FlexVPN の移行： 同じデバイスでの DMVPN から FlexVPN への完全移行

目次

概要

このドキュメントでは、同じデバイスで既存の DMVPN ネットワークから FlexVPN に移行する方法について説明します。

両方のフレームワークのコンフィギュレーションは、デバイスに共存します。

このドキュメントでは、一般的な状況である 認証および EIGRP にルーティング プロトコルとして事前共有キーを使用する DMVPN についてのみ説明します。

このドキュメントでは、BGP（推奨ルーティング プロトコル）および EIGRP（あまりお勧めしません）への移行について説明します。

前提条件

要件

このドキュメントでは、DMVPN および FlexVPN の基本概念について理解していることを前提としています。

使用するコンポーネント

ソフトウェアおよびハードウェアによっては、IKEv2 はサポートされません。 詳細は、『Cisco Feature Navigator』を参照してください。 推奨されるソフトウェア バージョンは次のとおりです。

- ISR - 15.2(4)M1 かより新しい
- 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およびソフトウェアを使用するメリットは、IPSec の暗号化の AES GCM など、次世代暗号化を使用できるということです。 これは RFC 4106 で説明されています。

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、次を参照してください。

http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

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は同時に動作しません。

この制限事項は、CSCuc08066 など Cisco 側の複数の拡張要求により管理される ASR 3.10 リリースで導入される新しい移行機能により削除されます。 これらの機能は、2013 年 6 月下旬にリリースされる予定です。

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、フレームワーク間の影響は最小で、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コンフィギュレーションが共存するが同時に動作しない移行は、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、わずかでも VPN を介した通信が欠落することがあります。

同じデバイス上で完全移行

このドキュメントでは、同じデバイスの既存の DMVPN ネットワークから新しい FlexVPN ネットワークへの移行について説明します。

この移行では、両方のフレームワークが、同じデバイスで同時に動作しないことが前提で、本質的に、FlexVPN をイネーブルにする前に、全体的に DMVPN 機能をディセーブルにする必要があります。

新しい移行機能が使用可能になるまでの同じデバイスを使用した移行方法を次に示します。

1. DMVPN 上の接続性を確認する。
2. FlexVPN 設定を追加して、新しい設定に属するトンネルおよび仮想テンプレート インターフェイスをシャットダウンする。
3. （メンテナンス ウィンドウ中）手順 4 に進む前に、すべてのスポークおよびハブのすべての DMVPN トンネル インターフェイスをシャットダウンする。
4. FlexVPN トンネル インターフェイスをアクティブにする。
5. スポークからハブへの接続性を確認する。
6. スポークからスポークへの接続性を確認する。
7. *ポイント 5 または 6 での確認が正しく行われない場合、FlexVPN インターフェイスをシャットダウンし、DMVPN インターフェイスをアクティブにして DMVPN に戻る。*
8. *スポークからハブへの通信を確認する。*
9. *スポークからスポークへの通信を確認する。*

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、こ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

この図は、インターネットのホストの一般的な接続トポロジを示します。 このドキュメントでは、loopback0（172.25.1.1）のハブの IP アドレスは、IPSec セッションの終了に使用されます。

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（緑の接続）と FlexVPN 接続です。

ローカル エリア ネットワーク プレフィクスは、対応サイドに示されます。

10.1.1.0/24 サブネットは、インターフェイス アドレッシングでは実際のサブネットを示しませんが、FlexVPN クラウド専用の IP スペースのチャンクを示します。 この基本原理については、「FlexVPN のコンフィギュレーション」セクションで説明します。

設定

DMVPN の設定

ここでは、DMVPN のハブとスポークの基本的なコンフィギュレーション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、NHRP 登録がスポークからハブに実行されるので、ハブはスポークの 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が確立されてルートが交換されます。 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

これは、事前共有キー認証および EIGRP ルーティング プロトコルを使用した DMVPN の一般的な設定例です。

```
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 コンフィギュレーションでは、トンネルは、IP アドレス 172.25.1.1 で loopback0 から送信されます。

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 ハブの標準的な展開です。

```
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 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、復元力をはじめ、保護された D チャネルを確立するために必要なメッセージ数まで、IKEv1 よりも優れた機能を提供します。
- GRE： DMVPN とは異なり、スタティックおよびダイナミック ポイントツーポイント インターフェイスが使用され、スタティック マルチポイント GRE インターフェイスを介します。 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、スポークからハブへの直接通信が可能になります。

