Harde beweging van DMVPN naar FlexVPN op dezelfde apparaten

Inhoud

Inleiding

Dit document bevat informatie over de manier waarop u van een bestaand DMVPN-netwerk naar FlexVPN kunt migreren op dezelfde apparaten.

Beide raamformaties zullen op de apparaten naast elkaar bestaan.

In dit document wordt alleen het meest voorkomende scenario getoond: DMVPN met behulp van vooraf gedeelde sleutel voor authenticatie en DHCP als routingprotocol.

Dit document demonstreert migratie naar BGP (aanbevolen routingprotocol) en minder wenselijke DHCP.

Voorwaarden

Vereisten

Dit document gaat ervan uit dat de lezer basisconcepten van DMVPN en FlexVPN kent.

Gebruikte componenten

Let op dat niet alle software en hardware IKEv2 ondersteunen. Raadpleeg de Cisco Functie Navigator voor informatie. Idealiter worden softwareversies gebruikt:

- ISR - 15.2(4)M1 of nieuwer
- ASR1k - 3.6.2 release 15.2(2)S2 of nieuwer

Een van de voordelen van nieuwer platform en software is de mogelijkheid om cryptografie van de volgende generatie te gebruiken, bijvoorbeeld AES GCM voor encryptie in IPsec. Dit wordt besproken in RFC 4106.

Met AES GCM kan de coderingssnelheid van bepaalde hardware veel sneller worden bereikt.

Om de aanbevelingen van Cisco te zien over het gebruik en het migreren naar de Cryptografie van de volgende generatie, raadpleeg:

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

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Migratieprocedure

Op dit moment is de aanbevolen manier om van DMVPN naar FlexVPN te migreren: de twee raamwerken hoeven niet tegelijkertijd te werken.

Deze beperking zal worden opgeheven door nieuwe migratiekenmerken die moeten worden geïntroduceerd in de ASR 3.10 release, gevolgd door meerdere versterkingsverzoeken onder de Cisco-zijde, inclusief CSCuc08066. Deze functies zouden eind juni 2013 beschikbaar moeten zijn.

Een migratie waarbij beide raamwerken naast elkaar bestaan en tegelijkertijd op dezelfde apparaten werken, zal worden aangeduid als "zachte migratie", wat een minimale impact en een soepele uitvalmogelijkheid van het ene raamwerk naar het andere aangeeft.

Een migratie waarbij de configuratie van beide raamwerken naast elkaar bestaat, maar niet tegelijkertijd functioneert, wordt een harde migratie genoemd. Dit duidt erop dat een overgang van het ene naar het andere raamwerk een gebrek aan communicatie over VPN betekent, zelfs al is het minimaal.

Harde migratie op dezelfde apparaten

In dit document wordt de migratie van een bestaand DMVPN-netwerk naar een nieuw FlexVPN-netwerk op dezelfde apparaten besproken.

Deze migratie vereist dat beide raamwerken niet op hetzelfde moment op de apparaten werken, wat in wezen vereist is dat de DMVPN-functionaliteit over de hele lijn wordt uitgeschakeld voordat FlexVPN wordt ingeschakeld.

Totdat de nieuwe migratiefunctie beschikbaar is, kunt u migratie met dezelfde apparaten uitvoeren door:

1. Controleer de connectiviteit via DMVPN.
2. Voeg de configuratie van FlexVPN op zijn plaats toe en sluit Tunnel en Virtuele sjablooninterfaces die tot nieuwe configuratie behoren.
3. (Tijdens een onderhoudsvenster) Sluit alle DMVPN-tunnelinterfaces op alle spaken en hubs af voordat u naar stap 4 gaat.
4. Open FlexVPN-tunnelinterfaces.
5. Controleer of er verbinding is.
6. Controleer dat er een verbinding is.
7. *Als verificatie in punt 5 of 6 niet naar behoren terugkeert naar DMVPN door de FlexVPN-interface te sluiten en DMVPN-interfaces af te sluiten.*
8. *Controleer de communicatie.*
9. *Na raadpleging van de gesproken communicatie.*

