Configureer beveiligde overlay met BGP-routeaankondigingen

Inhoud

- Inleiding
- Gebruikte componenten
  - BGP-routeaankondiging
- Configuratievoorbeeld
  - Topologiediagram
  - Eerste configuratie
  - FlexVPN-serverconfiguratie op de Catalyst 8000v router
    - 1. Een IKEv2-voorstel maken
    - 2. Maak een IKEv2-beleid en koppel dit aan het voorstel.
    - 3. Configureer het IKEv2-autorisatiebeleid
    - 4. Een IKEv2-profiel maken
    - 5. Een IPsec-transformatieset maken
    - 6. Standaard IPsec-profiel verwijderen
    - 7. Maak een IPsec-profiel en koppel het aan een transformatieset en het IKEv2-profiel.
    - 8. Een virtuele sjabloon maken
  - Minimale configuratie voor NFVIS Secure Overlay
    - Overlay-status bekijken
  - BGP-configuratie voor routeaankondiging voor FlexVPN-server
  - BGP-configuratie op NFVIS
    - BGP-beoordeling
    - Zorg ervoor dat de Private Subnets van FlexVPN Server via BGP zijn geadverteerd
- Probleemoplossing
  - NFVIS (FlexVPN-client)
    - NFVIS-logbestanden
    - Inwendige Kernel strongswan geïnjecteerde routes
    - IPsec0-interfacestatus bekijken
  - Head-end (FlexVPN-server)
    - IPsec SA's bekijken die tussen peers zijn gebouwd
    - Actieve crypto-sessies (encryptie) weergeven
    - VPN-verbindingen opnieuw instellen
    - Debugs uitvoeren voor aanvullende probleemoplossing
- Verwante artikelen en documentatie

Inleiding

Dit document beschrijft hoe u beveiligde overlay en eBGP-aankondigingen op NFVIS kunt configureren voor exclusief vBranch-verkeersbeheer.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwarecomponenten:

- ENCS 5412 met NFVIS 4.7.1
- Catalyst 8000v met Cisco IOS® XE 17.09.03a

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

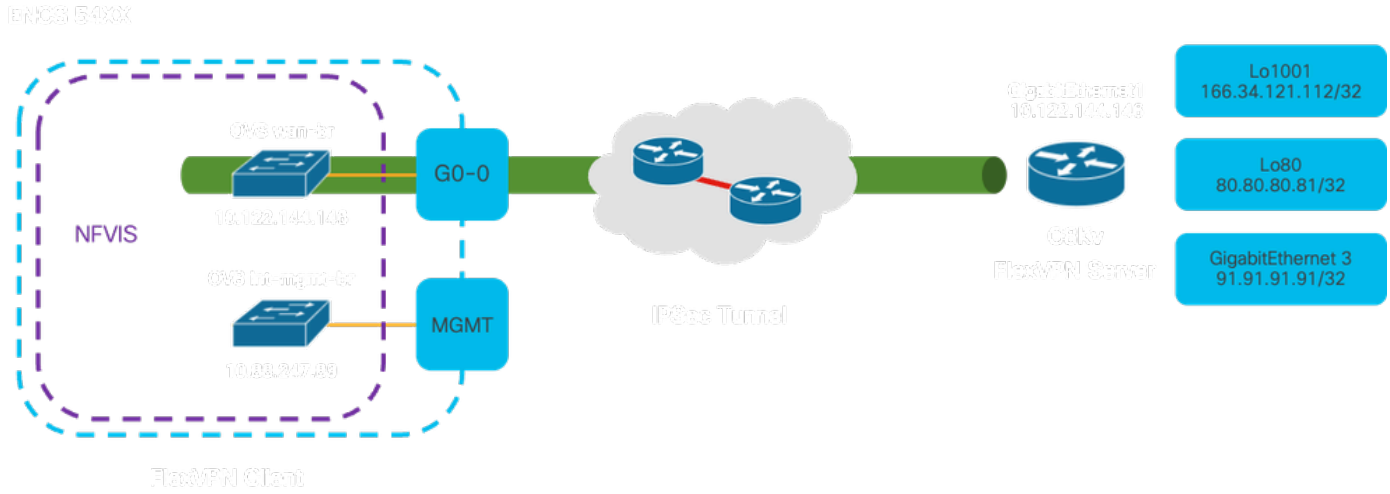
BGP-routeaankondiging

NFVIS BGP-functie werkt met de beveiligde overlay-functie om routes te leren van de BGP-buur via een beveiligde overlay-tunnel. Deze geleerde routes of subnetten worden toegevoegd aan de NFVIS-routeringstabel voor de beveiligde tunnel, die de routes toegankelijk maakt via de tunnel. Aangezien Secure Overlay slechts 1 enkele privé-route uit de tunnel laat leren; het configureren van BGP maakt het mogelijk om deze beperking te overkomen door nabijheid door de versleutelde tunnel tot stand te brengen en geëxporteerde routes te injecteren in de NFVIS vpnv4-routeringstabel en vice versa.

Configuratievoorbeeld

Topologiediagram

Het doel van deze configuratie is om het IP-adres voor beheer van NFVIS te bereiken vanaf de c8000v. Zodra de tunnel is opgezet, is het mogelijk om meer routes van de privé-vrf subnetten te adverteren met behulp van eBGP-routeaankondigingen.