DMVPN から FlexVPN の完全移行では、2 つのフレームワークが、同じデバイスで同時に動作しません。 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： 別の NHRP ネットワーク ID（推奨）を使用して下さい。
- 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）。
- VRF：VRF の分離によって柔軟性が増しますが、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 のスポーク コンフィギュレーションの相違点の 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。

スポークからハブへ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を選択した場合は、バーチャルテンプレート 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よって受け取った IP アドレスを持つことにも注意してください。 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 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
 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
```

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 172.25.1.1
 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 PKI を推奨します。

ただし、制限を認識したうえで事前共有キー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
```

FlexVPN ハブのコンフィギュレーション

ハブでは一般的にスポークからハブへのダイナミック トンネルの終端のみが行われます。 このため、ハブのコンフィギュレーションでは、FlexVPN のスタティック トンネル インターフェイスではなく、仮想テンプレート インターフェイスが使用されます。 これにより、各接続の仮想アクセス インターフェイスが生成されます。

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、後でルーティング テーブルに、/32 ルートとしてスポークごとに追加されます。

```
aaa new-model
aaa authorization network default local
aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
crypto ikev2 profile Flex_IKEv2
 match identity remote fqdn domain 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
```

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
```

次のコンフィギュレーションでは AES GCM の動作がコメント アウトされていることに注意してください。

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2
! set transform-set IKEv2
interface Loopback0
 description DMVPN termination
```

```
 ip address 172.25.1.1 255.255.255.255
interface Loopback100
 ip address 10.1.1.1 255.255.255.255
interface Virtual-Template1 type tunnel
 ip unnumbered Loopback100
 ip nhrp network-id 2
 ip nhrp redirect
 shutdown
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

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コンフィギュレーションを再利用できます。

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 RSA-SIG を使用することができます。

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 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、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。 BGP のダイナミック ルーティングをイネーブルにします。

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

BGP ネイバーが起動し（移行のこのセクションの「ハブの BGP コンフィギュレーション」を参照）、BGP 上の新しいプレフィ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

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て、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 アドレスの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、新しい FlexVPN クラウド内のすべてのアドレスになります。

```
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
```

トラフィックの FlexVPN への移行

前述のように、移行前に、DMVPN 機能をシャットダウンして、FlexVPN をアクティブにする必要があります。

この手順では、与える影響が最小限になります。

1. すべてのスポークで次を行います。`interface tunnel 0`
   `shut`
2. ハブで次を行います。`interface tunnel 0`
   `shut`この時点でスポークからこのハブへの IKEv1 セッションが何も確立されていないことを確認します。確認するには、**show crypto isakmp sa** コマンドの出力をチェックして、crypto logging session で生成される syslog メッセージを監視します。確認できたら FlexVPN の起動に進むことができます。
3. 引き続きハブで次を行います。`interface Virtual-template 1`
   `no shut`
4. スポークで次を行います。`interface tunnel 1`
   `no shut`

確認手順

IPsec の安定性

IPsec の安定性を評価する最善の方法は、次のコンフィギュレーション コマンドをイネーブルにして syslog を監視することです。

```
crypto logging session
```

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 レベルの問題を示しており、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、次のことを実行することで確認できます。

```
show bgp
! or
show bgp ipv4 unicast
! or
show ip bgp summary
```

ハブからの正しい情報の例：

```
Hub#show bgp
BGP router identifier 172.25.1.1, local AS number 65001
(...omitted...)
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
*10.1.1.101 4 65001 83 82 13 0 0 01:10:46 1 *10.1.1.102 4 65001 7 7 13 0 0 00:00:44 1
```

各スポークのプレフィクスが 1 で、両方のスポークがダイナミック（アスタリスク（*）記号）で

あるとハブが認識したことがわかります。

スポークからの同様の情報の例を示します。

```
Spoke1#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 11 11 6 0 0 00:03:43 1
```

スポークは、ハブから 1 プレフィクスを受信しています。 この設定のプレフィクスは、ハブでアドバタイズされたサマリーです。

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な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、スケールは BGP の方が優れていて、EIGRP は、BGP により簡単に使用できる多くの高度なメカニズムを提供しません。

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 つを説明します。

更新されたスポークのコンフィギュレーション

この例では、新しい AS は、個別の EIGRP プロセスで追加されます。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
 network 192.168.101.0
 passive-interface default
 no passive-interface Tunnel1
```