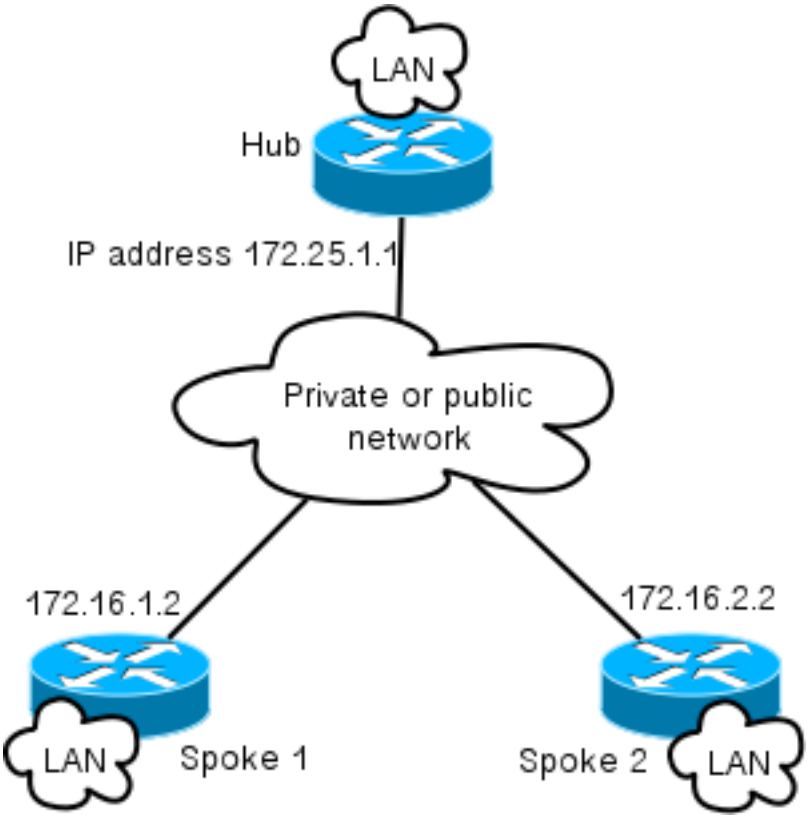
Aangepaste benadering

Als, door uw netwerk of routingcomplexiteit, de benadering niet het beste idee voor u zou kunnen zijn, start een discussie met uw Cisco vertegenwoordiger voordat u migreert. De beste persoon om een aangepast migratieproces te bespreken is uw System Engineer of Advanced Services Engineer.

Netwerktopologie

topologie van transportnetwerken

Dit diagram toont een typische topologie van verbindingen van hosts op het internet. In dit document wordt het IP-adres van de hub van loopback0 (172.25.1.1) gebruikt om de IPsec-sessie te beëindigen.

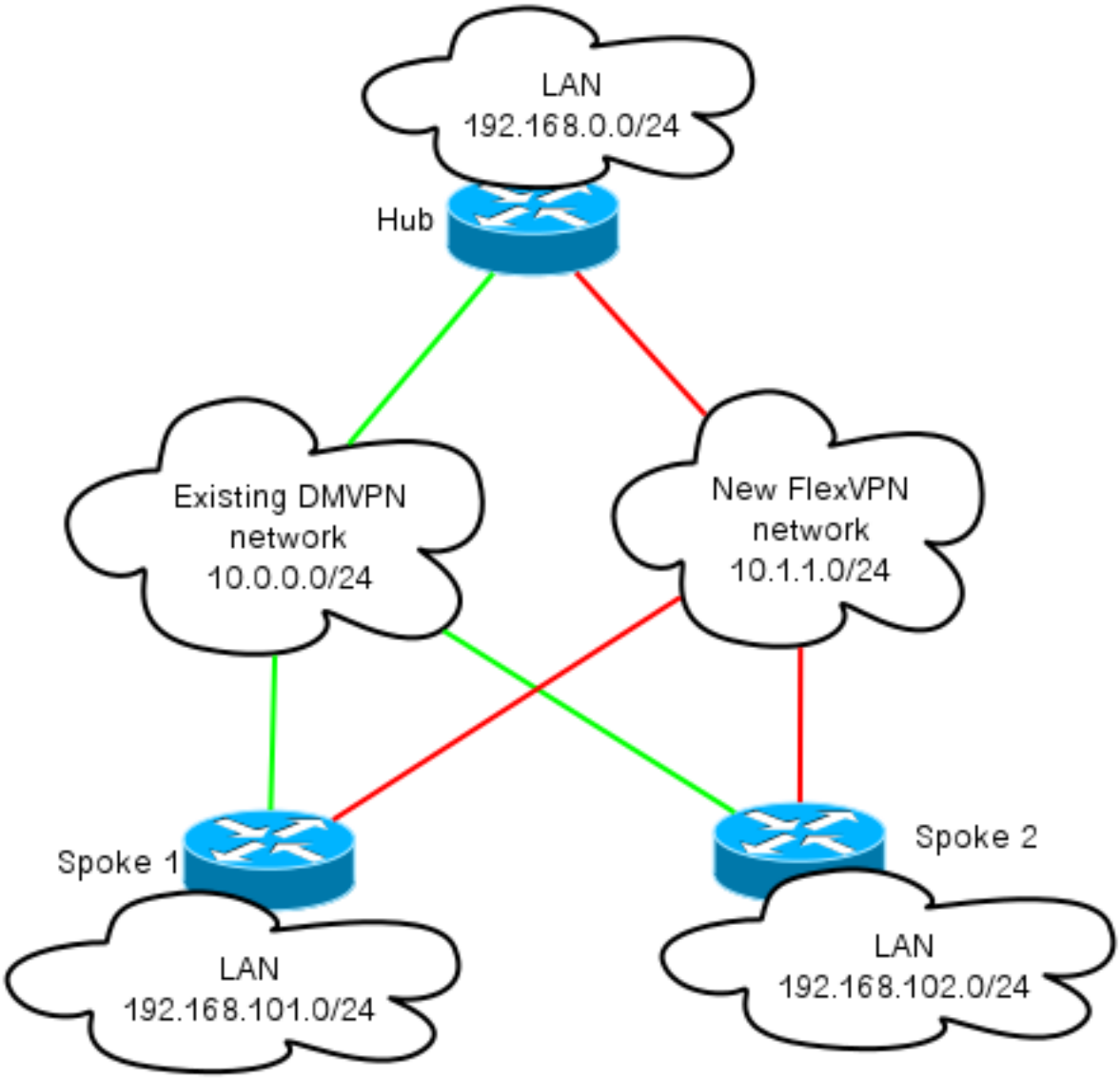


[topologie van het netwerk overlay]

In dit topologiediagram worden twee afzonderlijke wolken weergegeven die voor overlay worden gebruikt: DMVPN (groene verbindingen) en FlexVPN-verbindingen.

De lokale netwerkprefixes van het gebied worden voor de corresponderende zijkanten weergegeven.

Het 10.1.1.0/24-subnet vertegenwoordigt geen echte SUBNET in termen van interface het richten, maar eerder een deel van IP-ruimte die aan FlexVPN-cloud wordt besteed. De rationale achter wordt later besproken in het gedeelte FlexVPN Configuration.



Configuratie

DMVPN-configuratie

Deze sectie bevat basisconfiguratie van DMVPN hub en sprak.

Vooraf gedeelde sleutel (PSK) wordt gebruikt voor IKEv1-verificatie.

Wanneer IPsec is gevestigd, wordt de registratie NHRP uitgevoerd van uitgediept tot hub, zodat de hub de dynamisch spaken' NBMA adressering kan leren.

Wanneer NHRP registratie op SPD en hub uitvoert, kan het routeren van nabijheid en uitgewisselde routes tot stand brengen. In dit voorbeeld, wordt zij gebruikt als basisroutingprotocol voor het overlay netwerk.

Gesproken DMVPN-configuratie

Dit is een basale voorbeeldconfiguratie van DMVPN met pre-gedeelde zeer belangrijke authenticatie en Ecp als routingprotocol.

```
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-configuratie

In de hub-configuratie is de tunnel afkomstig van loopback0 met een IP-adres van 172.25.1.1.

De rest is standaardplaatsing van de hub van DMVPN met Ecp als Routing Protocol.

```
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: Anders dan standaard bij DMVPN wordt IKEv2 gebruikt in plaats van IKEv1 om IPsec SA's te onderhandelen. IKEv2 biedt verbeteringen in vergelijking met IKEv1, te beginnen met veerkracht en eindigend met het aantal berichten dat nodig is om een beveiligd gegevenskanaal op te zetten.
- GRE: In tegenstelling tot DMVPN worden statische en dynamische point-to-point interfaces gebruikt, en niet alleen op statische multipoint GRE-interfaces. Deze configuratie maakt extra flexibiliteit mogelijk, vooral voor het gedrag per spraken/per hub.
- NHRP: In FlexVPN wordt NHRP voornamelijk gebruikt om spraakte communicatie op te zetten. Spoken registreren zich niet op de hub.
- Routing: Omdat spokes geen NHRP-registratie naar de hub uitvoeren, moet je op andere mechanismen vertrouwen om te verzekeren dat hub en spokes bidirectioneel kunnen communiceren. Net als DMVPN kunnen dynamische routingprotocollen worden gebruikt. Maar FlexVPN kan IPsec gebruiken om routinginformatie te introduceren. Het standaard is om als /32 route voor het IP adres aan de andere kant van de tunnel te introduceren, wat een direct contact tussen de spits en de hub zal toestaan.

Bij 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).
- VRF - VRF-scheiding kan extra flexibiliteit toestaan, maar zal hier niet worden besproken (optioneel).

SPE FlexVPN-configuratie

Een van de verschillen in configuratie van FlexVPN in vergelijking met DMVPN is dat je mogelijk twee interfaces hebt.

Er is een noodzakelijke tunnel voor een verbinding met een hub en een optionele tunnel voor gesproken tunnels. Als u ervoor kiest dynamisch gesproken te hebben met een gesproken tunneling en liever zou dat alles door een naaf apparaat gaat, kunt u de virtuele-sjabloon interface verwijderen en NHRP-snelswitching uit de tunnelinterface verwijderen.

U zal ook opmerken dat de statische tunnelinterface een IP adres heeft dat op basis van onderhandeling wordt ontvangen. Dit staat het hub toe om IP van de tunnelinterface te verstrekken om dynamisch te spreken zonder de noodzaak om statische het richten in de FlexVPN wolk 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
 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 het gebruik van AES GCM aan in 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 172.25.1.1
 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 is de aanbevolen manier om grootschalige authenticatie in IKEv2 uit te voeren.

U kunt echter wel pre-Shared key gebruiken zolang u zich bewust bent van de beperkingen van deze toets.

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
```

FlexVPN-hubconfiguratie

Meestal zal een hub alleen dynamische spraak-to-hub tunnels beëindigen. Dit is waarom u in de configuratie van de hub geen statische tunnelinterface voor FlexVPN vindt, in plaats daarvan wordt een virtuele-sjabloon-interface gebruikt. Hierdoor wordt voor elke verbinding een virtuele-toegangsinterface gecreëerd.

Merk op dat u op de hub kant pooladressen moet wijzen die aan spokes moeten worden toegewezen.

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

```
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 raadt het gebruik van AES GCM aan in hardware die deze ondersteunt.

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

Merk op dat in de configuratie hieronder de AES GCM-werking is becommentarieerd.

```
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
```

Met authenticatie in IKEv2 is hetzelfde principe van toepassing op de hub als op het sprak.

Gebruik certificaten voor schaalbaarheid en flexibiliteit. U kunt echter voor PSK dezelfde configuratie opnieuw gebruiken als voor een PSK.

Opmerking: IKEv2 biedt flexibiliteit wat betreft authenticatie. De ene kant kan het gebruik van PSK authenticeren terwijl de andere RSA-SIG.

Verkeersmigratie

Migreren naar BGP als overlay-routingprotocol [Aanbevolen]

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

In dit voorbeeld wordt iBGP gebruikt.

Gesproken BGP-configuratie

Spraakmigratie bestaat uit twee delen. BGP inschakelen 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 omhoog komt (zie de Hub BGP-configuratie in dit gedeelte van migratie) en nieuwe prefixes via BGP worden geleerd, kunt u verkeer vanaf de bestaande DMVPN-cloud naar de nieuwe FlexVPN-cloud sturen.

Hub BGP-configuratie

Op een hub om te voorkomen dat de configuratie van de buren voor elke spreek afzonderlijk wordt bewaard, worden dynamische luisteraars geconfigureerd.

In deze installatie zal BGP geen nieuwe verbindingen initiëren, maar zal een verbinding vanuit de ingestelde pool van IP-adressen accepteren. In dit geval is de genoemde pool 10.1.1.0/24, wat alle adressen in de nieuwe FlexVPN-cloud is.

```
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
```

Migratie van verkeer naar FlexVPN

Zoals eerder vermeld voor migratie moet worden gedaan door de DMVPN-functionaliteit te sluiten en FlexVPN omhoog te brengen.

Deze procedure garandeert een minimum-effect.

1. Alle spreekwoorden:
   ```
   interface tunnel 0
      shut
   ```
2. Op de hub:
   ```
   interface tunnel 0
     shut
   ```

Zorg er op dit punt voor dat er geen IKEv1 sessies zijn die vanuit de spaken op dit knooppunt zijn ingesteld.Dit kan worden geverifieerd door de uitvoer van de **show crypto isakmp als** commando en controle van de syslogberichten die door de crypto houtkapsessie zijn gegenereerd te controleren.Nadat dit is bevestigd kunt u FlexVPN activeren.

3. Doorgaan op hub:
```
interface Virtual-template 1
 no shut
```
4. Op woordjes:
```
interface tunnel 1
   no shut
```

Verificatiestappen

Stabiliteit van IPsec

De beste manier om de stabiliteit van IPsec te evalueren is door sylogs te controleren met deze configuratie opdracht ingeschakeld:

```
crypto logging session
```

Als u sessies omhoog en omlaag ziet gaan, kan dit wijzen op een probleem op IKEv2/FlexVPN-niveau dat moet worden gecorrigeerd voordat de migratie kan beginnen.

BGP-informatie ingevuld

Als IPsec stabiel is, zorg er dan voor dat de BGP-tabel is bevolkt met items van spokes (op een hub) en samenvatting van een hub (op spokes).

In het geval van BGP kan dit worden bekeken door het volgende uit te voeren:

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

Voorbeeld van correcte informatie van 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
```

U kunt zien dat de hub heeft geleerd dat 1 prefix van elk van de spaken en beide spokes dynamisch zijn (gemarkeerd met sterretje (*) teken).

Voorbeeld van soortgelijke informatie uit het artikel:

```
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 heeft één voorvoegsel van de hub ontvangen. In het geval van deze instelling moet dit voorvoegsel de samenvatting zijn die op de hub wordt geadverteerd.

Migreren naar nieuwe tunnels met behulp van DHCP

DHCP is een populaire keus in netwerken DMVPN door het is relatief eenvoudige implementatie en snelle convergentie.

Deze zal echter groter worden dan BGP en biedt niet veel geavanceerde mechanismen die door BGP direct uit het doosje kunnen worden gebruikt.

In deze volgende sectie wordt een van de manieren beschreven om naar FlexVPN te verplaatsen met behulp van een nieuw EKE-proces.

Bijgewerkt configuratie

In dit voorbeeld, wordt een nieuw AS toegevoegd met een afzonderlijk Ecu-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: U zou moeten vermijden om protocol nabijheid toe te wijzen over gesproken tunnels, en zo slechts verbinding van tunnel1 (gesproken met hub) te maken niet passief.

Bijgewerkt hubconfiguratie

Op dezelfde manier zou DMVPN de favoriete manier moeten blijven om verkeer over te wisselen. FlexVPN moet echter al adverteren en dezelfde prefixes leren.

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

Er zijn twee manieren om een samenvatting te geven van het debat.

- Herdistributie van een statische route die naar nul wijst (voorkeuroptie).
  ```
  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
  ```
  Met deze optie kunt u controle hebben over summiere en herdistributie zonder de VT-configuratie van een hub te raken.
- Of, u kunt een DMVPN-stijl overzichtsadres op Virtual-sjabloon instellen. Deze configuratie wordt niet aanbevolen vanwege interne verwerking en replicatie van de samenvatting naar

elke virtuele toegang. Hier zie je ze ter referentie:

```
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
```

Migratie van verkeer naar FlexVPN

De migratie moet worden uitgevoerd door de DMVPN-functionaliteit te sluiten en FlexVPN omhoog te brengen.

De volgende procedure garandeert een minimum-effect.

1. Alle spreekwoorden:
   ```
   interface tunnel 0
      shut
   ```
2. Op de hub:
   ```
   interface tunnel 0
     shut
   ```
   Zorg er op dit punt voor dat er geen IKEv1 sessies zijn die vanuit de spaken op dit knooppunt zijn ingesteld.Dit kan worden geverifieerd door de uitvoer van de **show crypto isakmp als** commando en controle van de syslogberichten die zijn gegenereerd door crypto houtkapsessie te controleren.Nadat dit is bevestigd kunt u FlexVPN activeren.
3. Doorgaan op hub:
   ```
   interface Virtual-template 1
    no shut
   ```
4. Alle spreekwoorden:
   ```
   interface tunnel 1
      no shut
   ```

Verificatiestappen

Stabiliteit van IPsec

Zoals bij BGP moet u evalueren of IPsec stabiel is. De beste manier om dit te doen is door de controles van sylogs met deze configuratieopdracht toe te staan:

```
crypto logging session
```

Als u sessies omhoog en omlaag ziet gaan, kan dit wijzen op een probleem op IKEv2/FlexVPN-niveau dat moet worden gecorrigeerd voordat de migratie kan beginnen.

EurRom-informatie in topologietabel

Zorg ervoor dat u uw topologietabel hebt die met SPAARDIGE LAN ingangen op hub en samenvatting op SPELEN bevolkt. Dit kan worden geverifieerd door deze opdracht uit te geven op de hub(s) en de sprak(en).

```
show ip eigrp topology
```

Voorbeeld van een goede productie van een sprak:

```
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
```

U zult opmerken dat het sprak over zijn LAN SUBNET (in cursief) en de samenvattingen voor die (**vet**) kent.

Voorbeeld van juiste output van een 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
```

U merkt op dat hub weet van LAN-subnetten (cursief) van woordvoerders, het korte voorvoegsel dat het adverteert (**vet**) en het toegewezen IP-adres van elke spaak is via onderhandeling.

Aanvullende overwegingen

Bestaande gesproken tunnels

Omdat het sluiten van de DMVPN tunnelinterface ervoor zorgt dat NHRP-items worden verwijderd, wordt bestaande gesproken tunnels afgebroken.

NHRP-items wissen

Zoals eerder vermeld, zal een FlexVPN-hub niet vertrouwen op het NHRP-registratieproces van een spuit om te weten hoe het verkeer moet worden teruggeleid. Dynamisch gesproken met gesproken tunnels is echter afhankelijk van NHRP-ingangen.

In DMVPN, waar het opruimen van NHRP op hub kon hebben geresulteerd in kortstondige connectiviteitsproblemen.

Bij het opruimen van FlexVPN zal NHRP op spokes ervoor zorgen dat FlexVPN IPsec-sessie, gerelateerd aan spraaktunnels, wordt afgebroken. Bij het opruimen van NHRP zal geen hub een effect hebben op FlexVPN-sessie.

Dit is het gevolg van het feit dat in FlexVPN de standaardinstelling:

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

gekende Caveats

Gesproken aan spraakverkeer kunnen door CSCub07382 worden beïnvloed.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems