FlexVPN-Migration: Harte Migration von DMVPN zu FlexVPN auf einem anderen Hub

Inhalt

Einleitung

Dieses Dokument enthält Informationen zur Migration von einem Dynamic Multipoint VPN (DMVPN)-Netzwerk zu FlexVPN auf verschiedenen Hub-Geräten. Die Konfigurationen für beide Frameworks existieren gleichzeitig auf den Geräten. In diesem Dokument wird nur das gängigste Szenario dargestellt: DMVPN mit dem vorinstallierten Schlüssel für die Authentifizierung und EIGRP (Enhanced Interior Gateway Routing Protocol) als Routing-Protokoll. In diesem Dokument wird die Migration zum Border Gateway Protocol (BGP), dem empfohlenen Routing-Protokoll, und zum weniger wünschenswerten EIGRP gezeigt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- DMVPN
- FlexVPN

Verwendete Komponenten

> **Anmerkung:** Nicht alle Software und Hardware unterstützt Internet Key Exchange Version 2 (IKEv2). Weitere Informationen finden Sie im Cisco Feature Navigator.

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Integrated Service Router (ISR) Version 15.2(4)M1 oder höher
- Cisco Aggregation Services Router der Serie 1000 (ASR1K) 3.6.2 Version 15.2(2)S2 oder höher

Einer der Vorteile einer neueren Plattform und Software besteht in der Möglichkeit, Kryptografie der nächsten Generation zu verwenden, z. B. AES-Galois/Counter Mode (GCM) für die Verschlüsselung in IPsec (Internet Protocol Security), wie unter Request for Comments (RFC) 4106 beschrieben. Mit AES GCM können Sie eine wesentlich schnellere Verschlüsselungsgeschwindigkeit auf einigen Hardwarekomponenten erreichen. Empfehlungen von Cisco zur Verwendung von und Migration zur Verschlüsselung der nächsten Generation finden Sie im Artikel Verschlüsselung der nächsten Generation.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Migrationsverfahren

Die empfohlene Methode für die Migration von DMVPN zu FlexVPN besteht derzeit darin, dass die beiden Frameworks nicht gleichzeitig funktionieren. Diese Einschränkung soll aufgehoben werden, da neue Migrationsfunktionen in der Version ASR 3.10 eingeführt werden sollen, die unter mehreren Erweiterungsanforderungen von Cisco nachverfolgt werden, darunter die Cisco Bug-ID CSCuc08066. Diese Funktionen dürften Ende Juni 2013 verfügbar sein.

Eine Migration, bei der beide Frameworks nebeneinander existieren und gleichzeitig auf denselben Geräten betrieben werden, wird als **Soft Migration** bezeichnet, was die minimalen Auswirkungen und das reibungslose Failover von einem Framework zum anderen anzeigt. Eine Migration, bei der Konfigurationen für beide Frameworks nebeneinander existieren, aber nicht gleichzeitig funktionieren, wird als **harte Migration** bezeichnet. Dies weist darauf hin, dass ein Switchover von einem Framework zum anderen einen Mangel an Kommunikation über das VPN bedeutet, selbst wenn dieser minimal ist.

Hard Migration zwischen zwei verschiedenen Hubs

In diesem Dokument wird die Migration vom derzeit verwendeten DMVPN-Hub zu einem neuen FlexVPN-Hub behandelt. Diese Migration ermöglicht die Kommunikation zwischen bereits zu FlexVPN migrierten Stationen und solchen, die noch auf DMVPN laufen und in mehreren Phasen, jeweils separat, ausgeführt werden können.

Sofern die Routing-Informationen korrekt ausgefüllt sind, sollte die Kommunikation zwischen migrierten und nicht migrierten Stationen möglich bleiben. Eine zusätzliche Latenz ist jedoch zu beobachten, da migrierte und nicht migrierte Spokes keine Spoke-to-Spoke-Tunnel erstellen. Zugleich sollten migrierte Spokes in der Lage sein, untereinander direkte Spoke-to-Spoke-Tunnel einzurichten. Gleiches gilt für nicht migrierte Stationen.

