FlexVPN の移行： DMVPN から別のハブの FlexVPN への完全移行

目次

概要

このドキュメントでは、現在存在している Dynamic Multipoint VPN（DMVPN）ネットワークから別のハブ デバイス上の FlexVPN への移行方法について説明します。 両方のフレームワークの設定をデバイス上で共存させることができます。 このドキュメントでは、最も一般的なシナリオ、つまり認証に事前共有キーを使用し、ルーティング プロトコルとして Enhanced Interior Gateway Routing Protocol（EIGRP）を使用する DMVPN だけを扱います。 このドキュメントでは、推奨されるルーティング プロトコルである Border Gateway Protocol（BGP）と、BGP ほど望ましくない EIGRP への移行について説明します。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- DMVPN
- FlexVPN

使用するコンポーネント

> **注:** 一部のソフトウェアとハードウェアでは、インターネット キー エクスチェンジ バージョン 2（IKEv2）がサポートされていません。 詳細については、『Cisco Feature Navigator』を参照してください。

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くものです。

- Cisco サービス統合型ルータ（ISR）バージョン 15.2(4)M1 以降
- Cisco アグリゲーション サービス ルータ 1000 シリーズ（ASR1K）3.6.2 リリース 15.2(2)S2 以降

新しいプラットフォームとソフトウェアの利点の 1 つとして、次世代暗号化を使用できることがあります。たとえば、Request for Comments（RFC）4106 に記述されている IPSec（Internet Protocol Security）での暗号化の Advanced Encryption Standard（AES）Galois/Counter Mode（GCM）の使用などです。 AES GCM により、一部のハードウェアでは暗号化速度の大幅な向上が実現できます。 シスコが推奨する次世代暗号化の使用と移行については、『Next Generation Encryption 』を参照してください。

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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

移行手順

現在、DMVPN から FlexVPN への推奨される移行方法では、2 つのフレームワークが同時に動作

することはありません。 この制限は、ASR 3.10 リリースで導入される新しい移行機能によって解除される予定です。このリリースは Cisco Bug ID CSCuc08066 を含むシスコ側の複数の拡張要求に対応するものです。 これらの機能は 2013 年 6 月後半に提供予定です。

両方のフレームワークが同じデバイスに共存し同時に動作する移行は、**穏やかな移行**と呼ばれ、影響は最小で、フレームワーク間のフェールオーバーは効率的に行われます。 両方のフレームワークの設定が共存するものの同時には動作しない移行は、**完全移行**と呼ばれます。 つまり、フレームワーク間のスイッチオーバーにより、わずかとはいえ、VPN を介した通信が欠落することがあります。

異なる 2 つのハブ間の完全移行

このドキュメントでは、現在使用されている DMVPN ハブから新しい FlexVPN ハブへの移行について説明します。 この移行では、FlexVPN へ移行済みのスポーク間の通信、および DMVPN でまだ実行しているスポーク間の通信が可能であり、移行はスポークごとに複数フェーズで実行できます。

ルーティング情報が正しく登録された場合は、移行後のスポークと移行していないスポークの間の通信も可能なままです。 ただし、移行後のスポークと移行していないスポークの間にスポーク間トンネルが構築されないため、追加の遅延が発生する場合があります。 一方で、移行後のスポークは移行後のスポークとの間で、直接スポーク間トンネルを確立できます。 移行していないスポークについても同様です。

新しい移行機能が提供されるまでは、異なるハブを使用した DMVPN から FlexVPN への移行を行うには、次の手順に従います。

1. DMVPN 上の接続性を確認する。
2. FlexVPN の設定を追加し、新しい設定に含まれるトンネルをシャットダウンする。
3. （メンテナンスの時間帯に）各スポークで、1 つずつ、DMVPN トンネルをシャットダウンする。
4. ステップ 3 と同じスポークで FlexVPN トンネル インターフェイスのシャットダウンを解除する。
5. スポークとハブとの間の接続を検証する。
6. FlexVPN 内のスポーク間の接続を検証する。
7. FlexVPN からの DMVPN によるスポーク間の接続を検証する。
8. スポークごとにステップ 3 ~ 7 を繰り返す。
9. ステップ 5、6、7 で説明されている検証で問題が発生する場合は、FlexVPN インターフェイスをシャットダウンしてから、DMVPN を復元するために DMVPN インターフェイスのシャットダウンを解除します。
10. バックアップ DMVPN でスポークとハブとの間の通信を検証する。
11. バックアップ DMVPN でスポーク間の通信を検証する。