Afbeelding 1. Topologiediagram voor het Voorbeeld voorbereid op dit artikel

Eerste configuratie

Configureer de relevante IP-adressering op de FlexVPN-server (alle binnen de algemene configuratiemodus)

```
vrf definition private-vrf
 rd 65000:7
 address-family ipv4
 exit-address-family

vrf definition public-vrf
 address-family ipv4
 exit-address-family

interface GigabitEthernet1
 description Public-Facing Interface
 vrf forwarding public-vrf
 ip address 10.88.247.84 255.255.255.224

interface Loopback1001
 description Tunnel Loopback
 vrf forwarding private-vrf
 ip address 166.34.121.112 255.255.255.255

interface Loopback80
 description Route Announced Loopback
 vrf forwarding private-vrf
 ip address 81.81.81.1 255.255.255.255

interface GigabitEthernet3
 description Route Announced Physical Interface
 vrf forwarding private-vrf
 ip address 91.91.91.1 255.255.255.0
```

Voor NFVIS moet u de WAN- en MGMT-interface dienovereenkomstig configureren

```
system settings mgmt ip address 192.168.1.1 255.255.255.0
system settings wan ip address 10.88.247.89 255.255.255.224
system settings default-gw 10.88.247.65
system settings ip-receive-acl 0.0.0.0/0
 service  [ ssh https netconf scpd ]
 action   accept
 priority 10
!
```

FlexVPN-serverconfiguratie op de Catalyst 8000v router

1. Een IKEv2-voorstel maken

Het specificeert de beveiligingsprotocollen en algoritmen die twee VPN-endpoints moeten gebruiken tijdens de eerste fase (fase 1) van het opzetten van een beveiligd communicatiekanaal. Het doel van het IKEv2-voorstel is de parameters voor authenticatie, encryptie, integriteit en

sleuteluitwisseling te schetsen, waarbij ervoor wordt gezorgd dat beide eindpunten het eens worden over een gemeenschappelijke reeks beveiligingsmaatregelen voordat ze gevoelige gegevens uitwisselen.

```
crypto ikev2 proposal uCPE-proposal
 encryption aes-cbc-256
 integrity sha512
 group 16 14
```

Waarbij:

encryptie <algoritme>	Het voorstel bevat de versleutelingsalgoritmen (zoals AES of 3DES) die VPN moet gebruiken om de gegevens te beschermen. Encryptie voorkomt dat afluisteraars het verkeer kunnen lezen dat door de VPN-tunnel gaat.
integriteit <hash>	Het specificeert de algoritmen (zoals SHA-512) die worden gebruikt voor het verzekeren van de integriteit en de authenticiteit van de berichten die tijdens de IKEv2-onderhandeling worden uitgewisseld. Dit voorkomt geknoei en speelt aanvallen terug.

2. Maak een IKEv2-beleid en koppel dit aan het voorstel.

Het is een configuratieset die de parameters bepaalt voor de eerste fase (fase 1) van het opzetten van een IPsec VPN-verbinding. Het richt zich primair op hoe de VPN-endpoints elkaar verifiëren en een veilig communicatiekanaal opzetten voor de VPN-instellingen.

```
crypto ikev2 policy uCPE-policy
 match fvrf public-vrf
 proposal uCPE-proposal
```

3. Configureer het IKEv2-autorisatiebeleid

IKEv2 is een protocol dat wordt gebruikt om een beveiligde sessie tussen twee endpoints op een netwerk in te stellen en het autorisatiebeleid is een set regels die bepaalt welke bronnen en services een VPN-client mag gebruiken nadat de VPN-tunnel is opgezet.

```
crypto ikev2 authorization policy uCPE-author-pol
 pfs
 route set interface Loopback1001
```

Waarbij:

PFS	Perfect Forward Secrecy (PFS) is een functie die de beveiliging van een VPN-verbinding verbetert door ervoor te zorgen dat elke nieuwe coderingssleutel onafhankelijk veilig is, zelfs als eerdere sleutels worden gecompromitteerd.
route vastgestelde interface <interface-name>	Wanneer een VPN-sessie met succes is ingesteld, worden de routes die in het IKEv2-autorisatiebeleid zijn gedefinieerd, automatisch toegevoegd aan de tabel met apparaatrouting. Dit zorgt ervoor dat verkeer dat bestemd is voor de netwerken die in de routeset zijn gespecificeerd, correct door de VPN-tunnel wordt geleid.

4. Een IKEv2-profiel maken

Een IKEv2 (Internet Key Exchange versie 2)-beleid is een verzameling regels of parameters die worden gebruikt tijdens de IKEv2-fase van het instellen van een IPsec (Internet Protocol Security) VPN-tunnel. IKEv2 is een protocol dat de veilige uitwisseling van sleutels en de onderhandeling van veiligheidsverenigingen (SAs) tussen twee partijen vergemakkelijkt die veilig willen communiceren over een onbetrouwbaar netwerk, zoals het internet. Het IKEv2-beleid definieert hoe deze onderhandeling moet plaatsvinden, waarbij verschillende veiligheidsparameters worden gespecificeerd waarover beide partijen het eens moeten worden om een veilig en versleuteld communicatiekanaal op te zetten.