Führen Sie bis zur Bereitstellung dieser neuen Migrationsfunktion die folgenden Schritte aus, um Migrationen mit einem anderen Hub als DMVPN und FlexVPN durchzuführen:

1. Überprüfen der Verbindung über DMVPN
2. Fügen Sie die FlexVPN-Konfiguration hinzu, und schließen Sie den Tunnel, der zur neuen Konfiguration gehört.
3. (Während eines Wartungsfensters) Fahren Sie bei jedem Spoke einzeln den DMVPN-Tunnel herunter.
4. Fahren Sie bei denselben Spokes wie in Schritt 3 die FlexVPN-Tunnelschnittstellen aus.
5. Überprüfen der Spoke-to-Hub-Verbindung
6. Überprüfen der Spoke-to-Spoke-Konnektivität in FlexVPN
7. Überprüfen Sie die Spoke-to-Spoke-Konnektivität mit DMVPN von FlexVPN.
8. Wiederholen Sie die Schritte 3 bis 7 für jedes Spoke separat.
9. Wenn bei den in den Schritten 5, 6 oder 7 beschriebenen Prüfungen Probleme auftreten, fahren Sie die FlexVPN-Schnittstelle herunter und deaktivieren Sie die DMVPN-Schnittstellen, um zum DMVPN zurückzukehren.
10. Überprüfen der Spoke-to-Hub-Kommunikation über das gesicherte DMVPN
11. Überprüfen der Spoke-to-Spoke-Kommunikation über das gesicherte DMVPN

Individueller Ansatz

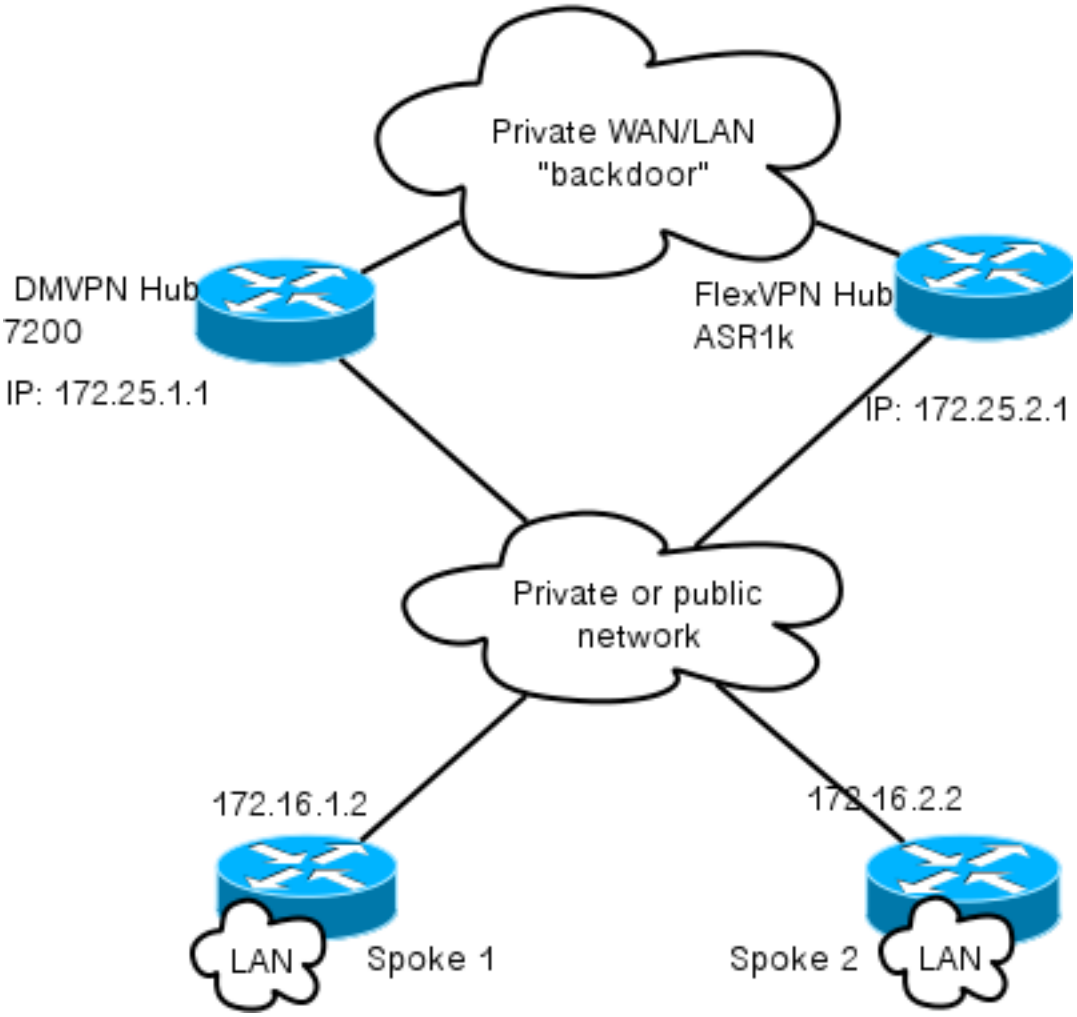
Sollte der vorherige Ansatz aufgrund der Komplexität Ihres Netzwerks oder der Routing-

