスを確認します。

- ハブでは、仮想テンプレートのステータスはアップ/ダウンで、これは正常です。仮想アクセスは、ハブとの接続を確立し、アップ/アップステータスを示すスポークごとに作成されます。
- スポークでは、トンネルインターフェイスがIPアドレスを受信し、up/upステータスを示しています。

<#root>

FlexVPN_HUB#

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
GigabitEthernet2       10.10.1.10      YES manual up               up
Loopback1              10.1.1.1        YES manual up               up

Virtual-Access1        10.1.1.1        YES unset  up               up
```

```
 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up


FlexVPN_Spoke#
```

show ip interface brief

```
Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up
```

Tunnel0 10.1.1.8 YES manual up up <<<<<<

```
The tunnel interface received an IP address from pool defined
```

- show crypto ikev2 saコマンドを使用して、ハブとスポーク間にセキュアな接続が確立されていることを確認します。

<#root>

```
FlexVPN_HUB#
```

show crypto ikev2 sa

```
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none
```

READY

```
 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec


 IPv6 Crypto IKEv2 SA
```

- show crypto ipsec saコマンドを使用して、encapカウンタとdecapsカウンタが増加していることを確認することにより、トラフィックが暗号化されており、トンネルを通過していることを確認します。

<#root>

```
FlexVPN_HUB#
```

show crypto ipsec sa

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
current_peer 192.168.0.20 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#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.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xAFC2F841(2948790337)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x7E780336(2121794358)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h

sa timing: remaining key lifetime (k/sec): (4607998/3010)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAFC2F841(2948790337)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-

```
sa timing: remaining key lifetime (k/sec): (4607998/3010)

         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- show ip routeコマンドを使用して、ルートがスポークにプッシュされたことを確認します。
  - 10.1.1.1/32のルートは、HUB設定のroute set interface文により、IKEv2設定ペイロードを介してプッシュされました。
  - 10.10.1.0/24のルートは、HUB設定のroute set access-list FlexTraffic文により、IKEv2設定ペイロードを介してプッシュされました。

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- pingコマンドを使用して、アドバタイズされたネットワークへの接続を確認します。

