FlexVPN-Migration: Umstieg von DMVPN auf FlexVPN auf denselben Geräten

Inhalt

Einleitung

Dieses Dokument enthält Informationen zur Migration des vorhandenen DMVPN-Netzwerks auf FlexVPN auf den gleichen Geräten.

Die Konfigurationen beider Frameworks werden gleichzeitig auf den Geräten vorhanden sein.

In diesem Dokument wird nur das häufigste Szenario angezeigt: DMVPN mit Pre-Shared Key für die Authentifizierung und EIGRP als Routing-Protokoll.

In diesem Dokument wird die Migration zum BGP (empfohlenes Routing-Protokoll) und zum weniger erwünschten EIGRP veranschaulicht.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass der Leser grundlegende Konzepte von DMVPN und FlexVPN kennt.

Verwendete Komponenten

Beachten Sie, dass nicht alle Software und Hardware IKEv2 unterstützt. Weitere Informationen finden Sie im Cisco Feature Navigator. Im Idealfall sind folgende Softwareversionen zu verwenden:

- ISR - 15.2(4)M1 oder höher
- ASR1k - Version 3.6.2, Version 15.2(2)S2 oder höher

Zu den Vorteilen einer neueren Plattform und Software gehört die Möglichkeit der Verwendung von Verschlüsselungstechniken der nächsten Generation, z. B. AES GCM zur Verschlüsselung in IPsec. Dies wird in RFC 4106 erläutert.

AES GCM ermöglicht eine wesentlich schnellere Verschlüsselungsgeschwindigkeit auf einigen Hardwarekomponenten.

Empfehlungen von Cisco zur Verwendung und Migration auf die Verschlüsselung der nächsten Generation finden Sie unter:

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

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Migrationsverfahren

Derzeit wird empfohlen, die Migration von DMVPN zu FlexVPN nicht gleichzeitig durchzuführen.

Diese Einschränkung wird aufgehoben, da neue Migrationsfunktionen in die Version ASR 3.10 eingeführt werden sollen, die bei mehreren Erweiterungsanfragen von Cisco verfolgt werden,

darunter CSCuc08066. Diese Funktionen sollten Ende Juni 2013 verfügbar sein.

Eine Migration, bei der beide Frameworks nebeneinander existieren und gleichzeitig auf denselben Geräten betrieben werden, wird als weiche Migration bezeichnet, die minimale Auswirkungen und ein reibungsloses Failover von einem Framework zum anderen anzeigt.

Eine Migration, bei der die Konfiguration beider Frameworks gleichzeitig existiert, aber nicht gleichzeitig funktioniert, wird als harte Migration bezeichnet. Dies weist darauf hin, dass ein Switchover von einem Framework zum anderen einen Mangel an VPN-Kommunikation bedeutet, selbst wenn dieser minimal ist.

Hard Migration auf dieselben Geräte

In diesem Dokument wird die Migration von einem vorhandenen DMVPN-Netzwerk zu einem neuen FlexVPN-Netzwerk auf denselben Geräten behandelt.

Diese Migration erfordert, dass beide Frameworks nicht gleichzeitig auf den Geräten ausgeführt werden. Im Wesentlichen muss die DMVPN-Funktion vor der Aktivierung von FlexVPN generell deaktiviert werden.

Bis die neue Migrationsfunktion verfügbar ist, können Migrationen mit denselben Geräten wie folgt durchgeführt werden:

1. Überprüfen der Verbindung über DMVPN
2. Fügen Sie die FlexVPN-Konfiguration hinzu, und schalten Sie Tunnel- und virtuelle Vorlagenschnittstellen aus, die der neuen Konfiguration angehören.
3. (Während eines Wartungsfensters) Fahren Sie alle DMVPN-Tunnelschnittstellen an allen Stationen und Hubs herunter, bevor Sie mit Schritt 4 fortfahren.
4. FlexVPN-Tunnelschnittstellen deaktiviert.
5. Überprüfen der Verbindung zwischen Spoke und Hub
6. Überprüfen der Spoke-to-Spoke-Konnektivität
7. *Wenn die Überprüfung in Nummer 5 oder 6 nicht ordnungsgemäß durchgeführt wurde, kehren Sie zum DMVPN zurück, indem Sie die FlexVPN-Schnittstelle herunterfahren und die DMVPN-Schnittstellen deaktivieren.*
8. *Überprüfen der Kommunikation zwischen Hub und Hub*
9. *Überprüfen der Spoke-to-Spoke-Kommunikation*