Umgebung nicht die beste Lösung für Sie sein, sollten Sie sich vor der Migration mit Ihrem Ansprechpartner bei Cisco in Verbindung setzen. Die beste Person, mit der Sie einen individuellen Migrationsprozess besprechen können, ist Ihr Systemingenieur oder Advanced Services Engineer.

Netzwerktopologie

Transportnetz-Topologie

Dieses Diagramm zeigt die typische Verbindungstopologie von Hosts im Internet. Die IP-Adresse des Hubs **loopback0** (**172.25.1.1**) wird zum Beenden der DMVPN-IPsec-Sitzung verwendet. Die IP-Adresse des neuen Hubs (**172.25.2.1**) wird für FlexVPN verwendet.

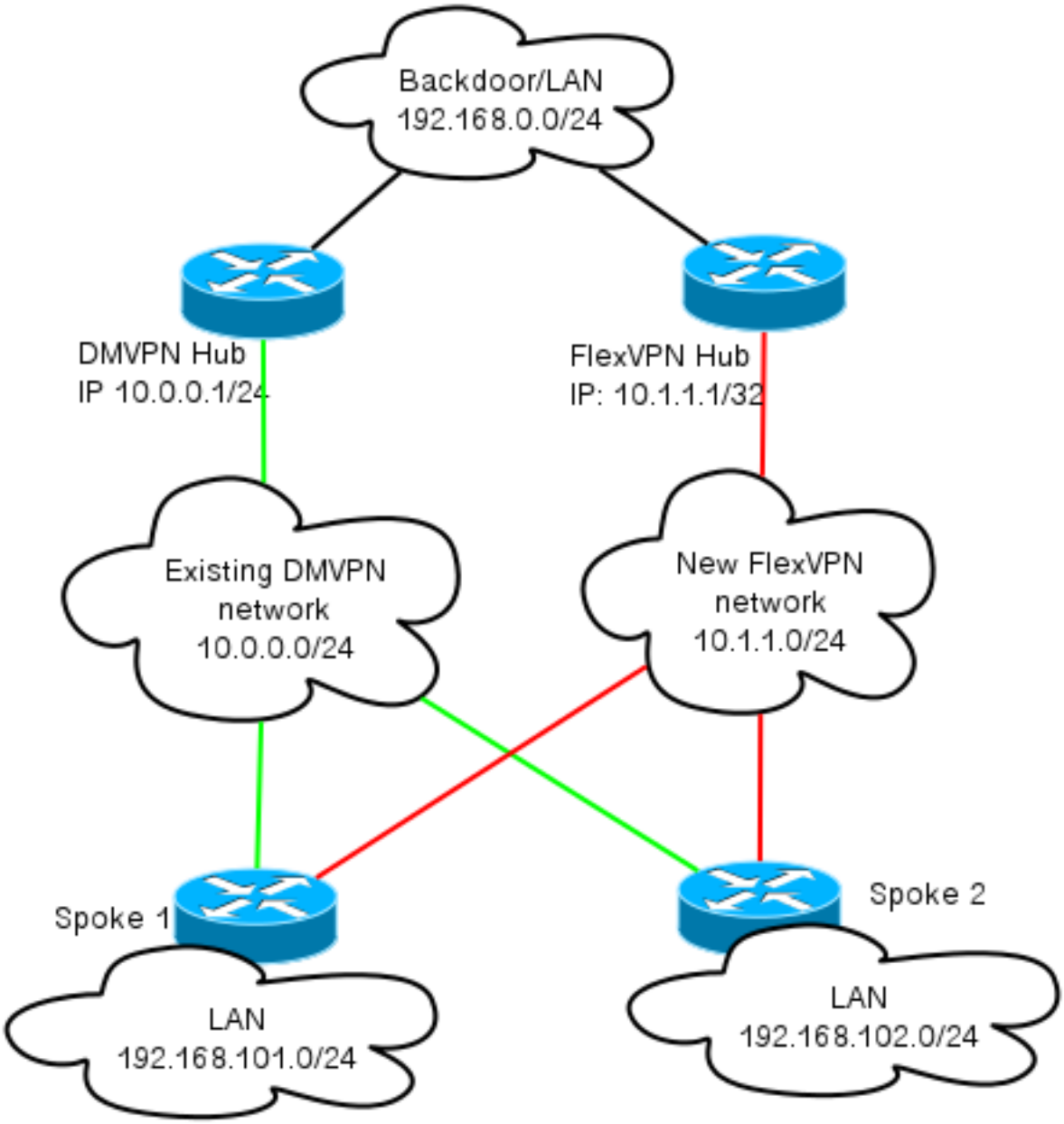


Beachten Sie die Verbindung zwischen den beiden Hubs. Diese Verbindung ist wichtig, um während der Migration Verbindungen zwischen den FlexVPN- und DMVPN-Clouds zu ermöglichen. Sie ermöglicht Spokes, die bereits zu FlexVPN migriert wurden, die Kommunikation mit DMVPN-Netzwerken und umgekehrt.

Overlay-Netzwerktopologie

Dieses Topologiediagramm zeigt zwei separate Clouds, die für Overlay verwendet werden: DMVPN (grüne Verbindungen) und FlexVPN (rote Verbindungen). LAN-Präfixe werden für die

entsprechenden Standorte angezeigt. Das **10.1.1.0/24**-Subnetz stellt kein tatsächliches Subnetz für die Schnittstellenadressierung dar, stellt jedoch einen Teil des IP-Raumes dar, der der FlexVPN-Cloud gewidmet ist. Die Gründe hierfür werden später im Abschnitt **FlexVPN Configuration** erläutert.



Konfiguration

In diesem Abschnitt werden die DMVPN- und die FlexVPN-Konfigurationen beschrieben.

DMVPN-Konfiguration

In diesem Abschnitt wird die grundlegende Konfiguration für den DMVPN-Hub und die Spoke-Funktion beschrieben.

Der Pre-Shared Key (PSK) wird für die IKEv1-Authentifizierung verwendet. Nach der Einrichtung von IPsec wird die NHRP-Registrierung (Next Hop Resolution Protocol) von Spoke-to-Hub durchgeführt, sodass der Hub die NBMA-Adressierung (Nonbroadcast Multiaccess) dynamisch

erlernen kann.

Wenn das NHRP die Registrierung für den Spoke-Router und den Hub durchführt, kann eine Routing-Adjacancy eingerichtet und Routen ausgetauscht werden. In diesem Beispiel wird EIGRP als einfaches Routing-Protokoll für das Overlay-Netzwerk verwendet.

Spoke-DMVPN-Konfiguration

Hier finden Sie ein einfaches Beispiel für die Konfiguration von DMVPN mit PSK-Authentifizierung und EIGRP als Routing-Protokoll.

```
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
```

Hub-DMVPN-Konfiguration

In der Hub-Konfiguration wird der Tunnel von **loopback0** mit der IP-Adresse **172.25.1.1** bezogen. Der Rest ist eine Standardbereitstellung eines DMVPN-Hubs mit EIGRP als Routing-Protokoll.

```
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-Konfiguration

FlexVPN basiert auf den folgenden grundlegenden Technologien:

- **IPsec:** Im Gegensatz zum Standard in DMVPN wird IKEv2 anstelle von IKEv1 verwendet, um IPsec Security Associations (SAs) auszuhandeln. IKEv2 bietet im Vergleich zu IKEv1 Verbesserungen wie Ausfallsicherheit und die Anzahl der Nachrichten, die für die Einrichtung eines geschützten Datenkanals erforderlich sind.

- **GRE :** Im Gegensatz zu DMVPN werden statische und dynamische Point-to-Point-Schnittstellen verwendet und nicht nur eine statische Multipoint-GRE-Schnittstelle. Diese Konfiguration bietet zusätzliche Flexibilität, insbesondere für das Verhalten pro Spoke/Hub.

- **NHRP**: In FlexVPN wird NHRP hauptsächlich zur Herstellung einer Spoke-to-Spoke-Kommunikation verwendet. Spokes registrieren sich nicht beim Hub.

- **Routing**: Da Stationen keine NHRP-Registrierung für den Hub durchführen, müssen Sie sich auf andere Mechanismen verlassen, um sicherzustellen, dass der Hub und die Stationen bidirektional kommunizieren können. Ähnlich wie bei DMVPN können dynamische Routing-Protokolle verwendet werden. FlexVPN ermöglicht Ihnen jedoch die Verwendung von IPsec, um Routing-Informationen einzuführen. Standardmäßig wird als **/32-**Route für die IP-Adresse auf der anderen Seite des Tunnels eingeführt, was eine direkte Spoke-to-Hub-Kommunikation ermöglicht.

Bei einer harten Migration von DMVPN zu FlexVPN funktionieren die beiden Frames nicht gleichzeitig auf den gleichen Geräten. Es wird jedoch empfohlen, sie separat zu halten.

Trennen Sie sie auf mehreren Ebenen:

- NHRP - Verwenden Sie eine andere NHRP-Netzwerk-ID (empfohlen).
- Routing - Verwenden Sie separate Routing-Prozesse (empfohlen).
- Virtual Routing and Forwarding (VRF) - Die VRF-Trennung erhöht die Flexibilität, wird hier jedoch nicht behandelt (optional).

Spoke FlexVPN-Konfiguration

Einer der Unterschiede in der Spoke-Konfiguration in FlexVPN im Vergleich zu DMVPN besteht darin, dass Sie potenziell über zwei Schnittstellen verfügen. Für die Kommunikation zwischen Spoke-to-Hub ist ein erforderlicher Tunnel und für Spoke-to-Spoke-Tunnel ein optionaler Tunnel erforderlich. Wenn Sie kein dynamisches Spoke-to-Spoke-Tunneling verwenden und es vorziehen, dass alles über das Hub-Gerät läuft, können Sie die virtuelle Vorlagenschnittstelle entfernen und das NHRP-Shortcut-Switching von der Tunnelschnittstelle entfernen.

Beachten Sie, dass die statische Tunnelschnittstelle eine auf Aushandlung basierende IP-Adresse empfängt. Auf diese Weise kann der Hub die IP-Adresse der Tunnelschnittstelle dynamisch für das Spoke bereitstellen, ohne dass eine statische Adressierung in der FlexVPN-Cloud erstellt werden muss.

```
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
```

> **Anmerkung:** Standardmäßig wird die lokale Identität festgelegt, um die IP-Adresse zu verwenden. Daher muss die entsprechende Match-Anweisung auf dem Peer auch auf Basis der Adresse übereinstimmen. Wenn die Anforderung auf Basis des DNs (Distinguished Name) im Zertifikat übereinstimmt, muss die Übereinstimmung mithilfe einer Zertifikatszuordnung erfolgen.

Cisco empfiehlt die Verwendung von AES GCM mit unterstützender Hardware.

```
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
```

Public Key Infrastructure (PKI) ist die empfohlene Methode für die Durchführung einer groß angelegten Authentifizierung in IKEv2. Sie können PSK jedoch weiterhin verwenden, solange Sie sich der Einschränkungen bewusst sind.

Hier ist eine Beispielkonfiguration, die **cisco** als PSK verwendet.

```
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
```

Konfiguration des FlexVPN-Hubs

In der Regel terminiert ein Hub nur dynamische Spoke-to-Hub-Tunnel. Aus diesem Grund finden Sie in der Hub-Konfiguration keine statische Tunnelschnittstelle für FlexVPN. Stattdessen wird eine virtuelle Vorlagenschnittstelle verwendet.

> **Anmerkung:** Auf der Hub-Seite müssen Sie die Pooladressen angeben, die Spokes zugewiesen werden sollen.

Adressen aus diesem Pool werden später in der Routing-Tabelle als **/32** Routen für jeden Spoke hinzugefügt.

```
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
local identity fqdn hub.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
```

Cisco empfiehlt die Verwendung von AES GCM mit unterstützender Hardware.

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

Anmerkung: In dieser Konfiguration wurde der AES-GCM-Vorgang kommentiert.

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

interface Loopback0
description DMVPN termination
ip address 172.25.2.1 255.255.255.255
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
tunnel path-mtu-discovery
tunnel protection ipsec profile default
ip local pool FlexSpokes 10.1.1.100 10.1.1.254
```

Bei der Authentifizierung in IKEv2 gilt für den Hub das gleiche Prinzip wie für den Spoke-Router. Für Skalierbarkeit und Flexibilität sollten Sie Zertifikate verwenden. Sie können jedoch dieselbe Konfiguration für PSK wie in der Spoke-Anwendung verwenden.

Anmerkung: IKEv2 bietet Flexibilität bei der Authentifizierung. Eine Seite kann sich mit PSK authentifizieren, die andere Seite mit Rivest-Shamir-Adleman Signature (RSA-SIG).

