FlexVPN クライアント ブロックによる冗長ハブ設計での FlexVPN スポークの設定例

内容

概要

このドキュメントでは、複数のハブを使用できるシナリオで、FlexVPN クライアント設定ブロックを使用して、FlexVPN ネットワーク内にスポーク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。

- FlexVPN
- Cisco のルーティング プロトコル

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 G2 シリーズのサービス統合型ルータ（ISR）
- Cisco IOS® バージョン 15.2M

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

冗長性のために、スポークを複数のハブに接続することが必要になる場合があります。スポーク側の冗長性によって、ハブ側でのシングル ポイント障害の発生しない継続的な運用が可能になります。

スポークの設定を使用する最も一般的な 2 つの FlexVPN 冗長ハブ設計は、次のとおりです。

- **2 つのクラウド アプローチ**：スポークに、両方のハブに常にアクティブな 2 つの別のトンネルがある。
- **フェールオーバー アプローチ**：スポークに、任意の時点で 1 つのハブを持つアクティブなトンネルがある。

両方のアプローチに特有の長所と短所がいくつかあります。

アプローチ	賛成論
2 つのクラウド	• 障害時の迅速なリカバリ（ルーティング プロトコル タイマーに基づく） • ハブ間のトラフィックを配信する可能性がより高い（両方のハブへの接続がアクティ め）
フェールオーバー	• 設定が容易（FlexVPN に組み込まれる） • 障害時にルーティング プロトコルに依存しない

このドキュメントでは、2 番目のアプローチについて説明します。

設定

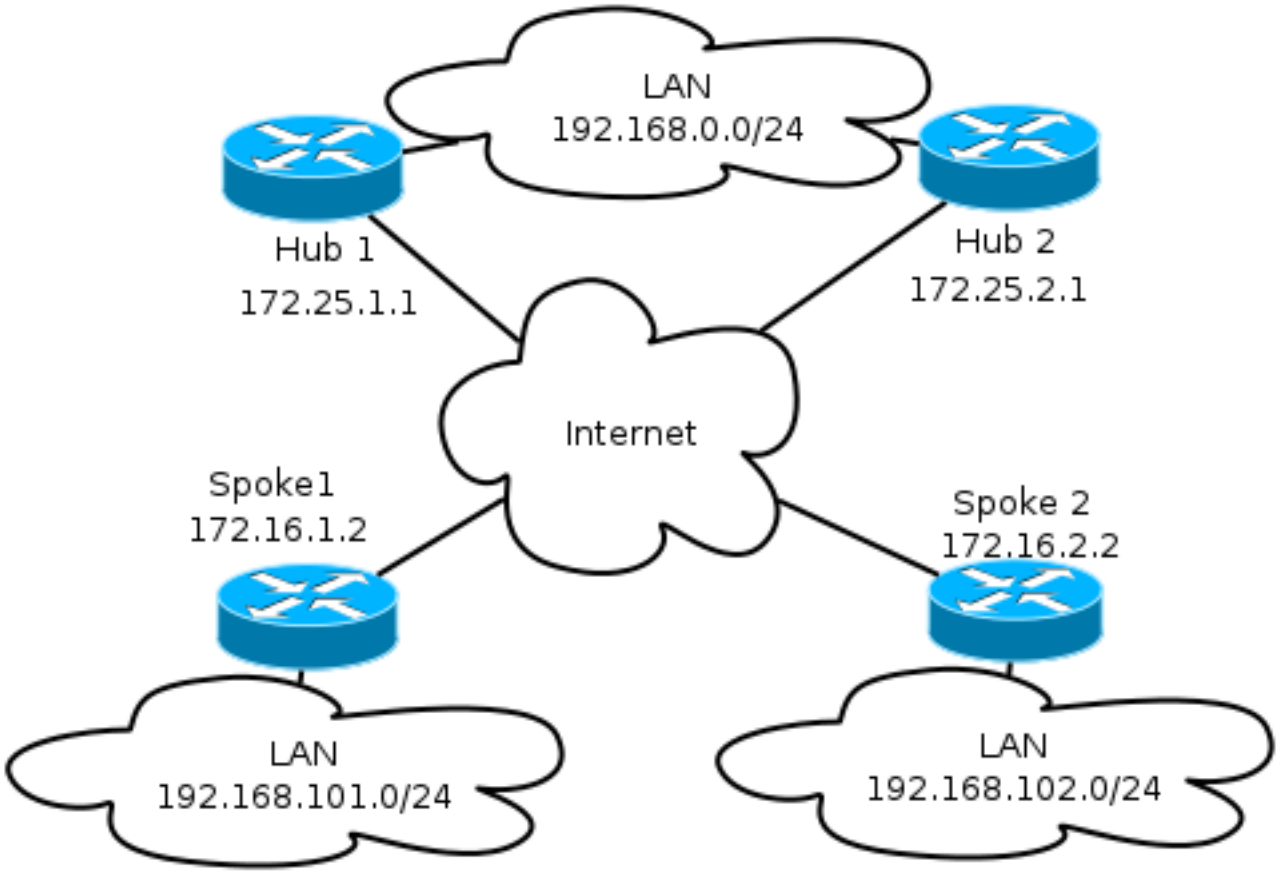
> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