Individueller Ansatz

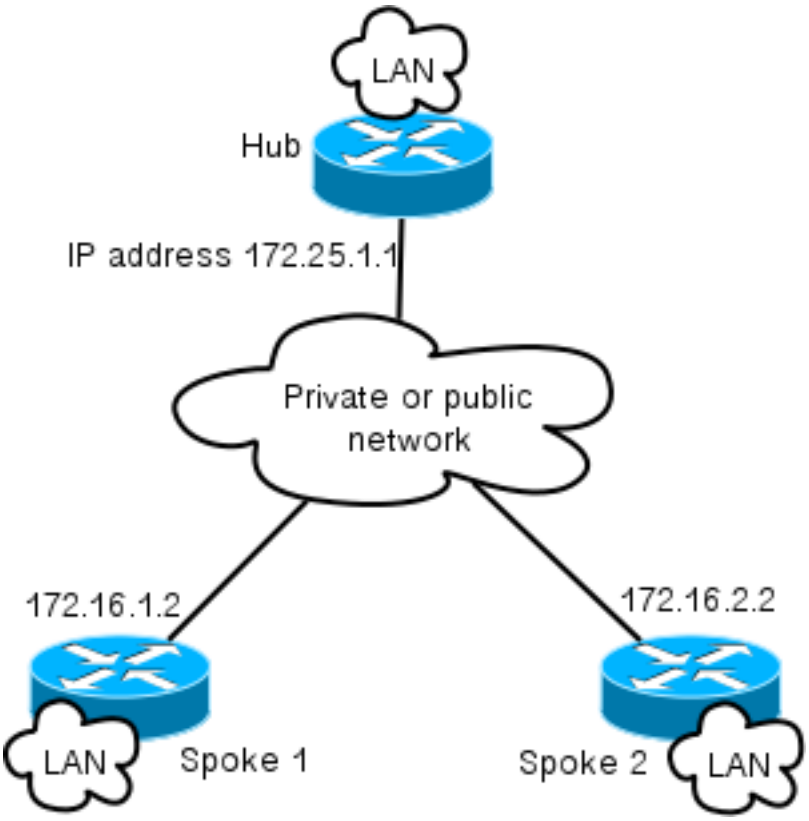
Sollte der Ansatz aufgrund komplexer Netzwerk- oder Routing-Prozesse für Sie nicht die beste Lösung sein, sprechen Sie mit Ihrem Cisco Ansprechpartner über die Migration. Ein individueller Migrationsprozess lässt sich am besten mit Ihrem Systemtechniker oder Advanced Services Engineer besprechen.

Netzwerktopologie

Transportnetz-Topologie

Dieses Diagramm zeigt eine typische Verbindungstopologie von Hosts im Internet. In diesem

Dokument wird die IP-Adresse des Hubs "loopback0" (172.25.1.1) verwendet, um die IPsec-Sitzung zu beenden.

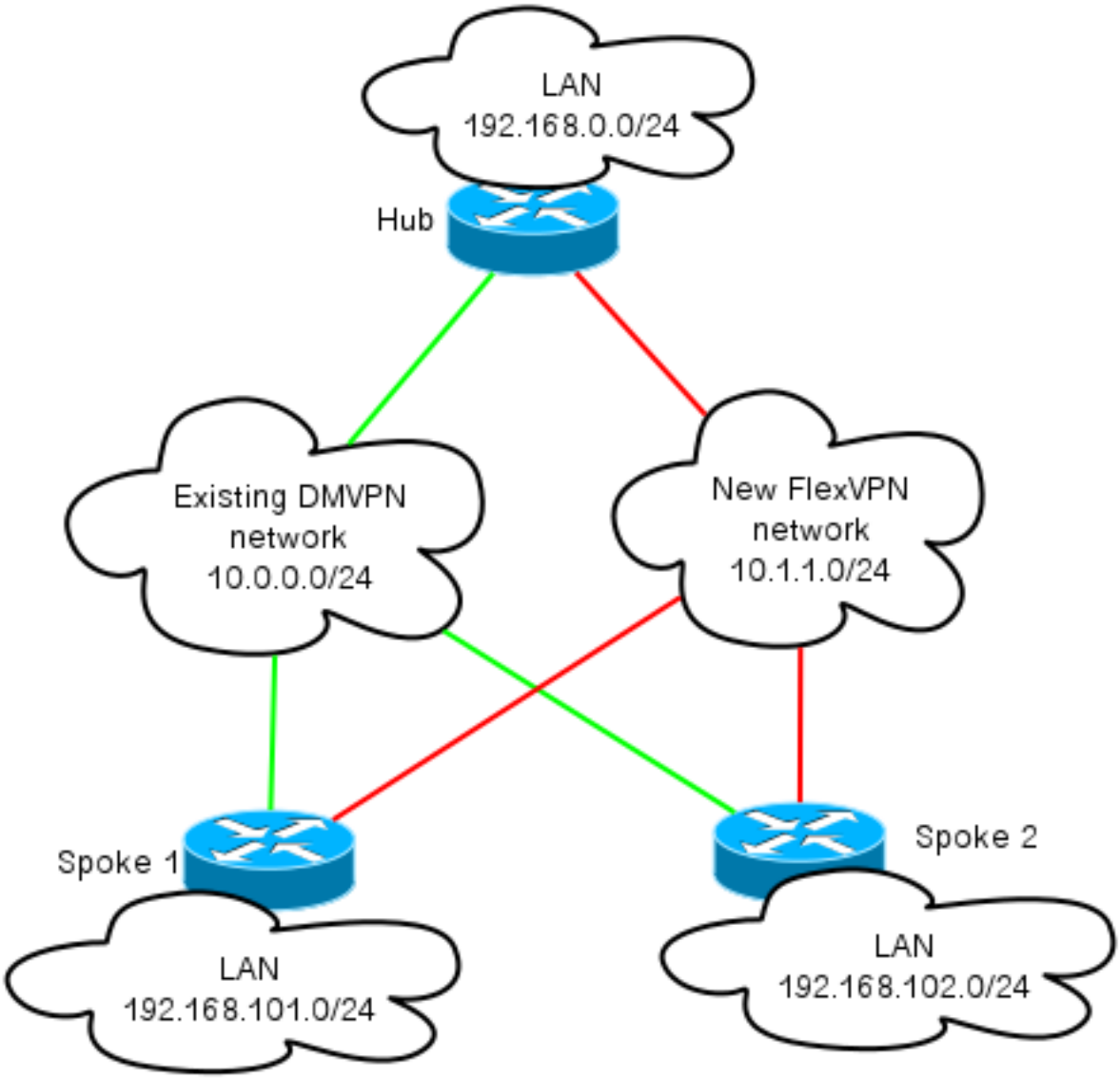


Overlay-Netzwerktopologie

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

Präfixe für das Local Area Network werden für die entsprechenden Seiten angezeigt.

Das 10.1.1.0/24-Subnetz stellt kein tatsächliches Subnetz für die Schnittstellenadressierung dar, sondern einen für die FlexVPN-Cloud reservierten IP-Platz. Die Begründung dafür wird später im Abschnitt zur FlexVPN-Konfiguration erläutert.



Konfiguration

DMVPN-Konfiguration

Dieser Abschnitt enthält die grundlegende Konfiguration von DMVPN-Hub and Spoke.

Pre-Shared Key (PSK) wird für die IKEv1-Authentifizierung verwendet.

Nach der Einrichtung von IPsec erfolgt die NHRP-Registrierung von Spoke zu Hub, sodass der Hub die NBMA-Adressierung der dynamisch sprechenden Hub erlernen kann.

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

Spoke-DMVPN-Konfiguration

Dies ist ein einfaches Beispiel für die Konfiguration von DMVPN mit vorinstallierter Schlüsselauthentifizierung 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

Bei der Hub-Konfiguration wird der Tunnel von loopback0 mit der IP-Adresse 172.25.1.1 bezogen.

