DMVPN から FlexVPN へのソフト移行の設定例

内容

概要

このドキュメントでは、Dynamic Multipoint VPN（DMVPN）と FlexVPN の両方が回避策を必要とせず同時にデバイスで機能する、*ソフト移行の方法を説明するとともに、設定例を提供します*。

> **注**：このドキュメントでは、「FlexVPN の移行：同じデバイスでの DMVPN から FlexVPN への完全移行」と「FlexVPN の移行：DMVPN から別のハブの FlexVPN への完全移行」のシスコの記事で説明されている概念をさらに拡張しています。これらのドキュメントは両方とも、移行中にトラフィックの一時中断が発生する*完全移行を説明*しています。これらの記事にある制限は、現在は修正されている、Cisco IOS® ソフトウェアの不具合が原因です。

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。

- DMVPN
- 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 サービス統合型ルータ（ISR）バージョン 15.3(3)M 以降
- Cisco 1000 シリーズ Aggregated Service Router（ASR1K）リリース 3.10 以降

> **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、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

新しい Cisco IOS プラットフォームおよびソフトウェアの利点の 1 つは、次世代の暗号化を使用できることです。1 つの例は、RFC 4106 で論じられているとおり、IPSec の暗号化に Galois/Counter Mode（GCM）の Advanced Encryption Standard（AES）を使用することです。AES GCM により、一部のハードウェアでは暗号化の速度が大幅に向上します。

> **注**：シスコが推奨する次世代暗号化の使用と移行の詳細については、シスコの記事「Next Generation Encryption 」を参照してください。

設定

この設定例では、、DMVPN フェーズ 3 設定から FlexVPN への移行に重点を置いています。それは、これらの設計が同様に機能するからです。

	DMVPN フェーズ 2	DMVPN フェーズ 3	FlexVPN
トランスポート	GRE over IPsec	GRE over IPsec	GRE over IPsec VTI
NHRP の使用	登録と解決策	登録と解決策	解決方法
スポークからのネクスト ホ	他のスポークまたはハブ	ハブからのサマリー	ハブからのサマ

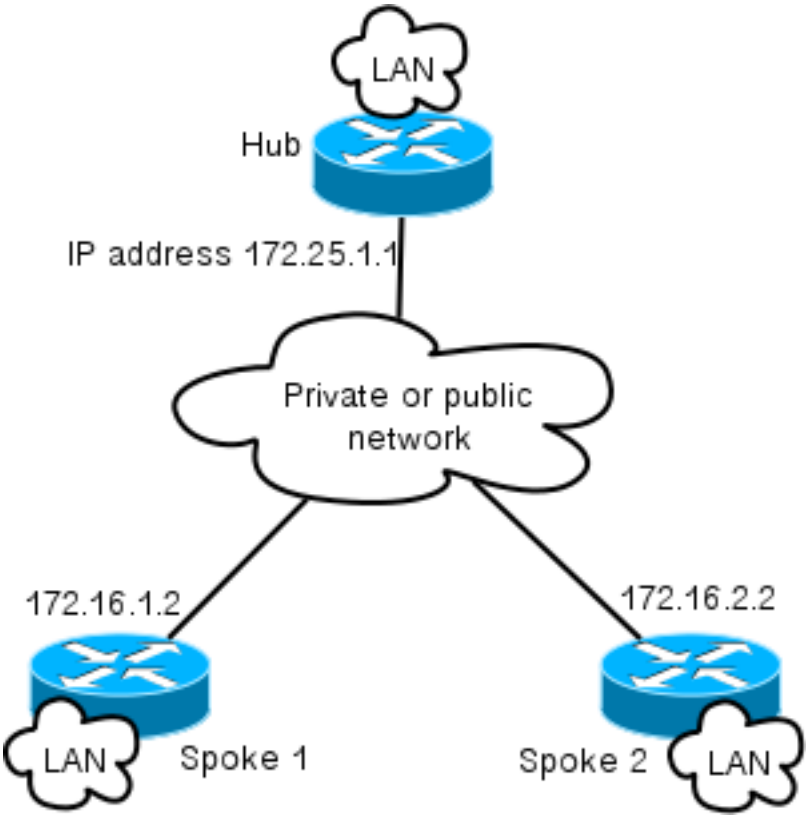
ップ			
NHRP ショートカット スイッチング	No	Yes	あり（オプショ
NHRP リダイレクション	No	Yes	Yes
IKE および IPsec	オプションの IPsec、通常の IKEv1	オプションの IPsec、通常の IKEv1	IPsec、IKEv2