カスタム アプローチ

ネットワークまたはルーティングが複雑なために前述の方法が最善でないと考えられる場合には、移行前にシスコの担当者にご連絡ください。 カスタム移行プロセスについては、担当のシステム エンジニアまたはアドバンスド サービス エンジニアにご相談ください。

ネットワーク トポロジ

転送ネットワーク トポロジ

次の図は、インターネット上のホストの一般的な接続トポロジを示しています。 ハブの **loopback0** の IP アドレス（**172.25.1.1**）が DMVPN IPsec セッションを終了するために使用されています。 FlexVPN では新しいハブの IP（**172.25.2.1**）が使用されます。

2 つのハブ間のリンクに注目してください。 このリンクは、移行中に FlexVPN クラウドと DMVPN クラウドの間の接続を可能にするために重要です。 FlexVPN に移行済みのスポークが DMVPN ネットワークと通信できるようにしたり、その逆を可能にします。

オーバーレイ ネットワーク トポロジ

このトポロジ図には、オーバーレイに使用される 2 つの分離されたクラウドが示されています。 DMVPN（緑色の接続）と FlexVPN（赤色の接続）です。 LAN のプレフィックスは対応するサイトを表しています。 **10.1.1.0/24** サブネットはインターフェイス アドレッシングに関して実際のサブネットを表している訳ではなく、FlexVPN クラウド専用の IP 空間の集まりを表しています。 この背景にある理由については、「**FlexVPN の設定**」セクションで後ほど説明します。

設定

このセクションでは、DMVPN と FlexVPN の設定について説明します。

DMVPN のコンフィギュレーション

ここでは、DMVPN のハブとスポークの基本的な設定について説明します。

事前共有キー（PSK）は、IKEv1 認証に使用されます。 IPsec が確立されると、スポークとハブとの間の Next Hop Resolution Protocol（NHRP）登録が実行され、ハブはスポークのノンブロードキャスト マルチアクセス（NBMA）アドレッシングを動的に学習できます。

NHRP がスポークとハブで登録を実行すると、ルーティングの隣接関係の確立とルートの交換が可能になります。 この例では、オーバーレイ ネットワーク用の基本的なルーティング プロトコルとして EIGRP を使用します。

スポークの DMVPN コンフィギュレーション

PSK の認証を行いルーティング プロトコルとして EIGRP を使用する DMVPN の設定の基本的な例を次に示します。

```
crypto isakmp policy 10
 encr aes
 authentication pre-share

crypto isakmp key cisco address 0.0.0.0
```

```
crypto isakmp keepalive 30 5

crypto isakmp profile DMVPN_IKEv1
 keyring DMVPN_IKEv1
 match identity address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
 mode transport

crypto ipsec profile DMVPN_IKEv1
 set transform-set IKEv1
  set isakmp-profile DMVPN_IKEv1

interface Tunnel0

ip address 10.0.0.101 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map 10.0.0.1 172.25.1.1
ip nhrp map multicast 172.25.1.1
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp nhs 10.0.0.1
ip nhrp shortcut
ip tcp adjust-mss 1360
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.102.0
passive-interface default
no passive-interface Tunnel0
```

ハブの DMVPN コンフィギュレーション

ハブ設定では、トンネルは、IP アドレス 172.25.1.1 の loopback0 から作成されます。 それ以外はルーティング プロトコルとして EIGRP を使用する DMVPN ハブの標準的な導入です。

```
crypto isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set IKEv1 esp-aes esp-sha-hmac
mode transport
crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

interface Tunnel0
ip address 10.0.0.1 255.255.255.0
no ip redirects
ip mtu 1400
ip nhrp map multicast dynamic
ip nhrp network-id 1
ip nhrp holdtime 900
ip nhrp server-only
ip nhrp redirect
ip summary-address eigrp 100 192.168.0.0 255.255.0.0
```

```
ip tcp adjust-mss 1360
tunnel source Loopback0
tunnel mode gre multipoint
tunnel protection ipsec profile DMVPN_IKEv1

router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.0.0 0.0.255.255
passive-interface default
no passive-interface Tunnel0
```

FlexVPN のコンフィギュレーション

FlexVPN は、次の基礎となる同じテクノロジーに基づいています。

- **IPsec**： DMVPN のデフォルトとは異なり、IPsec Security Association（SA）のネゴシエーションには IKEv1 ではなく IKEv2 が使用されます。 IKEv2 は、保護されたデータ チャネルを確立するために必要な復元力やメッセージ数など、IKEv1 よりも優れた機能を提供します。

- **GRE**： DMVPN とは異なり、1 つの静的なマルチポイント GRE インターフェイスだけではなく、静的および動的なポイントツーポイント インターフェイスが使用されます。 この設定により、特にスポークごとまたはハブごとの動作の柔軟性が増します。

- **NHRP**： FlexVPN では、NHRP は主にスポーク間の通信の確立に使用されます。 スポークはハブに登録されません。

- **ルーティング**： スポークはハブへの NHRP 登録を実行しないため、ハブとスポークが双方向の通信を行うための別のメカニズムが必要になります。 DMVPN と同様、ダイナミック ルーティング プロトコルを使用できます。 ただし、FlexVPN では IPsec を使用してルーティング情報を通知できます。 デフォルトではトンネルの反対側に IP アドレスの **/32** ルートとして通知するため、スポークとハブとの間の直接通信が可能になります。

DMVPN から FlexVPN への完全移行では、同じデバイス上で 2 つのフレームワークが同時に動作することはありません。 ただしそれらを分離しておくことをお勧めします。

複数のレベルで分離を行います。

- NHRP： 異なる NHRP ネットワーク ID を使用します（推奨）。
- ルーティング：別のルーティング プロセスを使用します（推奨）。
- Virtual Routing and Forwarding（VRF）：VRF の分離によって柔軟性が向上しますが、これについてはここでは説明しません（任意）。

スポークの FlexVPN コンフィギュレーション

DMVPN と比較した場合、FlexVPN でのスポークの設定の相違点の 1 つは、インターフェイスが 2 つある可能性があることです。 スポークとハブとの間の通信の必須トンネルと、スポーク間トンネルのオプション トンネルがあります。 スポーク間のダイナミック トンネリングを使用せずすべてハブ デバイスを経由して送信することにした場合は、仮想テンプレート インターフェイスを削除し、トンネル インターフェイスから NHRP ショートカット スイッチングを削除できます。

スタティック トンネル インターフェイスは、ネゴシエーションに基づく IP アドレスを受け取ることに注意してください。 これにより、FlexVPN クラウド内でスタティック アドレスを作成しなくても、トンネル インターフェイス IP アドレスをハブからスポークへ動的に提供できます。

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 profile Flex_IKEv2
match identity remote fqdn domain cisco.com
local identity fqdn spoke.cisco.com
authentication remote rsa-sig
authentication local rsa-sig
aaa authorization group cert list default default
virtual-template 1
crypto ikev2 dpd 30 5 on-demand
```

> **注:** デフォルトでは、IP アドレスを使用するためにローカル ID が設定されます。 したがって、ピアでの対応する match ステートメントは、アドレスに基づいて一致する必要もあります。 証明書の識別名（DN）に基づく一致が要件である場合は、証明書マップを使用して照合が実行されます。

ハードウェアが対応している場合は、AES GCM の使用を推奨します。

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2
! set transform-set IKEv2

interface Tunnel1
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
shutdown
tunnel source Ethernet0/0
tunnel destination 172.25.2.1
tunnel path-mtu-discovery
tunnel protection ipsec profile default

interface Virtual-Template1 type tunnel
ip unnumbered Tunnel1
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
```

IKEv2 で大規模な認証を実行する方法として Public Key Infrastructure（PKI）を推奨します。 ただし、PSK の制限を認識した上で PSK を使用することもできます。

次に、PSK として **cisco** を使用する設定例を示します。

```
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
```

FlexVPN ハブのコンフィギュレーション

一般的に、ハブではスポークとハブとの間のダイナミック トンネルの終了のみが行われます。 このため、ハブの設定では、FlexVPN のスタティック トンネル インターフェイスが見つかりません。 代わりに仮想テンプレート インターフェイスが使用されます。

注: ハブ側では、スポークへ割り当てるプール アドレスを指定する必要があります。

このプールのアドレスは、スポークごとに /32 ルートとして、後でルーティング テーブルに追加されます。

```
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
```

ハードウェアが対応している場合は、AES GCM の使用を推奨します。

```
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
```

注: 次の設定では AES GCM の動作がコメント アウトされています。

```
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
```

IKEv2 の認証では、スポークと同じ原則がハブにも適用されます。 拡張性と柔軟性のために証明書を使用します。 ただし、PSK にはスポークと同じ設定を再利用できます。

> **注:** IKEv2 は認証に関する柔軟性を提供します。 一方で PSK を使用して認証を行い、他方で Rivest-Shamir-Adleman Signature (RSA-SIG) を使用することができます。

認証に事前共有キーを使用することが要件である場合、設定の変更は、ここで説明するスポークルータの変更と似たものになります。

ハブ間 BGP 接続

ハブが特定のプレフィックスがどこにあるかを認識できるようにしておく必要があります。 これは、一部のスポークを FlexVPN に移行し、残りのスポークを DMVPN のままにしているために、さらに重要になっていきます。

DMVPN のハブの設定に基づくハブ間 BGP 接続を次に示します。

```
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
```

トラフィックの移行

オーバーレイ ルーティング プロトコルとしての BGP に移行 (推奨)

BGP は、ユニキャスト エクスチェンジに基づいたルーティング プロトコルです。 その特性から DMVPN ネットワークでは最も拡張性があるプロトコルです。

この例では、内部 BGP (iBGP) を使用します。

スポークの BGP コンフィギュレーション

スポークの移行は 2 つの部分から成ります。 最初に、ダイナミック ルーティングとして BGP を有効にします。

```
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
```

BGP ネイバーが起動し（次のセクションを参照）、BGP 上の新しいプレフィックスが学習された後で、トラフィックを既存の DMVPN クラウドから新しい FlexVPN クラウドに振り向けることができます。

ハブの BGP コンフィギュレーション

FlexVPN ハブ：フル BGP の設定

ハブではネイバーシップ設定をスポークごとに個別に保持することを避けるため、ダイナミック リスナーを設定します。 この設定では、BGP は新しい接続を開始しませんが、提供された IP アドレス プールからの接続を受け入れます。 この例ではそのプールは 10.1.1.0/24 であり、これは新しい FlexVPN クラウド内のすべてのアドレスになります。

注意点が 2 つあります。

- FlexVPN ハブは DMVPN ハブに対し特定のプレフィックスをアドバタイズします。 したがって、unsupress map が使用されます。
- FlexVPN サブネット 10.1.1.0/24 をルーティング テーブルにアドバタイズするか、または DMVPN ハブが FlexVPN ハブをネクスト ホップとして認識するようにします。

このドキュメントでは後者のアプローチについて示します。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
```

```
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

DMVPN ハブ：フル BGP および EIGRP の設定

DMVPN ハブの設定は、特定のプレフィックスを FlexVPN ハブから受け取り、EIGRP から学習したプレフィックスをアドバタイズするだけなので、基本的なものです。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

トラフィックの BGP/FlexVPN への移行

前述のように、移行を実施するには DMVPN 機能をシャットダウンし、FlexVPN を起動する必要があります。

次の手順によって影響を最小にできます。

1. スポークごとに次のように入力します。
   ```
   access-list 1 permit any
   route-map ALL permit 10
   match ip address 1

   route-map SET_NEXT_HOP permit 10
   set ip next-hop 192.168.0.2

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

   neighbor 192.168.0.1 remote-as 65001
   neighbor 192.168.0.1 route-reflector-client
   neighbor 192.168.0.1 unsuppress-map ALL
   neighbor 192.168.0.1 route-map SET_NEXT_HOP out
   ```
   この時点でこのスポークへの IKEv1 セッションが確立されていないことを確認します。 検証するには、**show crypto isakmp sa** コマンドの出力を調べ、**crypto logging session** コマンドにより生成される syslog メッセージをモニタします。 確認できたら FlexVPN の起動に進むことができます。

2. 同じスポークで、次のように入力します。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

確認手順

IPsec の安定性

IPsec の安定性を評価する最適な方法は、次の crypto logging session 設定コマンドを有効にして syslog をモニタすることです。 セッションがアップ ダウンを繰り返している場合は、IKEv2/FlexVPN レベルの問題が発生している可能性があります。この問題は、移行を始める前に修正する必要があります。

BGP 情報の登録

IPsec が安定している場合、BGP テーブルにスポークからのエントリ（ハブ上）およびハブからのサマリー（スポーク上）が登録されていることを確認します。 BGP の場合、これは次のコマンドで表示できます。

```
access-list 1 permit any
route-map ALL permit 10
match ip address 1

route-map SET_NEXT_HOP permit 10
set ip next-hop 192.168.0.2

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

neighbor 192.168.0.1 remote-as 65001
neighbor 192.168.0.1 route-reflector-client
neighbor 192.168.0.1 unsuppress-map ALL
neighbor 192.168.0.1 route-map SET_NEXT_HOP out
```

FlexVPN ハブの正しい情報の例を次に示します。

```
BGP router identifier 172.25.2.1, local AS number 65001
```

```
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.100 4 65001 112 123 16 0 0 01:35:58 1
192.168.0.1 4 65001 97 99 16 0 0 01:24:12 4
```

上記の出力から、ハブがそれぞれのスポークから 1 つのプレフィックスを学習しており、両方のスポークは動的でありアスタリスク (*) 記号が付いていることがわかります。 また、ハブ間接続から合計 4 つのプレフィックスを受信していることがわかります。

スポークからの同様の情報の例を示します。

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

スポークはハブから 2 つのプレフィックスを受信しています。 この設定例では、1 つのプレフィックスは FlexVPN ハブでアドバタイズされたサマリーです。 もう 1 つは DMVPN スポーク上で BGP に再配布された DMVPN 10.0.0.0/24 ネットワークです。

EIGRP を使用した新しいトンネルへの移行

EIGRP は、比較的簡単な導入と高速コンバージェンスから、DMVPN ネットワークでは一般的な選択です。 ただし、BGP に比べて拡張性が低く、BGP ではすぐに使用可能な高度なメカニズムの多くが提供されません。 次のセクションでは、新しい EIGRP プロセスを使用して FlexVPN に移行する方法の 1 つについて説明します。

更新されたスポークのコンフィギュレーション

別の EIGRP プロセスを使用する新しい自律システム (AS) を追加します。

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

> **注:** スポーク間トンネルでルーティング プロトコル隣接関係を確立しないことが最適な方法です。 このため、tunnel1 (スポークとハブの間) のインターフェイスのみを非パッシブにします。

更新された FlexVPN ハブのコンフィギュレーション

同様に FlexVPN ハブでも、スポークで設定されたルーティング プロトコルに合わせて適切な AS でルーティング プロトコルを準備します。

```
show ip bgp summary
BGP router identifier 192.168.101.1, local AS number 65001
(...omitted...)
```

```
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
```

スポークにサマリーを戻す方法は、2 通りあります。

- null0 を指すスタティック ルートを再配布します（推奨）。

  ```
  show ip bgp summary
  BGP router identifier 192.168.101.1, local AS number 65001
  (...omitted...)

  Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
  10.1.1.1 4 65001 120 109 57 0 0 01:33:23 2
  ```

  この方法では、ハブの Virtualization Technology（VT）設定に修正を加えずにサマリーと再配布を制御することができます。 関連したアクティブなバーチャル アクセスがある場合、ハブの VT 設定は変更できないため、これは重要です。

- 仮想テンプレートで DMVPN スタイルのサマリー アドレスを設定します。

  このコンフィギュレーションは、サマリーの内部処理と複製がすべての仮想アクセスに対して行われることから*推奨されません*。 ここでは参考のために紹介します。

  ```
  interface Virtual-Template1 type tunnel
   ip summary-address eigrp 200 192.168.0.0 255.255.0.0
  ```

  その他の考慮事項として、ハブ間のルーティング交換があります。 これは EIGRP インスタンスを iBGP へ再配布する場合に行うことができます。

DMVPN ハブ：更新された BGP のコンフィギュレーション

このコンフィギュレーションは基本のままです。 特定のプレフィックスを EIGRP から BGP へ再配布する必要があります。

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

FlexVPN ハブ：更新された BGP のコンフィギュレーション

DMVPN ハブと同様に、FlexVPN で新しい EIGRP プロセスのプレフィックスを BGP へ再配布する必要があります。

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

トラフィックの FlexVPN への移行

移行を行うには、一度に 1 つずつ、各スポークで DMVPN 機能をシャットダウンし、FlexVPN を起動する必要があります。 次の手順によって影響を最小にできます。

1. スポークごとに次のように入力します。

   ```
   interface Virtual-Template1 type tunnel
    ip summary-address eigrp 200 192.168.0.0 255.255.0.0
   ```

   この時点でこのスポークの IKEv1 セッションが確立されていないことを確認します。 検証

するには、**show crypto isakmp sa** コマンドの出力を調べ、**crypto logging session** コマンドにより生成される syslog メッセージをモニタします。 確認できたら FlexVPN の起動に進むことができます。

2. 同じスポークで、次のように入力します。

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

確認手順

IPsec の安定性

BGP の場合、IPsec が安定しているかどうかを評価する必要があります。 このための最適な方法は、**crypto logging session** 設定コマンドを有効にして syslog をモニタすることです。 セッションがアップ ダウンを繰り返している場合は、IKEv2/FlexVPN レベルの問題が発生している可能性があります。この問題は、移行を始める前に修正する必要があります。

トポロジ テーブル内の EIGRP 情報

EIGRP トポロジ テーブルに、ハブのスポーク LAN エントリおよびスポークのサマリーが登録されていることを確認します。 これはハブとスポークで次のコマンドを実行することで検証できます。

show ip eigrp [AS_NUMBER] topology
スポークからの出力の例を次に示します。

```
Spoke1#show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

P 10.1.1.1/32, 1 successors, FD is 26112000
via Rstatic (26112000/0)
via 10.1.1.1 (26240000/128256), Tunnel1

P 192.168.101.0/24, 1 successors, FD is 281600
via Connected, Ethernet1/0

P 192.168.0.0/16, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1

P 10.1.1.100/32, 1 successors, FD is 26112000
via Connected, Tunnel1

P 10.1.1.0/24, 1 successors, FD is 26114560
via 10.1.1.1 (26114560/2562560), Tunnel1
```

この出力から、スポークが LAN サブネット（*イタリック体*）とそれらのサマリー（**太字**）を認識していることがわかります。

ハブからの出力の例を次に示します。

```
hub2# show ip eigrp 200 topology
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.2.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
```

```
P 10.1.1.1/32, 1 successors, FD is 128256
via Connected, Loopback200

P 192.168.101.0/24, 1 successors, FD is 26905600
via 10.1.1.100 (26905600/281600), Virtual-Access1

P 192.168.0.0/16, 1 successors, FD is 2562560
via Rstatic (2562560/0)

P 10.1.1.0/24, 1 successors, FD is 2562560
via Rstatic (2562560/0)
```

この出力から、ハブがスポークの LAN サブネット（*イタリック体*）、アドバタイズしているサマリー プレフィックス（**太字**）、ネゴシエーションによって各スポークに割り当てられた IP アドレスを認識していることがわかります。

その他の考慮事項

既存のスポーク間トンネル

DMVPN トンネル インターフェイスのシャットダウンによって、NHRP エントリが削除されるため、既存のスポーク間トンネルは解除されます。

NHRP エントリのクリア

FlexVPN ハブは、トラフィックのルーティングを逆にたどるのに、スポークからの NHRP 登録プロセスに依存しません。 ただし、スポーク間のダイナミック トンネルは NHRP エントリに依存します。

DMVPN では、ハブで NHRP がクリアされている場合、短期間の接続の問題が発生する場合があります。 FlexVPN では、スポークの NHRP をクリアすると、スポーク間トンネルに関連する FlexVPN IPsec セッションが切断されます。 ハブでの NHRP のクリアは、FlexVPN セッションには影響しません。

この理由は、デフォルトで FlexVPN において次のように動作するからです。

- スポークはハブに登録されません。
- ハブは NHRP リダイレクタとしてのみ動作し、NHRP エントリをインストールしません。
- NHRP ショートカット エントリは、スポーク間でスポークにインストールされ、ダイナミックになります。

既知の警告

スポーク間トラフィックは Cisco Bug ID CSCub07382 の影響を受ける可能性があります。

関連情報

- DMVPN から FlexVPN へのソフト移行の設定例
- テクニカルサポートとドキュメント - Cisco Systems