Der Rest ist die Standardbereitstellung eines DMVPN-Hub 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-SAs auszuhandeln. IKEv2 bietet Verbesserungen gegenüber IKEv1, angefangen bei der Ausfallsicherheit bis hin zur Anzahl der Nachrichten, die für die Einrichtung eines geschützten Datenkanals erforderlich sind.
- GRE : Im Gegensatz zu DMVPN werden statische und dynamische Punkt-zu-Punkt-Schnittstellen verwendet, und nicht nur statische Multipoint-GRE-Schnittstellen. Diese Konfiguration bietet zusätzliche Flexibilität, insbesondere für das Verhalten pro Spoke/Hub.
- NHRP: In FlexVPN wird NHRP hauptsächlich zum Herstellen einer Spoke-to-Spoke-Kommunikation verwendet. Spokes registrieren sich nicht beim Hub.
- Routing: Da Stationen die NHRP-Registrierung nicht für den Hub ausführen, müssen Sie sich auf andere Mechanismen verlassen, um sicherzustellen, dass Hub und Spokes bidirektional kommunizieren können. Ähnlich wie bei DMVPN können dynamische Routing-Protokolle verwendet werden. Mit FlexVPN können Sie jedoch mithilfe von IPsec Routing-Informationen einführen. Der Standardwert ist "/32 route" für die IP-Adresse auf der anderen Seite des Tunnels, wodurch eine direkte Spoke-to-Hub-Kommunikation ermöglicht wird.

Bei der harten Migration von DMVPN zu FlexVPN funktionieren die beiden Frames nicht gleichzeitig auf denselben 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).
- VRF: Die VRF-Trennung kann zusätzliche Flexibilität ermöglichen, wird hier jedoch nicht behandelt (optional).

Spoke FlexVPN-Konfiguration

Einer der Unterschiede bei der Spoke-Konfiguration in FlexVPN im Vergleich zu DMVPN besteht darin, dass Sie potenziell zwei Schnittstellen haben.

Es gibt einen notwendigen Tunnel für Spoke-to-Hub-Kommunikation und einen optionalen Tunnel für Spoke-to-Spoke-Tunnel. Wenn Sie kein dynamisches Spoke-to-Spoke-Tunneling verwenden und lieber über ein Hub-Gerät laufen möchten, können Sie die Virtual-Template-Schnittstelle entfernen und das NHRP-Shortcut-Switching von der Tunnelschnittstelle entfernen.

Sie werden auch bemerken, dass die statische Tunnelschnittstelle über eine auf Aushandlung empfangene IP-Adresse verfügt. Dadurch kann der Hub die IP-Adresse der Tunnelschnittstelle dynamisch bereitstellen, ohne dass in der FlexVPN-Cloud eine statische Adressierung 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
 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 in der Hardware, die diesen unterstützt.

```
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
```

PKI ist die empfohlene Methode für die Durchführung einer groß angelegten Authentifizierung in IKEv2.

Sie können jedoch weiterhin einen vorinstallierten Schlüssel verwenden, solange Sie sich der Einschränkungen bewusst sind.

Hier ein Beispiel für eine Konfiguration mit "cisco" als PSK:

```
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-Hub-Konfiguration

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, sondern eine Virtual-Template-Schnittstelle. Dadurch wird für jede Verbindung eine Virtual-Access-Schnittstelle erstellt.

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

Die Adressen aus diesem Pool werden zu einem späteren Zeitpunkt 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
 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 in der Hardware, die diesen unterstützt.

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

Beachten Sie, dass in der unten stehenden Konfiguration der AES-GCM-Vorgang kommentiert wurde.

```
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
```

Bei der Authentifizierung in IKEv2 gilt für den Hub dasselbe Prinzip wie für den Spoke-Modus.

Für Skalierbarkeit und Flexibilität sollten Sie Zertifikate verwenden. Sie können jedoch dieselbe Konfiguration für PSK wie auf Spoke verwenden.

Hinweis: IKEv2 bietet Flexibilität bei der Authentifizierung. Eine Seite kann sich mithilfe von PSK authentifizieren, die andere RSA-SIG.

Datenverkehrsmigration

Migration zu BGP als Overlay-Routing-Protokoll [empfohlen]

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

In diesem Beispiel wird iBGP verwendet.

Spoke-BGP-Konfiguration

Die Spoke-Migration besteht aus zwei Teilen. Aktivierung von 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 Hub-BGP-Konfiguration in diesem Abschnitt der Migration) und neue Präfixe über BGP abgerufen werden, können Sie Datenverkehr aus der vorhandenen DMVPN-Cloud in die neue FlexVPN-Cloud verlagern.

Hub-BGP-Konfiguration

Auf dem Hub werden dynamische Listener konfiguriert, um zu verhindern, dass die Nachbarschaftskonfiguration für jedes Spoke separat beibehalten wird.

In dieser Konfiguration initiiert das BGP keine neuen Verbindungen, akzeptiert jedoch Verbindungen aus dem bereitgestellten Pool von IP-Adressen. In diesem Fall lautet der Pool 10.1.1.0/24, also alle Adressen in der neuen FlexVPN-Cloud.

```
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
```

Migration des Datenverkehrs auf FlexVPN

Wie bereits erwähnt, muss die Migration erfolgen, indem die DMVPN-Funktionalität heruntergefahren und FlexVPN aktiviert wird.

Dieses Verfahren garantiert eine minimale Wirkung.

1. Alle Sprecher:
   ```
   interface tunnel 0
      shut
   ```
2. Hub:
   ```
   interface tunnel 0
     shut
   ```
   Stellen Sie an diesem Punkt sicher, dass keine IKEv1-Sitzungen für diesen Hub von den Stationen eingerichtet wurden.Dies kann überprüft werden, indem die Ausgabe des Befehls **show crypto isakmp sa** sowie die von der Crypto-Protokollierungssitzung generierten Syslog-

Meldungen überprüft werden.Sobald dies bestätigt wurde, können Sie mit der Installation von FlexVPN fortfahren.

3. Fortsetzung am Hub:
```
interface Virtual-template 1
 no shut
```
4. Zu den Sprechern:
```
interface tunnel 1
   no shut
```

Überprüfungsschritte

IPsec-Stabilität

Die beste Methode zur Bewertung der IPsec-Stabilität ist die Überwachung von Sylogs mit diesem 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.

Ausgefüllte BGP-Informationen

Wenn IPsec stabil ist, stellen Sie sicher, dass die BGP-Tabelle mit Einträgen von Spokes (auf dem Hub) und Zusammenfassung vom Hub (auf Spokes) gefüllt ist.

Im Fall von BGP kann dies angezeigt werden, indem Sie:

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

Beispiel für korrekte Informationen vom Hub:

```
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
```

Sie sehen, dass der Hub gelernt hat, dass ein Präfix von jedem der Stationen und beiden Stationen dynamisch ist (mit Sternchen (*) gekennzeichnet).

Beispiel für ähnliche Informationen aus Spoke:

```
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
```

Spoke hat ein Präfix vom Hub erhalten. Bei dieser Konfiguration sollte dieses Präfix die Zusammenfassung sein, die auf dem Hub angekündigt wird.

Migration auf neue Tunnel mit EIGRP

EIGRP ist in DMVPN-Netzwerken aufgrund seiner relativ einfachen Bereitstellung und schnellen Konvergenz eine beliebte Wahl.

Es lässt sich jedoch schlechter skalieren als BGP und bietet nicht viele erweiterte Mechanismen, die BGP sofort nutzen kann.

In diesem nächsten Abschnitt wird eine Möglichkeit beschrieben, wie Sie mit einem neuen EIGRP-Prozess zu FlexVPN wechseln können.

Aktualisierte Spoke-Konfiguration

In diesem Beispiel wird ein neues AS 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
```

Hinweis: Sie sollten vermeiden, eine Routing-Protokoll-Adjazenz für Spoke-to-Spoke-Tunnel einzurichten. Daher sollte die Schnittstelle von Tunnel1 (Spoke-to-Hub) nur passiv sein.

Aktualisierte Hub-Konfiguration

Ähnlich wie beim Hub sollte DMVPN die bevorzugte Methode für den Datenaustausch über Hub bleiben. FlexVPN sollte jedoch bereits dieselben Präfixe ankündigen und erlernen.

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

Es gibt zwei Möglichkeiten, um eine Zusammenfassung für das Gespräch bereitzustellen.

- Verteilen einer statischen Route, die auf null0 verweist (bevorzugte Option).
  ```
  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
  ```
  Diese Option ermöglicht die Kontrolle über Zusammenfassung und Neuverteilung, ohne die VT-Konfiguration des Hubs zu berühren.
- Alternativ können Sie eine zusammengefasste Adresse im DMVPN-Stil auf einer virtuellen Vorlage einrichten. Diese Konfiguration wird aufgrund der internen Verarbeitung und der Replikation dieser Zusammenfassung auf jeden virtuellen Zugriff nicht empfohlen. Sie wird hier als Referenz angezeigt:

```
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
```

Migration des Datenverkehrs auf FlexVPN

Die Migration muss durch das Herunterfahren der DMVPN-Funktionalität und die Aktivierung von FlexVPN erfolgen.

Das folgende Verfahren garantiert minimale Auswirkungen.

1. Alle Sprecher:
   ```
   interface tunnel 0
      shut
   ```
2. Hub:
   ```
   interface tunnel 0
     shut
   ```
   Stellen Sie an diesem Punkt sicher, dass keine IKEv1-Sitzungen für diesen Hub von den Stationen eingerichtet wurden.Dies lässt sich überprüfen, indem die Ausgabe des Befehls **show crypto isakmp sa** sowie die von der Crypto-Protokollierungssitzung generierten Syslog-Meldungen überprüft werden.Sobald dies bestätigt wurde, können Sie mit der Installation von FlexVPN fortfahren.
3. Fortsetzung am Hub:
   ```
   interface Virtual-template 1
    no shut
   ```
4. Alle Sprecher:
   ```
   interface tunnel 1
      no shut
   ```

Überprüfungsschritte

IPsec-Stabilität

Wie beim BGP müssen Sie prüfen, ob IPsec stabil ist. Die beste Methode hierfür ist die Überwachung von Sylogs mit aktiviertem 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 die EIGRP-Topologietabelle mit Spoke-LAN-Einträgen auf dem Hub und Zusammenfassung auf den Stationen gefüllt ist. Dies kann durch die Ausführung dieses Befehls auf Hub(s) und Spoke(s) überprüft werden.

```
show ip eigrp topology
```

Beispiel für eine ordnungsgemäße Ausgabe von Spoke:

```
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
```

Sie werden feststellen, dass Spoke über sein LAN-Subnetz (in kursiv) und die Zusammenfassungen für diese (in **Fettschrift**) Bescheid weiß.

Beispiel für eine ordnungsgemäße Ausgabe vom Hub.

```
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
```

Sie werden feststellen, dass der Hub über die LAN-Subnetze der Stationen (kursiv), das zusammengefasste Präfix, das er anzeigt (**fett**) und die zugewiesene IP-Adresse jedes Spokes über Aushandlung weiß.

Zusätzliche Überlegungen

Vorhandene Spoke-to-Spoke-Tunnel

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

Löschen von NHRP-Einträgen

Wie bereits erwähnt, verlässt sich ein FlexVPN-Hub nicht auf den NHRP-Registrierungsprozess von "Spoke", um zu erfahren, wie der Datenverkehr zurückgeleitet wird. Dynamische Spoke-to-Spoke-Tunnel basieren jedoch auf NHRP-Einträgen.

In DMVPN, wo das Löschen von NHRP auf dem Hub zu kurzlebigen Verbindungsproblemen hätte führen können.

In FlexVPN Clearing NHRP on Spokes wird die FlexVPN IPsec-Sitzung in Verbindung mit Spoke-to-Spoke-Tunneln abgebrochen. Beim Löschen des NHRP hat kein Hub 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-Umleitung 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 CSCub07382 betroffen sein.

Zugehörige Informationen

- Technischer Support und Dokumentation für Cisco Systeme