<#root>

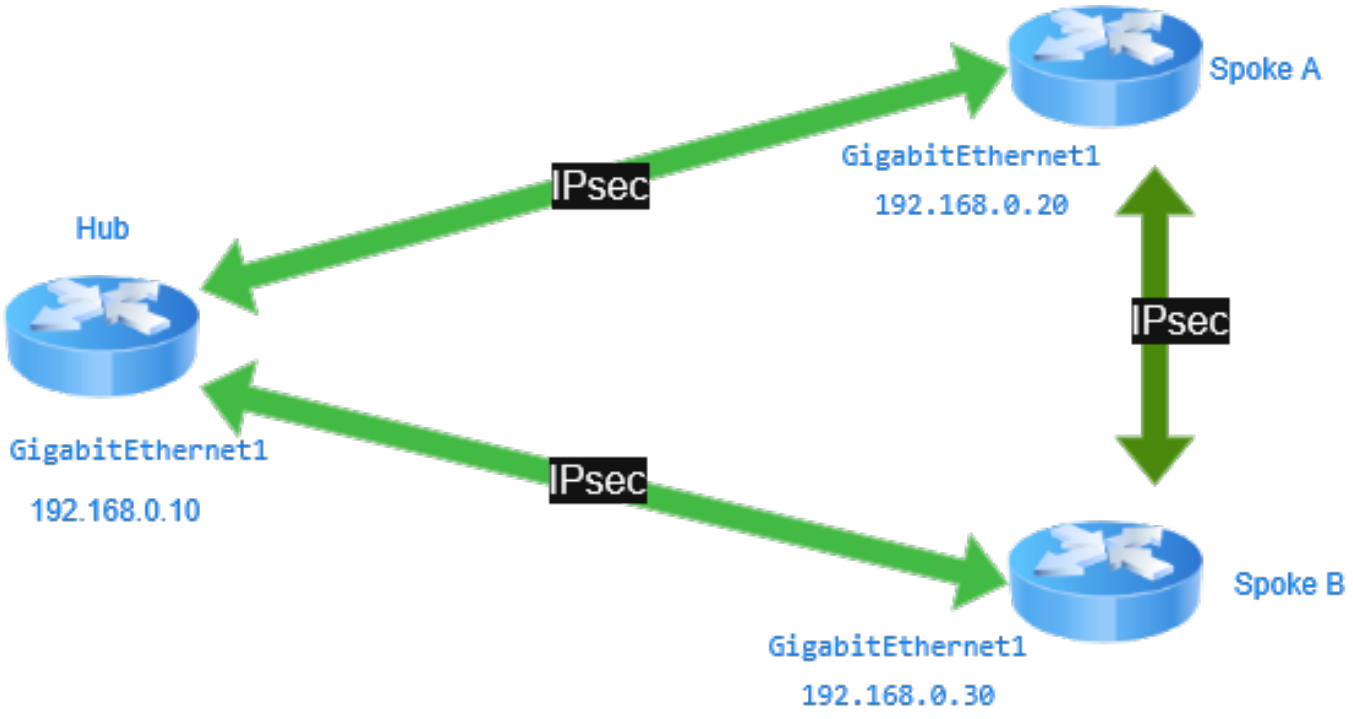
```
FlexVPN_HUB#
ping 10.20.2.20
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms



FlexVPN_Spoke#

ping 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

スポーク間FlexVPN

スポーク間接続を使用したハブアンドスポークトポロジでのFlexVPNは、動的でスケーラブル、かつセキュアなVPN通信を実現します。ハブは、NHRPがスポークが他のスポークのIPアドレスについてハブに照会できる中央集中型コントロールポイントとして機能します。これにより、スポーク間の直接IPsecトンネルが有効になり、効率的な通信と遅延の低減が可能になります。

ハブでは、**ip nhrp redirect**コマンドを使用して、スポークに対して直接スポーク間通信が可能であることを通知し、データプレーントラフィックのハブをバイパスすることでトラフィックフローを最適化します。スポークでは、**ip nhrp shortcut**コマンドにより、ハブからのリダイレクトを受信した後、他のスポークとの直接トンネルを動的に確立できます。この図は、ハブアンドスポーク間およびスポーク間の通信のトラフィックを参照しています。



スポーク間のダイアグラム

ステップ1：ハブの設定

a. IKEv2のポリシーとプロファイルを定義します。

b. キーリングを設定し、スポークの認証に使用する事前共有キー(PSK)を入力します。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.ハブルータでAAAサービスを有効にし、ローカルデバイス設定からのポリシーを指定する**FlexAuth**という名前のネットワーク認証リストを定義します。次に、IPアドレスとルートをFlexVPNスポークにプッシュするようにモード設定ポリシーを設定します。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. **FlexPool**という名前のIPアドレスプールを定義します。このプールには、10.1.1.2 ~ 10.1.1.254のアドレスが含まれています。 このプールは、スポークのトンネルインターフェイスにIPアドレスを自動的に割り当てるために使用されます。

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. FlexTrafficという名前の標準IPアクセスリストを定義して、ネットワーク10.0.0.0/8を許可します。このACLでは、ハブに接続されている他のスポークのネットワークを含め、FlexVPNスポークにプッシュされるネットワークを定義します。これにより、これらのネットワークに最初にハブを介して到達することが、スポークによって認識されます。

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

アクセスリストとIPアドレスプールは、**IKEv2**許可ポリシーで割り当てられます。

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. IKEv2プロファイルを作成し、キーリングとAAA許可グループを割り当てます。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

h. IPsecプロファイルを作成し、IKEv2プロファイルと作成済みのトランスポートセットを割り当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. **virtual-template 1**を**type tunnel**として設定します。インターフェイスを**IP**アンナンバードアドレスとして参照し、**IPsec** プロファイルを適用します。

ip nhrp

redirectコマンドは、ネットワークに到達するために他のスポークとの直接接続を確立するようにスポークに通知するために、仮想テンプレート上で設定されます。

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

ステップ2：スポークAの設定

a. IKEv2のポリシーとプロファイルを定義します。

b. キーリングを設定し、スポークの認証に使用する事前共有キー(PSK)を入力します。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.ハブルータでAAAサービスを有効にし、ローカルデバイス設定からのポリシーを指定する**FlexAuth**という名前のネットワーク認証リストを定義します。次に、IPアドレスとルートをFlexVPNスポークにプッシュするようにモードコンフィギュレーションポリシーを設定します。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. **FlexTraffic**という名前の標準IPアクセスリストを定義して、ネットワーク10.20.2.0/24を許可しま

す。 このACLは、トンネルを通過するためにこのスポークによって共有されるネットワークを定義します。

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

アクセスリストはIKEv2許可ポリシーで割り当てられます。

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. IKEv2プロファイルを作成し、キーリングとAAA許可グループを割り当てます。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

g. IPsecプロファイルを作成し、前に作成したIKEv2プロファイルとトランスポートセットを割り当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h.トンネルインターフェイスとvirtualtemplateを設定します。 **NHRP** ショートカットをサポートするために作成されたdVTIに対して**Virtual-Template1**を指定します。また、tunnel0をvirtual-templateの非番号アドレスとして設定します。

スポークで**ip nhrp shortcut**コマンドが設定され、ハブからのNHRPリダイレクトメッセージに基づいて、スポークが他のスポークへの直接トンネルを動的に確立できるようになります。

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

ステップ3：スポークBの設定

a. IKEv2のポリシーとプロファイルを定義します。

b. キーリングを設定し、スポークの認証に使用する事前共有キー(PSK)を入力します。

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c.ハブルータでAAAサービスを有効にし、ローカルデバイス設定からのポリシーを指定する

FlexAuthという名前のネットワーク認証リストを定義します。次に、IPアドレスとルートをFlexVPNスポークにプッシュするようにモード設定ポリシーを設定します。

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. **FlexTraffic**という名前の標準IPアクセスリストを定義して、ネットワーク10.30.3.0/24を許可します。 このACLは、トンネルを通過するためにこのスポークによって共有されるネットワークを定義します。

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

アクセスリストはIKEv2許可ポリシーで参照されます。

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. IKEv2プロファイルを作成し、キーリングとAAA許可グループを割り当てます。

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. トランスポートセットを作成し、データの保護に使用する暗号化アルゴリズムとハッシュアルゴリズムを定義します。

g. IPsecプロファイルを作成し、前に作成したIKEv2プロファイルとトランスポートセットを割り当てます。

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. トンネルインターフェイスと仮想テンプレートを設定します。NHRPショートカットをサポートするために作成されたdVTIに対して**Virtual-Template1**を指定します。また、tunnel0をvirtual-templateの非番号アドレスとして設定します。

スポークで**ip nhrp shortcut**コマンドが設定され、ハブからのNHRPリダイレクトメッセージに基づいて、スポークが他のスポークへの直接トンネルを動的に確立できるようになります。

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

確認

show ip interface briefコマンドを使用して、トンネル、バーチャルテンプレート、バーチャルアクセスのステータスを確認します。現在は、スポーク間の直接接続です。

- スポークでは、バーチャルテンプレートのアップ/ダウンステータスは正常です。アップ/アップ状態の接続用に仮想アクセスが作成されます。