ネットワーク図

このセクションでは、トランスポートとオーバーレイの両方のネットワーク図を提供します。

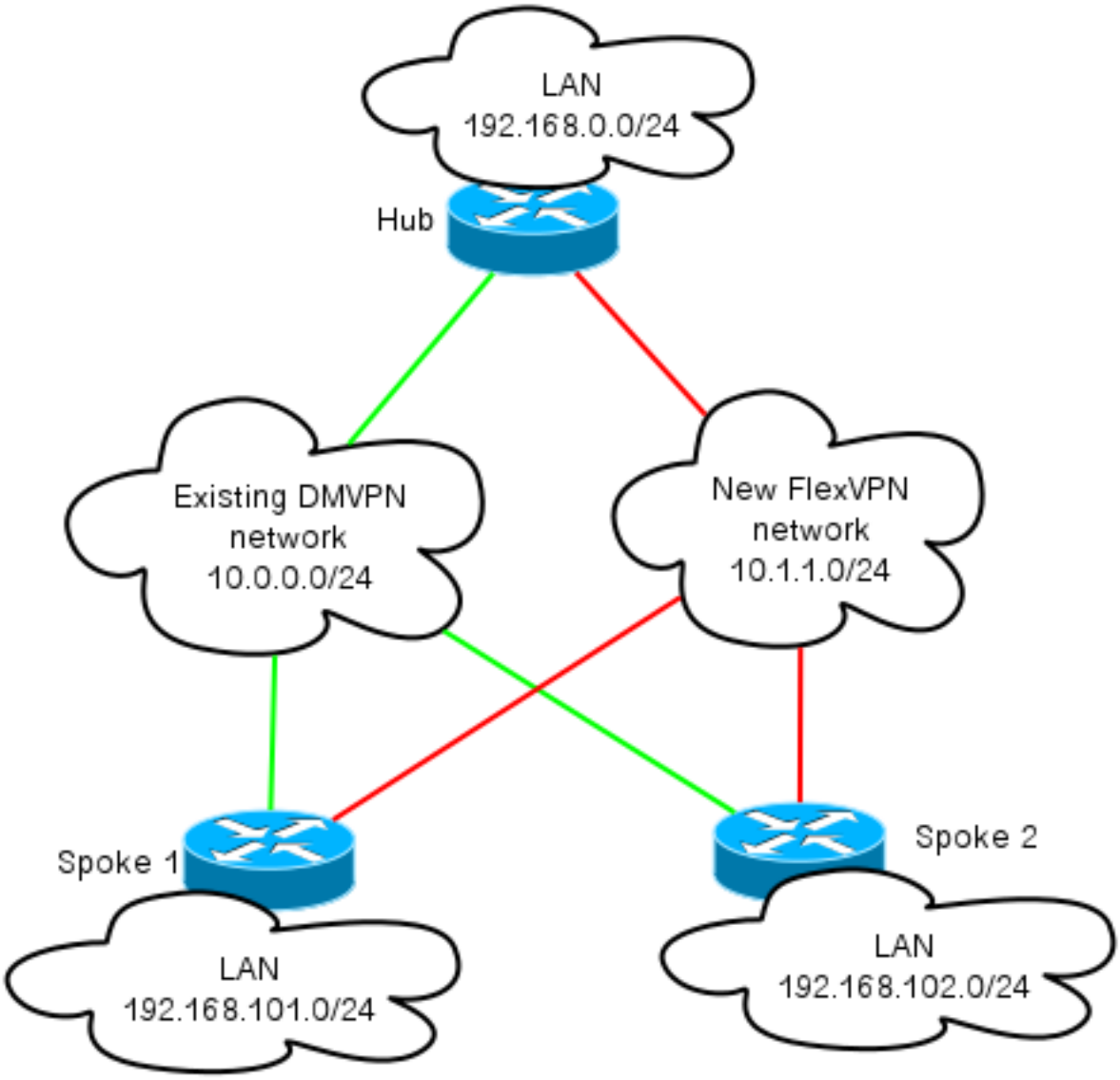
トランスポート ネットワーク図

この例で使用されるトランスポート ネットワークには、2 つのスポークが接続された 1 つのハブが含まれます。すべてのデバイスがインターネットをシミュレートするネットワークを介して接続されます。



オーバーレイ ネットワーク図

この例で使用するオーバーレイネットワークには、2つのスポークが接続された1つのハブが含まれます。DMVPNとFlexVPNの両方が同時にアクティブですが、異なるIPアドレス空間を使用することに注意してください。



設定

この設定では、Enhanced Interior Gateway Routing Protocol(EIGRP)を介したDMVPNフェーズ3の最も一般的な展開を、Border Gateway Protocol(BGP)を使用したFlexVPNに移行します。そのため、FlexVPNを使用することをお勧めします。

> **注**：ハブは同じ IP アドレスの IKEv1（DMVPN）セッションおよび IKEv2（FlexVPN）セッションを終了します。これは、最新の Cisco IOS リリースでのみ実行可能です。

スポーク設定

これは非常に基本的な設定で、IKEv1 と IKEv2 の両方の相互運用を可能にする 2 つの顕著な例外と、共存のために Generic Routing Encapsulation（GRE）over IPsec をトランスポートに使用する 2 つのフレームワークがあります。

> **注**：Internet Security Association and Key Management Protocol（ISAKMP）と IKEv2 の設定に関する変更点は太字で強調表示されます。

```
crypto keyring DMVPN_IKEv1
pre-shared-key address 0.0.0.0 0.0.0.0 key cisco

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 isakmp policy 10
encr aes
authentication pre-share

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

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

interface Tunnel0
 desciption DMVPN tunnel
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 key 0
tunnel protection ipsec profile DMVPN_IKEv1 isakmp-profile DMVPN_IKEv1

interface Tunnel1
description FlexVPN spoke-to-hub 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
tunnel source Ethernet0/0
tunnel destination 172.25.1.1
 tunnel protection ipsec profile default ikev2-profile Flex_IKEv2
```

```
interface Virtual-Template1 type tunnel
description FlexVPN spoke-to-spoke
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 protection ipsec profile default ikev2-profile Flex_IKEv2
```

Cisco IOSリリース15.3では、IKEv2とISAKMPの両方のプロファイルをトンネル保護*設定で結び付けることが*できます。コードの内部変更に加えて、IKEv1とIKEv2を同じデバイスで操作できます。

15.3 以前のリリースで Cisco ISO がプロファイル（IKEv1 または IKEv2）を選択する方法のために、IKEv1 がピアを介して IKEv2 に対して始動される状況など、いくつか警告が必要でした。IKE の分離は、インターフェイス レベルではなくプロファイル レベルに基づき、新しい CLI によって達成されるようになりました。

新しい Cisco IOS リリースのもう 1 つのアップグレードは *トンネル キー*の追加です。これは、DMVPN と FlexVPN の両方が同じ送信元インターフェイスと同じ宛先 IP アドレスを使用するために必要です。このため、トラフィックのカプセル化解除のために、使用されているトンネル インターフェイスを GRE トンネルが検知する方法はありません。トンネルキーを使用すると、tunnel0とtunnel1を小さな（4バイト）オーバーヘッドを追加して区別できます。両方のインターフェイスで異なるキーを設定できますが、通常は1つのトンネルを区別するだけで済みます。

> **注：**共有トンネル保護オプションは、DMVPN と FlexVPN が同じインターフェイスを共有する場合は必要ありません。

したがって、スポーク ルーティング プロトコル設定が基本です。EIGRPとBGPは別々に動作します。EIGRPはスポークツースポークトンネルを介したピアリングを回避するためにトンネルインターフェイスでのみアドバタイズし、拡張性を制限します。BGPはハブルータ(10.1.1.1)とだけ関係を維持します。

```
router eigrp 100
network 10.0.0.0 0.0.0.255
network 192.168.101.0
passive-interface default
no passive-interface Tunnel0

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

ハブ設定

「スポークの設定」で説明されているように、同様の変更をハブ側の設定で実行する必要があります。

注：ISAKMP と IKEv2 の設定に関する変更点は太字で強調表示されます。

```
crypto ikev2 authorization policy default
pool FlexSpokes
route set interface

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 isakmp policy 10
encr aes
authentication pre-share

crypto isakmp key cisco address 0.0.0.0


crypto ipsec profile DMVPN_IKEv1
set transform-set IKEv1

crypto ipsec profile default
set ikev2-profile Flex_IKEv2

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 key 0
 tunnel protection ipsec profile DMVPN_IKEv1

interface Virtual-Template1 type tunnel
ip unnumbered Loopback100
ip mtu 1400
 ip nhrp network-id 2
ip tcp adjust-mss 1360
 tunnel protection ipsec profile default
```

ハブ側では、IKEプロファイルとIPsecプロファイルの間のバインディングは、**tunnel protectionコマンドを使用して完了するスポーク設定とは異なり、プロファイルレベルで発生します。どちらのアプローチも、このバインディングを完了する有効な方法です。**

Next Hop Resolution Protocol（NHRP）ネットワーク ID はクラウドの DMVPN と FlexVPN で異なることに注意してください。ほとんどの場合、NHRP が両方のフレームワークで単一のドメインを作成することは望ましくありません。

トンネル キーは GRE レベルで DMVPN トンネルと FlexVPN トンネルを区別し、**「スポークの設定」セクションで述べているものと同じ目標を達成します。**

ハブのルーティング設定はかなり基本的です。ハブデバイスは、任意のスポークとの2つの関係（EIGRPを使用する関係とBGPを使用する関係）を維持します。BGP設定は、長いスポーク単位の設定を回避するためにlisten-rangeを使用します。

サマリー アドレスは二度導入されます。EIGRP設定は、**tunnel0**設定（IP集約アドレスEIGRP 100）を使用して集約を送信し、BGPは集約アドレスを使用して集約を導入します。集約は、NHRPリダイレクションを実行するために必要です。特定の宛先に対してより良いホップが存在し、スポーク間トンネルを確立できるかどうかを示すコントロールメッセージプロトコル(ICMP)リダイレクト)です。これらのサマリーは、ハブと各スポーク間で送信されるルーティング更新の量を最小限に抑えるために使用されます。

```
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

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
```

確認

この設定例の検証は複数のセクションに分かれています。

移行前のチェック

DMVPN/EIGRP と FlexVPN/BGP は両方が同時に動作するため、スポークが IKEv1 と IKEv2 の両方と IPSec での関係を維持し、適切なプレフィックスが EIGRP と BGP で学習されていることを確認する必要があります。

この例で、**Spoke1 は、2 つのセッションがハブ ルータによって維持されていることを示します**。1 つは IKEv1/Tunnel0 を使用し、1 つは IKEv2/Tunnel1 を使用します。

> **注：**2 つの IPSec セキュリティ アソシエーション（SA）（1 つのインバウンドと 1 つのアウトバウンド）がトンネルごとに維持されます。

```
Spoke1#show cry sess
Crypto session current status

Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
 IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

ルーティングプロトコルを確認する際は、ネイバーシップが形成され、正しいプレフィクスが学習されたことを確認する必要があります。これは最初にEIGRPで確認されます。ハブがネイバーとして見えること、および 192.168.0.0/16 アドレス (サマリー) がハブから学習されていることを確認します。

```
Spoke1#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.0.0.1 Tu0 10 00:04:02 7 1398 0 13

Spoke1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.101.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status

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 26880000
via 10.0.0.1 (26880000/256), Tunnel0
P 10.0.0.0/24, 1 successors, FD is 26880000
via Connected, Tunnel0
```

次に、BGP を確認します。

```
Spoke1#show bgp summary
(...)

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
10.1.1.1 4 65001 13 11 3 0 0 00:06:56 1
Spoke1#show bgp
BGP table version is 3, 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
r>i 192.168.0.0/16 10.1.1.1 0 100 0 i
*> 192.168.101.0 0.0.0.0 0 32768 i
```

出力により、ハブ FlexVPN IP アドレス（10.1.1.1）は、スポークがそれを介して 1 つのプレフィックス（192.168.0.0/16）を受信するネイバーであることが示されます。 さらに、BGP はルーティング情報ベース（RIB）障害が 192.168.0.0/16 プレフィックスに対して発生したことを管理者に知らせます。この障害は、ルーティング テーブルにすでに存在する、そのプレフィックスのより適切なルートがあるために発生します。このルートは EIGRP により発生し、ルーティング テーブルを調べることで確認できます。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
 Known via "eigrp 100", distance 90, metric 26880000, type internal
Redistributing via eigrp 100
Last update from 10.0.0.1 on Tunnel0, 00:10:07 ago
Routing Descriptor Blocks:
* 10.0.0.1, from 10.0.0.1, 00:10:07 ago, via Tunnel0
Route metric is 26880000, traffic share count is 1
Total delay is 50000 microseconds, minimum bandwidth is 100 Kbit
Reliability 255/255, minimum MTU 1400 bytes
Loading 1/255, Hops 1
```

移行

前のセクションでは、IPSec とルーティング プロトコルの両方が設定され、想定したとおりに機能していることを確認しました。同じデバイスでDMVPNからFlexVPNに移行する最も簡単な方法の1つは、アドミニストレーティブディスタンス(AD)を変更することです。この例では、内部BGP(iBGP)のADは200で、EIGRPののADはは90です。

トラフィックがFlexVPNを正しく通過するには、BGPの方が優れたADが必要です。この例では、内部ルートと外部ルートにそれぞれEIGRP ADが230と240に変更されます192.168.0.0/16プレフィクス

これを実現するためのもう 1 つの方法は、BGP AD を減らすことです。ただし、移行後に動作するプロコトルはデフォルト以外の値を含み、導入の他の部分に影響を与える可能性があります。

この例では、スポーク上の動作を確認するために、debug ip routing コマンドが使用されます。

> **注**：このセクションの情報が実稼働ネットワークで使用されている場合は、debugコマンドの使用を避け、次のセクションに示すshowコマンドに依存します。また、スポークEIGRPプロセスはハブとの隣接関係を再確立する必要があります。

```
Spoke1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Spoke1(config)#router eigrp 100
Spoke1(config-router)# distance eigrp 230 240
Spoke1(config-router)#^Z
Spoke1#
*Oct 9 12:12:34.207: %SYS-5-CONFIG_I: Configured from console by console
*Oct 9 12:12:43.648: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is down: route configuration changed

*Oct 9 12:12:43.648: RT: delete route to 192.168.0.0 via 10.0.0.1,
```

```
 eigrp metric [90/26880000]
*Oct 9 12:12:43.648: RT: no routes to 192.168.0.0, delayed flush
*Oct 9 12:12:43.648: RT: delete network route to 192.168.0.0/16
*Oct 9 12:12:43.650: RT: updating bgp 192.168.0.0/16 (0x0) :
via 10.1.1.1