Het IKEv2-profiel MOET het volgende hebben:

- Een lokale en externe verificatiemethode.
- Een match-identiteit of een match-certificaat of match een statement.

```
crypto ikev2 profile uCPE-profile
 description uCPE profile
 match fvrf public-vrf
 match identity remote any
 authentication remote pre-share key ciscociscocisco123
 authentication local pre-share key ciscociscocisco123
 dpd 60 2 on-demand
 aaa authorization group psk list default uCPE-author-pol local
 virtual-template 1 mode auto
```

Waarbij:

match fvrf public-vrf	Maak een profiel vrf-bewust.
match-identiteit op afstand	Meten om een inkomende sessie als geldig te herkennen; in dit geval iedereen.
verificatie van externe pre-share sleutel Cisco123	Specificeert dat de externe peer moet worden geverifieerd met behulp van vooraf gedeelde sleutels.
verificatie lokale pre-share sleutel Cisco123	Specificeert dat dit (lokale) apparaat moet worden geverifieerd met behulp van vooraf gedeelde sleutels.
dpd 60,2 on-demand	Dead Peer Detection; als er geen pakketten werden ontvangen over een minutec (60 seconden), verstuur 2 dpd pakketten binnen dit 60

	seconden interval.
aaa autorisatie groep psk lijst standaard CPE-auteur-pol lokaal	Routetoewijzing.
Virtual-template 1-modus automatisch	Bind aan een virtueel-malplaatje.

5. Een IPsec-transformatieset maken

Het definieert een verzameling beveiligingsprotocollen en -algoritmen die moeten worden toegepast op het gegevensverkeer dat door de IPsec-tunnel gaat. Hoofdzakelijk, specificeert de transformatieset hoe de gegevens moeten worden versleuteld en worden geverifieerd, verzekerend veilige transmissie tussen VPN-endpoints. In de tunnelmodus wordt de IPsec-tunnel geconfigureerd om het gehele IP-pakket in te kapselen voor veilig transport over het netwerk.

```
crypto ipsec transform-set tset_aes_256_sha512 esp-aes 256 esp-sha512-hmac
 mode tunnel
```

Waarbij:

set transformatie-set <transform-set-name>	Specificeert de encryptie en integriteitsalgoritmen (Voorbeeld: AES voor encryptie en SHA voor integriteit) die moeten worden gebruikt om de gegevens te beschermen die door de tunnel van VPN stromen.
ikev2-profiel instellen <ikev2-profile-name>	Bepaalt de parameters voor de onderhandeling van de veiligheidsverenigingen (SAs) in fase 1 van de VPN-installatie, inclusief encryptie-algoritmen, hash-algoritmen, verificatiemethoden en de Diffie-Hellman groep.
PDF-bestanden instellen <groep>	Een optionele instelling die, indien ingeschakeld, garandeert dat elke nieuwe coderingssleutel niets te maken heeft met een vorige sleutel, waardoor de beveiliging wordt verbeterd.

6. Standaard IPsec-profiel verwijderen

Het verwijderen van het standaard IPsec profiel is een praktijk die wordt toegepast om verschillende redenen die te maken hebben met beveiliging, aanpassing en systeemhelderheid. Het standaard IPsec-profiel kan niet voldoen aan de specifieke beveiligingsregels of -vereisten van uw netwerk. Het verwijderen ervan zorgt ervoor dat geen VPN-tunnels onbedoeld suboptimale of onveilige instellingen gebruiken, waardoor het risico op kwetsbaarheden wordt verminderd.

Elk netwerk heeft unieke beveiligingsvereisten, waaronder specifieke versleuteling- en hashingalgoritmen, sleutellengtes en verificatiemethoden. Het verwijderen van het standaardprofiel moedigt de creatie van aangepaste profielen aan, afgestemd op deze specifieke behoeften, waarbij de best mogelijke bescherming en prestaties worden gewaarborgd.

```
no crypto ipsec profile default
```

7. Maak een IPsec-profiel en koppel het aan een transformatieset en het IKEv2-profiel.

Een IPsec-profiel (Internet Protocol Security) is een configuratie-entiteit die de instellingen en het beleid inkapselt dat wordt gebruikt om IPsec VPN-tunnels op te zetten en te beheren. Het fungeert als een sjabloon die kan worden toegepast op meerdere VPN-verbindingen, standaardiseert beveiligingsparameters en vereenvoudigt het beheer van beveiligde communicatie via een netwerk.

```
crypto ipsec profile uCPE-ips-prof
 set security-association lifetime seconds 28800
 set security-association idle-time 1800
 set transform-set tset_aes_256_sha512
 set pfs group14
 set ikev2-profile uCPE-profile
```

8. Een virtuele sjabloon maken

De Virtual-Template interface fungeert als een dynamisch sjabloon voor virtuele toegangsinterfaces, en biedt een schaalbare en efficiënte manier om VPN-verbindingen te beheren. Het maakt de dynamische instantiatie van Virtual-Access interfaces mogelijk. Wanneer een nieuwe VPN-sessie wordt gestart, maakt het apparaat een Virtual-Access-interface op basis van de configuratie die in de Virtual-Template is gespecificeerd. Dit proces ondersteunt een groot aantal externe clients en locaties door dynamisch bronnen toe te wijzen zoals nodig is, zonder dat er voor elke verbinding vooraf geconfigureerde fysieke interfaces nodig zijn.