```
<#root>

FlexVPN_Spoke#

show ip interface brief
```

```
Interface                  IP-Address      OK?  Method  Status                Protocol
GigabitEthernet1           192.168.0.30    YES  NVRAM   up                    up
GigabitEthernet2           10.20.2.20      YES  manual  up                    up

Tunnel0                    10.1.1.12       YES  manual  up                    up


Virtual-Access1            10.1.1.12       YES  unset   up                    up

Virtual-Template1          10.1.1.12       YES  unset   up                    down
```

- show crypto ikev2 saコマンドを使用して、各デバイス間でセキュアな接続が確立されていることを確認します。
- show crypto ipsec saコマンドを使用して、encapカウンタとdecapsカウンタが増加していることを確認することにより、トラフィックが暗号化されており、トンネルを通過していることを確認します。
- スポーク間のトラフィックのリダイレクションを確認するには、show ip nhrpコマンドを使用します。
  <#root>

```
FlexVPN_Spoke#

show ip nhrp


10.1.1.10/32 via 10.1.1.10
   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router nhop rib nho
   NBMA address: 192.168.0.30

10.30.3.0/24 via 10.1.1.10


   Virtual-Access1 created 00:00:13, expire 00:09:46
   Type:

dynamic

, Flags: router rib nho
   NBMA address: 192.168.0.30
```

show ip routeコマンドを使用して、ルートがスポークにプッシュされたことを確認します。

- Virtual-Access1インターフェイスに関連付けられている2つのルートは新しく、NHRPショートカットに関連付けられています。
- %文字は、ネクストホップの上書きを示します。

<#root>

```
FlexVPN_Spoke#sh ip route
```

```
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0
S  %     10.1.1.10/32 is directly connected, Virtual-Access1


C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2
S  %     10.30.3.0/24 is directly connected, Virtual-Access1


      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- pingコマンドを使用して、アドバタイズされたネットワークへの接続を確認します。

```
<#root>

FlexVPN_Spoke#

ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:

.!!!!


Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を紹介します。トンネルネゴシエーションプロセスをデバッグするには、次のコマンドを使用します。

```
debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
```

debug crypto ipsec states

NHRPデバッグは、スポーク間接続のトラブルシューティングに役立ちます。

debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。