

デュアル クラウド アプローチによる冗長ハブ設計での FlexVPN スポークの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[トランスポート層 ネットワーク](#)

[オーバーレイ ネットワーク](#)

[スポークの設定](#)

[スポーク トンネル インターフェイスの設定](#)

[スポーク Border Gateway Protocol \(BGP \) の設定](#)

[ハブの設定](#)

[ローカルプール](#)

[ハブ BGP の設定](#)

[確認](#)

[トラブルシューティング](#)

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 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。

設定

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。

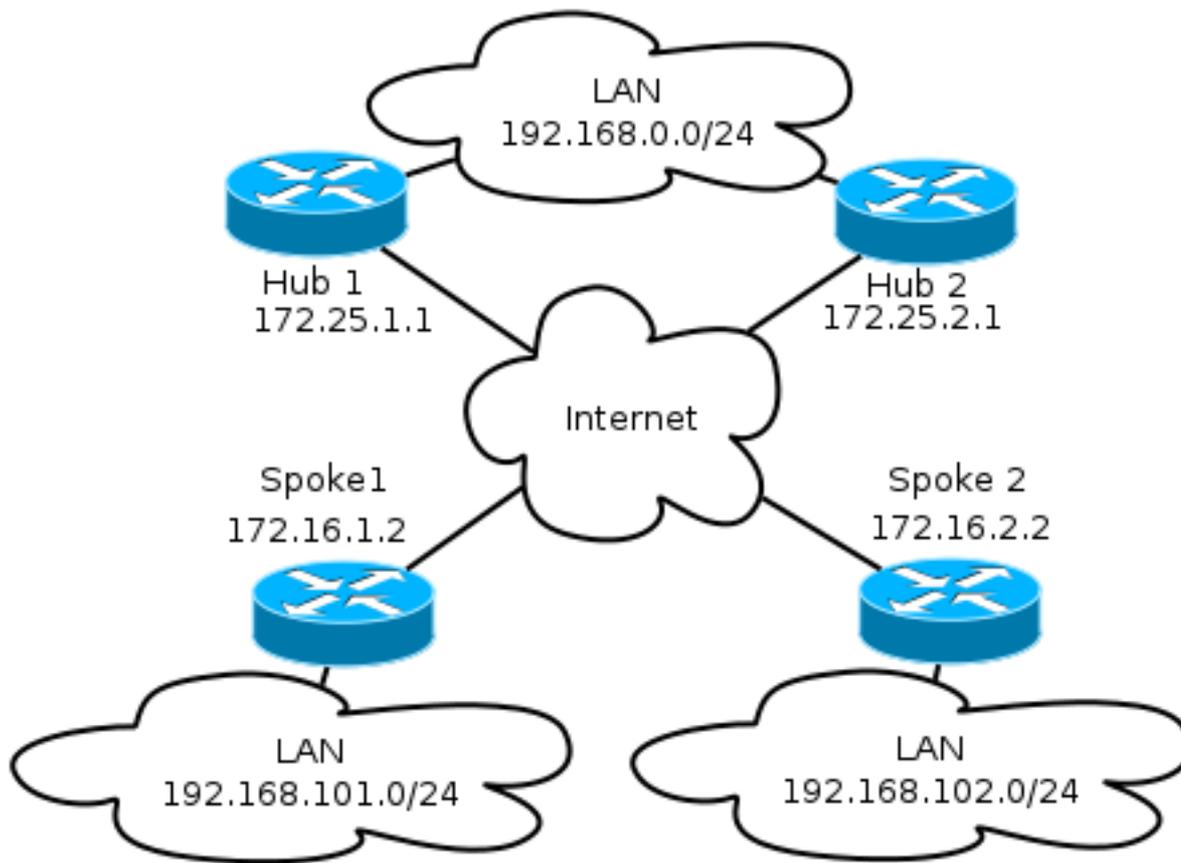
アプローチ	賛成論
2 つのクラウド	<ul style="list-style-type: none">• 障害発生時の迅速なリカバリ (ルーティング プロトコル タイマーに基づく)• ハブ間のトラフィックを配信する可能性がより高い (両方のハブへの接続がアクティブ)
フェールオーバー	<ul style="list-style-type: none">• 設定が容易 (FlexVPN に組み込まれる)• 障害時にルーティング プロトコルに依存しない

このドキュメントでは、1 番目のアプローチについて説明します。この設定へのアプローチは、Dynamic Multipoint VPN (DMVPN) デュアル クラウド設定に似ています。ハブ アンド スポークの基本設定は、DMVPN から FlexVPN への移行のドキュメントに基づいています。この設定の説明については、『[FlexVPN Migration:同じデバイスでの DMVPN から FlexVPN への完全移行](#)』を参照してください。

ネットワーク図

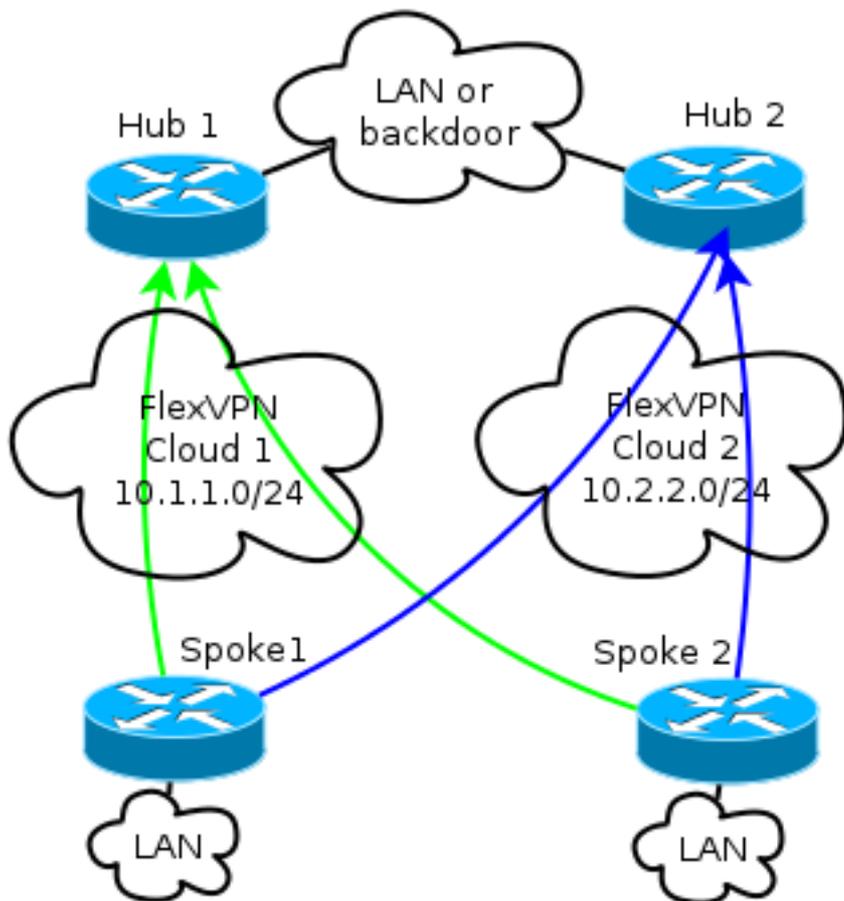
トランスポート層 ネットワーク

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たオーバーレイ 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 は両方のハブとの関係を維持しています。障害が発生すると、ルーティング プロトコルは 1 つのハブから別のハブへ切り替えます。



注：この図では、緑の線は Hub 1 へのインターネット 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、青色の線は Hub 2 への接続を示します。

オーバーレイクラウドでは両方のハブが個別の IP アドレッシングを維持します。/24 アドレッシングは、実際のインターフェイスのアドレッシングではなく、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。

スポークの設定

スポークトンネルインターフェイスの設定

この例で使用される一般的な設定は、異なる 2 つの宛先アドレスが設定されている単純な 2 つのトンネルインターフェイスです。

```
interface Tunnell
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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
tunnel path-mtu-discovery
```

```
tunnel protection ipsec profile default

interface Tunnel2
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
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

スポーク間トンネルが適切に確立されるようにするため、仮想テンプレート (VT) が必要です。

```
interface Virtual-Templatel type tunnel
ip unnumbered ethernet1/0
ip mtu 1400
ip nhrp network-id 2
ip nhrp shortcut virtual-template 1
ip nhrp redirect
ip tcp adjust-mss 1360
tunnel path-mtu-discovery
tunnel protection ipsec profile default
```

スポークは、Virtual Routing and Forwarding (VRF) の LAN インターフェイスを示すアンナンバード インターフェイスを使用します (この場合はグローバル)。ただし、ループバック インターフェイスを参照することが適切な場合もあります。これは、ほとんどの状況ではループバック インターフェイスがオンラインのままになるためです。

スポーク Border Gateway Protocol (BGP) の設定

シスコではオーバーレイ ネットワークで使用するルーティング プロトコルとして iBGP を推奨しているため、このドキュメントではこの設定についてのみ説明します。

注： スポークは、両方のハブへ BGP で到達できる状態を維持する必要があります。

```
router bgp 65001
bgp log-neighbor-changes
network 192.168.101.0
neighbor 10.1.1.1 remote-as 65001
neighbor 10.1.1.1 fall-over
neighbor 10.2.2.1 remote-as 65001
neighbor 10.2.2.1 fall-over
```

この設定の FlexVPN には、プライマリ/セカンダリ ハブという概念はありません。管理者はルーティング プロトコルがいずれのハブを優先するかを決定し、場合によってはロード バランシングを実行します。

スポークのフェールオーバーおよびコンバージェンスに関する考慮事項

スポークによる障害検出にかかる時間を最小限に抑えるため、次の 2 種類の一般的な方法を使用します。

- BGP タイマーを短く設定する。デフォルトの保持時間ではフェールオーバーが発生します。

- BGP フォールオーバーを設定します。これについては、『[高速ピアリングセッションの非アクティブ化に対する BGP サポート](#)』を参照してください。
- Bidirectional Forwarding Detection (BFD) は、ほとんどの FlexVPN 導入環境では推奨されないため、BFD は使用しないでください。

スポーク間のトンネルとフェールオーバー

スポーク間トンネルでは、Next Hop Resolution Protocol (NHRP) ショートカット スイッチングが使用されます。Cisco IOS は、これらのショートカットが NHRP ルートであることを示します。次に例を示します。

```
Spoke1#show ip route nhrp  
(...)
```

```
192.168.102.0/24 is variably subnetted, 2 subnets, 2 masks  
H 192.168.102.0/24 [250/1] via 10.2.2.105, 00:00:21, Virtual-Access1
```

これらのルータは、BGP 接続が期限切れになっても期限切れになりません。その代わりに、NHRP 保留時間にわたり保持されます (デフォルトでは 2 時間)。つまり、アクティブなスポーク間トンネルは、障害発生時でも引き続き稼働します。

ハブの設定

ローカル プール

「ネットワーク図」で説明したように、両方のハブは個別の IP アドレッシングを維持します。

ハブ 1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

ハブ 2

```
ip local pool FlexSpokes 10.2.2.100 10.2.2.254
```

ハブ BGP の設定

ハブ BGP の設定は、前述の例に似ています。

この出力は、LAN IP アドレスが 192.168.0.1 のハブ 1 からの出力です。

```
router bgp 65001  
bgp log-neighbor-changes  
bgp listen range 10.1.1.0/24 peer-group Spokes  
network 192.168.0.0  
aggregate-address 192.168.0.0 255.255.0.0 summary-only  
neighbor Spokes peer-group  
neighbor Spokes remote-as 65001  
neighbor Spokes fall-over  
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
```

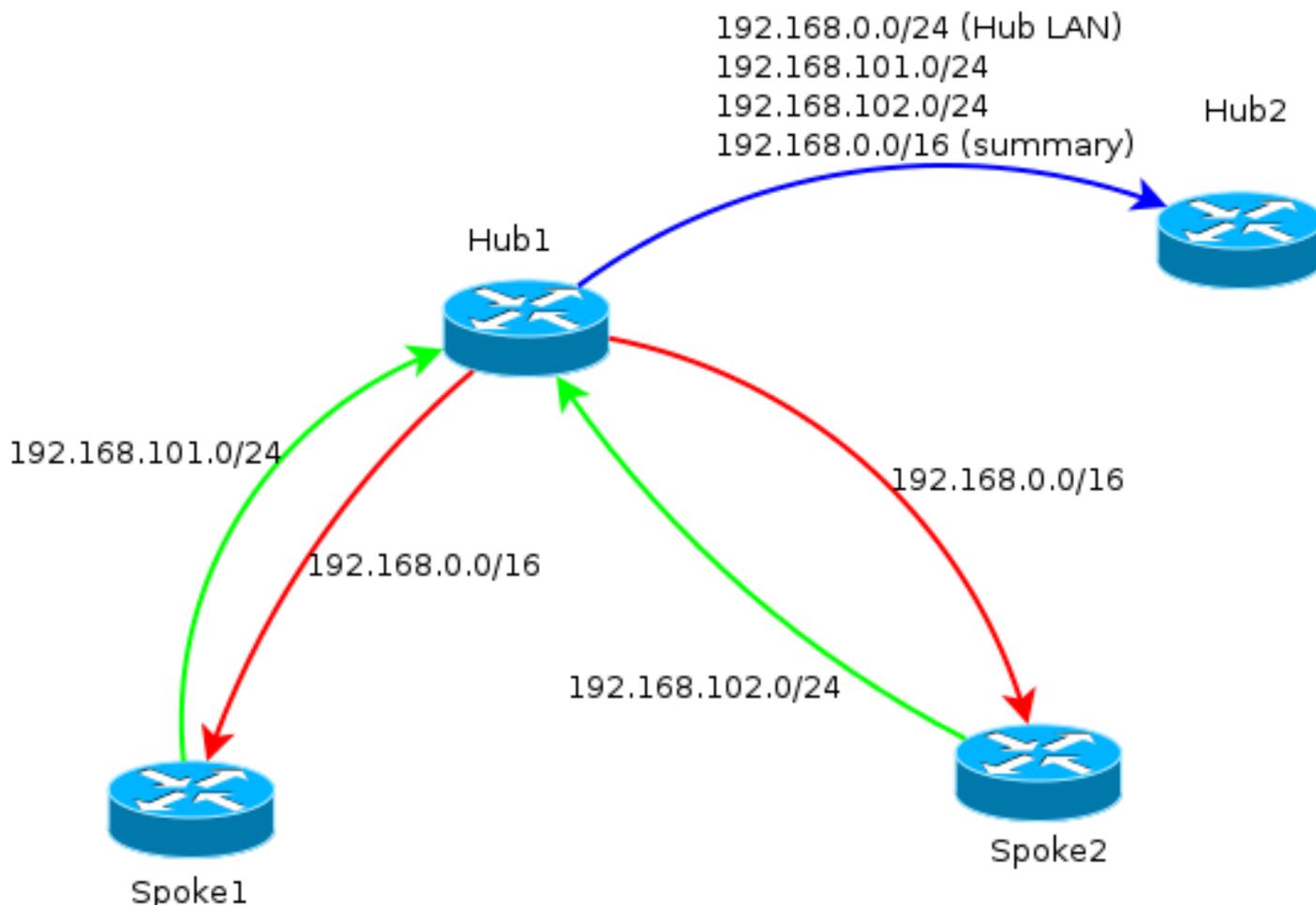
```
route-map ALL permit 10
match ip address 1
```

```
ip access-list standard 1
permit any
```

設定内容の要約を次に示します。

- FlexVPN ローカル アドレス プールは BGP リッスン範囲内にあります。
- ローカル ネットワークは 192.168.0.0/24 です。
- サマリーはスポークだけにアドバタイズされます。集約アドレスの設定により、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 ルートが作成されます。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。
- 特定プレフィックスはすべて、もう一方のハブへアドバタイズされます。これは iBGP 接続でもあるため、ルート リフレクタの設定が必要です。

この図は、1つの FlexVPN クラウド内のスポークとハブの間での BGP プレフィックスの交換を示します。



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（サマリーのみ）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。

確認

各スポークが両方のハブとの関連付けを維持するため、**show crypto ikev2 sa** コマンドを実行すると2つのIKEv2セッションが表示されます。

```
IPv4 Crypto IKEv2 SA
```

```
Tunnel-id Local Remote fvrf/ivrf Status
3 172.16.1.2/500 172.16.2.2/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3147 sec
```

```
Tunnel-id Local Remote fvrf/ivrf Status
1 172.16.1.2/500 172.25.2.1/500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA512, DH Grp:5, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3256 sec
```

ルーティングプロトコル情報を表示するには、次のコマンドを入力します:

```
show bgp ipv4 unicast
```

```
show bgp summary
```

スポークでは、サマリープレフィックスをハブから受信したものと、両方のハブへの接続がアクティブであることがわかります。

```
Spokel#show bgp ipv4 unicast
```

```
BGP table version is 4, local router ID is 192.168.101.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

```
Network Next Hop Metric LocPrf Weight Path
```

```
*>i 192.168.0.0/16 10.1.1.1 0 100 0 i
```

```
* i 10.2.2.1 0 100 0 i
```

```
*> 192.168.101.0 0.0.0.0 0 32768 i
```

```
Spokel#show bgp summa
```

```
Spokel#show bgp summary
```

```
BGP router identifier 192.168.101.1, local AS number 65001
BGP table version is 4, main routing table version 4
2 network entries using 296 bytes of memory
3 path entries using 192 bytes of memory
3/2 BGP path/bestpath attribute entries using 408 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 896 total bytes of memory
BGP activity 2/0 prefixes, 3/0 paths, scan interval 60 secs
```

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
```

```
10.1.1.1 4 65001 7 7 4 0 0 00:00:17 1
```

```
10.2.2.1 4 65001 75 72 4 0 0 01:02:24 1
```

トラブルシューティング

トラブルシューティング対象の主要ブロックが2つあります。

- インターネット キー交換 (IKE)

- IPSec (Internet Protocol Security)
関連する show コマンドを以下に示します。

```
show crypto ipsec sa
```

```
show crypto ikev2 sa
```

関連する debug コマンドを下に示します。

```
debug crypto ikev2 [internal|packet]
```

```
debug crypto ipsec
```

```
debug vtemplate event
```

関連するルーティング プロトコルを以下に示します。

```
show bgp ipv4 unicast (or show ip bgp)
```

```
show bgp summary
```