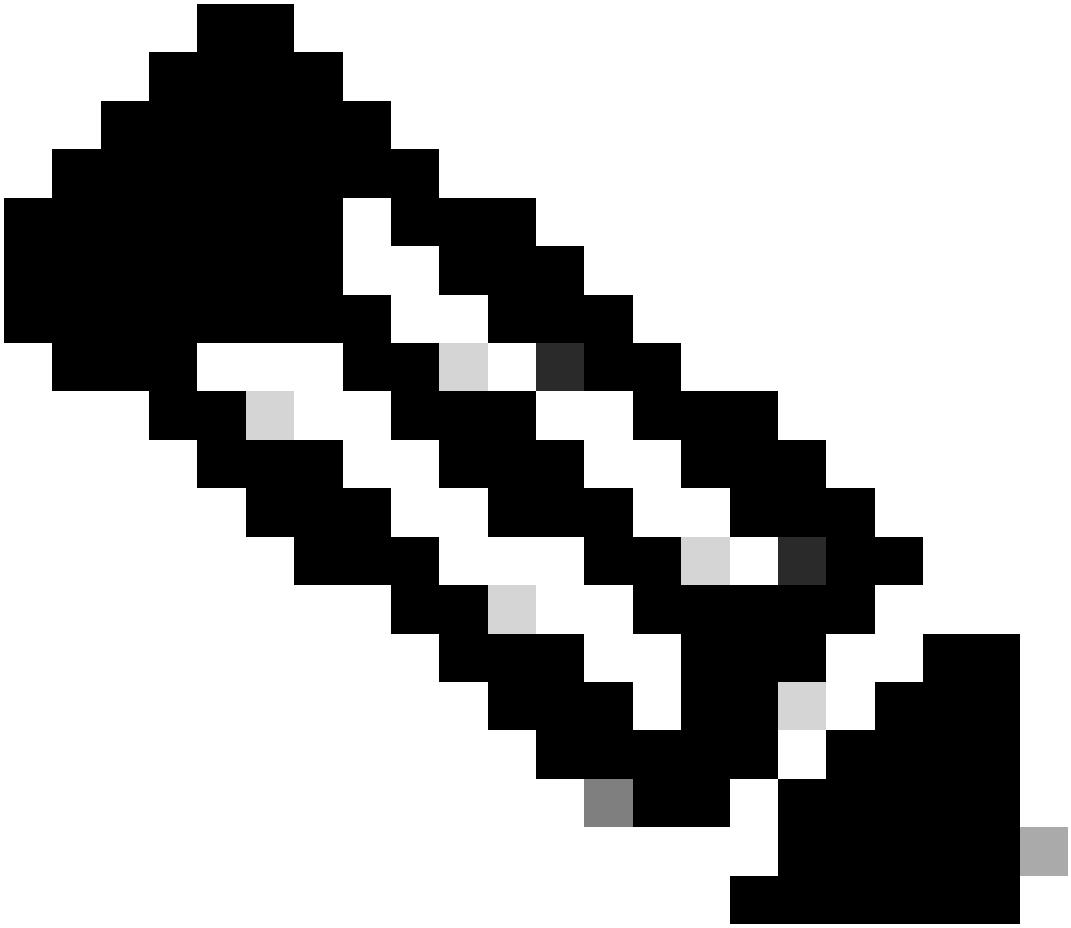
Door gebruik te maken van Virtual-Templates kunnen FlexVPN-implementaties efficiënt worden geschaald naarmate nieuwe verbindingen tot stand worden gebracht, zonder dat handmatige configuratie van elke afzonderlijke sessie nodig is.

```
interface Virtual-Template1 type tunnel
 vrf forwarding private-vrf
 ip unnumbered Loopback1001
 ip mtu 1400
 ip tcp adjust-mss 1380
 tunnel mode ipsec ipv4
 tunnel vrf public-vrf
 tunnel protection ipsec profile uCPE-ips-prof
```

Minimale configuratie voor NFVIS Secure Overlay

Configureer de beveiligde overlay-instantie

```
secure-overlay myconn local-bridge wan-br local-system-ip-addr 10.122.144.146 local-system-ip-subnet 10
 ike-cipher aes256-sha512-modp4096 esp-cipher aes256-sha512-modp4096
 psk local-psk ciscociscocisco123 remote-psk ciscociscocisco123
 commit
```



Opmerking: wanneer u BGP-routeaankondiging via een IPSec-tunnel configureert, dient u ervoor te zorgen dat u de beveiligde overlay configureert om een virtueel IP-adres (niet afkomstig van een fysieke interface of OVS-brug) te gebruiken voor het IP-adres van de lokale tunnel. In het bovenstaande voorbeeld zijn dit de virtuele adresseringsopdrachten die zijn gewijzigd: local-system-ip-addr 10.122.144.146 local-system-ip-sub 10.122.144.128/27