*Oct 9 12:12:43.650: RT: add 192.168.0.0/16 via 10.1.1.1, bgp metric [200/0]
Spoke1#
*Oct 9 12:12:45.750: %DUAL-5-NBRCHANGE: EIGRP-IPv4 100: Neighbor 10.0.0.1
 (Tunnel0) is up: new adjacency
```

この出力には、次のように、注目すべき 3 つの重要なアクションがあります。

- スポークは AD が変更されたことを認識し、隣接関係を無効にします。
- ルーティング テーブルで、EIGRP プレフィクスが再度関連付けられ、BGP が導入されます。
- EIGRP によるハブへの隣接関係が再度オンラインになります。

デバイスで AD を変更すると、デバイスから他のネットワークへのパスのみが影響を受けます。他のルータがルーティングをどのように行うかには影響しません。たとえば、EIGRP ディスタンスが **Spoke1 で増やされると（また、トラフィックをルーティングするためにクラウドで FlexVPN を使用すると）、ハブは設定された（デフォルトの）AD を維持します。**つまり、トラフィックを **Spoke1** に返すために DMVPN が使用されます。

特定のシナリオでは、ファイアウォールが同じインターフェイスでリターントラフィックを期待するような問題が発生する可能性があります。したがって、ハブでADを変更する前に、すべてのスポークでADを変更する必要があります。これが完了した後でのみ、トラフィックは FlexVPN に完全移行されます。

EIGRP 間の移行

DMVPN から EIGRP のみを実行する FlexVPN への移行については、このドキュメントで詳しく説明しません。ただし、すべてを網羅するためにここで述べます。

DMVPNとEIGRPの両方を同じEIGRP Autonomous System（AS；自律システム）ルーティングインスタンスに追加できます。これにより、両方のタイプのクラウド上でルーティング隣接関係が確立されます。これは通常は推奨されません。

FlexVPNまたはDMVPNのいずれかを選択するには、管理者がインターフェイスごとに異なる遅延値を割り当てることができます。ただし、対応する仮想アクセスインターフェイスが存在する間は、仮想テンプレートインターフェイスでは変更が可能ではないことに注意してください。

移行後のチェック

「**移行前のチェック**」セクションで使用されるプロセスと同様に、IPsec とルーティング プロトコルを確認する必要があります。

最初に、IPSec を確認します。

```
Spoke1#show crypto session
Crypto session current status
```

```
Interface: Tunnel0
Profile: DMVPN_IKEv1
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 0
IKEv1 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
 Active SAs: 2, origin: crypto map

Interface: Tunnel1
Profile: Flex_IKEv2
Session status: UP-ACTIVE
Peer: 172.25.1.1 port 500
Session ID: 1
IKEv2 SA: local 172.16.1.2/500 remote 172.25.1.1/500 Active
IPSEC FLOW: permit 47 host 172.16.1.2 host 172.25.1.1
Active SAs: 2, origin: crypto map
```

前と同じように、2 つのセッションが表示され、両方に 2 つのアクティブな IPsec SA があります。

スポークで、集約ルート（192.168.0.0/16）は、ハブからの向きになっており、BGP で学習されます。

```
Spoke1#show ip route 192.168.0.0 255.255.0.0
Routing entry for 192.168.0.0/16, supernet
Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.1 00:14:07 ago
Routing Descriptor Blocks:
* 10.1.1.1, from 10.1.1.1, 00:14:07 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none
```

同様に、ハブの前に付加されているスポークLANは、EIGRPを介して認識されている必要があります。この例では、スポーク2 LANサブネットがチェックされています。

```
Hub#show ip route 192.168.102.0 255.255.255.0
Routing entry for 192.168.102.0/24
 Known via "bgp 65001", distance 200, metric 0, type internal
Last update from 10.1.1.106 00:04:35 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:04:35 ago
Route metric is 0, traffic share count is 1
AS Hops 0
MPLS label: none

Hub#show ip cef 192.168.102.100
192.168.102.0/24
nexthop 10.1.1.106 Virtual-Access2
```

出力で、転送パスは正常に更新され、virtual-access インターフェイスからの向きになっています。

その他の考慮事項

このセクションでは、この設定例に関連するその他の重要な領域について説明します。

既存のスポーク間トンネル

EIGRPからBGPへの移行では、ショートカットスイッチングが引き続き動作するため、スポーク間トンネルは影響を受けません。スポークのショートカットスイッチングは、ADが250の、より具体的なNHRPルートを挿入します。

そうしたルートの例を次に示します。

```
Spoke1#show ip route 192.168.102.100
Routing entry for 192.168.102.0/24
Known via "nhrp", distance 250, metric 1
Last update from 10.1.1.106 on Virtual-Access1, 00:00:42 ago
Routing Descriptor Blocks:
* 10.1.1.106, from 10.1.1.106, 00:00:42 ago, via Virtual-Access1
Route metric is 1, traffic share count is 1
```

移行スポークおよび非移行スポーク間の通信

FlexVPN/BGP にすでにあるスポークが移行プロセスがまだ始まっていないデバイスと通信する場合、トラフィックは常にハブを流れます。

発生するプロセスを次に示します。

1. スポークは、宛先のルート ルックアップを実行します。これは、ハブによってアドバタイズされる集約ルートを通じて指し示すものになります。
2. パケットはハブに向けて送信されます。
3. ハブはパケットを受け取り、宛先のルート ルックアップを実行します。これは、異なる NHRP ドメインの一部である別のインターフェイスから指し示すものになります。

   注：前のハブ設定の NHRP ネットワーク ID は FlexVPN および DMVPN の両方で異なります。

NHRP ネットワーク ID が統一されていても、移行済みのスポークが FlexVPN ネットワークでオブジェクトをルーティングする場合、問題が発生する可能性があります。この中にはショートカット スイッチングを設定するために使用される指令が含まれています。非移行のスポークは、ショートカット スイッチングを実行する特定の目的で、DMVPN ネットワークでオブジェクトを実行しようとします。

トラブルシュート

このセクションでは、移行のトラブルシューティングを行うために一般に使用される 2 つのカテゴリについて説明します。

トンネルの確立試行の問題

IKE ネゴシエーションが失敗する場合、次の手順を実行します。

1. 次のコマンドで現在の状態を確認します。

show crypto isakmp sa - このコマンドは IKEv1 セッションの量、送信元、および宛先を明らかにします。**show crypto ipsec sa- このコマンドは IPsec SA のアクティビティを明らかにします。注：**IKEv1 の場合とは異なり、この出力の Perfect Forward Secrecy（PFS）Diffie-Hellman（DH）Group 値は、最初のトンネル ネゴシエーション時に、**PFS (Y/N):N, DH group:none と表示されます。**ただし、キー再生成が発生した後、正しい値が表示されます。この動作はCSCug67056で説明されていますが、バグではありません。IKEv1とIKEv2の違いは、後者では子SAが**AUTH交換の一部として作成されるということです。**暗号マップに設定された DH グループは、キー再生成時にのみ使用されます。このため、最初のキー再生成までは、**PFS (Y/N):N, DH group:none が表示されます。**IKEv1 では、クイック モード時に子 SA の作成が発生し、**CREATE_CHILD_SA メッセージに鍵交換ペイロードを伝送するためのプロビジョニングがあり、これによって新しい共有秘密を取得する DH パラメータが指定されるため、異なる動作であることがわかります。show crypto ikev2 sa - このコマンドは ISAKMP と同様の出力を提供しますが、IKEv2 に固有です。show crypto session - このコマンドはこのデバイスでの暗号化セッションの要約出力を提供します。show crypto socket - このコマンドは暗号化ソケットの状態を示します。show crypto map - このコマンドはインターフェイスに対する IKE プロファイルと IPsec プロファイルのマッピングを示します。show ip nhrp - このコマンドはデバイスからの NHRP 情報を提供します。**これは FlexVPN セットアップのスポーク間、および DMVPN セットアップのスポーク間およびスポークとハブ間の両方のバインディングに役立ちます。

2. トンネルの確立をデバッグするためには、次のコマンドを使用します。

   debug crypto ikev2debug crypto isakmpdebug crypto ipsecdebug crypto kmi

ルート伝達の問題

EIGRP とトポロジをトラブルシュートするために使用できる、便利なコマンドの一部を次に示します。

- **show bgp summary - このコマンドを使用して、接続されたネイバーおよびその状態を確認します。**
- **show ip eigrp neighbor - このコマンドを使用して、EIGRP により接続されているネイバーを示します。**
- **show bgp - このコマンドを使用して、BGP で学習されたプレフィックスを確認します。**
- **show ip eigrp topology - このコマンドを使用して、EIGRP を通じて学習されたプレフィックスを示します。**

学習したプレフィックスがルーティングテーブルにインストールされているプレフィックスと異なることを知っておくことが重要です。詳細については、シスコの記事の「Route Selection in Cisco Routers」、または『Routing TCP/IP Cisco Press』を参照してください。

既知の注意事項

ASR1K には GRE トンネル処理と同じような制限があります。これは、Cisco Bug ID CSCue00443で追跡されています。現時点では、Cisco IOS XEソフトウェアリリース3.12で修正がスケジュールされています。

修正リリースが利用可能になった際の通知を要望する場合はこのバグをモニタしてください。