Wenn vorinstallierte Schlüssel für die Authentifizierung verwendet werden sollen, ähneln die Konfigurationsänderungen den für den Spoke-Router hier beschriebenen.

BGP-Verbindung zwischen Hub und Hub

Stellen Sie sicher, dass die Hubs wissen, wo sich bestimmte Präfixe befinden. Dies gewinnt zunehmend an Bedeutung, da einige Stationen auf FlexVPN migriert wurden, während andere Stationen auf DMVPN verbleiben.

Die BGP-Verbindung zwischen Hub basiert auf der DMVPN-Hub-Konfiguration:

```
router bgp 65001
network 192.168.0.0
neighbor 192.168.0.2 remote-as 65001
```

Datenverkehrsmigration

Migration zum BGP als Overlay Routing Protocol [empfohlen]

BGP ist ein Routing-Protokoll, das auf einem Unicast-Austausch basiert. Aufgrund seiner Eigenschaften ist es das beste Skalierungsprotokoll in DMVPN-Netzwerken.

In diesem Beispiel wird das interne BGP (iBGP) verwendet.

Spoke-BGP-Konfiguration

Die Spoke-Migration besteht aus zwei Teilen. Aktivieren Sie zunächst BGP als dynamisches Routing:

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

Wenn der BGP-Nachbar aktiviert ist (siehe nächster Abschnitt) und neue Präfixe über BGP abgerufen werden, können Sie Datenverkehr von der aktuellen DMVPN-Cloud in eine neue FlexVPN-Cloud verlagern.

Hub-BGP-Konfiguration

FlexVPN-Hub - vollständige BGP-Konfiguration

Konfigurieren Sie auf dem Hub dynamische Listener, um zu verhindern, dass die Nachbarschaftskonfiguration für jedes Spoke separat beibehalten wird. In dieser Konfiguration initiiert das BGP keine neuen Verbindungen, sondern akzeptiert Verbindungen aus dem bereitgestellten Pool von IP-Adressen. In diesem Fall lautet der Pool **10.1.1.0/24**, d. h. alle Adressen in der neuen FlexVPN-Cloud.

Zwei Punkte sind zu beachten:

- Der FlexVPN-Hub kündigt dem DMVPN-Hub bestimmte Präfixe an. so wird die nicht unterdrückte Karte verwendet.
- Weisen Sie entweder das FlexVPN-Subnetz von **10.1.1.0/24** der Routing-Tabelle zu, oder stellen Sie sicher, dass der DMVPN-Hub den FlexVPN-Hub als nächsten Hop anzeigt.

Dieses Dokument zeigt den letzteren Ansatz.

```
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-Hub - Vollständige BGP- und EIGRP-Konfiguration

Die Konfiguration des DMVPN-Hub ist einfach, da er nur bestimmte Präfixe vom FlexVPN-Hub empfängt und Präfixe ankündigt, die er von EIGRP erhält.

```
router bgp 65001
bgp log-neighbor-changes
redistribute eigrp 100
neighbor 192.168.0.2 remote-as 65001
```

Datenverkehr auf BGP/FlexVPN migrieren

Wie bereits erwähnt, müssen Sie die DMVPN-Funktionalität herunterfahren und FlexVPN aktivieren, um die Migration durchzuführen.

Dieses Verfahren garantiert minimale Auswirkungen:

1. Geben Sie bei jedem Spoke einzeln Folgendes ein:

   ```
   interface tunnel 0
    shut
   ```

   Stellen Sie an diesem Punkt sicher, dass für diesen Spoke keine IKEv1-Sitzungen eingerichtet wurden. Dies kann überprüft werden, wenn Sie die Ausgabe des Befehls **show crypto isakmp sa** überprüfen und Syslog-Meldungen überwachen, die durch den Befehl **crypto logging session** generiert wurden. Sobald dies bestätigt ist, können Sie mit der Aktivierung von FlexVPN fortfahren.

2. Geben Sie in das gleiche Feld Folgendes ein:

   ```
   interface tunnel 1
     no shut
   ```

Überprüfungsschritte

IPsec-Stabilität

Die beste Methode zur Bewertung der IPsec-Stabilität ist die Überwachung von Sylogs mit dem Konfigurationsbefehl **Crypto Logging Session** Configuration. Wenn Sitzungen nach oben und unten angezeigt werden, kann dies auf ein Problem auf IKEv2/FlexVPN-Ebene hinweisen, das behoben werden muss, bevor die Migration beginnen kann.

Eingesetzte BGP-Informationen

Wenn IPsec stabil ist, stellen Sie sicher, dass die BGP-Tabelle mit Einträgen der Stationen (auf dem Hub) und Zusammenfassung vom Hub (auf den Stationen) gefüllt ist. Im Fall von BGP kann dies mit den folgenden Befehlen angezeigt werden:

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

Hier ein Beispiel für korrekte Informationen vom FlexVPN-Hub:

```
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
```

Die Ausgabe zeigt, dass der Hub ein Präfix von jedem der Stationen gelernt hat, und beide Stationen sind dynamisch und mit einem Sternchen (*) gekennzeichnet. Es zeigt auch, dass insgesamt vier Präfixe aus der Verbindung zwischen den Hubs empfangen werden.

Hier ein Beispiel für ähnliche Informationen aus dem Spoke:

```
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
```

Der Spoke-Router hat zwei Präfixe vom Hub erhalten. Bei dieser Konfiguration sollte ein Präfix die auf dem FlexVPN-Hub angegebene Zusammenfassung sein. Das andere ist das DMVPN **10.0.0.0/24**-Netzwerk, das auf dem DMVPN-Spoke in das BGP umverteilt wird.

Migration zu neuen Tunneln mit EIGRP

EIGRP ist aufgrund seiner relativ einfachen Bereitstellung und schnellen Konvergenz eine beliebte Wahl in DMVPN-Netzwerken. Es lässt sich jedoch schlechter skalieren als BGP und bietet nicht viele erweiterte Mechanismen, die BGP sofort nutzen kann. Im nächsten Abschnitt wird eine Möglichkeit beschrieben, wie Sie mit einem neuen EIGRP-Prozess zu FlexVPN wechseln können.

Aktualisierte Spoke-Konfiguration

Ein neues autonomes System (AS) wird mit einem separaten EIGRP-Prozess hinzugefügt:

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

> **Anmerkung:** Es ist am besten, keine Routing-Protokoll-Adjacency über Spoke-to-Spoke-Tunnel einzurichten. Daher sollte die Schnittstelle von **tunnel1** (Spoke-to-Hub) nur nicht passiv sein.

Aktualisierte FlexVPN-Hub-Konfiguration

Bereiten Sie für den FlexVPN-Hub ebenfalls das Routing-Protokoll im entsprechenden AS vor, indem Sie es mit einem auf den Stationen konfigurierten Protokoll abgleichen.

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

Es gibt zwei Methoden, um eine Zusammenfassung zurück zum Spoke bereitzustellen.

- Verteilen Sie eine statische Route, die auf **null0** zeigt (bevorzugte Option).

```
ip route 192.168.0.0 255.255.0.0 null 0
ip route 10.1.1.0 255.255.255.0 null 0

ip prefix-list EIGRP_SUMMARY_ONLY seq 5 permit 192.168.0.0/16
ip prefix-list EIGRP_SUMMARY_ONLY seq 10 permit 10.1.1.0/24

route-map EIGRP_SUMMARY permit 20
match ip address prefix-list EIGRP_SUMMARY_ONLY

router eigrp 200
distribute-list route-map EIGRP_SUMMARY out Virtual-Template1
redistribute static metric 1500 10 10 1 1500 route-map EIGRP_SUMMARY
```

  Diese Option ermöglicht die Kontrolle der Zusammenfassung und Neuverteilung ohne Änderungen an der VT-Konfiguration (Virtualization Technology) des Hubs. Dies ist wichtig, da die VT-Konfiguration des Hubs nicht geändert werden kann, wenn ihm ein aktiver virtueller Zugriff zugeordnet ist.

- Richten Sie eine zusammengefasste Adresse im DMVPN-Stil auf einer virtuellen Vorlage ein.

  Diese Konfiguration wird *nicht empfohlen*, da diese Zusammenfassung intern verarbeitet und auf jeden virtuellen Zugriff repliziert wird. Sie wird hier als Referenz angezeigt.

```
interface Virtual-Template1 type tunnel
```

```
ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Ein weiterer Aspekt, der berücksichtigt werden muss, ist der Routing-Austausch zwischen den Hub. Dies ist möglich, wenn Sie EIGRP-Instanzen an iBGP verteilen.

DMVPN-Hub - aktualisierte BGP-Konfiguration

Die Konfiguration bleibt einfach. Bestimmte Präfixe müssen von EIGRP an BGP neu verteilt werden:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

FlexVPN-Hub - aktualisierte BGP-Konfiguration

Ähnlich wie beim DMVPN-Hub müssen Sie in FlexVPN die Präfixe des neuen EIGRP-Prozesses an BGP verteilen:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Datenverkehr auf FlexVPN migrieren

Sie müssen die DMVPN-Funktionalität herunterfahren und FlexVPN in jedem Spoke einzeln aktivieren, um die Migration durchzuführen. Dieses Verfahren garantiert minimale Auswirkungen:

1. Geben Sie bei jedem Spoke einzeln Folgendes ein:

   ```
   interface tunnel 0
    shut
   ```

   Stellen Sie an diesem Punkt sicher, dass keine IKEv1-Sitzungen für diesen Spoke-Server eingerichtet wurden. Dies kann überprüft werden, wenn Sie die Ausgabe des Befehls **show crypto isakmp sa** überprüfen und Syslog-Meldungen überwachen, die durch den Befehl **crypto logging session** generiert wurden. Sobald dies bestätigt ist, können Sie mit der Aktivierung von FlexVPN fortfahren.
2. Geben Sie in das gleiche Feld Folgendes ein:

   ```
   interface tunnel 1
     no shut
   ```

Überprüfungsschritte

IPsec-Stabilität

Wie beim BGP müssen Sie beurteilen, ob IPsec stabil ist. Am besten überwachen Sie Sylogs mit dem Konfigurationsbefehl **Crypto logging session**. Wenn Sitzungen nach oben und unten verlaufen, kann dies auf ein Problem auf IKEv2/FlexVPN-Ebene hinweisen, das behoben werden muss, bevor die Migration beginnen kann.

EIGRP-Informationen in der Topologietabelle

Stellen Sie sicher, dass in der EIGRP-Topologietabelle Spoke-LAN-Einträge auf dem Hub und in der Zusammenfassung auf den Stationen enthalten sind. Dies kann überprüft werden, wenn Sie den folgenden Befehl auf dem (den) Hub(n) und den Spoke(s) eingeben:

show ip eigrp [AS_NUMBER] topology

Im Folgenden finden Sie ein Beispiel für die Ausgabe von Spoke:

```
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
```

Die Ausgabe zeigt, dass das Spoke über sein LAN-Subnetz (in *kursiv*) und die Zusammenfassungen für diese (in **Fettschrift**) weiß.

Im Folgenden finden Sie ein Beispiel für die Ausgabe vom Hub:

```
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)
```

Die Ausgabe zeigt, dass der Hub über die LAN-Subnetze der Stationen (*kursiv*), das von ihm angekündigte summarische Präfix (**fett**) und die zugewiesene IP-Adresse jedes Spokes per Aushandlung Bescheid weiß.

Weitere Überlegungen

Spoke-to-Spoke-Tunnel sind bereits vorhanden

Da bei einem Herunterfahren der DMVPN-Tunnelschnittstelle NHRP-Einträge entfernt werden, werden bereits vorhandene Spoke-to-Spoke-Tunnel gelöscht.

NHRP-Einträge löschen

Ein FlexVPN-Hub verlässt sich nicht auf den NHRP-Registrierungsprozess vom Spoke, um zu erfahren, wie der Datenverkehr zurückgeleitet wird. Dynamische Spoke-to-Spoke-Tunnel basieren jedoch auf NHRP-Einträgen.

Wenn im DMVPN NHRP auf dem Hub gelöscht wird, kann dies zu kurzlebigen Verbindungsproblemen führen. In FlexVPN bewirkt das Löschen von NHRP auf den Stationen, dass die FlexVPN IPsec-Sitzung für Spoke-to-Spoke-Tunnel beendet wird. Das Löschen von NHRP auf dem Hub hat keine Auswirkungen auf die FlexVPN-Sitzung.

Dies liegt daran, dass in FlexVPN standardmäßig Folgendes gilt:

- Spokes registrieren sich nicht bei Hubs.
- Hubs arbeiten nur als NHRP-Umleitungen und installieren keine NHRP-Einträge.
- NHRP-Verknüpfungseinträge werden auf Spoke-to-Spoke-Tunneln installiert und sind dynamisch.

Bekannte Einwände

Spoke-to-Spoke-Datenverkehr kann von der Cisco Bug-ID CSCub07382 betroffen sein.

Zugehörige Informationen

- Konfigurationsbeispiel für die Migration von DMVPN zu FlexVPN Soft
- Technischer Support und Dokumentation für Cisco Systeme