Overlay-status bekijken

```
show secure-overlay
secure-overlay myconn
 state                           up
 active-local-bridge             wan-br
 selected-local-bridge           wan-br
 active-local-system-ip-addr     10.122.144.146
 active-remote-interface-ip-addr 10.88.247.84
 active-remote-system-ip-addr    166.34.121.112
 active-remote-system-ip-subnet  166.34.121.112/32
 active-remote-id                10.88.247.84
```

BGP-configuratie voor routeaankondiging voor FlexVPN-server

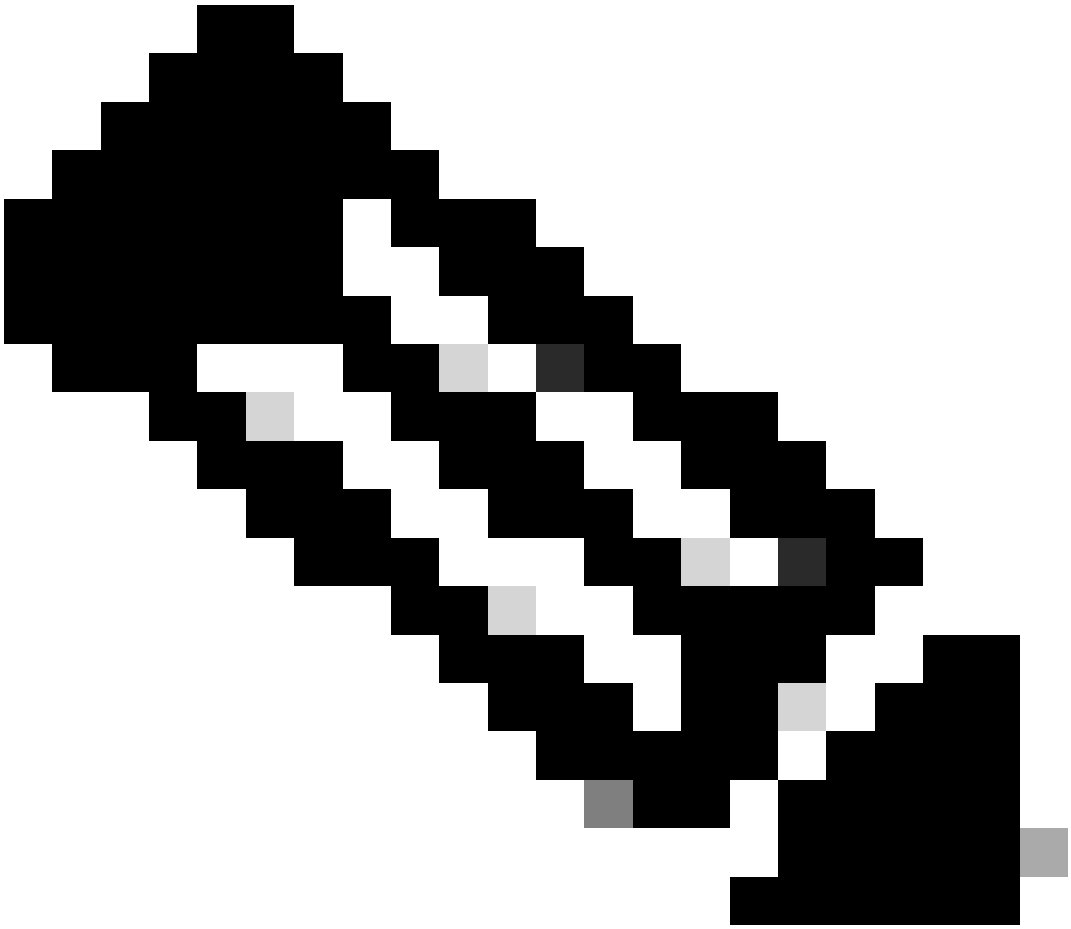
Bij deze installatie moet eBGP worden gebruikt voor de peerings, waarbij het bronadres (virtueel IP-adres voor het lokale IP-tunnelnetwerk) van NFVIS-zijde moet worden toegevoegd aan het luisterbereik.

```
router bgp 65000
 bgp router-id 166.34.121.112
 bgp always-compare-med
 bgp log-neighbor-changes
 bgp deterministic-med
 bgp listen range 10.122.144.0/24 peer-group uCPEs
 bgp listen limit 255
 no bgp default ipv4-unicast
 address-family ipv4 vrf private-vrf
  redistribute connected
  redistribute static
  neighbor uCPEs peer-group
  neighbor uCPEs remote-as 200
  neighbor uCPEs ebgp-multihop 10
  neighbor uCPEs timers 610 1835
 exit-address-family
```