次の各図には、トランスポートとオーバーレイのトポロジ図の両方が示されています。

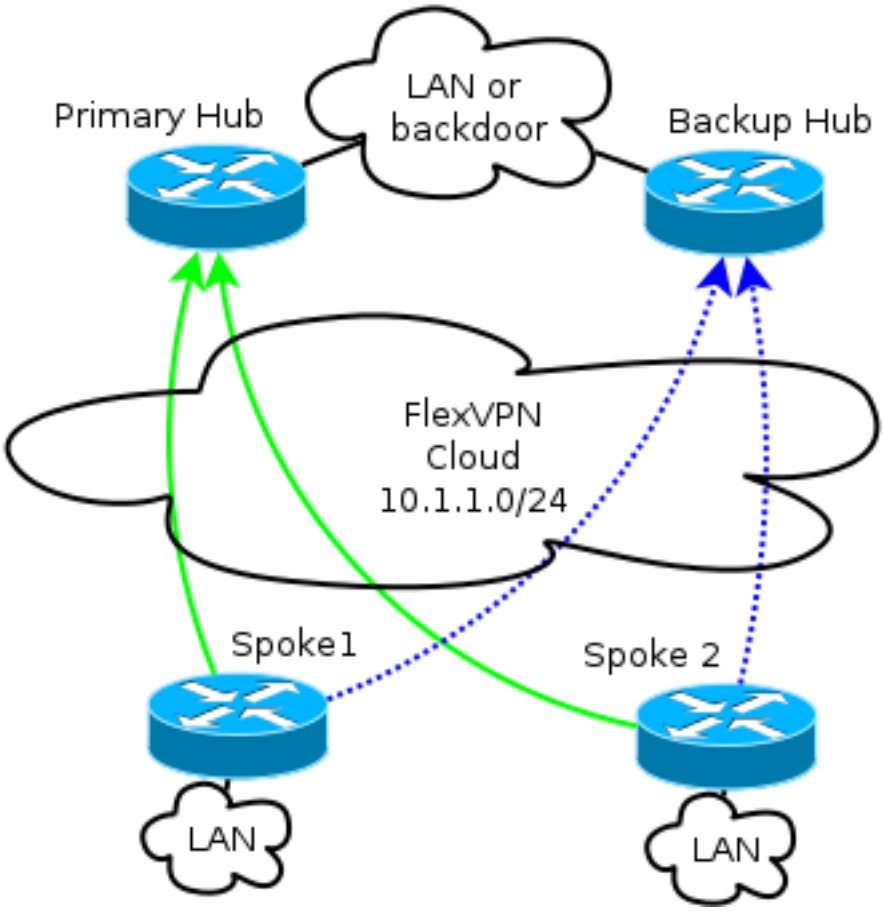
トランスポート層 ネットワーク

次の図は、FlexVPN ネットワークで通常使用される基本のトランスポート ネットワークを示しています。



オーバーレイ ネットワーク

次の図は、フェールオーバーの動作方法を示す論理的な接続を使用してオーバーレイ ネットワークを示しています。通常の動作中は、Spoke 1 と Spoke 2 は 1 つのハブとだけの関係を維持しています。



注：図では、緑の実線はプライマリ インターネット キー エクスチェンジ バージョン 2（IKEv2）/Flex セッションの接続と方向を示し、青の点線はプライマリ ハブへのインターネット キー エクスチェンジ（IKE ）のセッションで万一障害が発生した場合のバックアップ接続を示しています。

/24 のアドレス指定は、実際のインターフェイスのアドレス指定ではなく、このクラウドに割り当てられているアドレスの プールを表しています。これは、FlexVPN ハブでは、通常スポークのインターフェイスにダイナミック IP アドレスを割り当て、FlexVPN の許可ブロックに route コマンドで動的に挿入されたルートに依存するためです。

スポークとハブの基本設定

ハブ アンド スポークの基本設定は、Dynamic Multipoint VPN（DMVPN）から FlexVPN への移行のドキュメントに基づいています。この設定は、「FlexVPN の移行：同じデバイスでの DMVPN から FlexVPN への完全移行」という記事で説明されています。

スポークの設定の調整

スポークの設定：クライアント設定ブロック

スポークの設定は、クライアント設定ブロックによって拡張する必要があります。

基本設定では、複数のピアを指定します。最も高いプリファレンス（最も低い数値）のピアが他

のものよりも優先されます。

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

トンネル設定は、トンネルの宛先を FlexVPN のクライアント設定ブロックに基づいて動的に選択できるように、変更される必要があります。

```
interface Tunnel1
 tunnel destination dynamic
```

FlexVPN のクライアント設定ブロックは、インターフェイスに結び付けられ、IKEv2 にも IPSec（Internet Protocol Security）のプロファイルにも結び付けられないことを覚えておくことが重要です。

クライアント設定ブロックには、フェールオーバー時間と動作を調整するための複数のオプションが用意されており、オブジェクトのトラッキングの使用、ダイヤル バックアップ、バックアップ グループなどの機能があります。

基本設定によって、スポークでは、DPD を使用してスポークが応答しなくなっていないかどうかを検出し、ピアがデッドと宣言された場合に、変更をトリガーします。DPD を使用するオプションは、DPD の動作方法のせいで、即効性のあるオプションではありません。管理者は、オブジェクト トラッキングまたは同様の拡張を使用して設定を拡張することができます。

詳細については、このドキュメントの最後の「**関連情報**」の項にリンクが記載されている **Cisco IOS の構成ガイドの「FlexVPN クライアント設定」の章を参照してください。**

完全なスポークの設定：参照用

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN tunnel
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

ハブ設定

ハブの設定も大部分は同じですが、いくつかの設定を行う必要があります。行う設定のほとんどは、1 つ以上のスポークが 1 つのハブに接続されているが、他のスポークは別のハブと関係しているような状況に関連しています。

スポークのアドレス

スポークでは IP アドレスをハブから取得するため、ハブで、別個のサブネットのアドレス、または 1 つのサブネットの異なる部分を割り当てることが通常望ましいです。

以下に、いくつかの例を示します。

ハブ 1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

ハブ 2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

これにより、トラブルシューティングを妨げることがある、アドレスが FlexVPN クラウドの外部にルーティングされない場合でも、アドレスの重複生成が発生しなくなります。

ハブのオーバーレイ アドレス

両方のハブで、仮想テンプレート インターフェイスに同じ IP アドレスを保持できます。ただし、この設定はトラブルシューティングに影響を与える可能性があります。この設計の選択により、スポークには Border Gateway Protocol（BGP）のピアのアドレスを 1 つだけ保持する必要があるため、導入と計画が行いやすくなります。

場合によっては、オーバーレイ アドレスが望ましくないか、または不要なことがあります。

ルーティング

各ハブでは、接続されているスポークに関する情報を交換する必要があります。

各ハブでは、接続されたデバイスの特定のルートを交換でき、またスポークに集約も提供できる必要があります。

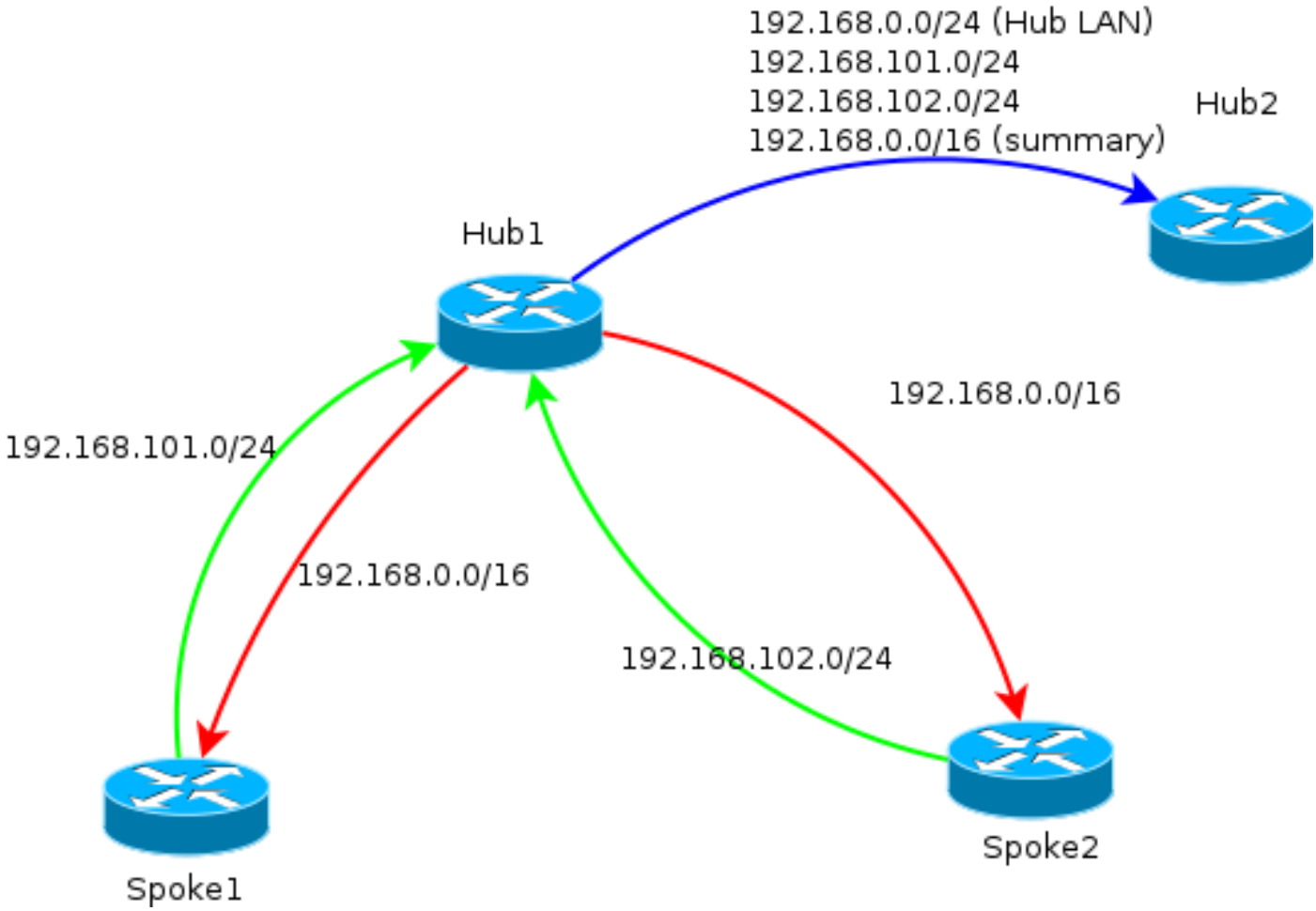
FlexVPN および DMVPN による iBGP を使用することを推奨しているため、そのルーティング プロトコルだけが示されています。

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

この設定によって、次のことが可能になります。

- スポークに割り当てられたアドレスからのダイナミック リスナー
- **192.168.0.0/24 のネットワークのアドバタイジング**
- すべてのスポークへの **192.168.0.0/16 という集約ルートのアドバタイジング。**集約アドレスの設定が、null0 インターフェイスを介したそのプレフィックスのスタティック ルートを作成します。このルートは、ルーティング ループを防ぐために使用される廃棄ルートです。
- もう一方のハブへの特定のプレフィックスの転送
- 各ハブが相互の間で、スポークから取得した情報を交換するようにするためのルート リフレクタ クライアント

次の図は、ハブの 1 つから見た場合の、この設定での BGP のプレフィックス交換を表しています。



注：この図では、緑の線はスポークによってハブに提供される情報を表し、赤い線は各ハブによってスポークに提供される情報（集約のみ）を表し、青い線はハブ間で交換されるプレフィックスを表しています。

ネットワーク集約の使用

集約は、シナリオによっては適切でないか、または望ましくない場合があります。iBGP ではネクスト ホップがデフォルトではオーバーライドされないため、プレフィックスで宛先 IP を指定する場合は注意してください。

集約は、状態が頻繁に変更されるネットワークで推奨されます。たとえば、状態が変更されやすいインターネット接続では、プレフィックスの削除と追加の回避、更新回数の制限、ほとんどの設定の適切なスケーリングの可能化を行うために集約が必要になる場合があります。

スポーク間トンネル

前の項で説明したシナリオと設定では、異なるハブのスポークは直接のスポーク間トンネルを確立できません。異なるハブに接続されたスポーク間のトラフィックは、中央の各デバイスを超えてフローします。

この問題には簡単な回避策があります。ただし、同じネットワーク ID の Next Hop Resolution Protocol（NHRP）をハブ間で有効にする必要があります。これは、たとえばハブ間でポイントツーポイントの Generic Routing Encapsulation（GRE）トンネルを作成した場合に実現できます。

こうすれば、IPsec は不要になります。

確認

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

show crypto ikev2 saコマンドでは、スポークが現在接続されている場所について報告します。

show crypto ikev2 client flexvpn コマンドを使用すれば、管理者は FlexVPN クライアントの動作の現在の状態が分かります。

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

show logging の設定を使用したフェールオーバーが正常に終了すると、スポーク デバイスに関する次の出力がログに記録されます。

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

この出力では、スポークが**ハブの 172.25.1.1** から切断され、Flex_Client のクライアント設定ブロックによって障害が検出され、トンネルがアップする **172.25.2.1 に強制的に接続され、スポークに 10.1.1.177** の IP が割り当てられます。

トラブルシュート

アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

> **注：debug コマンドを使用する前に、「**デバッグ コマンドの重要な情報」を参照してください。

関連する debug コマンドを下に示します。

- debug crypto ikev2
- debug radius

関連情報

- FlexVPN とインターネット キー エクスチェンジ バージョン 2 の構成ガイド、Cisco IOS リリース 15 M&T
- テクニカル サポートとドキュメント – Cisco Systems