FlexVPN-oplossing configureren en verifiëren

Inhoud

Inleiding

Dit document beschrijft de Flex Virtual Private Network-omgeving, introduceert de functies ervan en legt uit hoe u elke FlexVPN-topologie kunt configureren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS en Cisco IOS XE
- Internet Key Exchange (IKE) versie 2
- Internet Protocol Security (IPsec)
- FlexVPN

Gebruikte componenten

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

- Cisco IOS XE Amsterdam-17.3.6

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.

Achtergrondinformatie

FlexVPN is een veelzijdige en uitgebreide VPN-oplossing van Cisco, ontworpen om een uniform framework te bieden voor verschillende soorten VPN-verbindingen. FlexVPN is gebouwd op basis van het IKEv2-protocol (Internet Key Exchange versie 2) en is ontworpen om de configuratie, het beheer en de implementatie van VPN te vereenvoudigen, waarbij gebruik wordt gemaakt van een consistente reeks tools, dezelfde opdrachten en configuratiestappen gelden voor verschillende VPN-typen (site-to-site, externe toegang, enzovoort). Deze consistentie helpt bij het verminderen van fouten en maakt het implementatieproces intuïtiever.

IKEv2 vs IKEv1

FlexVPN maakt gebruik van IKEv2, dat moderne cryptografische algoritmen zoals AES (Advanced Encryption Standard) en SHA-256 (Secure Hash Algorithm) ondersteunt. Deze algoritmen zorgen voor een sterke encryptie en data-integriteit, waardoor de gegevens die via de VPN worden verzonden, worden beschermd tegen onderschepping of manipulatie.

IKEv2 biedt meer verificatiemethoden in vergelijking met IKEv1. Naast Pre-Shared Key (PSK) en op certificaten gebaseerde en hybride authenticatietypen, biedt IKEv2 de responder de mogelijkheid om het Extensible Authentication Protocol (EAP) te gebruiken voor clientverificatie.

In FlexVPN wordt EAP gebruikt voor clientverificatie. De router fungeert als een relais en geeft EAP-berichten door tussen de client en de back-end EAP-server, meestal een RADIUS-server. FlexVPN ondersteunt verschillende EAP-methoden, waaronder EAP-TLS, EAP-PEAP, EAP-PSK en andere, voor het beveiligen van het verificatieproces.

De tabel toont de verschillen tussen de IKEv1- en IKEv2-functies:

	IKEv2	IKEv1
Berichten over het opstellen van protocollen	4 Bericht	6 Bericht

EAP-ondersteuning	Ja (2 extra berichten)	Nee
Onderhandelen over veiligheidsorganisaties	2 extra berichten	3 extra bericht
Run over UDP 500/4500	Ja	Ja
NAT-traversal (NAT-T)	Ja	Ja
Herverzendingen en erkenningsfuncties	Ja	Ja
Biedt identiteitsbescherming, een DoS-beschermingsmechanisme en Perfect Forward Secrecy (PFS)	Ja	Ja
Ondersteuning voor de volgende generatie coders	Ja	Nee

Schaalbaarheid

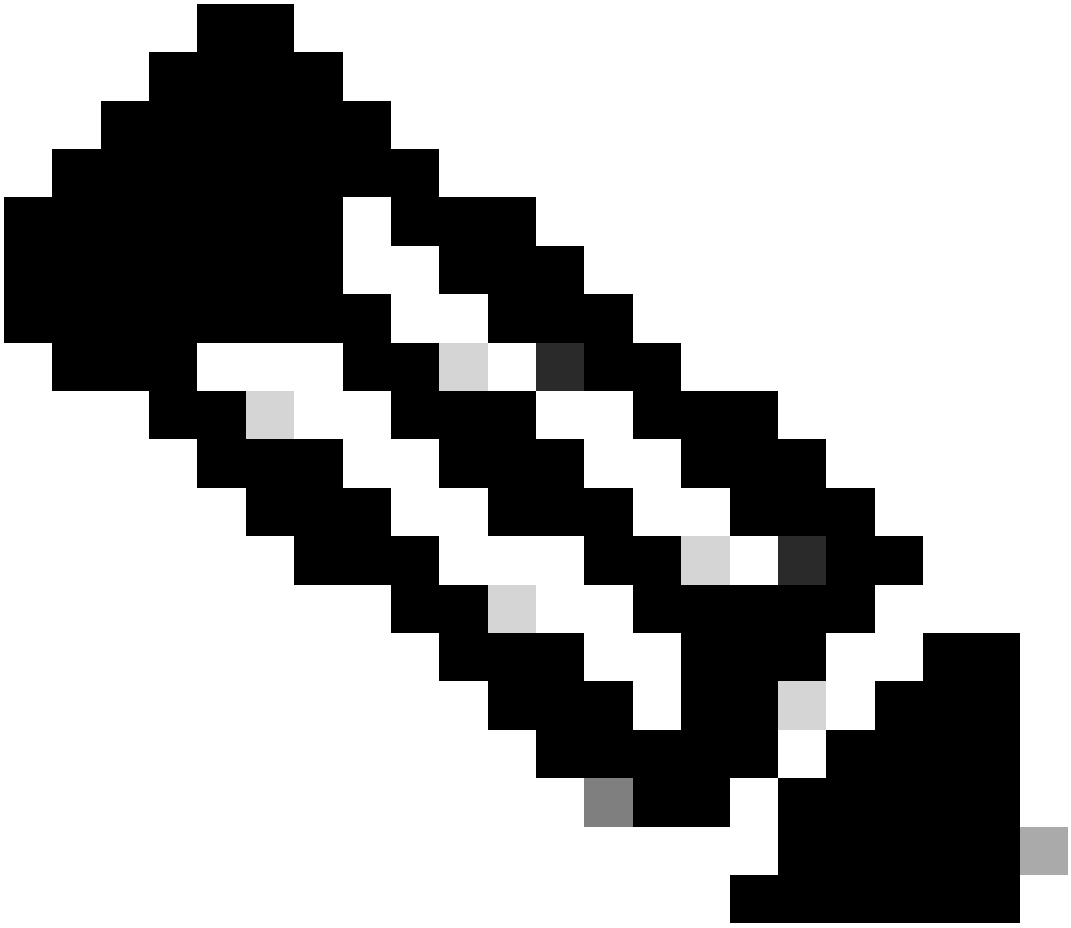
FlexVPN kan eenvoudig worden uitgebreid van kleine kantoren naar grote bedrijfsnetwerken. Dit maakt het een ideale keuze voor organisaties met een aanzienlijk aantal externe gebruikers die veilige en betrouwbare netwerktoegang nodig hebben.

Belangrijkste kenmerken

- Dynamische configuratie en on-demand tunnels:
  - Wanneer de FlexVPN-verbinding wordt gestart, genereert het systeem een virtuele toegangsinterface op basis van een vooraf geconfigureerde sjabloon. Deze interface fungeert als het tunneleindpunt voor de duur van de verbinding. Zodra de tunnel niet langer nodig is, wordt de virtuele toegangsinterface afgebroken, waardoor systeembronnen vrijkomen.

- Flexibiliteit bij implementatie:
  - Hub-and-Spoke Model: Een centrale hub verbindt meerdere filialen. FlexVPN vereenvoudigt het instellen van deze verbindingen met één framework, waardoor het ideaal is voor grote netwerken.
  - Full Mesh en Partial Mesh Topologies: Alle sites kunnen rechtstreeks communiceren zonder door een centrale hub te gaan, waardoor vertraging wordt verminderd en de prestaties worden verbeterd.

- Hoge beschikbaarheid en redundantie:
  - Redundante hubs: ondersteunt meerdere hubs voor back-up. Als een hub uitvalt, kunnen takken verbinding maken met een andere hub, waardoor continue connectiviteit wordt gewaarborgd.
  - Load Balancing: Dit verdeelt VPN-verbindingen over meerdere apparaten om te voorkomen dat één apparaat overbelast raakt, wat cruciaal is voor het behoud van de prestaties in grote implementaties.



Opmerking: de volgende handleiding bevat meer informatie over de configuratie voor taakverdeling voor de verbinding met de hub.

IKEv2-taakverdeling configureren

- Schaalbare verificatie en autorisatie:
  - AAA-integratie: werkt met AAA-servers zoals Cisco ISE of RADIUS voor gecentraliseerd beheer van gebruikersreferenties en -beleid, essentieel voor grootschalig gebruik.
  - PKI en certificaten: ondersteunt Public Key Infrastructure (PKI) en digitale certificaten voor veilige verificatie, die schaalbaarder is dan het gebruik van Pre-Shared Key, vooral in grote omgevingen.

routering

De routeringsfunctionaliteit in FlexVPN is ontworpen om de schaalbaarheid te verbeteren en meerdere VPN-verbindingen efficiënt te beheren en een dynamische manier mogelijk te maken

om verkeer naar elk van hen te routeren. De volgende belangrijke componenten en mechanismen die FlexVPN-routering efficiënt maken:

- Virtual Template Interface: Dit is een configuratiesjabloon dat alle noodzakelijke instellingen voor een VPN-verbinding bevat, zoals IP-adrestoewijzing, tunnelbron en IPsec-instellingen. In deze interface wordt de opdracht geconfigureerd`ip unnumbered`om een IP-adres te lenen, meestal van een loopback in plaats van een specifiek IP-adres te configureren als bron van de tunnel. Hierdoor kan dezelfde sjabloon worden gebruikt door elke spaak, waardoor elke spaak zijn eigen bron-IP-adres kan gebruiken.

- Virtual Access Interface: Dit zijn dynamisch gemaakte interfaces die hun instellingen overerven van de virtuele sjablooninterface. Telkens wanneer een nieuwe VPN-verbinding tot stand wordt gebracht, wordt een nieuwe virtuele toegangsinterface gemaakt op basis van de virtuele sjabloon. Dit betekent dat elke VPN-sessie zijn eigen unieke interface heeft, wat het beheer en de schaalbaarheid vereenvoudigt.

- Dynamische routeringsprotocollen: Het werkt met routeringsprotocollen zoals OSPF, EIGRP en BGP over VPN-tunnels. Hierdoor blijft routeringsinformatie automatisch bijgewerkt, wat belangrijk is voor grote en dynamische netwerken.

- IKEv2 adverteert routes door de FlexVPN-server toe te staan netwerkattributen naar de client te pushen, die deze routes op de tunnelinterface installeert. De client communiceert ook zijn eigen netwerken met de server tijdens de uitwisseling van de configuratiemodus, waardoor routeupdates aan beide uiteinden mogelijk zijn.

- NHRP (Next Hop Resolution Protocol) is een protocol voor dynamische adresresolutie dat wordt gebruikt in hub- en spaaktopologieën om openbare IP-adressen toe te wijzen aan particuliere VPN-eindpunten. Het stelt spokes in staat om andere spokes-IP's te ontdekken voor directe communicatie.

machtigingsbeleid

Een IKEv2-autorisatiebeleid voor FlexVPN kan worden geconfigureerd om verschillende aspecten van de VPN-verbinding te regelen. Een IKEv2-autorisatiebeleid definieert het lokale autorisatiebeleid en bevat lokale en/of externe kenmerken:

- Lokale attributen, zoals VPN-routing en -forwarding (VRF) en het QOS-beleid, worden lokaal toegepast.
- Externe attributen, zoals routes, worden via de configuratiemodus naar de peer gepusht.
- Gebruik de opdracht voor het autorisatiebeleid voor crypto ikev2 om het lokale beleid te definiëren.
- Het IKEv2-autorisatiebeleid wordt vanuit het IKEv2-profiel doorverwezen via de opdracht AAA-autorisatie.

Deze tabel geeft een overzicht van de belangrijkste parameters die kunnen worden geconfigureerd onder het IKEv2-autorisatiebeleid.

Parameter	Beschrijving

AAA	Integratie met AAA-servers om gebruikersreferenties te valideren, toegang te autoriseren en een account voor gebruik aan te maken. Het beleid kan specificeren of de validatie lokaal op de router of op afstand wordt uitgevoerd, bijvoorbeeld via een RADIUS-server.
Clientconfiguratie	Hiermee worden configuratie-instellingen naar de client gepusht, zoals time-outwaarden bij inactiviteit, keepalives, toewijzing van DNS- en WINS-servers, enzovoort.
Clientspecifieke configuratie	Maakt verschillende configuraties mogelijk voor verschillende clients op basis van hun identiteit of groepslidmaatschap.
routeset	Met deze configuratie kan bepaald verkeer door de VPN-tunnel gaan. Dit voert de route-injectie uit die naar de VPN-client wordt geduwd bij een succesvolle verbinding.

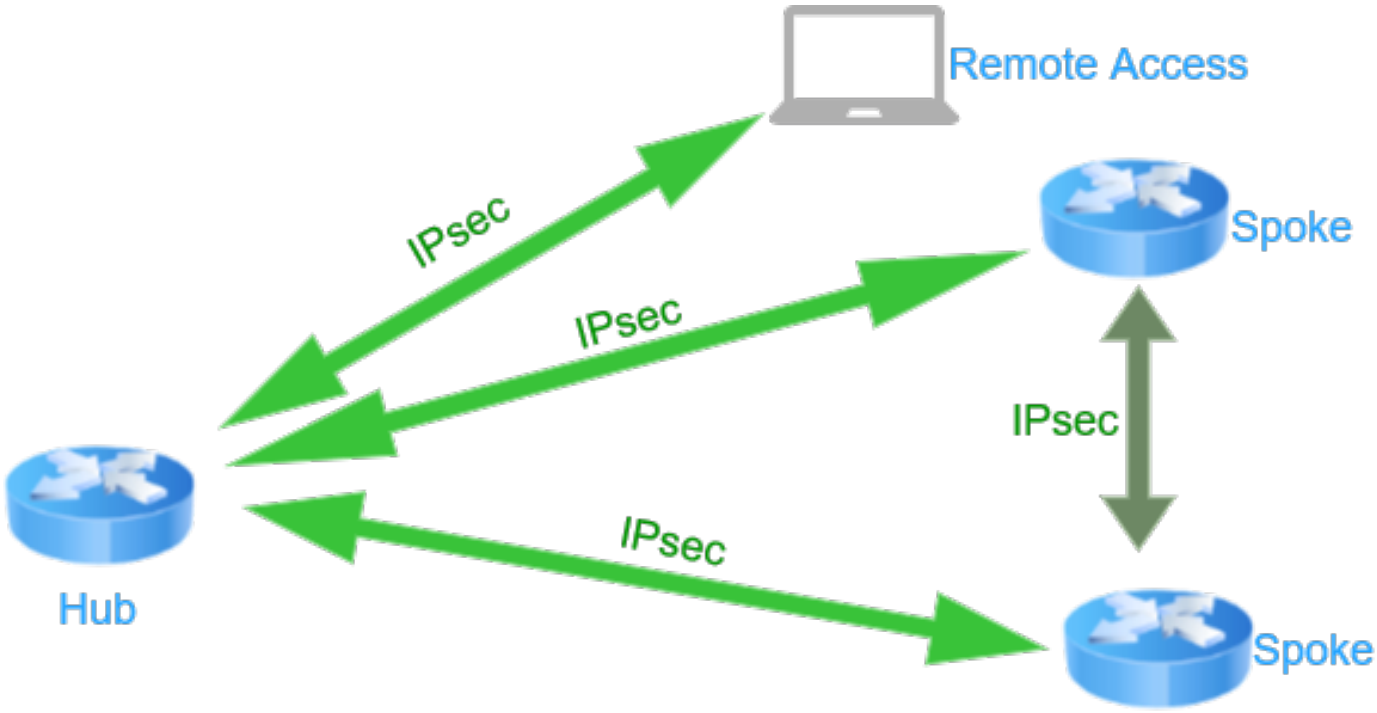
FlexVPN versus andere technologieën

FlexVPN biedt een reeks voordelen die het een aantrekkelijke keuze maken voor moderne netwerkomgevingen. Door een uniform framework te bieden, vereenvoudigt FlexVPN de configuratie en het beheer, verbetert het de beveiliging, ondersteunt het de schaalbaarheid, zorgt het voor interoperabiliteit en vermindert het de complexiteit.

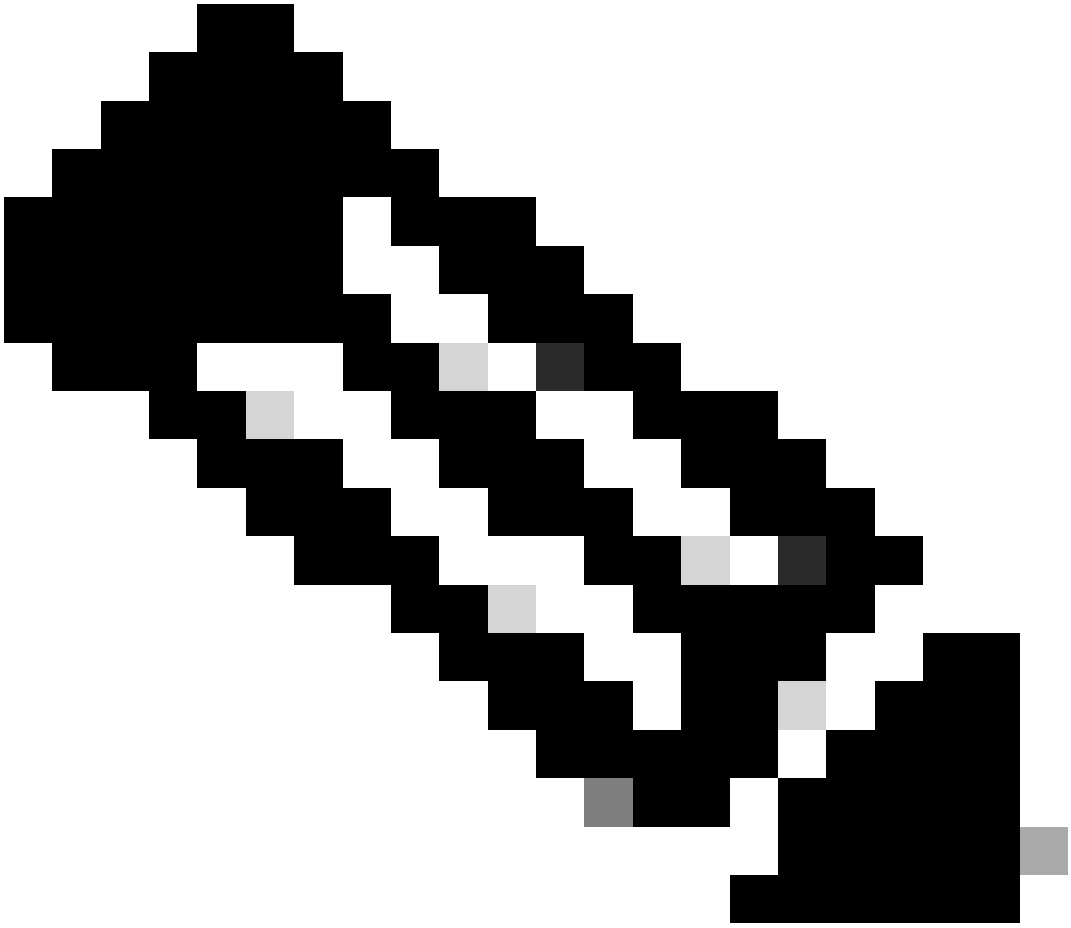
	Crypto-kaart	DMVPN	FlexVPN
dynamische routering	Nee	Ja	Ja
Dynamic Spoke-to-Spoke direct	Nee	Ja	Ja
Remote Access VPN	Ja	Nee	Ja
Configuratiepush	Nee	Nee	Ja
Peer-peer-configuratie	Nee	Nee	Ja
Peer-peer QoS	Nee	Ja	Ja
AAA-serverintegratie	Nee	Nee	Ja

Netwerkdiagram

FlexVPN maakt het mogelijk om tunnels tussen apparaten te maken en communicatie tussen de Hub en de Spokes tot stand te brengen. Het maakt ook het maken van tunnels voor directe communicatie tussen spaken en verbinding voor Remote Access VPN-gebruikers mogelijk, zoals weergegeven in het diagram.



FlexVPN-diagram



Opmerking: De configuratie voor Remote Access VPN wordt niet behandeld in deze handleiding. Voor meer informatie over de configuratie raadpleegt u de gids:

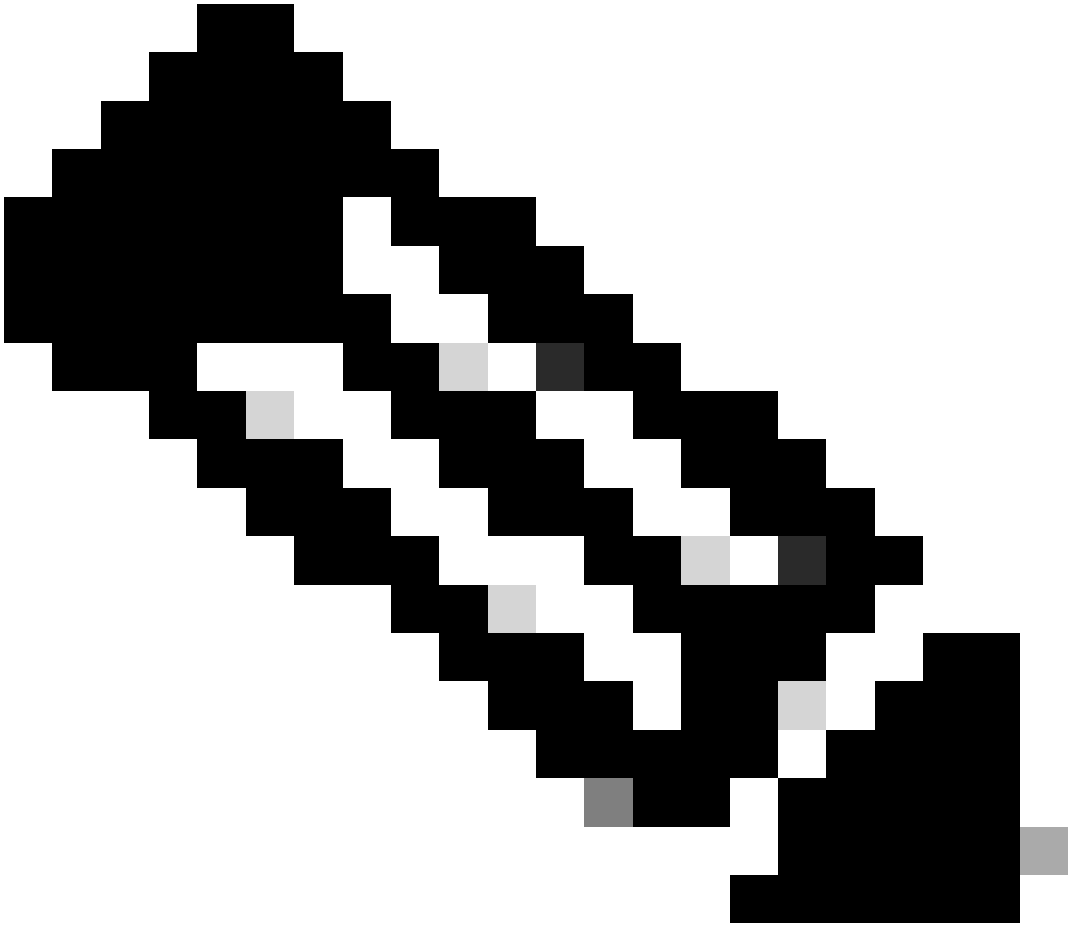
FlexVPN Headend configureren voor beveiligde client (AnyConnect) IKEv2 externe toegang met lokale gebruikersdatabase

Configureren

FlexVPN wordt gekenmerkt door de eenvoud van de configuratie. Deze eenvoud is duidelijk in de consistente configuratieblokken die worden gebruikt voor verschillende soorten VPN's. FlexVPN biedt eenvoudige configuratieblokken die over het algemeen van toepassing zijn, met optionele configuraties of extra stappen die beschikbaar zijn, afhankelijk van de specifieke functies of vereisten van de topologie:

- IKEv2-voorstel: definieert de algoritmen die worden gebruikt bij de onderhandelingen over de IKEv2 Security Association (SA). Als dit voorstel eenmaal is gemaakt, voegt u het toe aan een IKEv2-beleid zodat het tijdens de onderhandelingen kan worden geselecteerd.

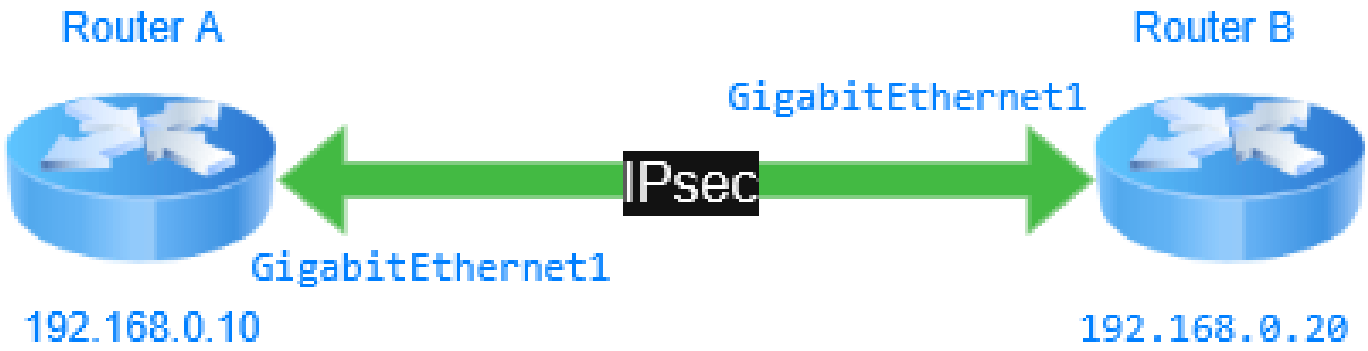
- IKEv2-beleid: koppelt het voorstel aan een Virtual Routing and Forwarding (VRF)-instantie of lokaal IP-adres. De beleidslink naar het IKEv2-voorstel.
- IKEv2-sleutelhanger: geeft Pre-Shared Keys (PSK's) op, die asymmetrisch kunnen zijn als ze worden gebruikt voor peer-verificatie.
- Trustpoint (optioneel): Configureert kenmerken van identiteit en certificeringsinstantie (CA) voor peer-verificatie bij gebruik van Public Key Infrastructure (PKI) als verificatiemethode.
- AAA-integratie (optioneel): FlexVPN integreert AAA-servers, zoals Cisco ISE (Identity Services Engine) of RADIUS-servers als verificatiemethode.
- IKEv2-profiel: slaat niet-onderhandelbare parameters van de IKE SA op, zoals het VPN-peer-adres en de verificatiemethoden. Er is geen standaard IKEv2-profiel, dus u moet er een configureren en deze koppelen aan een IPsec-profiel op de initiator. Als PSK-verificatie wordt gebruikt, verwijst het IKEv2-profiel naar de IKEv2-sleutelring. Als PKI-authenticatie of AAA-authenticatiemethode wordt gebruikt, wordt hier naar verwezen.
- IPsec-transformatieset: geeft een combinatie van algoritmen aan die acceptabel zijn voor de IPsec SA.
- IPsec-profiel: consolideert FlexVPN-instellingen in één profiel dat kan worden toegepast op een interface. Dit profiel verwijst naar de IPsec-transformatieset en het IKEv2-profiel.



Opmerking: De configuratievoorbeelden maken gebruik van vooraf gedeelde sleutels om de FlexVPN-configuratie en -eenvoud eenvoudig te demonstreren. Hoewel vooraf gedeelde sleutels kunnen worden gebruikt voor eenvoudige implementatie en kleine topologieën, zijn AAA- of PKI-methoden geschikter voor grotere topologieën.

Site-to-Site FlexVPN-configuratie

FlexVPN site-to-site topologie is ontworpen voor directe VPN-verbindingen tussen twee sites. Elke site is uitgerust met een tunnelinterface die een veilig kanaal vormt waarover verkeer kan stromen. In de configuratie wordt uitgelegd hoe u een directe VPN-verbinding tot stand kunt brengen tussen twee sites, zoals wordt weergegeven in het diagram.



Site_to_Site_Diagram

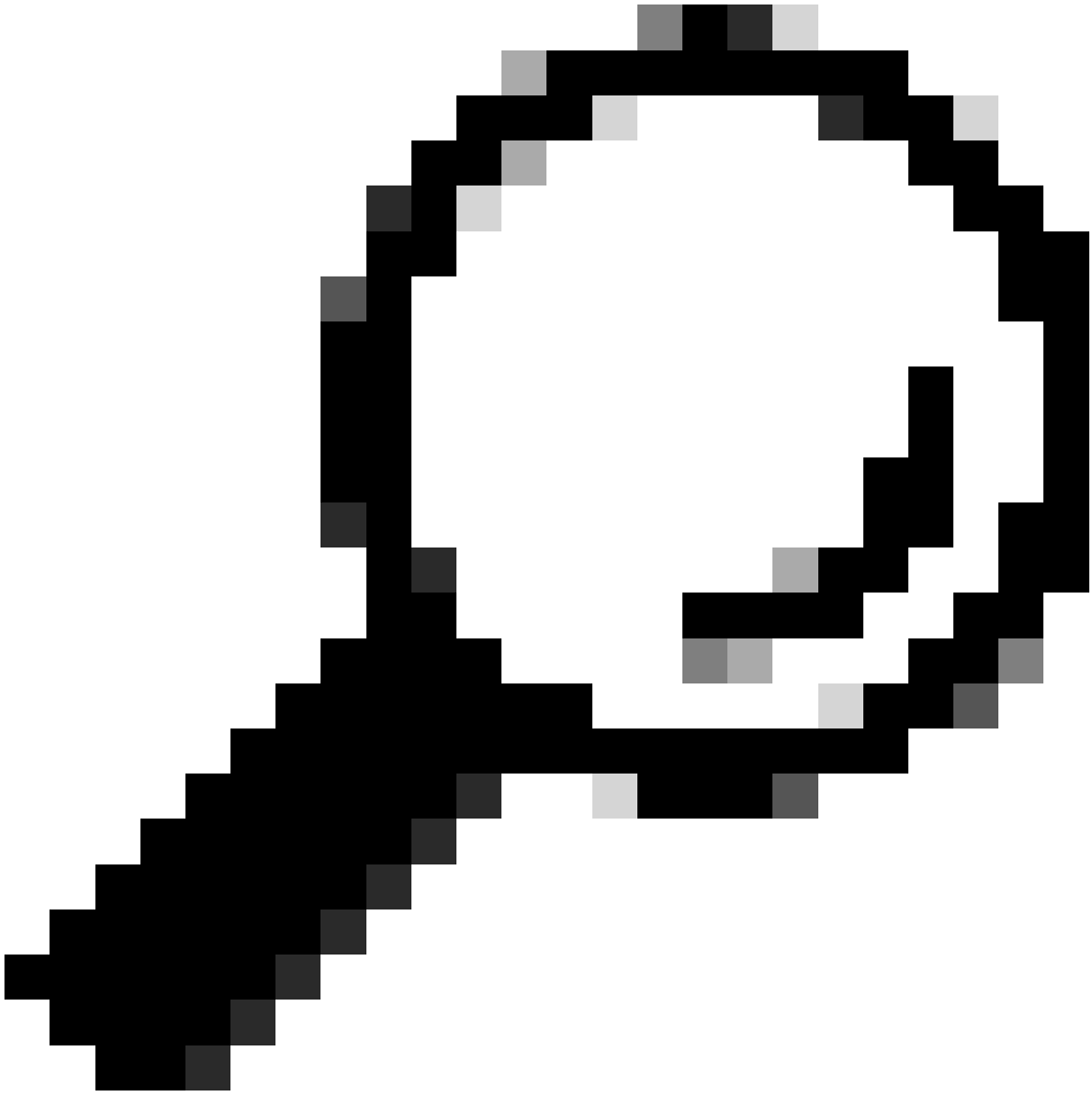
Stap 1: Een routerconfiguratie

a. Bepaal het IKEv2-voorstel en -beleid.

b. Configureer een sleutelhanger en voer een sleutel in Pre-Shared Key die wordt gebruikt om de peer te verifiëren.

c. Maak een IKEv2 profile map en wijs de keyringmap toe.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.20
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.20
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```



Tip: **IKEv2 Smart Defaults** de functie minimaliseert de configuratieFlexVPNdoor de meeste use cases te behandelen. U kunt aanpassen **IKEv2 Smart Defaults** voor specifieke gebruikssituaties, hoewel Cisco deze praktijk niet aanbeveelt.

d. Maak een Transport Set codering en definieer de hash-algoritmen die worden gebruikt om gegevens te beschermen.

e. Maak een **IPsec profile**website.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
```

```
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. De tunnelinterface configureren.

```
!
interface Tunnel0
 ip address 10.1.120.10 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.20
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.10 255.255.255.0
!
```

g. Dynamische routering configureren om de tunnelinterface te promoten. Daarna kan het reclame maken voor andere netwerken die door de tunnel moeten gaan.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Stap 2: Router B-configuratie

a. Bepaal het IKEv2-voorstel en -beleid.

b. Configureer a keyring en voer een code in Pre-Shared Key die wordt gebruikt om de peer te verifiëren.

c. Maak een IKEv2 profile map en wijs de keyringmap toe.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 192.168.0.10
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

```
crypto ikev2 profile FLEXVPN_PROFILE
match identity remote address 192.168.0.10
authentication remote pre-share
authentication local pre-share
keyring local FLEXVPN_KEYRING
lifetime 86400
dpd 10 2 on-demand
!
```

d. Maak een Transport Set codering en definieer de hash-algoritmen die worden gebruikt om gegevens te beschermen.

e. Maak een IPsec profile profiel en wijs het IKEv2-profiel en de eerder gemaakte transformatieset toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

f. Configureer de Tunnel interfaceinstellingen.

```
!
interface Tunnel0
 ip address 10.1.120.20 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
 ip address 192.168.0.20 255.255.255.0
!
```

g. Dynamische routering configureren om de tunnelinterface te promoten. Daarna kan het reclame maken voor andere netwerken die door de tunnel moeten gaan.

```
router eigrp 100
 no auto-summary
 network 10.1.120.0 0.0.0.255
```

Verifiëren

- Gebruik de opdracht show ip interface brief om de status van de tunnelinterface te bekijken en te controleren of de tunnel een up/up status heeft.

<#root>

```
RouterB#
```

show ip interface brief

```
Interface              IP-Address      OK?   Method    Status   Protocol
GigabitEthernet1       192.168.0.20    YES   NVRAM     up       up
Tunnel0                10.1.120.11     YES   manual
```

up

```
 up
```

1. Gebruik de opdracht show crypto ikev2 sa om te bevestigen dat de beveiligde verbinding tussen de routers tot stand is gebracht.

<#root>

```
RouterB#
```

show crypto ikev2 sa

```
IPv4 Crypto IKEv2 SA

Tunnel-id  Local                Remote               fvrf/ivrf   Status
2          192.168.0.20/500     192.168.0.10/500     none/none
```

READY

```
    Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
```

Life/Active Time: 86400/3139 sec

```
IPv6 Crypto IKEv2 SA
```

- Gebruik de opdracht show crypto ipsec sa om te bevestigen dat het verkeer is gecodeerd en door de tunnel gaat door te controleren of de encaps en decaps tellers toenemen.

<#root>

```
RouterB#
```

show crypto ipsec sa

```
interface: Tunnel0
    Crypto map tag: Tunnel0-head-0, local addr 192.168.0.20

   protected vrf: (none)
   local ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
   current_peer 192.168.0.10 port 500
     PERMIT, flags={origin_is_acl,}


#pkts encaps: 669, #pkts encrypt: 669, #pkts digest: 669




#pkts decaps: 668, #pkts decrypt: 668, #pkts verify: 668


    #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.: 192.168.0.20, remote crypto endpt.: 192.168.0.10
      plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
      current outbound spi: 0x93DCB8AE(2480715950)
      PFS (Y/N): N, DH group: none

      inbound esp sas:


spi: 0x89C141EB(2311143915)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5578, flow_id: CSR:3578, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607913/520)


         IV size: 16 bytes
         replay detection support: Y


Status: ACTIVE(ACTIVE)



      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:


spi: 0x93DCB8AE(2480715950)


         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5577, flow_id: CSR:3577, sibling_flags FFFFFFFF80000048, crypto map: Tunnel0-head-0


sa timing: remaining key lifetime (k/sec): (4607991/3137)
```

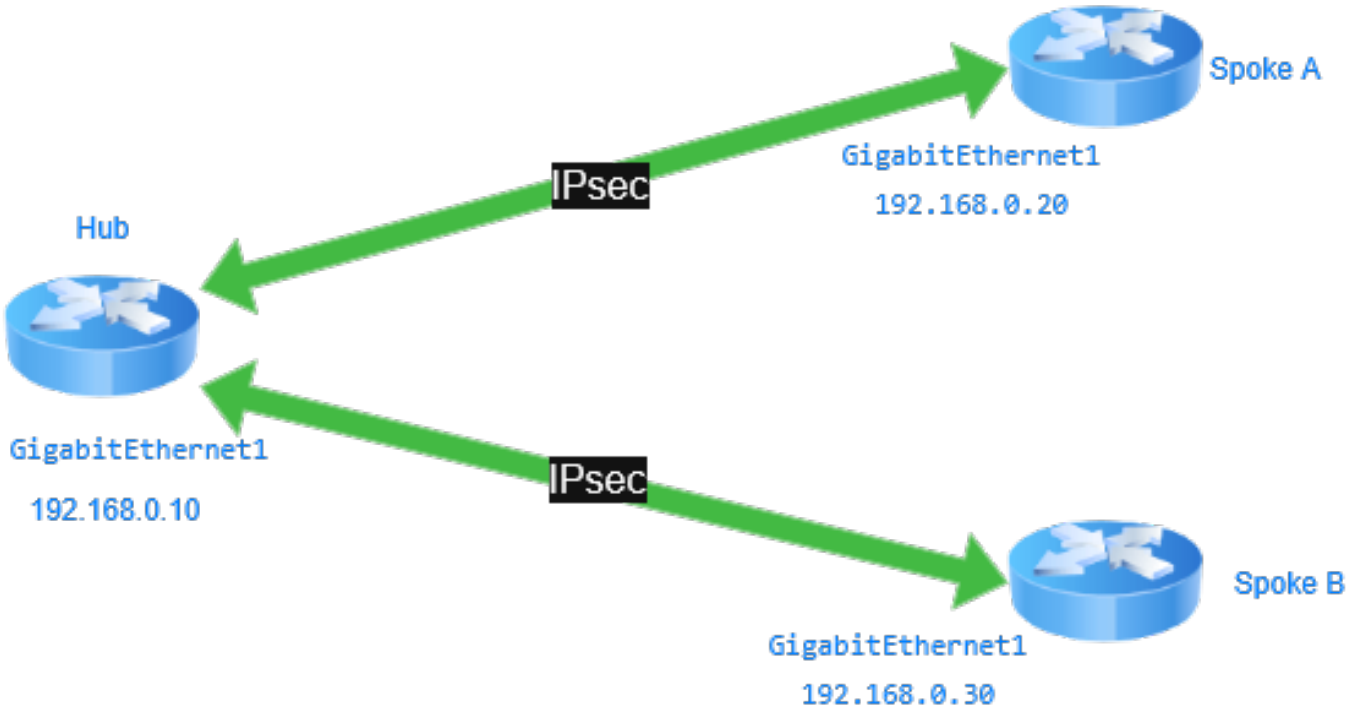
```
         IV size: 16 bytes
         replay detection support: Y

Status: ACTIVE(ACTIVE)


      outbound ah sas:

      outbound pcp sas:
```

- Gebruik de opdracht ip-buren weergeven om te bevestigen dat de EIGRP-nabijheid is vastgesteld met de andere site.

```
RouterB#show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(100)
H   Address                 Interface              Hold  Uptime     SRTT    RTO    Q   Seq
                                                   (sec)            (ms)          Cnt  Num
0   10.1.120.10             Tu0                     13   00:51:26    3      1470   0   2
```

Hub-and-Spoke FlexVPN

In de hub-and-spoke-topologie maken meerdere spaakrouters verbinding met een centrale hub-router. Deze configuratie is optimaal voor scenario's waarbij spaken voornamelijk communiceren met de hub. In FlexVPN kunnen dynamische tunnels worden geconfigureerd om de communicatie-efficiëntie te verbeteren. De hub maakt gebruik van IKEv2-routering om routes naar spaakrouters te distribueren, waardoor naadloze connectiviteit wordt gegarandeerd. Zoals het in het diagram wordt genoemd, legt de configuratie de VPN-verbinding tussen een Hub en Spoke uit en hoe de Hub is geconfigureerd om een dynamische verbinding met meerdere Spokes tot stand te brengen en het is in staat om meer Spokes toe te voegen.



Hub_and_Spoke_Diagram

Stap 1: Hub-configuratie

a. Bepaal het IKEv2-voorstel en -beleid.

b. Configureer a keyring en voer een code in Pre-Shared Key die wordt gebruikt om de spaken te verifiëren.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Schakel AAA-services in op de Hub-router en definieer vervolgens een lijst met netwerkautorisaties met de naamFlexAuthdie beleidsregels van de lokale apparaatconfiguratie opgeeft.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieer eenIP address poolnaamFlexPool, die de adressen 10.1.1.2 tot en met 10.1.1.254 bevat. Deze pool wordt gebruikt om automatisch een IP-adres toe te wijzen aan de tunnelinterface van de spaken.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definieer een standaard IP-toegangslijst met een naamFlexTrafficen machtigt het netwerk 10.10.1.0/24. Deze ACL definieert de netwerken die naar de FlexVPN-spaken worden geduwd om ze via de tunnel te bereiken.

```
!
ip access-list standard FlexTraffic
 permit 10.10.1.0 0.0.0.255
!
```

De toegangslijst en de IP-adressengroep worden vermeld in de **IKEv2 Authorization Policy**lijst.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Maak een IKEv2 profileaccount aan, wijs de keyring AAA- en autorisatiegroep toe.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
 virtual-template 1
!
```

g. Maak een Transport Setwachtwoord, definieer de codering en hash-algoritmen die worden gebruikt om gegevens te beschermen.

h. Maak een IPsec profilemap, wijs de IKEv2 profile en Transport Set eerder aangemaakte toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configureer de **virtual-template 1** as **type tunnel**instellingen. Verwijs naar de interface als eenIP unnumbered addressen pas de **IPsec profile**

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Stap 2: Spaakconfiguratie

a. Bepaal het IKEv2-voorstel en -beleid.

b. Configureer een sleutelhanger en voer een vooraf gedeelde sleutel in die wordt gebruikt voor verificatie naar de hub.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
```

```
!
```

c. Schakel AAA-services in op de Hub-router en definieer vervolgens een lijst met netwerkautorisaties met de naam **FlexAuth** die beleidsregels van de lokale apparaatconfiguratie opgeeft. Configureer vervolgens het modusconfiguratiebeleid om het IP-adres en de routes naar de FlexVPN-spaken te pushen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieer een standaard IP-toegangslijst die een naam heeft **FlexTraffic** en het netwerk toestaat 10.20.2.0/24. Deze ACL definieert de netwerken die worden gedeeld door deze spreker om door de tunnel te gaan.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

De toegangslijst wordt toegewezen in de **IKEv2 Authorization Policy**lijst.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Maak een IKEv2 profileaccount aan, wijs de keyring AAA- en autorisatiegroep toe.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
!
```

f. Maak een transportset en definieer de codering en hash-algoritmen die worden gebruikt om gegevens te beschermen.

g. Maak een IPsec-profiel, wijs het IKEv2-profiel en de eerder gemaakte transportset toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configureer de tunnelinterface met de eigenschap van het overeengekomen IP-adres, dat wordt verkregen uit de pool die op de hub is geconfigureerd.

```
!
interface tunnel 0
 ip address negotiated
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Verifiëren

Gebruik de opdracht show ip interface brief om de status Tunnel, Virtual-Template en Virtual-Access te bekijken:

- Op de Hub heeft de Virtual-Template een up/down-status die normaal is. Voor elke Spoke wordt een Virtual-Access gemaakt die een verbinding met de Hub tot stand brengt en een up/up-status weergeeft.
- Op de Spoke heeft de tunnelinterface een IP-adres ontvangen en een up/up-status weergegeven.

<#root>

```
FlexVPN_HUB#
```

show ip interface brief

```
Interface              IP-Address      OK? Method Status           Protocol
GigabitEthernet1       192.168.0.10    YES NVRAM  up               up
```

```
GigabitEthernet2       10.10.1.10      YES manual up              up
Loopback1              10.1.1.1        YES manual up              up

Virtual-Access1        10.1.1.1        YES unset  up              up

 <<<<<<< This Virtual-Access has been created and is up/up
Virtual-Template1      10.1.1.1        YES unset  up



FlexVPN_Spoke#

show ip interface brief

Interface              IP-Address      OK? Method  Status            Protocol
GigabitEthernet1       192.168.0.20    YES NVRAM   up                up
GigabitEthernet2       10.20.2.20      YES manual  up                up

Tunnel0                10.1.1.8        YES manual  up                up <<<<<<

The tunnel interface received an IP address from pool defined
```

- Gebruik de opdracht show crypto ikev2 sa om te bevestigen dat de beveiligde verbinding tussen de Hub en Spoke tot stand is gebracht.

<#root>

```
FlexVPN_HUB#

show crypto ikev2 sa

 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf                Status
1         192.168.0.10/500      192.168.0.20/500      none/none

READY

 Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
 Life/Active Time: 86400/587 sec



 IPv6 Crypto IKEv2 SA
```

- Gebruik de opdracht show crypto ipsec sa om te bevestigen dat het verkeer is gecodeerd en door de tunnel gaat door te controleren of de encaps en decaps tellers toenemen.

<#root>

```
FlexVPN_HUB#

show crypto ipsec sa
```

interface: Virtual-Access1

Crypto map tag: Virtual-Access1-head-0, local addr 192.168.0.10

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.0.10/255.255.255.255/47/0)
remote ident (addr/mask/prot/port): (192.168.0.20/255.255.255.255/47/0)
current_peer 192.168.0.20 port 500
PERMIT, flags={origin_is_acl,}

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10

#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10

#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.: 192.168.0.10, remote crypto endpt.: 192.168.0.20
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1
current outbound spi: 0xAFC2F841(2948790337)
PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x7E780336(2121794358)

transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 5581, flow_id: CSR:3581, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-h

sa timing: remaining key lifetime (k/sec): (4607998/3010)

IV size: 16 bytes
replay detection support: Y

Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xAFC2F841(2948790337)

```
         transform: esp-256-aes esp-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 5582, flow_id: CSR:3582, sibling_flags FFFFFFFF80000048, crypto map: Virtual-Access1-
```

sa timing: remaining key lifetime (k/sec): (4607998/3010)

```
         IV size: 16 bytes
         replay detection support: Y
```

Status: ACTIVE(ACTIVE)

```
      outbound ah sas:

      outbound pcp sas:
```

- Gebruik de opdracht ip-route tonen om te controleren of de routes naar de spaken zijn geduwd:
  - De route voor 10.1.1.1/32 werd via IKEv2-configuratie-payloads gepusht vanwege de interface-instructie voor routeset in de HUB-configuratie.
  - De route voor 10.10.1.0/24 werd via IKEv2-configuratie payloads verschoven vanwege de routeset-toegangslijst FlexTraffic-instructie in de HUB-configuratie.

<#root>

```
FlexVPN_Spoke#show ip route
<<< Omitted >>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S        10.1.1.1/32 is directly connected, Tunnel0   <<<<<<<


C        10.1.1.8/32 is directly connected, Tunnel0
S        10.10.1.0/24 is directly connected, Tunnel0  <<<<<<<


C        10.20.2.20/32 is directly connected, GigabitEthernet2
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.20/32 is directly connected, GigabitEthernet1
```

- Gebruik de ping-opdracht om de connectiviteit met de geadverteerde netwerken te

controleren.

<#root>

```
FlexVPN_HUB#
```

ping 10.20.2.20

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.20.2.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

```
FlexVPN_Spoke#
```

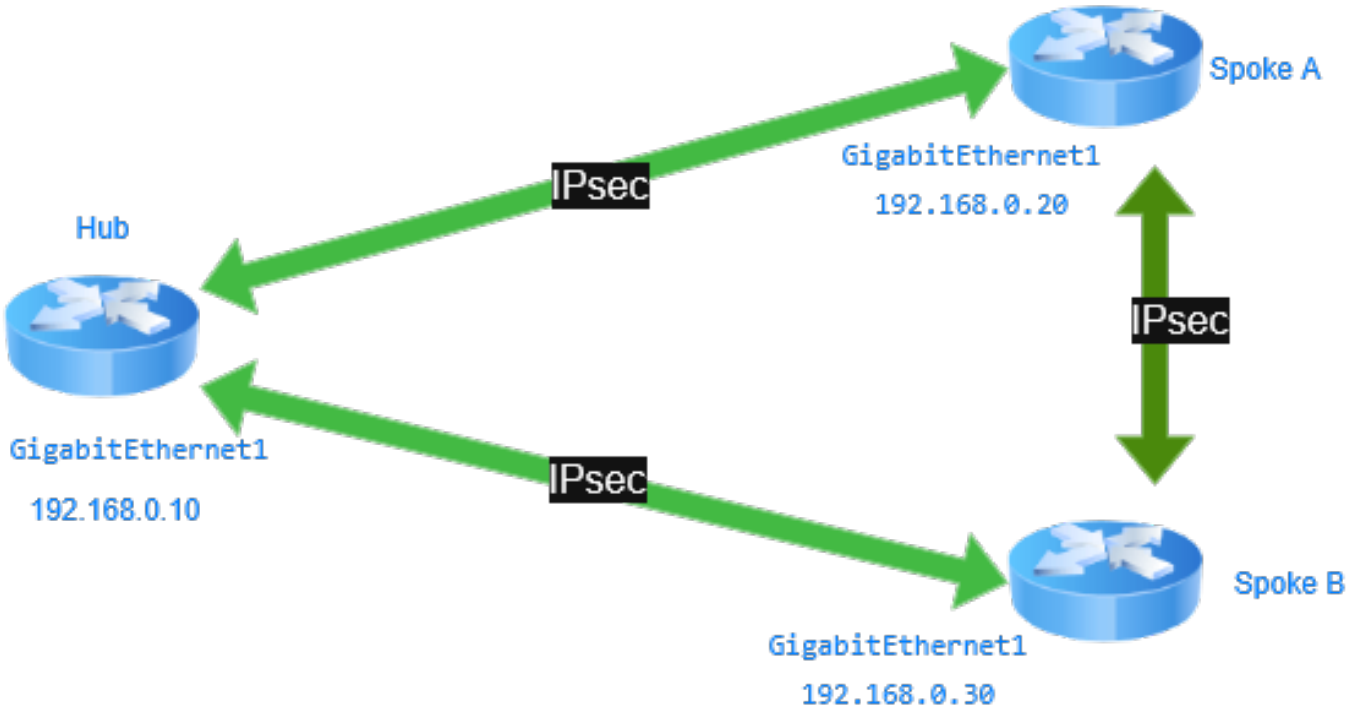
ping 10.10.1.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

Gesproken met Spoke FlexVPN

FlexVPN in een Hub- en Spoke-topologie met Spoke-to-Spoke-connectiviteit maakt dynamische, schaalbare en veilige VPN-communicatie mogelijk. De hub fungeert als een gecentraliseerd controlepunt waar NHRP-spokes de hub kunnen doorzoeken naar andere spaken IP-adressen, waardoor direct gesproken IPsec-tunnels voor efficiënte communicatie en verminderde latentie mogelijk zijn.

Op de hub wordt de **ip nhrp redirect** opdracht gebruikt om spaken te melden dat directe spraakcommunicatie mogelijk is, waardoor de verkeersstroom wordt geoptimaliseerd door de hub te omzeilen voor dataverkeer. Op spaken, het **ip nhrp shortcut** commando stelt hen in staat om dynamisch vast te stellen directe tunnels met andere spaken na het ontvangen van omleiding van de hub. Het diagram verwijst naar het verkeer tussen de hub en Spoke en Spoke-communicatie.



Spoke_to_Spoke_Diagram

Stap 1: Hub-configuratie

a. IKEv2-beleid en -profielen definiëren.

b. Configureer a keyring en voer een code in Pre-Shared Key die wordt gebruikt om de spaken te verifiëren.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Schakel AAA-services in op de Hub-router en definieer vervolgens een lijst met netwerkautorisaties met de naam **FlexAuth** die beleidsregels van de lokale apparaatconfiguratie opgeeft. Configureer vervolgens het modusconfiguratiebeleid om het IP-adres en de routes naar de FlexVPN-spaken te pushen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieer een IP address pool naam **FlexPool**, die de adressen 10.1.1.2 tot en met 10.1.1.254 bevat. Deze pool wordt gebruikt om automatisch een IP-adres toe te wijzen aan de tunnelinterface van de spaken.

```
!
ip local pool FlexPool 10.1.1.2 10.1.1.254
!
```

e. Definieer een standaard IP-toegangslijst met een naam FlexTraffic en machtigt het netwerk 10.0.0.0/8. Deze ACL definieert de netwerken die naar de FlexVPN-spaken worden gepusht, inclusief de netwerken voor andere spaken die met de Hub zijn verbonden, zodat de spaken weten dat die netwerken eerst via de Hub worden bereikt.

```
!
ip access-list standard FlexTraffic
 permit 10.0.0.0 0.255.255.255
!
```

De toegangslijst en -IP address pool gegevens worden toegewezen in de **IKEv2 Authorization Policy** lijst.

```
!
crypto ikev2 authorization policy HUBPolicy
 pool FlexPool
 route set interface
 route set access-list FlexTraffic
!
```

f. Maak een IKEv2 profile account aan, wijs de keyring AAA- en autorisatiegroep toe.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth HUBPolicy
```

```
 virtual-template 1
!
```

g. Maak een Transport Set codering en definieer de hash-algoritmen die worden gebruikt om gegevens te beschermen.

h. Maak een IPsec profilemap, wijs de IKEv2 profile en Transport Set eerder aangemaakte toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

i. Configureer de **virtual-template 1** as **type tunnel**instellingen. Verwijs naar de interface als een **IP unnumbered address** interface en pas de **IPsec profile**code toe.

Het **ip nhrp redirect** commando is geconfigureerd op de Virtual-Template om de spokes te informeren om een directe verbinding met andere spokes tot stand te brengen om hun netwerken te bereiken.

```
!
interface virtual-template 1 type tunnel
 ip unnumbered loopback1
 ip nhrp network-id 1
 ip nhrp redirect
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
```

Stap 2: Een spraakconfiguratie

a. IKEv2-beleid en -profielen definiëren.

b. Configureer a keyring en voer een code in Pre-Shared Key die wordt gebruikt om de spaken te verifiëren.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
```

```
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Schakel AAA-services in op de Hub-router en definieer vervolgens een lijst met netwerkautorisaties met de naam **FlexAuth** die beleidsregels van de lokale apparaatconfiguratie opgeeft. Configureer vervolgens het modusconfiguratiebeleid om het IP-adres en de routes naar de FlexVPN-spaken te pushen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieer een standaard IP-toegangslijst die een naam heeft **FlexTraffic** en het netwerk toestaat 10.20.2.0/24. Deze ACL definieert de netwerken die worden gedeeld door deze spreker om door de tunnel te gaan.

```
!
ip access-list standard FlexTraffic
 permit 10.20.2.0 0.0.0.255
!
```

De toegangslijst wordt toegewezen in de **IKEv2 Authorization Policy.**

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Maak een IKEv2 profileaccount aan, wijs de keyring AAA- en autorisatiegroep toe.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
```

```
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Maak een Transport Set codering en definieer de hash-algoritmen die worden gebruikt om gegevens te beschermen.

g. Maak een IPsec-profiel, wijs het IKEv2-profiel en de eerder gemaakte transportset toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configureer de tunnelinterface en virtuele sjabloon. Specificeer **Virtual-Template1** voor dVTI's die zijn gemaakt om **NHRP shortcuts**ondersteuning te bieden. Stel ook eentunnel0ongenummerd adres in op devirtual-templatepagina.

Het **ip nhrp shortcut** commando is geconfigureerd op de Spokes om hen in staat te stellen om dynamisch directe tunnels naar andere spokes te maken op basis van NHRP-redirect-berichten van de hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.20 255.255.255.0
!
```

Stap 3: Spaak B-configuratie

a. IKEv2-beleid en -profielen definiëren.

b. Configureer a keyring en voer een code in Pre-Shared Key die wordt gebruikt om de spaken te verifiëren.

```
crypto ikev2 proposal FLEXVPN_PROPOSAL
 encryption aes-cbc-256
 integrity sha256
 group 14
!
crypto ikev2 policy FLEXVPN_POLICY
 proposal FLEXVPN_PROPOSAL
!
crypto ikev2 keyring FLEXVPN_KEYRING
peer FLEVPNPeers
address 0.0.0.0 0.0.0.0
pre-shared-key local cisco123
pre-shared-key remote cisco123
!
```

c. Schakel AAA-services in op de Hub-router en definieer vervolgens een lijst met netwerkautorisaties met de naam **FlexAuth** die het beleid van de lokale apparaatconfiguratie opgeeft. Configureer vervolgens het modusconfiguratiebeleid om het IP-adres en de routes naar de FlexVPN-spaken te pushen.

```
!
aaa new-model
 aaa authorization network FlexAuth local
!
```

d. Definieer een standaard IP-toegangslijst met een naam **FlexTraffic** en machtigingen voor het netwerk 10.30.3.0/24. Deze ACL definieert de netwerken die worden gedeeld door deze spreker om door de tunnel te gaan.

```
!
ip access-list standard FlexTraffic
 permit 10.30.3.0 0.0.0.255
!
```

De toegangslijst wordt vermeld in de IKEv2 Authorization Policy.

```
!
crypto ikev2 authorization policy SpokePolicy
 route set interface
 route set access-list FlexTraffic
!
```

e. Maak een IKEv2 profileaccount aan, wijs de keyring AAA- en autorisatiegroep toe.

```
!
crypto ikev2 profile FLEXVPN_PROFILE
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local FLEXVPN_KEYRING
 aaa authorization group psk list FlexAuth SpokePolicy
 virtual-template 1
!
```

f. Maak een Transport Set codering en definieer de hash-algoritmen die worden gebruikt om gegevens te beschermen.

g. Maak een IPsec profilemap, wijs de IKEv2 profile en Transport Set eerder aangemaakte toe.

```
!
crypto ipsec transform-set FLEXVPN_TRANSFORM esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile FLEXVPN_PROFILE
 set transform-set FLEXVPN_TRANSFORM
 set ikev2-profile FLEXVPN_PROFILE
!
```

h. Configureer de tunnel interface en virtual template. Specificeer **Virtual-Template1** voor dVTI's die zijn gemaakt om NHRP shortcutsondersteuning te bieden. Stel ook eentunnel0ongenummerd adres in op devirtual-templatepagina.

Het **ip nhrp shortcut** commando is geconfigureerd op de Spokes om hen in staat te stellen om dynamisch directe tunnels naar andere spokes te maken op basis van NHRP-redirect-berichten van de hub.

```
!
interface tunnel 0
 ip address negotiated
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
```

```
 tunnel destination 192.168.0.10
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface virtual-template 1 type tunnel
 ip unnumbered tunnel0
 ip nhrp network-id 1
 ip nhrp shortcut virtual-template 1
 tunnel source GigabitEthernet1
 tunnel protection ipsec profile FLEXVPN_PROFILE
!
interface GigabitEthernet1
ip address 192.168.0.30 255.255.255.0
!
```

Verifiëren

Gebruik de opdracht show ip interface brief om de status Tunnel, Virtual-Template en Virtual-Access te bekijken. Nu is het een directe verbinding met gesproken taal:

- Op de Spokes heeft de Virtual-Template een up/down status wat normaal is. Er wordt een Virtual-Access gemaakt voor verbinding in de status up/up.

<#root>

```
FlexVPN_Spoke#

show ip interface brief


Interface                  IP-Address      OK?  Method  Status              Protocol
GigabitEthernet1           192.168.0.30    YES  NVRAM   up                  up
GigabitEthernet2           10.20.2.20      YES  manual  up                  up

Tunnel0                    10.1.1.12       YES  manual  up                  up


Virtual-Access1            10.1.1.12       YES  unset   up                  up

Virtual-Template1          10.1.1.12       YES  unset   up                  down
```

- Gebruik de opdracht show crypto ikev2 sa om te bevestigen dat de beveiligde verbinding tussen elk apparaat tot stand is gebracht.
- Gebruik de opdracht show crypto ipsec sa om te bevestigen dat het verkeer is gecodeerd en door de tunnel gaat door te controleren of de encaps en decaps tellers toenemen.
- Gebruik de opdracht show ip nhrp om de omleiding van het verkeer tussen de spaken te controleren.
  <#root>

  ```
  FlexVPN_Spoke#

  show ip nhrp
  ```

```
      10.1.1.10/32 via 10.1.1.10
         Virtual-Access1 created 00:00:13, expire 00:09:46
         Type:
      dynamic
      , Flags: router nhop rib nho
         NBMA address: 192.168.0.30
      10.30.3.0/24 via 10.1.1.10
         Virtual-Access1 created 00:00:13, expire 00:09:46
         Type:
      dynamic
      , Flags: router rib nho
         NBMA address: 192.168.0.30
```

Gebruik de opdracht show ip route om te controleren of de routes naar de spaak zijn geduwd:

- De twee routes zijn gekoppeld aan de Virtual-Access1-interface zijn nieuw en gekoppeld aan de NHRP-snelkoppelingen.
- Het teken % geeft een next-hop override aan.

<#root>

```
FlexVPN_Spoke#sh ip route
<<<< Omitted >>>>

Gateway of last resort is 192.168.0.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.0.1
      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
S        10.0.0.0/8 is directly connected, Tunnel0
S        10.1.1.1/32 is directly connected, Tunnel0
S  %     10.1.1.10/32 is directly connected, Virtual-Access1
C        10.1.1.12/32 is directly connected, Tunnel0
C        10.20.2.20/32 is directly connected, GigabitEthernet2
S  %     10.30.3.0/24 is directly connected, Virtual-Access1
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.0.0/24 is directly connected, GigabitEthernet1
L        192.168.0.30/32 is directly connected, GigabitEthernet1
```

- Gebruik de opdracht ping om de connectiviteit met de geadverteerde netwerken te controleren.

<#root>

```
FlexVPN_Spoke#
ping 10.30.3.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.30.3.30, timeout is 2 seconds:
.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

Probleemoplossing

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen. Gebruik deze opdrachten om het tunnelonderhandelingsproces te debuggen:

debug crypto interface

debug crypto ikev2
debug crypto ikev2 client flexvpn
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ikev2 packet

debug crypto ipsec
debug crypto ipsec error
debug crypto ipsec message
debug crypto ipsec states

NHRP-debugs kunnen helpen bij het oplossen van problemen met de gesproken verbindingen.

debug nhrp
debug nhrp detail
debug nhrp event
debug nhrp error
debug nhrp packet
debug nhrp routing

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.