Waarbij:

bgp altijd-vergelijken-med	Configureert de router om altijd het MED-kenmerk (Multi-Exit Discriminator) te vergelijken voor alle routes, ongeacht hun oorspronkelijke AS.
bgp log-buurwijzigingen	Schakelt logboekregistratie in voor gebeurtenissen die verband houden met wijzigingen in BGP-buurrelaties.
bgp deterministisch-med	Zorgt voor de vergelijking van de MED voor paden uit buurlanden in verschillende autonome systemen.
bgp-luisterbereik <netwerk>/<masker> peer-group <peer-group-name>	Schakelt dynamische buurdetectie binnen het opgegeven IP-bereik (netwerk/masker) in en wijst ontdekte buren toe aan de naam van de peer-groep. Dit vereenvoudigt de configuratie door algemene instellingen toe te passen op alle peers in de groep.
BGP-luisterlimiet 25	Stelt het maximale aantal dynamische BGP-buren in dat binnen

	het luisterbereik kan worden geaccepteerd, op 255.
geen bgp standaard ipv4-unicast	Schakelt het automatisch verzenden van IPv4-unicast routeringsinformatie naar BGP-buren uit waarvoor expliciete configuratie vereist is om dit in te schakelen.
verbonden herverdelen	Verdeelt routes van direct verbonden netwerken opnieuw naar BGP (Private subnets van de FlexVPN-server die tot de private-vrf behoren)
statisch herverdelen	Verdeelt statische routes opnieuw in BGP.
buurland CPE's bgp-multihop 10	Maakt EBGP-verbindingen (Externe BGP) met peers in de peer-groep mogelijk van maximaal 10 hop, wat handig is voor het aansluiten van apparaten die niet direct aangrenzend zijn.
naburige CPE's timers <keep-live>	Hiermee worden de BGP-keepalive- en hold-down-timers voor buren in de peer-groep respectievelijk ingesteld (610 seconden en 1835 seconden bij het voorbeeld).



Opmerking: een uitgaand prefixlijst kan worden geconfigureerd om buurrouteradvertenties in de peer-groep te controleren: buurprefix-lijst uit

BGP-configuratie op NFVIS

Start het BGP-proces met instellingen voor de eBGP-groep

```
router bgp 200
 router-id 10.122.144.146
 neighbor 166.34.121.112 remote-as 65000
 commit
```

BGP-beoordeling

Deze output onthult de voorwaarde van een BGP zitting zoals die door BIRD Internet Routing Daemon wordt gemeld. Deze routersoftware is verantwoordelijk voor de afhandeling van IP-routes en het nemen van beslissingen over hun richting. Uit de verstrekte informatie blijkt duidelijk dat de BGP-sessie in een "gevestigde" staat verkeert, wat duidt op een succesvolle afronding van het BGP-peeringproces, en dat de sessie momenteel actief is. Het heeft vier routes met succes geïmporteerd en het heeft opgemerkt dat er een bovengrens van vijftien routes is die geïmporteerd kunnen worden.

```
nfvis# support show bgp
BIRD 1.6.8 ready.
name     proto    table    state  since       info
bgp_166_34_121_112 BGP      bgp_table_166_34_121_112 up     09:54:14    Established
  Preference:     100
  Input filter:   ACCEPT
  Output filter:  ACCEPT
  Import limit:   15
    Action:       disable
  Routes:         4 imported, 0 exported, 8 preferred
  Route change stats:     received   rejected   filtered    ignored   accepted
    Import updates:              4          0          0          0          4
    Import withdraws:            0          0        ---          0          0
    Export updates:              4          4          0        ---          0
    Export withdraws:            0        ---        ---        ---          0
  BGP state:          Established
    Neighbor address: 166.34.121.112
    Neighbor AS:      65000
    Neighbor ID:      166.34.121.112
    Neighbor caps:    refresh enhanced-refresh AS4
    Session:          external multihop AS4
    Source address:   10.122.144.146
    Route limit:      4/15
    Hold timer:       191/240
    Keepalive timer:  38/80
```

Zorg ervoor dat de Private Subnets van FlexVPN Server via BGP zijn geadverteerd

Bij het configureren van BGP-routeaankondiging is de enige configureerbare adresfamilie of transmissiecombinatie ipv4-unicastfor IPSec. Om de BGP-status te bekijken, is de configureerbare adresfamilie of transmissie voor IPSec vpnv4 unicast.

```
nfvis# show bgp vpnv4 unicast
Family Transmission Router ID       Local AS Number
vpnv4  unicast      10.122.144.146  200
```

Met de show bgp vpnv4 unicast route opdracht, kunt u informatie ophalen over de VPNv4 unicast routes die bekend zijn bij het BGP proces.

```
nfvis# show bgp vpnv4 unicast route
Network            Next-Hop        Metric LocPrf Path
81.81.81.1/32      166.34.121.112  0      100    65000 ?
91.91.91.0/24      166.34.121.112  0      100    65000 ?
10.122.144.128/27  166.34.121.112  0      100    65000 ?
166.34.121.112/32  166.34.121.112  0      100    65000 ?
```

Voor de head-end VPN-server kan een overzicht van de BGP-configuratie en de operationele status worden gegenereerd om de status en configuratie van BGP-sessies snel te beoordelen.

```
c8000v# show ip bgp summary
Number of dynamically created neighbors in vrf private-vrf: 1/(100 max)
Total dynamically created neighbors: 1/(255 max), Subnet ranges: 1
```

Bovendien kan gedetailleerde informatie over de VPNv4 (VPN over IPv4)-routeringangen die door BGP worden beheerd, worden weergegeven. Deze informatie moet specifieke kenmerken van elke VPNv4-route bevatten, zoals het routevoorvoegsel, het IP-adres van de volgende hop, het oorspronkelijke AS-nummer en verschillende BGP-kenmerken zoals lokale voorkeur, MED (Multi-Exit Discriminator) en gemeenschapswaarden.

```
c8000v# show ip bgp vpnv4 all
BGP table version is 5, local router ID is 166.34.121.112
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,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:7 (default for vrf private-vrf)
 *>   10.122.144.128/27
```

```
                    0.0.0.0                  0         32768 ?
 *>   81.81.81.1/32    0.0.0.0                  0         32768 ?
 *>   91.91.91.0/24    0.0.0.0                  0         32768 ?
 *>   166.34.121.112/32
                    0.0.0.0                  0         32768 ?
```

Probleemoplossing

NFVIS (FlexVPN-client)

NFVIS-logbestanden

U kunt alle initialisatie- en foutlogboeken voor de IPsec-fasen bekijken vanuit het logbestand NFVIS charon.log:

```
nfvis# show log charon.log
Feb  5 07:55:36.771 00[JOB] spawning 16 worker threads
Feb  5 07:55:36.786 05[CFG] received stroke: add connection 'myconn'
Feb  5 07:55:36.786 05[CFG] added configuration 'myconn'
Feb  5 07:55:36.787 06[CFG] received stroke: initiate 'myconn'
Feb  5 07:55:36.787 06[IKE] <myconn|1> initiating IKE_SA myconn[1] to 10.88.247.84
Feb  5 07:55:36.899 06[ENC] <myconn|1> generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_
Feb  5 07:55:36.899 06[NET] <myconn|1> sending packet: from 10.88.247.89[500] to 10.88.247.84[500] (741
Feb  5 07:55:37.122 09[NET] <myconn|1> received packet: from 10.88.247.84[500] to 10.88.247.89[500] (80
Feb  5 07:55:37.122 09[ENC] <myconn|1> parsed IKE_SA_INIT response 0 [ SA KE No V V V V N(NATD_S_IP) N(
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco Delete Reason vendor ID
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:56:50:4e:2d:52:45:56:
Feb  5 07:55:37.122 09[ENC] <myconn|1> received unknown vendor ID: 43:49:53:43:4f:2d:44:59:4e:41:4d:49:
Feb  5 07:55:37.122 09[IKE] <myconn|1> received Cisco FlexVPN Supported vendor ID
Feb  5 07:55:37.122 09[CFG] <myconn|1> selected proposal: IKE:AES_CBC_256/HMAC_SHA2_512_256/PRF_HMAC_SH
Feb  5 07:55:37.235 09[IKE] <myconn|1> cert payload ANY not supported - ignored
Feb  5 07:55:37.235 09[IKE] <myconn|1> authentication of '10.88.247.89' (myself) with pre-shared key
Feb  5 07:55:37.235 09[IKE] <myconn|1> establishing CHILD_SA myconn{1}
Feb  5 07:55:37.236 09[ENC] <myconn|1> generating IKE_AUTH request 1 [ IDi N(INIT_CONTACT) IDr AUTH SA
Feb  5 07:55:37.236 09[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (4
Feb  5 07:55:37.322 10[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.322 10[ENC] <myconn|1> parsed IKE_AUTH response 1 [ V IDr AUTH SA TSi TSr N(SET_WINSIZE
Feb  5 07:55:37.323 10[IKE] <myconn|1> authentication of '10.88.247.84' with pre-shared key successful
Feb  5 07:55:37.323 10[IKE] <myconn|1> IKE_SA myconn[1] established between 10.88.247.89[10.88.247.89].
Feb  5 07:55:37.323 10[IKE] <myconn|1> scheduling rekeying in 86190s
Feb  5 07:55:37.323 10[IKE] <myconn|1> maximum IKE_SA lifetime 86370s
Feb  5 07:55:37.323 10[IKE] <myconn|1> received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padd
Feb  5 07:55:37.323 10[CFG] <myconn|1> selected proposal: ESP:AES_CBC_256/HMAC_SHA2_512_256/NO_EXT_SEQ
Feb  5 07:55:37.323 10[IKE] <myconn|1> CHILD_SA myconn{1} established with SPIs cfc15900_i 49f5e23c_o a
Feb  5 07:55:37.342 11[NET] <myconn|1> received packet: from 10.88.247.84[4500] to 10.88.247.89[4500] (
Feb  5 07:55:37.342 11[ENC] <myconn|1> parsed INFORMATIONAL request 0 [ CPS(SUBNET VER U_PFS) ]
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing informational configuration payload CONFIGURATION
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing information configuration payload of type CFG_SET
Feb  5 07:55:37.342 11[IKE] <myconn|1> Processing attribute INTERNAL_IP4_SUBNET
Feb  5 07:55:37.342 11[ENC] <myconn|1> generating INFORMATIONAL response 0 [ ]
Feb  5 07:55:37.342 11[NET] <myconn|1> sending packet: from 10.88.247.89[4500] to 10.88.247.84[4500] (9
```

Inwendige Kernel strongswan geïnjecteerde routes

Op Linux installeert strongswan (multiplatform IPsec-implementatie die door NFVIS wordt gebruikt) routes (inclusief BGP VPNv4 unicast routes) naar routingtabel 220 standaard en vereist daarom dat de kernel beleidsgebaseerde routing ondersteunt.

```
nfvis# support show route 220
10.122.144.128/27 dev ipsec0 proto bird scope link
81.81.81.1 dev ipsec0 proto bird scope link
91.91.91.0/24 dev ipsec0 proto bird scope link
166.34.121.112 dev ipsec0 scope link
```

IPsec0-interfacestatus bekijken

U kunt meer informatie krijgen over de virtuele interface ipsec0 met het gebruik van ifconfig

```
nfvis# support show ifconfig ipsec0
ipsec0: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 9196
        inet 10.122.144.146  netmask 255.255.255.255  destination 10.122.144.146
        tunnel   txqueuelen 1000  (IPIP Tunnel)
        RX packets 5105  bytes 388266 (379.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 5105  bytes 389269 (380.1 KiB)
        TX errors 1  dropped 0 overruns 0  carrier 1  collisions 0
```

Head-end (FlexVPN-server)

IPsec SA's bekijken die tussen peers zijn gebouwd

Van de output hieronder, wordt de gecodeerde tunnel gebouwd tussen 10.88.247.84 door de interface Virtual-Access1 en 10.88.247.89 voor verkeer dat tussen netwerken 0.0.0.0/0 en 10.122.144.128/27 gaat; twee Insluitend die de payload van de Veiligheid (ESP) SAs inkomende en uitgaande wordt gebouwd.

```
c8000v# show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.88.247.84

   protected vrf: private-vrf
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (10.122.144.128/255.255.255.224/0/0)
   current_peer 10.88.247.89 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 218, #pkts encrypt: 218, #pkts digest: 218
```

```
    #pkts decaps: 218, #pkts decrypt: 218, #pkts verify: 218
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.88.247.84, remote crypto endpt.: 10.88.247.89
     plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
     current outbound spi: 0xC91BCDE0(3374042592)
     PFS (Y/N): Y, DH group: group16

     inbound esp sas:
      spi: 0xB80E6942(3087952194)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2123, flow_id: CSR:123, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607969/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xC91BCDE0(3374042592)
        transform: esp-256-aes esp-sha512-hmac ,
        in use settings ={Tunnel, }
        conn id: 2124, flow_id: CSR:124, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-he
         sa timing: remaining key lifetime (k/sec): (4607983/27078)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

Actieve encryptie (encryptie) sessies weergeven

De output voor het show crypto sessiedetail moet uitgebreide details geven over elke actieve crypto sessie, inclusief het type VPN (zoals site-to-site of externe toegang), de encryptie- en hashingalgoritmen in gebruik, en de security associaties (SA's) voor zowel inkomend als uitgaand verkeer. Aangezien het ook statistieken over het versleutelde en gedecrypteerde verkeer weergeeft, zoals het aantal pakketten en bytes, kan dit handig zijn voor het controleren van de hoeveelheid gegevens die door VPN worden beveiligd en voor het oplossen van doorvoerproblemen.

```
c8000v# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
```

```
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Virtual-Access1
Profile: uCPE-profile
Uptime: 11:39:46
Session status: UP-ACTIVE
Peer: 10.88.247.89 port 4500 fvrf: public-vrf ivrf: private-vrf
      Desc: uCPE profile
      Phase1_id: 10.88.247.89
  Session ID: 1235
  IKEv2 SA: local 10.88.247.84/4500 remote 10.88.247.89/4500 Active
          Capabilities:D connid:2 lifetime:12:20:14
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 10.122.144.128/255.255.255.224
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 296 drop 0 life (KB/Sec) 4607958/7 hours, 20 mins
        Outbound: #pkts enc'ed 296 drop 0 life (KB/Sec) 4607977/7 hours, 20 mins
```

VPN-verbindingen opnieuw instellen

De duidelijke cryptocommando's worden gebruikt om de VPN-verbindingen handmatig te resetten, of om beveiligingsassociaties (SA's) te wissen zonder het hele apparaat opnieuw te hoeven opstarten.

- duidelijke crypto ikev2 zou IKEv2 security associaties (IKEv2 SA's) goedkeuren.
- de duidelijke cryptosessie zou IKEv1 (isakmp)/IKEv2 en IPSec SAs wissen.
- duidelijke crypto sa zou alleen de IPSec SA's wissen.
- duidelijke crypto ipsec zoals de actieve IPSec security associaties zou verwijderen.

Debugs uitvoeren voor aanvullende probleemoplossing

IKEv2-debugs kunnen helpen bij het identificeren en oplossen van problemen met fouten op het head-end apparaat (c800v) die kunnen optreden tijdens het IKEv2-onderhandelingsproces en FlexVPN-clientverbindingen, zoals problemen met het instellen van de VPN-sessie, beleidsapplicatie of client-specifieke fouten.

```
c8000v# terminal no monitor
c8000v(config)# logging buffer 1000000
c8000v(config)# logging buffered debugging
c8000v# debug crypto ikev2 error
c8000v# debug crypto ikev2 internal
c8000v# debug crypto ikev2 client flexvpn
```

Verwante artikelen en documentatie

Beveiligde overlay en één IP-configuratie

[BGP-ondersteuning op NFVIS]

[Secure Overlay- en BGP-opdrachten]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.