DMVPN naar FlexVPN softwareconfiguratie

Inhoud

Inleiding

Dit document beschrijft hoe u een *zachte* migratie kunt uitvoeren waarbij zowel Dynamic Multipoint VPN (DMVPN) als FlexVPN op een apparaat tegelijkertijd werkt zonder dat er een tijdelijke oplossing nodig is en een configuratievoorbeeld biedt.

> Opmerking: Dit document breidt de concepten uit die in de FlexVPN-migratie worden beschreven: Harde beweging van DMVPN naar FlexVPN op dezelfde apparaten en FlexVPN-migratie: Harde beweging van DMVPN naar FlexVPN op een andere Hub Cisco artikelen. Beide documenten beschrijven *harde* migraties, die enige verstoring van het verkeer tijdens de migratie veroorzaken. De beperkingen in deze artikelen zijn het gevolg van een tekortkoming in de software van Cisco IOS® die nu is gecorrigeerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- DMVPN
- FlexVPN

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco geïntegreerde services router (ISR) versies 15.3(3)M of hoger
- Cisco 1000 Series geaggregeerde services router (ASR1K) release 3.10 of hoger

> Opmerking: Niet alle software en hardware ondersteunen Internet Key Exchange versie 2 (IKEv2). Raadpleeg de Cisco Functie Navigator voor informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Een van de voordelen van het nieuwere Cisco IOS platform en de software is de capaciteit om de Cryptografie van de Volgende Generatie te gebruiken. Een voorbeeld is het gebruik van Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) voor encryptie in IPsec, zoals besproken in RFC 4106. AES GCM maakt een veel snellere coderingssnelheden mogelijk op bepaalde hardware.

> Opmerking: Raadpleeg het Cisco-artikel van de volgende generatie voor aanvullende informatie over het gebruik van en de migratie naar Cryptografie van de volgende generatie.

Configureren

Dit configuratievoorbeeld concentreert zich op een migratie van een DMVPN Fase 3 configuratie naar een FlexVPN, omdat beide ontwerpen vergelijkbaar werken.

	DMVPN fase 2	DMVPN fase 3	FlexVPN
Vervoer	GRE via IPsec	GRE via IPsec	GRE via IPsec,
NHRP-gebruik	Registratie en oplossing	Registratie en oplossing	Resolutie
Volgende week van Spoke	Andere Spoelen of hub	Samenvatting van hub	Samenvatting v hub

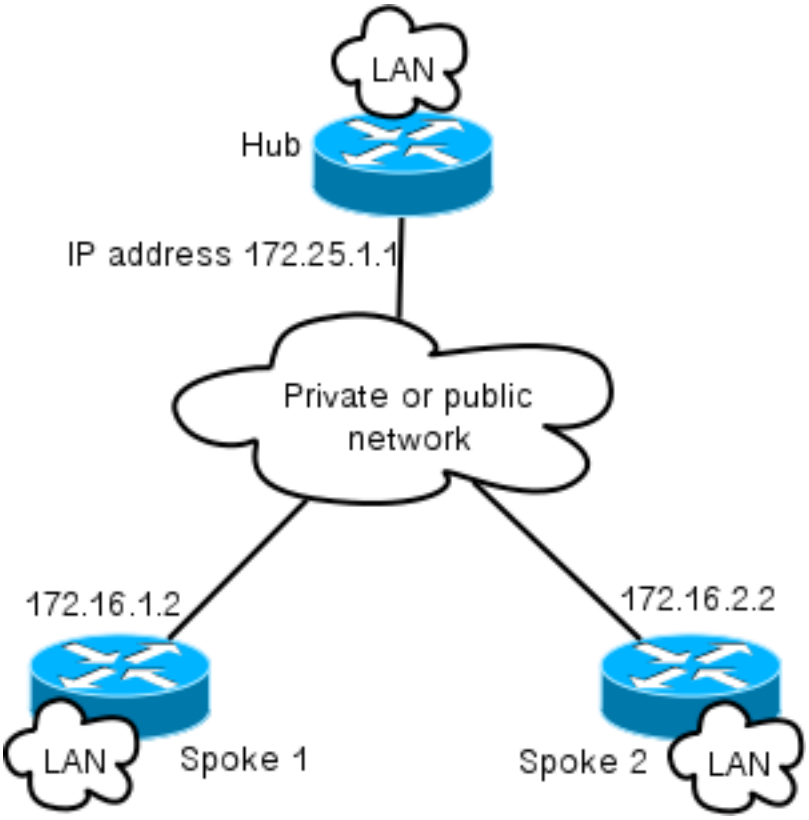
NHRP-snelswitching	Nee	Ja	Ja (optioneel)
NHRP-omleiding	Nee	Ja	Ja
IKE en IPsec	IPsec optioneel, standaard IKEv1	IPsec optioneel, standaard IKEv1	IPsec, IKEv2

Netwerkdiagrammen

Deze sectie verschaft zowel netwerkdiagrammen voor transport als overlay.

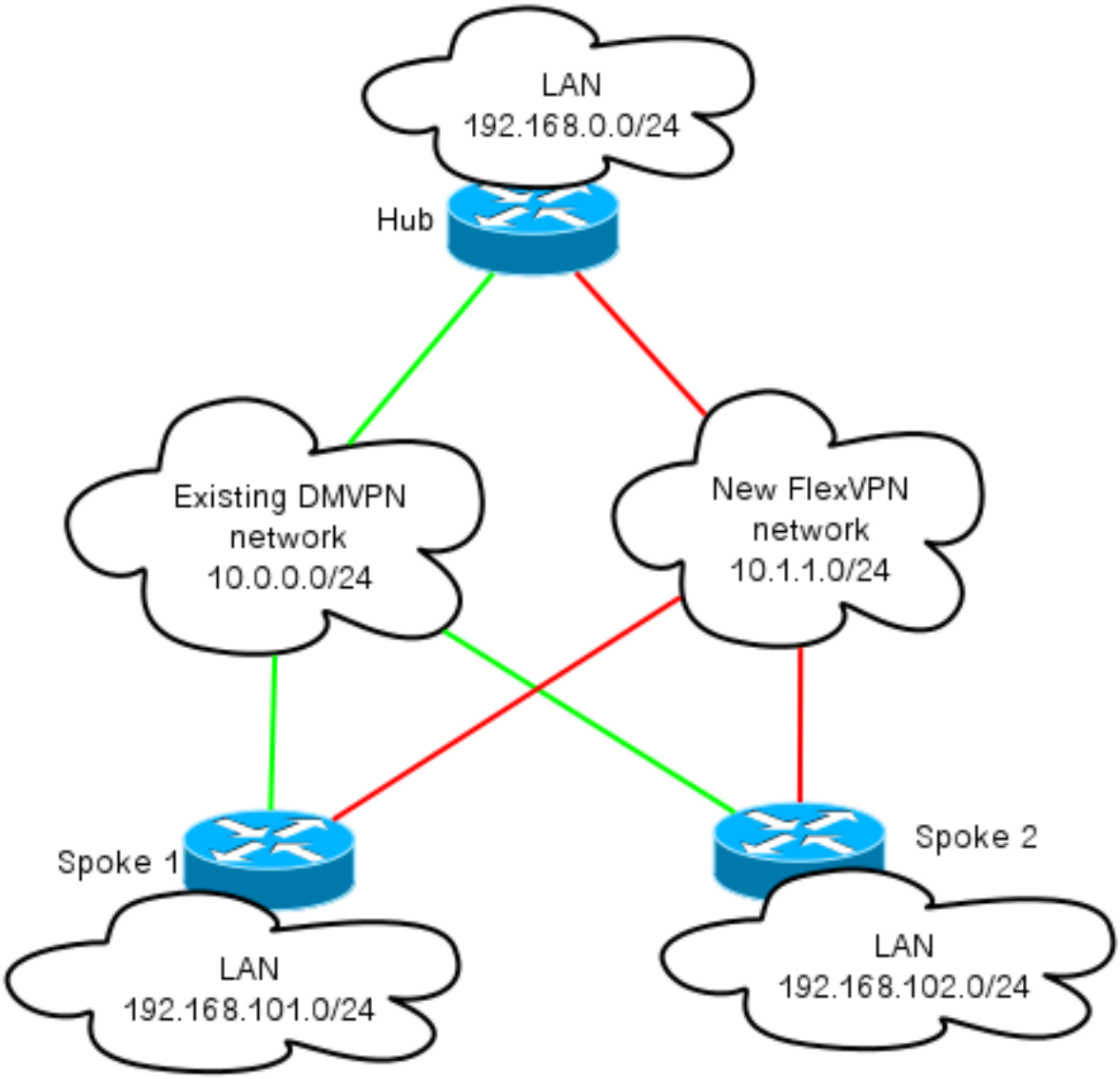
Netwerkdiagram voor transport

Het in dit voorbeeld gebruikte transportnetwerk omvat één enkel knooppunt met twee verbonden spaken. Alle apparaten worden aangesloten door een netwerk dat het internet simuleert.



Netwerkdiagram overlay

Het overlay netwerk dat in dit voorbeeld gebruikt omvat één enkel hub met twee verbonden spaken. Vergeet niet dat zowel DMVPN als FlexVPN gelijktijdig actief zijn, maar zij gebruiken verschillende IP adresruimten.



Configuraties

Deze configuratie migreert de populairste uitrol van DMVPN Fase 3 via Enhanced Interior Gateway Routing Protocol (DHCP) naar FlexVPN met Border Gateway Protocol (BGP). Cisco raadt het gebruik van BGP met FlexVPN aan, omdat deze implementaties mogelijk maakt om beter te schalen.

> Opmerking: Het hub beëindigt de IKEv1 (DMVPN) en IKEv2 (FlexVPN) sessies op hetzelfde IP-adres. Dit is alleen mogelijk met recente Cisco IOS releases.

Spoelconfiguratie

Dit is een zeer basisconfiguratie, met twee opmerkelijke uitzonderingen die samenwerking van zowel IKEv1 als IKEv2 toestaan, zowel als twee raamwerken die Generic Routing Encapsulation (GRE) via IPsec gebruiken om samen te leven.

> Opmerking: De relevante wijzigingen in de configuratie van Internet Security Association en Key Management Protocol (ISAKMP) en IKEv2 worden in vet gemarkeerd.

```
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
```

Met Cisco IOS release 15.3 kunt u zowel IKEv2- als ISAKMP-profielen in een configuratie voor *tunnelbescherming* verbinden. Samen met enkele interne veranderingen in de code, kunnen IKEv1 en IKEv2 op hetzelfde apparaat tegelijkertijd werken.

Vanwege de manier waarop Cisco IOS de profielen (IKEv1 of IKEv2) in releases eerder dan 15.3 selecteert, heeft dit geleid tot bepaalde voorbehouden, zoals situaties waarin IKEv1 via de peer wordt gestart op IKEv2. De scheiding van IKE is nu gebaseerd op profiel-level en niet op interface-niveau, hetgeen bereikt wordt via de nieuwe CLI.

Een andere upgrade in de nieuwe Cisco IOS-release is de toevoeging van de *tunneltoets*. Dit is nodig omdat zowel DMVPN als FlexVPN dezelfde broninterface en hetzelfde bestemming IP-adres gebruiken. Met dit op zijn plaats is er geen manier voor de GRE-tunnel om te weten welke tunnelinterface wordt gebruikt om het verkeer te ontkoppelen. Met de tunneltoets kunt u **tunnel0** en **tunnel1** differentiëren met de toevoeging van een kleine (4 bytes) overhead. Een andere toets kan op beide interfaces worden ingesteld, maar u hoeft doorgaans slechts één tunnel te differentiëren.

> Opmerking: De gedeelde optie voor tunnelbescherming is niet vereist wanneer DMVPN en FlexVPN dezelfde interface delen.

Dus, de gesproken routingprotocolconfiguratie is basisch. Ecu en BGP werken afzonderlijk. Ecu adverteert alleen via de tunnelinterface om te voorkomen dat er over gesproken-aan-gesproken tunnels wordt doorgespeeld, wat de schaalbaarheid beperkt. BGP onderhoudt alleen een relatie met de hub router (**10.1.1.1**) om het lokale netwerk te adverteren (**192.168.101.0/24**).

```
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
```

Hub-configuratie

U moet voor de configuratie van de hub dezelfde wijzigingen aanbrengen als die welke in het gedeelte **Spoke Configuration** worden beschreven.

> Opmerking: De relevante wijzigingen in de ISAKMP- en IKEV2-configuratie worden in vet gemarkeerd.

```
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
```

Op de hub-kant komt de band tussen het IKE-profiel en het IPsec-profiel voor op het profiel-niveau, in tegenstelling tot de spaanconfiguratie, waar dit wordt voltooid via de opdracht **tunnelbescherming**. Beide benaderingen zijn levensvatbare methoden om deze binding te voltooien.

Het is belangrijk om op te merken dat de NHRP-netwerk (Next Hop Resolutie Protocol)-ID's verschillend zijn voor DMVPN en FlexVPN in de cloud. In de meeste gevallen is het ongewenst wanneer NHRP één domein creëert via beide raamwerken.

De tunneltoets differentieert DMVPN- en FlexVPN-tunnels op GRE-niveau om hetzelfde doel te bereiken dat in het gedeelte **Spoke Configuration** wordt vermeld.

De routerconfiguratie op de hub is tamelijk fundamenteel. Het naaf apparaat onderhoudt twee relaties met elke gesproken persoon, één die gebruik maakt van Ecu en één die BGP gebruikt. De configuratie van BGP gebruikt luisterbereik om een lange, per-vormige configuratie te vermijden.

De overzichtsadressen worden twee keer geïntroduceerd. De configuratie Ecu verstuurt een samenvatting met gebruik van de configuratie van de **tunnel**0 (IP samenvatting-adres Ecu 100), en de BGP introduceert een samenvatting met gebruik van het geaggregeerde adres. De samenvattingen zijn vereist om te verzekeren dat de NHRP-omleiding plaatsvindt, en om de routing updates te vereenvoudigen. U kunt een NHRP-omleiding (net als een Internet Control Message Protocol (ICMP)-protocol (ICMP) sturen die omleiding sturen geeft aan of er een betere hop bestaat voor een bepaalde bestemming, die het mogelijk maakt om een met de gesproken tunnel tot stand te brengen. Deze samenvattingen worden ook gebruikt om de hoeveelheid routingupdates die tussen de hub en elke sprak worden verstuurd, te minimaliseren, waardoor instellingen beter kunnen worden geschaald.

```
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
```

Verifiëren

De verificatie voor dit configuratievoorbeeld is in verschillende delen verdeeld.

Voorafgaande migratiecontroles

Aangezien zowel DMVPN/DHCP en FlexVPN/BGP gelijktijdig functioneren, moet u verifiëren dat het gesproken een relatie over IPsec met zowel IKEv1 als IKEv2 onderhoudt en dat de juiste prefixes via DHCP en BGP worden geleerd.

In dit voorbeeld toont **Spoke1** dat twee sessies met de hub router worden onderhouden; één gebruikt IKEv1/**Tunnel0** en één gebruikt IKEv2/**Tunnel1**.

> Opmerking: Er worden twee IPsec Security Associations (SAs) (één inkomende en één uitgaande) onderhouden voor elk van de tunnels.

```
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
```

Wanneer u de routingprotocollen controleert, moet u verifiëren dat een buren wordt gevormd, en dat de juiste prefixes worden geleerd. Dit wordt eerst gecontroleerd met de Ecu. Controleer dat het hub zichtbaar is als een buurman, en dat het **192.168.0.0/16** adres (de samenvatting) van het centrum wordt geleerd:

```
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
```

Controleer vervolgens de BGP:

```
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
```

De output toont dat het hub FlexVPN IP-adres (10.1.1.1) een buurman is waar de spits één prefix (192.168.0.0/16) ontvangt. Daarnaast informeert de BGP de beheerder dat een fout in de Routing Information Base (RIB) voor het 192.168.0.0/16 prefix is opgetreden. Deze mislukking komt voor omdat er een betere route voor dat prefix is dat al in de routingtabel bestaat. Deze route wordt voortgebracht door DHCP, en kan worden bevestigd als u de routingtabel controleert.

```
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
```

Migratie

De vorige sectie geverifieerde dat zowel IPsec als de routingprotocollen zijn geconfigureerd en werken zoals verwacht. Een van de makkelijkste manieren om van DMVPN naar FlexVPN over hetzelfde apparaat te migreren is de Administratieve Afstand (AD) te veranderen. In dit voorbeeld heeft de Interne BGP (iBGP) een AD van 200 en heeft de DHCP een AD van 90.

Om het verkeer door FlexVPN te kunnen stromen moet de BGP een betere AD hebben. In dit voorbeeld wordt de EHRM gewijzigd in 230 en 240 voor respectievelijk interne en externe routes. Dit maakt de BGP AD (van 200) verkieslijker voor het voorvoegsel 192.168.0.0/16.

Een andere methode die wordt gebruikt om dit te bereiken, is het verlagen van de BGP AD. Het protocol dat na de migratie draait, heeft echter niet-standaardwaarden, die andere delen van de implementatie kunnen beïnvloeden.

In dit voorbeeld, het debug ip routing bevel wordt gebruikt om handeling op het sprak te controleren.

> Opmerking: Als de informatie in deze sectie op een productienetwerk wordt gebruikt, vermijd het gebruik van debug opdrachten, en baseer zich op de show opdrachten in de volgende sectie die worden vermeld. Ook, moet het gesproken Ecu proces nabijheid met de hub opnieuw duidelijk maken.

```
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
```

In deze output worden drie belangrijke acties opgemerkt:

- De spreker merkt op dat de AD veranderde en de nabijheid blokkeert.
- In de routingtabel wordt het voorvoegsel Ecu beëindigd, en wordt de BGP geïntroduceerd.
- Adjacency to the hub over the HTTP komt online terug.

Wanneer u de AD op een apparaat verandert, beïnvloedt dit alleen het pad van het apparaat naar de andere netwerken; het heeft geen invloed op de manier waarop andere routers routing uitvoeren. Bijvoorbeeld, nadat de afstand Ecu op **Spoke1** verhoogd is (en het FlexVPN op de cloud gebruikt om verkeer te leiden), handhaaft de hub de geconfigureerde (standaard) ADs. Dit betekent dat het DMVPN gebruikt om verkeer terug te sturen naar **Spoke1**.

In bepaalde scenario's kan dit problemen veroorzaken, zoals wanneer firewalls het retourverkeer op dezelfde interface verwachten. Daarom moet u het AD op alle spaken wijzigen voordat u het op de hub wijzigt. Het verkeer wordt alleen volledig door FlexVPN gemigreerd zodra dit volledig is.

Migratie naar Ecp-RvE

Een migratie van DMVPN naar FlexVPN die alleen daarom draait wordt niet diepgaand in dit document besproken. het wordt hier evenwel ter volledigheid genoemd .

Het is mogelijk om zowel DMVPN als Ecp toe te voegen aan het zelfde Autonome Systeem (AS) dat van het Systeem (RSP) routeert instantie. Met dit op zijn plaats, wordt de routingnabijheid gevestigd over beide types van wolken. Dit kan lading-in evenwicht brengen veroorzaken om voor te komen, wat gewoonlijk niet wordt aanbevolen.

Om ervoor te zorgen dat FlexVPN of DMVPN wordt geselecteerd, kan een beheerder verschillende **vertragingswaarden** toewijzen per interface. Niettemin is het belangrijk om te onthouden dat er geen veranderingen mogelijk zijn op de virtuele-sjabloon interfaces terwijl er corresponderende virtuele-toegangsinterfaces aanwezig zijn.

Controle na migratie

Overeenkomstig het proces dat in het gedeelte **Pre-Migration Checks** wordt gebruikt, moeten het

IPsec- en routingprotocol worden geverifieerd.

Controleer eerst de IPsec:

```
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
```

Zoals eerder, worden twee sessies gezien, die twee actieve IPsec SAs hebben.

Op het gesproken wordt de gezamenlijke route (192.168.0.0/16) punten van de hub en er wordt geleerd via BGP.

```
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
```

Op dezelfde manier moet het gesproken LAN dat op de hub is voorgeprogrammeerd via de DHCP bekend zijn. In dit voorbeeld wordt Spoke2 LAN als LAN gecontroleerd:

```
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
```

In de output wordt het verzendpad correct bijgewerkt en wordt er gewezen op een virtuele-toegangsinterface.

Aanvullende overwegingen

In dit gedeelte worden enkele extra gebieden beschreven die van belang zijn voor dit configuratievoorbeeld.

Bestaande Spoke-to-Spoke tunnels

Met een migratie van een migratie van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van een netwerk van de pers, wordt de gesproken-aan-gesproken tunnels niet beïnvloed, omdat de snelweg nog in werking is. De snelweg-overschakeling op een spits voert een meer specifieke NHRP-route in met een AD van 250.

Hier is een voorbeeld van zo'n route:

```
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
```

Communicatie tussen gedistribueerde en niet-Gerichte ruimtes

Als een iemand die al op een FlexVPN/BGP staat wil communiceren met een apparaat waarmee het migratieproces nog niet is begonnen, stroomt het verkeer altijd over de hub.

Dit is het proces dat plaatsvindt:

1. De spits voert een route uit naar de bestemming, die door een summiere route wijst die door de hub wordt geadverteerd.
2. Het pakje wordt naar de hub gestuurd.
3. Het hub ontvangt het pakket en voert een routeraadpleging voor de bestemming uit, die uit een andere interface wijst die deel van een verschillend NHRP domein uitmaakt.

   Opmerking: De NHRP netwerk-id in de vorige hub-configuratie is verschillend voor zowel FlexVPN als DMVPN.

Zelfs als de NHRP netwerk IDs verenigd zijn, zou een probleem kunnen voorkomen waar de gemigreerde spatie routeobjecten via het FlexVPN netwerk. Hieronder valt ook de richtlijn die wordt gebruikt voor het configureren van snelswitching. De niet-gemigreerd sprak pogingen om voorwerpen over het netwerk DMVPN te lopen, met een specifiek doel om snelswitching uit te voeren.

Problemen oplossen

In dit deel worden de twee categorieën beschreven die doorgaans worden gebruikt om de migratie

aan te kunnen.

Problemen met pogingen om tunnels in te richten

Voltooi deze stappen als de IKE-onderhandeling mislukt:

1. Controleer de huidige status met deze opdrachten:

   toon crypto isakmp sa - Deze opdracht toont de hoeveelheid, de bron en de bestemming van een IKEv1 sessie.**toon crypto ipsec sa**- Deze opdracht onthult de activiteit van IPsec SAs.Opmerking: Anders dan in IKEv1 wordt in deze uitvoer de PFS Diffie-Hellman (DH) groepswaarde (Perfect Forward SecRITY) weergegeven als **PFS (Y/N): N, DH-groep: geen** tijdens de eerste tunnelonderhandelingen ; na een herhaling verschijnen echter de juiste waarden . Dit is geen bug, ook al is het gedrag beschreven in CSCug67056. Het verschil tussen IKEv1 en IKEv2 is dat in het laatste geval de Child SAs gecreëerd worden als onderdeel van de **AUTH-**uitwisseling. De DH Group die is geconfigureerd onder de crypto-kaart wordt alleen tijdens een zoekopdracht gebruikt. Om deze reden, ziet u **PFS (Y/N): N, DH-groep: niet tot de eerste rekey .** Met IKEv1 zie je een ander gedrag omdat de creatie van het Kind SA tijdens de Snelle Modus plaatsvindt en het **CREATE_CHILD_SA** bericht bevat bepalingen voor de overdracht van de Key Exchange payload die de DH parameters specificeert om een nieuw gedeeld geheim af te leiden.**toon crypto ikev2 sa** - Deze opdracht geeft uitvoer vergelijkbaar met ISAKMP maar is specifiek voor IKEv2.**toon crypto sessie** - Deze opdracht geeft de samenvatting van de resultaten van de cryptografische sessies op dit apparaat.**toon crypto socket** - deze opdracht toont de status van crypto-sokassen.**Toon crypto kaart** - deze opdracht toont de afbeelding van profielen van IKE en IPsec aan de interfaces.**toon ip Nhrp** - deze opdracht verstrekt de NHRP informatie van het apparaat. Dit is handig voor normaal gesproken gemaakte FlexVPN-constructies en voor zowel spraak-aan-spaak- als spraak-to-hub-verbindingen in DMVPN-instellingen.
2. Gebruik deze opdrachten om de tunnelinstelling te reinigen:

   debug van crypto ikev2debug van crypto isakmpcrypto ipsec debugdebug crypto kmi

Problemen met routedoorgifte

Hier zijn een paar nuttige opdrachten die u kunt gebruiken om een oplossing te vinden voor de problemen met de (middel) omgeving van de computer en de topologie:

- **toon de samenvatting van bgp** - gebruik deze opdracht om de aangesloten buren en hun staten te verifiëren.
- **toon ip eigrp buurman** - gebruik deze opdracht om de buren te tonen die via DHCP verbonden zijn.
- **tonen bgp** - gebruik deze opdracht om de voorfixes die boven de BGP zijn geleerd te controleren.
- **toon ip eigrp topologie** - gebruik deze opdracht om de prefixes te tonen die via DHCP geleerd worden.

Het is belangrijk om te weten dat een geleerd voorvoegsel anders is dan een voorvoegsel dat in de routingtabel is geïnstalleerd. Raadpleeg voor meer informatie over dit, de routeselectie in het artikel van Cisco Routers of het TCP/IP-persboek van Cisco.

gekende Caveats

Een beperking die de GRE-tunnelbehandeling weergeeft, bestaat op de ASR1K. Dit wordt gevolgd onder Cisco bug-ID CSCue0443. Op dit moment heeft de beperking een geplande oplossing in Cisco IOS XE-softwarerelease 3.12.

Controleer dit bug als u een waarschuwing wilt geven zodra de oplossing beschikbaar is.