注: スポーク間トンネルでルーティング プロトコルの隣接関係を確立せず、パッシブでない tunnel1（スポークからハブ）のインターフェイスを作成します。

更新されたハブのコンフィギュレーション

ハブでも、DMVPN は、トラフィックを交換する推奨方法です。 ただし、FlexVPN は、同じプレフィクスをアドバタイズおよび学習します。

```
router eigrp 200
 network 10.1.1.0 0.0.0.255
```

サマリーをスポークに戻す 2 つの方法があります。

- null0 を指すスタティック ルートを再配布します（推奨）。`ip route 192.168.0.0 255.255.0.0 null 0`
  ```
  ip access-list standard EIGRP_SUMMARY
   permit 192.168.0.0 0.0.255.255
  router eigrp 200
   distribute-list EIGRP_SUMMARY out Virtual-Template1
   redistribute static metric 1500 10 10 1 1500
  ```
  この方法では、ハブの VT コンフィギュレーション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。
- 別の方法として、バーチャルテンプレートで DMVPN スタイルのサマリー アドレスを設定で

きます。 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バーチャル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 200 172.16.1.0 255.255.255.0
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0 delay 2000
```

トラフィックの FlexVPN への移行

移行前に、DMVPN 機能をシャットダウンして、FlexVPN をアクティブにする必要があります。

次の手順では、与える影響が最小限になります。

1. すべてのスポークで次を行います。`interface tunnel 0`
   `shut`
2. ハブで次を行います。`interface tunnel 0`
   `shut`この時点でスポークからこのハブへの IKEv1 セッションが何も確立されていないことを確認します。確認するには、**show crypto isakmp sa** コマンドの出力をチェックして、crypto logging session で生成される syslog メッセージを監視します。確認できたら FlexVPN の起動に進むことができます。
3. 引き続きハブで次を行います。`interface Virtual-template 1`
   `no shut`
4. すべてのスポークで次を行います。`interface tunnel 1`
   `no shut`

確認手順

IPsec の安定性

BGP の場合、IPsec が安定しているか評価する必要があります。 最善の方法は、次のコンフィギュレーション コマンドをイネーブルにして syslog を監視することです。

`crypto logging session`
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 レベルの問題を示しており、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追加されていないことを確認します。 これはハブとスポークで次のコマンドを発行することで確認できます。

`show ip eigrp topology`
スポークからの正しい出力の例：

```
Spoke1#sh 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
(...omitted as output related to DMVPN cloud ...)
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)
```

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 (26114560/1709056), Tunnel1 P **10.1.1.107/32**, 1 successors, FD is 26112000 via Connected, Tunnel1
スポークが LAN のサブネット（イタリック体）とそれらのサマリー（**太字**）を知っていることがわかります。

ハブからの正しい出力の例：

```
Hub#sh ip eigrp topology
EIGRP-IPv4 Topology Table for AS(100)/ID(172.25.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
 r - reply Status, s - sia Status
(...omitted, related to DMVPN...)
EIGRP-IPv4 Topology Table for AS(200)/ID(172.25.1.1)
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, Loopback100
```

P *192.168.101.0/24, 1 successors, FD is 1561600 via 10.1.1.107 (1561600/281600), Virtual-Access1* **P 192.168.0.0/16, 1 successors, FD is 1709056 via Rstatic (1709056/0)** P 10.1.1.107/32, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 10.1.1.106/32, 1 successors, FD is 1709056 via Rstatic (1709056/0) P 0.0.0.0/0, 1 successors, FD is 1709056 via Rstatic (1709056/0) P *192.168.102.0/24, 1 successors, FD is 1561600 via 10.1.1.106 (1561600/281600), Virtual-Access2*
ハブがスポークの LAN のサブネット（イタリック体）、アドバタイジングしているサマリー プレフィクス（**太字**）、および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 アドレスを知っ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、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

前述のように、FlexVPN ハブは、トラフィックのルーティング方法を判別するために、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、ハブの NHRP をクリアすると、短期間の接続問題が発生することがあります。

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。 NHRP をクリアしても、ハブは、FlexVPN セッションには影響しません。

これは、次のような FlexVPN のデフォルト動作のためです。

- 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、CSCub07382 による影響を受ける可能性があります。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems