Harde beweging van DMVPN naar FlexVPN op een andere hub

Inhoud

Inleiding

Dit document geeft informatie over hoe u kunt migreren van een Dynamic Multipoint VPN (DMVPN) netwerk dat momenteel bestaat naar FlexVPN op verschillende hub-apparaten. De configuraties voor beide raamwerken bestaan op de apparaten samen. In dit document wordt alleen het meest gebruikelijke scenario getoond - DMVPN met het gebruik van de vooraf gedeelde sleutel voor authenticatie en het Uitgebreid Interior Gateway Routing Protocol (DHCP) als het Routing Protocol. In dit document, wordt de migratie naar het Protocol van de Rand Gateway (BGP), dat het aanbevolen routingprotocol is, en de minder wenselijke DHCP gedemonstreerd.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- DMVPN
- FlexVPN

Gebruikte componenten

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

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

- Cisco geïntegreerde services router (ISR) versie 15.2(4)M1 of hoger
- Cisco aggregation services router 1000 Series (ASR1K) 3.6.2 release 15.2(2)S2 of hoger

Een van de voordelen van een nieuwer platform en betere software is de mogelijkheid om next-generation encryptie te gebruiken, zoals Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) voor encryptie in Internet Protocol Security (IPsec), zoals besproken in Aanvraag voor Comments (RFC) 4106. Met AES GCM kunt u een veel snellere coderingssnelheid voor bepaalde hardware bereiken. Raadpleeg het artikel Encryption van de volgende generatie om de aanbevelingen van Cisco voor het gebruik van en de migratie naar de volgende generatie cryptografie te zien.

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.

Migratieprocedure

Op dit moment is de aanbevolen methode om van DMVPN naar FlexVPN te migreren voor de twee raamwerken niet tegelijkertijd te werken. Deze beperking is gepland om te worden verwijderd

vanwege nieuwe migratiekaarten die moeten worden geïntroduceerd in de ASR 3.10 release, gevolgd door meerdere versterkingsverzoeken aan de kant van Cisco, die Cisco bug ID CSCuc08066 omvatten. Deze functies zouden eind juni 2013 beschikbaar moeten zijn.

Een migratie waarbij beide raamwerken naast elkaar bestaan en tegelijkertijd op dezelfde apparaten werken wordt een **zachte migratie** genoemd, die de minimale impact en de soepele uitvalmogelijkheid van het ene raamwerk naar het andere aangeeft. Een migratie waarbij configuraties voor beide raamwerken naast elkaar bestaan, maar niet tegelijkertijd werken, wordt een **harde migratie** genoemd. Dit duidt erop dat een overgang van het ene naar het andere raamwerk een gebrek aan communicatie over het VPN betekent, zelfs al is het minimaal.

Harde migratie tussen twee verschillende Hubs

In dit document wordt de migratie van het DMVPN-knooppunt, dat momenteel wordt gebruikt voor een nieuw FlexVPN-knooppunt, besproken. Deze migratie maakt intercommunicatie tussen spaken die al naar FlexVPN zijn gemigreerd mogelijk, en spaken die nog steeds op DMVPN lopen en in meerdere fasen kunnen worden uitgevoerd, op elke afzonderlijke speld.

Op voorwaarde dat de routinginformatie goed wordt ingevuld, moet de communicatie tussen gemigreerde en niet-gemigreerde spaken mogelijk blijven. Er kan echter extra vertraging worden waargenomen, omdat gemigreerde en niet-gemigreerde spokes geen met elkaar gesproken tunnels bouwen. Tegelijkertijd zouden gemigreerde spreekwoordjes in staat moeten zijn om tunnels met een rechtstreekse stem tussen elkaar op te zetten. Hetzelfde geldt voor niet-gemigreerde spaken.

Totdat deze nieuwe migratieoptie beschikbaar is, voltooi deze stappen om migraties met een ander knooppunt van DMVPN en FlexVPN uit te voeren:

1. Controleer de connectiviteit via DMVPN.
2. Voeg de configuratie FlexVPN toe en sluit de tunnel die aan de nieuwe configuratie toebehoort.
3. (Tijdens een onderhoudsvenster) Op elk gesproken, één voor één, sloot de DMVPN-tunnel af.
4. Op het zelfde dat zoals in Stap 3 wordt gesproken, sluit de FlexVPN tunnelinterfaces los.
5. Controleer de verbinding van het spinnenweb.
6. Controleer de luidsprekende verbinding binnen FlexVPN.
7. Controleer de aan-sprak connectiviteit met DMVPN van FlexVPN.
8. Herhaal stap 3 tot en met 7 voor elke spits afzonderlijk.
9. Als u problemen ondervindt met de verificaties die in stappen 5, 6 of 7 worden beschreven, sluit u de FlexVPN-interface en sluit u de DMVPN-interfaces af om terug te keren naar DMVPN.
10. Controleer de verbinding op de hub via de ondersteunde DMVPN.
11. Controleer de communicatie via de back-up DMVPN.

Aangepaste aanpak

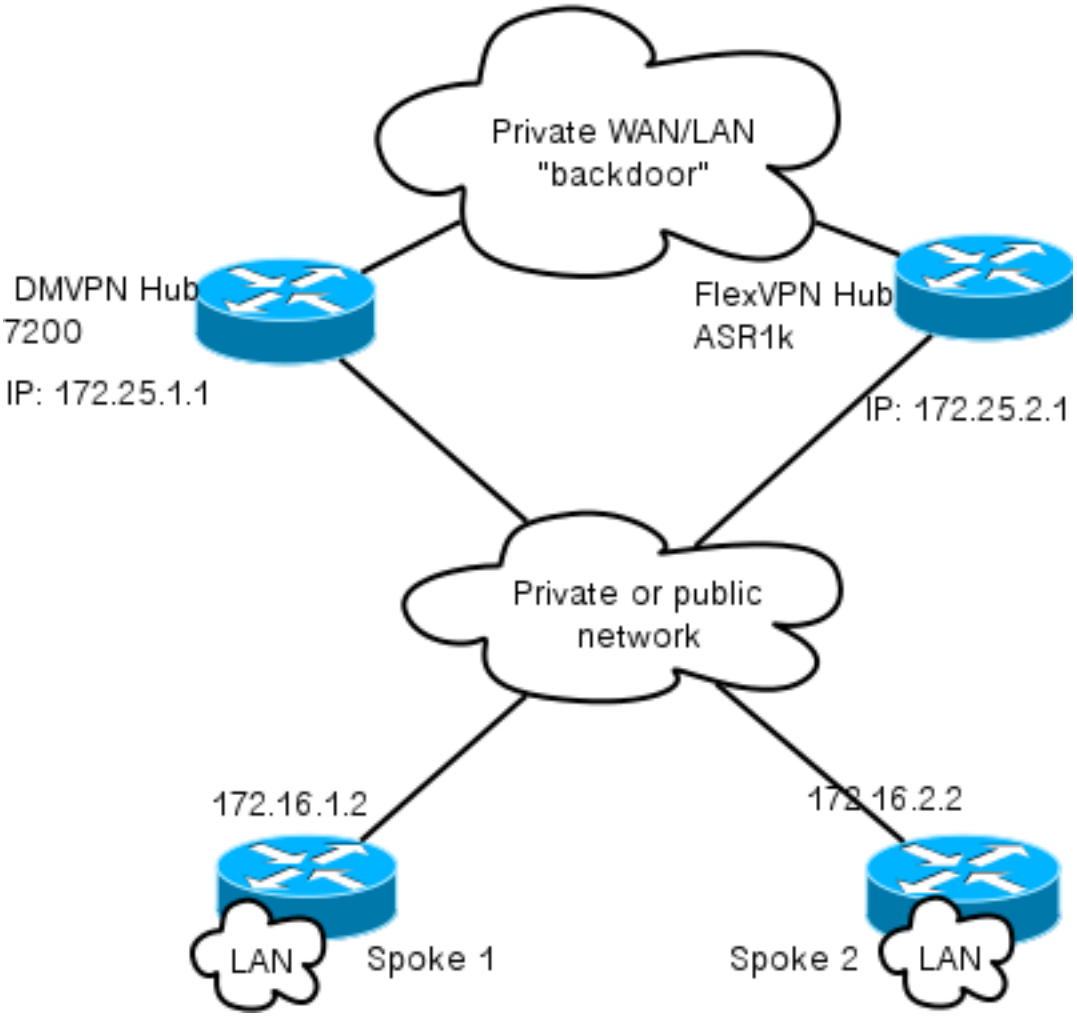
Als de vorige benadering mogelijk niet de beste oplossing voor u is door uw netwerk of routingcomplexiteit, start een discussie met uw Cisco-vertegenwoordiger voordat u migreert. De beste persoon waarmee u een aangepast migratieproces kunt bespreken, is uw System Engineer

of Advanced Services Engineer.

Netwerktopologie

Topologie voor transportnetwerk

In dit diagram wordt de typische verbindingstopologie van hosts op het internet getoond. Het IP-adres van de hub van **loopback0** (**172.25.1.1**) wordt gebruikt om de DMVPN IPsec-sessie te beëindigen. Het IP-adres in het nieuwe knooppunt (**172.25.2.1**) wordt gebruikt voor FlexVPN.

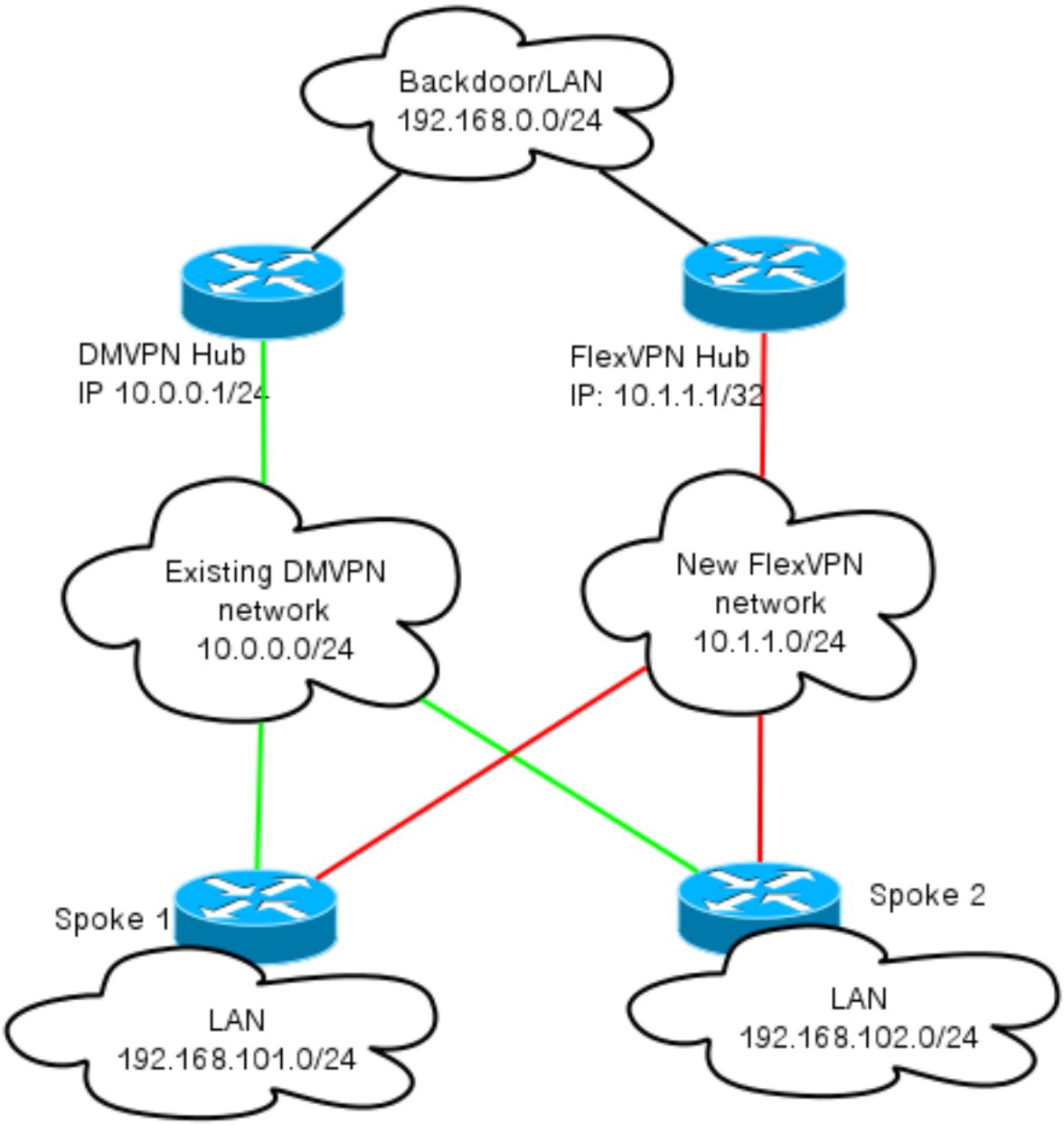


Merk het verband tussen de twee knooppunten op. Deze link is van cruciaal belang om connectiviteit tussen de FlexVPN en DMVPN wolken tijdens migratie toe te staan. Hiermee kunnen spaken die al naar FlexVPN zijn gemigreerd, communiceren met DMVPN-netwerken en vice versa.

Netwerktopologie overlay

In dit topologiediagram worden twee afzonderlijke wolken weergegeven die voor overlay worden gebruikt: DMVPN (groene verbindingen) en FlexVPN (rode verbindingen). LAN-prefixes worden weergegeven voor corresponderende locaties. Het **10.1.1.0/24**-subprogramma vertegenwoordigt geen echte SUBNET in termen van interface-adressering, maar vertegenwoordigt een deel van

IP-ruimte toegewijd aan de FlexVPN-cloud. De gedachte achter dit artikel wordt later besproken in het gedeelte **FlexVPN Configuration**.



Configuratie

In deze sectie worden de DMVPN- en de FlexVPN-configuraties beschreven.

DMVPN-configuratie

In dit gedeelte worden de basisconfiguratie voor het DMVPN-knooppunt beschreven.

De Pre-Shared Key (PSK) wordt gebruikt voor IKEv1-verificatie. Zodra IPsec is gevestigd, wordt de registratie van Next Hop Resolutie Protocol (NHRP) van sprak-to-hub uitgevoerd zodat het hub de niet-broadcast Multiaccess (NBMA) van de woordvoerders dynamisch kan leren.

Wanneer NHRP registratie op het gesproken en de hub uitvoert, kan het routeren van nabijheid zich, en routes kunnen worden uitgewisseld. In dit voorbeeld, wordt wanneer u een basisprotocol

voor het routingnetwerk gebruikt.

VPN-configuratie voor SPELDEN

Hier kunt u een basisvoorbeeldconfiguratie van DMVPN met PSK authenticatie en Ecp als het routingprotocol vinden.

```
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
```

Configuratie van hub DMVPN

In de hub configuratie, komt de tunnel uit **loopback0** met een IP-adres van **172.25.1.1**. De rest is een standaardimplementatie van een DMVPN-knooppunt met DHCP als routingprotocol.

```
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-configuratie

FlexVPN is gebaseerd op deze zelfde fundamentele technologieën:

- **IPsec**: In tegenstelling tot de standaard in DMVPN wordt IKEv2 gebruikt in plaats van IKEv1 om te onderhandelen over IPsec security associaties (SA's). IKEv2 biedt verbeteringen ten opzichte van IKEv1, zoals veerkracht en het aantal berichten dat nodig is om een beschermd gegevenskanaal op te zetten.

- **GRE:** In tegenstelling tot DMVPN worden statische en dynamische point-to-point interfaces gebruikt, en niet slechts één statische multi-point GRE interface. Deze configuratie maakt extra flexibiliteit mogelijk, vooral voor het gedrag per spraken/per hub.

- **NHRP**: In FlexVPN wordt NHRP voornamelijk gebruikt voor het opzetten van spraak-to-sprak communicatie. Spoken registreren zich niet op de hub.

- **Routing**: Omdat spokes geen NHRP registratie aan de hub uitvoeren moet u op andere mechanismen vertrouwen om te verzekeren dat de hub en de spokes bidirectioneel kunnen communiceren. Net als DMVPN kunnen dynamische routingprotocollen worden gebruikt. FlexVPN kan echter IPsec gebruiken om routinginformatie te introduceren. Het standaard is om als **32/32** route te introduceren voor het IP-adres aan de andere kant van de tunnel, wat de rechtstreekse communicatie tussen de spits en de hub toestaat.

Bij een harde migratie van DMVPN naar FlexVPN werken de twee frames niet tegelijkertijd op dezelfde apparaten. Het wordt echter aanbevolen deze gescheiden te houden.

Scheid deze op verschillende niveaus:

- NHRP - Gebruik een andere NHRP-netwerkid (aanbevolen).
- Routing - Gebruik afzonderlijke routingprocessen (aanbevolen).
- Virtual Routing and Forwarding (VRF) - VRF-scheiding biedt extra flexibiliteit, maar wordt hier niet besproken (optioneel).

SPE FlexVPN-configuratie

Een van de verschillen in de spaakconfiguratie in FlexVPN in vergelijking met DMVPN is dat je mogelijk twee interfaces hebt. Er is een vereiste tunnel voor spraak-naar-hub communicatie en een optionele tunnel voor gesproken tunnels. Als u ervoor kiest geen dynamisch gesproken-to-sprak tunneling te hebben en zou verkiezen dat alles door het naafapparaat gaat, kunt u de virtuele sjabloon interface verwijderen en de NHRP snelweg-switching uit de tunnelinterface verwijderen.

Merk op dat de statische tunnelinterface een IP-adres ontvangt dat gebaseerd is op onderhandeling. Dit staat het hub toe om het IP-adres van de tunnelinterface aan het gesproken dynamisch te verstrekken zonder de noodzaak om statische adressering in de FlexVPN-cloud te creëren.

```
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
```

> **Opmerking:** Standaard wordt de lokale identiteit ingesteld om het IP-adres te gebruiken. Dus moet het corresponderende overeenkomende overeenkomende verklaring op de peer ook overeenkomen op basis van het adres. Indien de vereiste moet overeenstemmen op basis van de opgegeven naam (DN) in het certificaat, dan moet de overeenkomst worden uitgevoerd met behulp van een kaart van het certificaat.

Cisco raadt u aan AES GCM te gebruiken met hardware die deze ondersteunt.

```
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
```

PKI (Public Key Infrastructure) is de aanbevolen methode om grootschalige verificatie uit te voeren in IKEv2. U kunt echter nog steeds PSK gebruiken zolang u op de hoogte bent van de beperkingen.

Hier is een voorbeeldconfiguratie die **cisco** als PSK gebruikt.

```
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
```

FlexVPN-hubconfiguratie

Meestal eindigt een hub alleen dynamische snelheidstuntunnels. Dit is waarom u geen statische tunnelinterface voor FlexVPN vindt in de hub configuratie. In plaats daarvan wordt een virtuele sjabloon-interface gebruikt.

> **Opmerking:** Op de hub kant, moet u de pooladressen aangeven die aan spokes moeten worden toegewezen.

Adressen uit deze pool worden later in de routingtabel toegevoegd als **/32** routes voor elk gesproken.

```
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 raadt u aan AES GCM te gebruiken met hardware die deze ondersteunt.

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

Opmerking: In deze configuratie is de AES GCM-werking becommentarieerd.

```
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
```

Met authenticatie in IKEv2 is hetzelfde principe van toepassing op de hub als op de sprak. Gebruik certificaten voor schaalbaarheid en flexibiliteit. U kunt echter dezelfde configuratie voor PSK opnieuw gebruiken als op de spits.

Opmerking: IKEv2 biedt flexibiliteit wat betreft authenticatie. De ene zijde kan authenticeren met PSK terwijl de andere zijde gebruik maakt van Rivest-Shamir-Adleman Signature (RSA-SIG).

Als de eis is om preShared keys voor authenticatie te gebruiken, dan zijn de configuratieveranderingen gelijk aan die welke hier voor de aangegeven router worden beschreven.

Inter-Hub BGP-verbinding

Zorg ervoor dat de hubs weten waar bepaalde prefixes zich bevinden. Dit wordt steeds belangrijker omdat sommige woordjes naar FlexVPN zijn gemigreerd terwijl sommige andere woordjes op DMVPN blijven staan.

Hier is de interhub BGP-verbinding die is gebaseerd op de DMVPN-hubconfiguratie:

```
router bgp 65001
network 192.168.0.0
```

```
neighbor 192.168.0.2 remote-as 65001
```

Verkeersmigratie

Naar BGP migreren als het Overlay Routing Protocol [Aanbevolen]

BGP is een routingprotocol dat gebaseerd is op eenastuitwisseling. Vanwege zijn eigenschappen is het het beste schaalprotocol in DMVPN-netwerken.

In dit voorbeeld wordt Interne BGP (iBGP) gebruikt.

BGP-configuratie

Spraakmigratie bestaat uit twee delen. Stel eerst BGP in als dynamische routing:

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

Nadat de BGP-buurman (zie de volgende sectie) naar boven komt en nieuwe prefixes via BGP worden geleerd, kunt u verkeer van de huidige DMVPN-cloud naar een nieuwe FlexVPN-cloud sturen.

Hub BGP-configuratie

FlexVPN-hub - volledige BGP-configuratie

Op de hub, om te voorkomen dat de configuratie van de buren voor elke sprak afzonderlijk wordt bewaard, moet u dynamische luisteraars configureren. In deze opstelling, opent BGP geen nieuwe verbindingen, maar aanvaardt verbindingen van de aangeboden pool van IP adressen. In dit geval is de genoemde pool **10.1.1.0/24**, wat alle adressen in de nieuwe FlexVPN-cloud is.

Er zijn twee opmerkingen:

- De FlexVPN-hub adverteert met specifieke prefixes bij de DMVPN-hub; de onderperskaart wordt dus gebruikt .
- Ofwel adverteer het FlexVPN-**net van 10.1.1.0/24** aan de routingtabel, of zorg ervoor dat het DMVPN-knooppunt het FlexVPN-knooppunt als de volgende hop ziet.

Dit document toont de laatste benadering.

```
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 - volledige BGP- en DHCP-configuratie

De configuratie op het DMVPN hub is fundamenteel, omdat het slechts specifieke prefixes van het FlexVPN knooppunt ontvangt en prefixes adverteert die het van DHCP leert.

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

Migratie van verkeer naar BGP/FlexVPN

Zoals eerder besproken moet u DMVPN-functionaliteit afsluiten en FlexVPN omhoog brengen om migratie uit te voeren.

Deze procedure garandeert een minimaal effect:

1. Voer op elke spreker afzonderlijk het volgende in:

   ```
   interface tunnel 0
    shut
   ```

   Zorg er op dit moment voor dat er geen IKEv1-zittingen zijn ingesteld voor deze spreker. Dit kan worden geverifieerd als u de uitvoer van de opdracht **show crypto** isakmp **als** opdracht controleert en de syslogberichten controleert die door de opdracht van de **crypto-logsessie** zijn gegenereerd. Zodra dit bevestigd is, kunt u FlexVPN opnieuw opstarten.

2. Voer op het zelfde moment het volgende in:

   ```
   interface tunnel 1
     no shut
   ```

Verificatiestappen

IPsec-stabiliteit

De beste manier om de stabiliteit van IPsec te evalueren is om sylogs te controleren met de configuratie van de **crypto-logsessie** ingeschakeld. Als u sessies ziet die omhoog en omlaag gaan, kan dit wijzen op een probleem op het IKEv2/FlexVPN-niveau dat moet worden gecorrigeerd

voordat de migratie kan beginnen.

BGP-informatie gevuld

Als IPsec stabiel is, zorg er dan voor dat de BGP-tabel is bevolkt met items uit de spaken (op de hub) en samenvatting uit de hub (op de spaken). In het geval van BGP, kan dit met deze opdrachten worden bekeken:

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

Hier is een voorbeeld van correcte informatie van de hub van FlexVPN:

```
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
```

De output toont dat de hub één prefix van elk van de spaken heeft geleerd, en beide spaken zijn dynamisch en gemarkeerd met een sterretje (*) teken. Het toont ook aan dat in totaal vier prefixes van de verbinding tussen de knooppunten worden ontvangen.

Hieronder volgen een paar voorbeelden van soortgelijke informatie uit het artikel:

```
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
```

De toespraak heeft twee prefixes van het centrum ontvangen. In het geval van deze instelling, zou één prefix de samenvatting moeten zijn die op de FlexVPN hub wordt geadverteerd. Het andere is DMVPN 10.0.0.0/24 netwerk dat op DMVPN is herverdeeld dat in BGP wordt gesproken.

Migreren naar nieuwe tunnels met NGEW

DHCP is een populaire keuze in netwerken DMVPN door zijn relatief eenvoudige implementatie en snelle convergentie. Deze schaalt echter verder dan BGP en biedt niet veel geavanceerde mechanismen aan die door BGP direct uit de doos kunnen worden gebruikt. De volgende sectie beschrijft een van de manieren om naar FlexVPN te bewegen met een nieuw EHRM proces.

Configuratie van bijgewerkt bereik

Een nieuw Autonoom Systeem (AS) wordt toegevoegd met een afzonderlijk EHBO-proces:

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

Opmerking: Het is best om geen routingprotocol nabijheid over gesproken-aan-gesproken tunnels vast te stellen. Om deze reden passief de interface van **tunnel1** (sprak-aan-hub) alleen.

Upload FlexVPN-hubconfiguratie

Op dezelfde manier, voor de FlexVPN hub, bereidt het routingprotocol in het geschikte AS voor, dat op de spaken wordt gevormd.

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

Er zijn twee methoden die worden gebruikt om een samenvatting te geven van de gemaakte opmerkingen.

- Verdeel een statische route die wijst op **nul** (voorkeuroptie).

```
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
```

Met deze optie kunt u controle over samenvatting en herdistributie uitvoeren zonder wijzigingen in de VT-configuratie (hub's Virtualization Technology). Dit is belangrijk, omdat de VT-configuratie van de hub niet kan worden aangepast als er actieve virtuele toegang aan gekoppeld is.

- Stel een Samenvattend adres in de stijl DMVPN in op een virtuele sjabloon.

Deze configuratie wordt *niet aanbevolen*, vanwege de interne verwerking en replicatie van de samenvatting naar elke virtuele toegang. Hier wordt dit ter referentie weergegeven.

```
interface Virtual-Template1 type tunnel
 ip summary-address eigrp 200 192.168.0.0 255.255.0.0
```

Een ander aspect om rekening mee te houden is de inter-hub routing exchange. Dit kan

worden gedaan als u EIS instanties aan iBGP herverdeelt.

DMVPN-hub - bijgewerkte BGP-configuratie

De configuratie blijft fundamenteel. U moet specifieke prefixes van DHCP aan BGP opnieuw verdelen:

```
router bgp 65001

redistribute eigrp 100

neighbor 192.168.0.2 remote-as 65001
```

FlexVPN-hub - bijgewerkte BGP-configuratie

Gelijkaardig aan het DMVPN hub, in FlexVPN, moet u de prefixes van het nieuwe EHRM proces aan BGP herverdelen:

```
router bgp 65001

 redistribute eigrp 200 redistribute static

 neighbor 192.168.0.1 remote-as 65001
```

Migreren van verkeer naar FlexVPN

U moet de DMVPN-functionaliteit afsluiten en FlexVPN op elke opgenomen persoon laten oplopen, één voor één, om migratie uit te voeren. Deze procedure garandeert een minimaal effect:

1. Voer op elke spreker afzonderlijk het volgende in:

   ```
   interface tunnel 0
    shut
   ```

   Zorg er op dit moment voor dat er geen IKEv1-zittingen zijn ingesteld op deze spreker. Dit kan worden geverifieerd als u de uitvoer van de opdracht **show crypto** isakmp **als** opdracht controleert en de syslogberichten controleert die door de opdracht van de **crypto-logsessie** zijn gegenereerd. Zodra dit bevestigd is, kunt u FlexVPN opnieuw opstarten.
2. Voer op het zelfde moment het volgende in:

   ```
   interface tunnel 1
     no shut
   ```

Verificatiestappen

IPsec-stabiliteit

Zoals bij BGP moet u evalueren of IPsec stabiel is. De beste manier om dit te doen is om sylogs te bewaken met de configuratie van de **crypto-logsessie** ingeschakeld. Als u sessies omhoog en

omlaag ziet, kan dit wijzen op een probleem op het IKEv2/FlexVPN-niveau dat moet worden gecorrigeerd voordat de migratie kan beginnen.

Eco-informatie in toeristentabel

Zorg ervoor dat uw topologietabel wanneer EHRM met gesproken LAN ingangen op de hub en samenvatting op de woordvormen bevolkt is. Dit kan worden geverifieerd als u deze opdracht op de hub(s) en de sprak(en) invoert:

```
show ip eigrp [AS_NUMBER] topology
```

Hier is een voorbeeld van de productie van het sprak:

```
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
```

De output toont dat het sprak over zijn LAN SUBNET (in *cursief*) en de samenvattingen voor die (**vet**) kent.

Hier is een voorbeeld van de output van het centrum:

```
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)
```

De output toont dat het hub weet over LAN-subnetten van de spaken (in het *cursief*), het korte voorvoegsel dat het adverteert (**vet**) en het toegewezen IP-adres van elke speld via

onderhandeling.

Aanvullende overwegingen

Spoke-to-Spoke tunnels die al bestaan

Omdat een shutdown van de DMVPN tunnelinterface ervoor zorgt dat NHRP-items worden verwijderd, zullen gesproken-to-sprak tunnels die al bestaan worden afgebroken.

Vermeldingen wissen NHRP

Een FlexVPN-hub is niet afhankelijk van het NHRP-registratieproces vanuit de computer om te weten hoe het verkeer moet worden teruggeleid. Desondanks zijn dynamische met een gesproken tunnel afhankelijk van NHRP-ingangen.

In DMVPN, als NHRP op de hub wordt gewist, kan dit leiden tot kortstondige connectiviteitsproblemen. In FlexVPN zal het opschonen van NHRP op de spaken ervoor zorgen dat de FlexVPN IPsec-sessie, gerelateerd aan tunnels met een toespraak aan een spaak, wordt afgebroken. Het opruimen van NHRP op de hub heeft geen effect op de FlexVPN-sessie.

Dit komt doordat, in FlexVPN, standaard:

- Sproken zich niet op knooppunten.
- Hubs werken alleen als NHRP-regisseurs en installeren geen NHRP-items.
- NHRP-sneltoetsen worden op spokes geïnstalleerd voor tunnels met een sprak bereik en zijn dynamisch.

gekende Caveats

Het gesproken verkeer kan door Cisco bug-ID CSCub07382 worden beïnvloed.

Gerelateerde informatie

- DMVPN naar FlexVPN softwareconfiguratie
- Technische ondersteuning en documentatie – Cisco Systems