FlexVPN configureren met ISE-integratie

Inhoud

Inleiding

In dit document wordt beschreven hoe FlexVPN kan worden geconfigureerd met behulp van Cisco Identity Services Engine (ISE) om dynamisch configuraties aan spaken toe te wijzen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie Cisco Identity Services Engine (ISE)
- RADIUS-protocol
- Flex Virtual Private Network (FlexVPN)

Gebruikte componenten

Dit document is gebaseerd op deze software- en hardwareversies:

- Cisco CSR1000V (VXE) - Versie 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

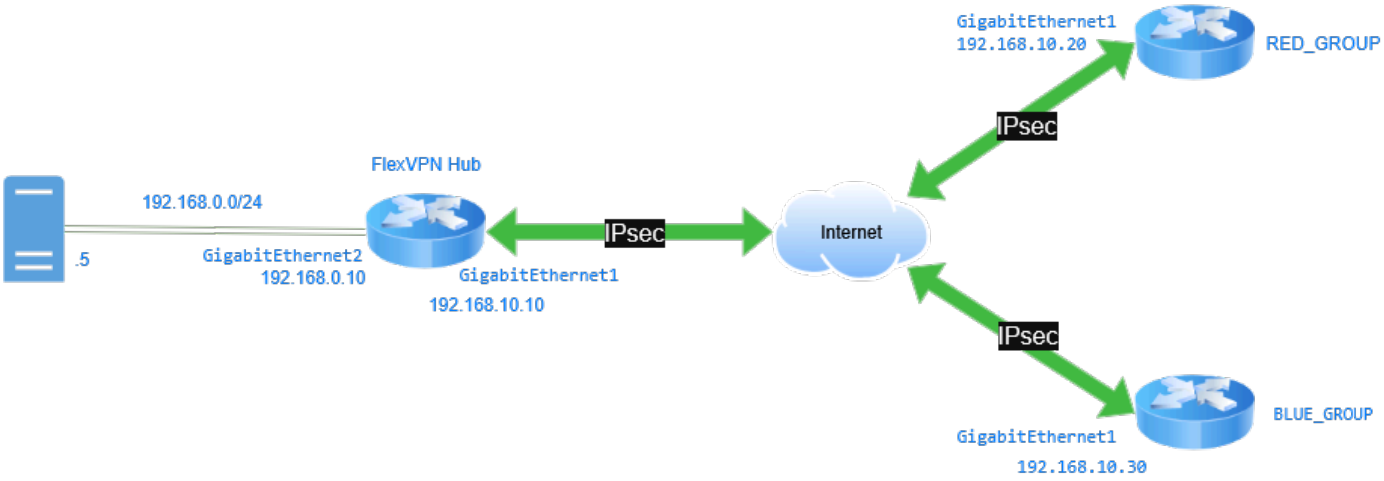
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram

FlexVPN kan een verbinding met spaken tot stand brengen en bepaalde configuraties toewijzen die communicatie en verkeersbeheer mogelijk maken. Verwezen in het diagram, toont dit hoe FlexVPN integreert met ISE, zodat, wanneer een spaak verbinding maakt met de HUB, de parameters van tunnelbron en DHCP-pool worden toegewezen, afhankelijk van de groep of tak waartoe de spaak behoort. Het gebruikt het certificaat om de spaken te authenticeren en vervolgens ISE met Radius als autorisatie- en boekhoudserver.



FlexVPN met ISE-integratie

Stap 1: Hub-configuratie

a. Configureer een`trustpoint`om het routercertificaat op te slaan. Certificaten worden gebruikt om de spaken te verifiëren.

```
crypto pki trustpoint FlexVPNCA
  enrollment url http://10.10.10.10:80
  subject-name cn=FlexvpnServer, o=Cisco, OU=IT_GROUP
  revocation-check crl
```

b. Configureer **certificate map**a. Het doel van de `certificate map` router is om certificaten te identificeren en te matchen op basis van de opgegeven informatie, in het geval dat de router meerdere certificaten heeft geïnstalleerd.

```
crypto pki certificate map CERT_MAP 5
```

```
  issuer-name co ca-server.cisco.com
```

c. Configureer een systeem RADIUS server voor autorisatie en boekhouding op het apparaat:

```
aaa new-model
!
aaa authorization network FLEX group ISE
aaa accounting network FLEX start-stop group ISE
```

d. Definieer het **RADIUS server group** bestand met het IP-adres, de communicatiepoorten, de gedeelde sleutel en de broninterface voor het RADIUS-verkeer.

```
radius server ISE25
  address ipv4 192.168.0.5 auth-port 1645 acct-port 1646
  key cisco1234

aaa group server radius ISE
  server name ISE25
  ip radius source-interface g2
```

e. Configureer de **loopback interfaces** instellingen. De verbindingen loopback interfaces worden gebruikt als de bronverbinding voor de tunnel en worden dynamisch toegewezen afhankelijk van de groep die is verbonden.

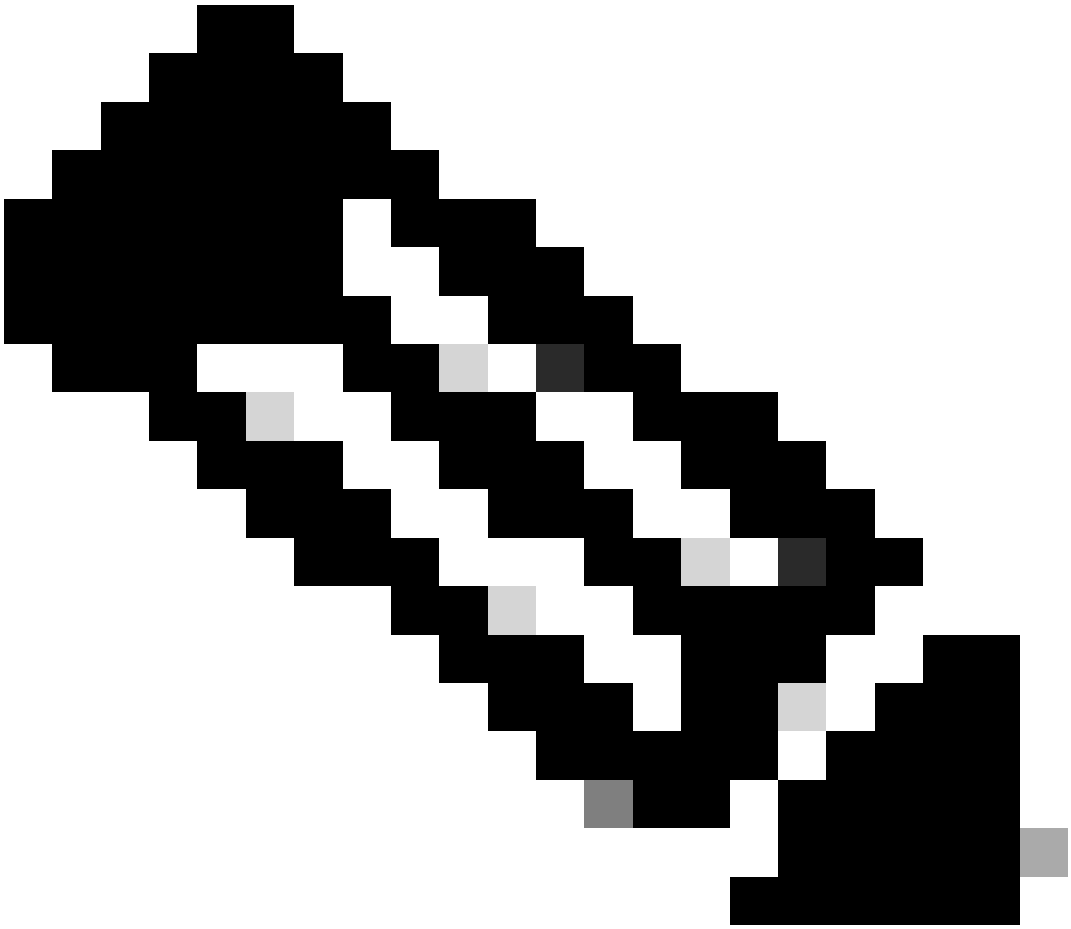
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f. Definieer een **IP local pool** naam voor elke groep.

```
ip local pool RED_POOL 172.16.10.10 172.16.10.254
ip local pool BLUE_POOL 172.16.0.10 172.16.0.254
```

g. Configureren van EIGRP en adverteren van de netwerken van elke groep.

```
router eigrp Flexvpn
address-family ipv4 unicast autonomous-system 10
topology base
exit-af-topology
network 10.100.100.0 0.0.0.255
network 10.10.1.0 0.0.0.255
network 10.200.200.0 0.0.0.255
network 10.10.2.0 0.0.0.255
network 172.16.0.0
```



Opmerking: FlexVPN ondersteunt dynamische routeringsprotocollen zoals OSPF, EIGRP en BGP via VPN-tunnels. In deze gids wordt EIGRP gebruikt.

---

h. Configureer de **crypto ikev2 name mangler**instellingen. Het IKEv2 name mangler wordt gebruikt om de gebruikersnaam voor IKEv2-autorisatie af te leiden. In dit geval is het geconfigureerd om de informatie van de Organisatie-eenheid uit de certificaten op de spaken te gebruiken als de gebruikersnaam voor autorisatie.

```
crypto ikev2 name-mangler NM
dn organization-unit
```

i. Configureer de **IKEv2 profile**instellingen. De certificate map, AAA server groupen worden name mangler vermeld in het IKEv2-profiel.

De lokale en externe verificatie worden in dit specifieke scenario geconfigureerd **RSA-SIG**als.

Er moet een lokale gebruikersaccount worden aangemaakt op het RADIUS server scherm met een gebruikersnaam die overeenkomt met deorganization-unitwaarde en het wachtwoordCisco1234(zoals aangegeven in de onderstaande configuratie).

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint FlexVPNCA
dpd 10 2 periodic
aaa authorization group cert list FLEX name-mangler NM password Cisco1234
aaa accounting cert FLEX
virtual-template 1 mode auto
```

j. Configureer deIPsec profileen de IKEv2 profilereferentie.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

k. Het virtual-templatesysteem maken. Het wordt gebruikt om een virtual-access interface link te maken en de IPsec profile gemaakte.

Stel het **virtual-template** wachtwoord in zonder IP-adres, aangezien dit is toegewezen door de RADIUS servergebruiker.

```
interface Virtual-Template2 type tunnel
no ip address
tunnel source GigabitEthernet1
tunnel destination dynamic
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

Configureer tweeloopbacksom een intern netwerk te simuleren.

```
interface Loopback1010
ip address 10.10.1.10 255.255.255.255
!
interface Loopback1020
ip address 10.10.2.10 255.255.255.255
```

Stap 2: Spaakconfiguratie

a. Configureer a trustpoint om het certificaat van de spaakrouter op te slaan.

```
crypto pki trustpoint FlexVPNSpoke
 enrollment url http://10.10.10.10:80
 subject-name cn=FlexVPNSpoke, o=Cisco, OU=RED_GROUP
 revocation-check crl
```

b. Configureer a certificate map. Het doel van de certificate map router is om certificaten te identificeren en te matchen op basis van de opgegeven informatie, in het geval dat de router meerdere certificaten heeft geïnstalleerd.

```
crypto pki certificate map CERT_MAP 5
issuer-name co ca-server.cisco.com
```

c. Configureer het lokale AAA-autorisatienetwerk.

Het autorisatienetwerk commando aaa wordt gebruikt om toegangsverzoeken met betrekking tot netwerkdiensten te autoriseren. Het omvat het controleren of een gebruiker toestemming heeft om toegang te krijgen tot de gevraagde service nadat deze is geverifieerd.

```
aaa new-model
aaa authorization network FLEX local
```

d. Configureer de IKEv2 profile instellingen. De certificate map lokale AAA- en AAA-autorisatie worden vermeld in de IKEv2 profile lijst.

De lokale en externe verificatie is geconfigureerd als **RSA-SIG**.

```
crypto ikev2 profile Flex_PROFILE
match certificate CERT_MAP
identity local dn
```

```
authentication local rsa-sig
authentication remote rsa-sig
pki trustpoint FlexVPNSpoke
dpd 10 2 on-demand
aaa authorization group cert list FLEX default
```

e. Configureer deIPsec profileen de referentie IKEv2 profile.

```
crypto ipsec profile IPSEC_FlexPROFILE
set ikev2-profile Flex_PROFILE
```

f. Configureer detunnel interfaceinstellingen. De server tunnel interface is geconfigureerd om een tunnel-IP-adres van de hub te ontvangen op basis van de autorisatieresultaten.

```
interface Tunnel0
ip address negotiated
tunnel source GigabitEthernet1
tunnel destination 192.168.10.10
tunnel protection ipsec profile IPSEC_FlexPROFILE
```

g. EIGRP configureren, reclame maken voor het lokale netwerk van de spreker en de tunnel interfacespreker.

```
router eigrp 10
network 10.20.1.0 0.0.0.255
network 172.16.0.0
```

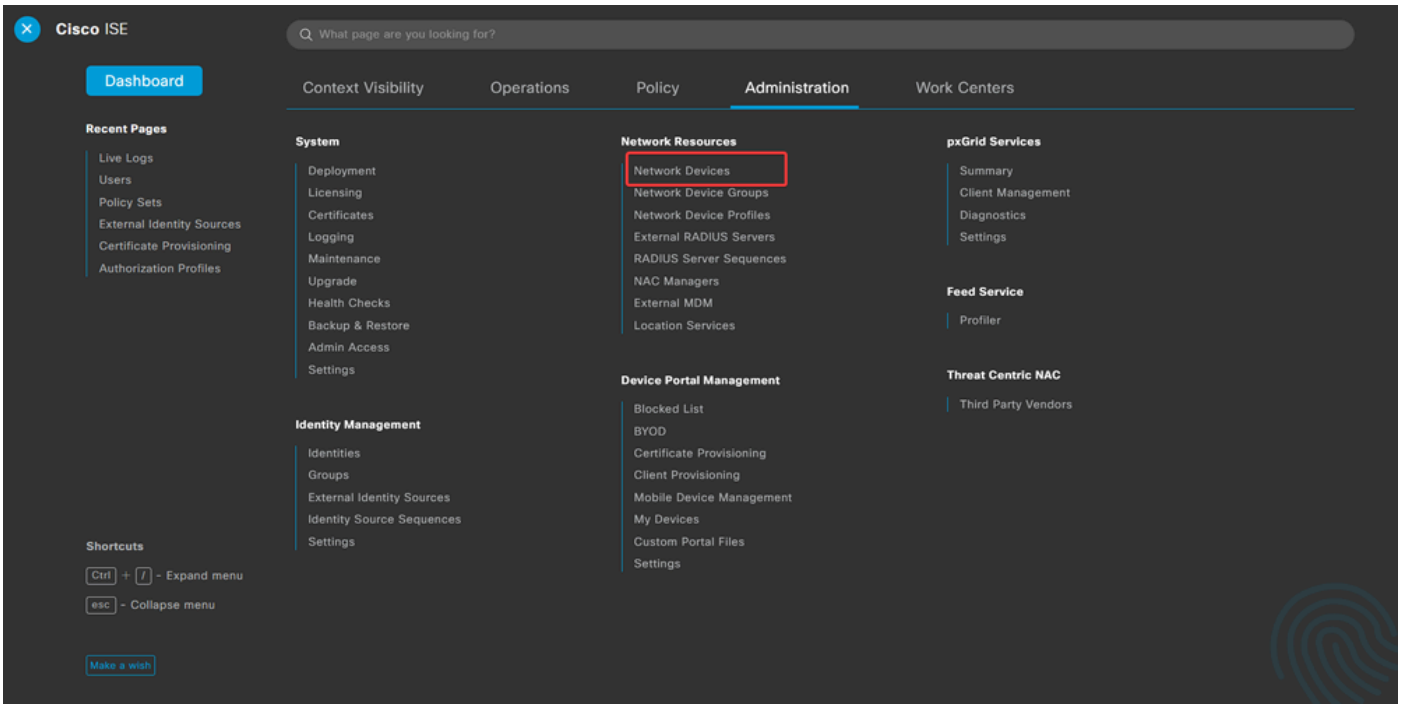
Configureer een computerloopbackom een intern netwerk te simuleren.

```
interface Loopback2010
ip address 10.20.1.10 255.255.255.255
```

Stap 3: ISE-configuratie

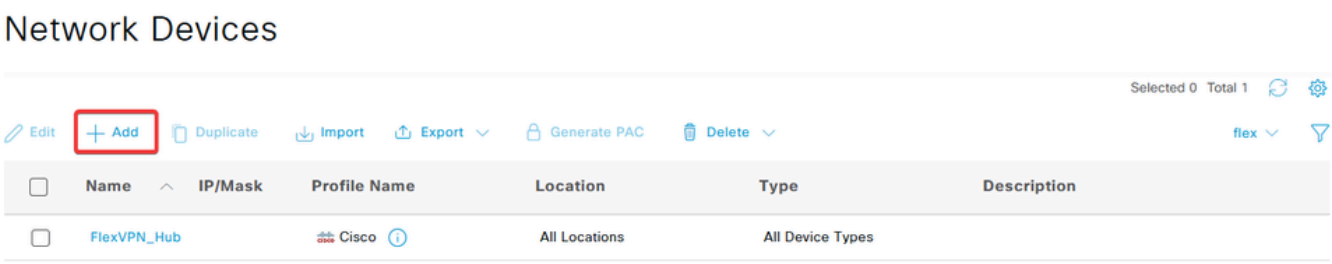
Stap 3.1: Gebruikers, groepen maken en netwerkapparaat toevoegen

a. Meld u aan bij de ISE-server en navigeer naar **Administration** > **Network Resources** > **Network Devices.**



beheer-netwerkbronnen-netwerkapparaten

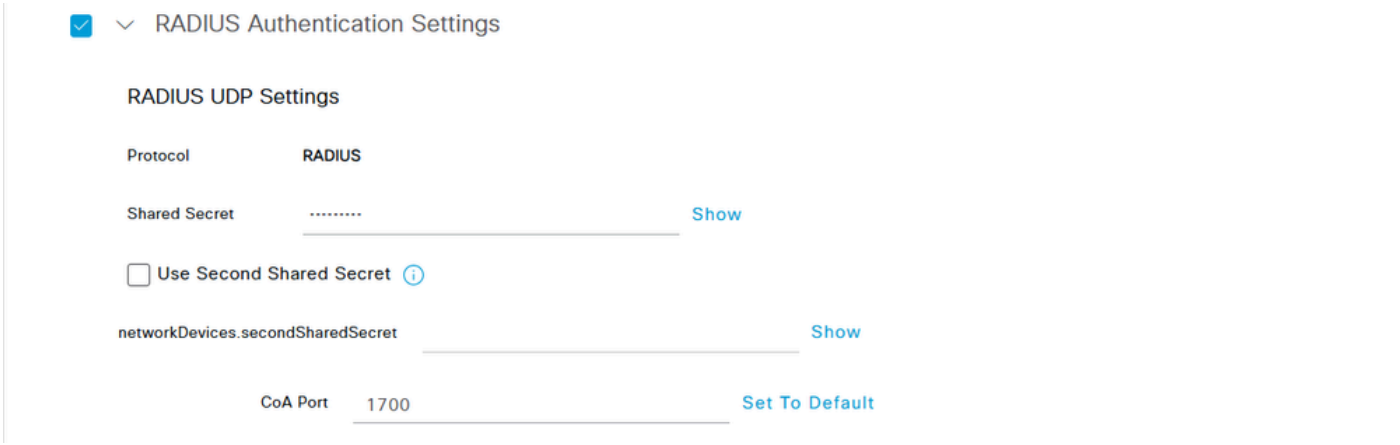
b. Klik **Add** hierop om de FlexVPN Hub te configureren als een AAA-client.



FlexVPN-router toevoegen als AAA-client

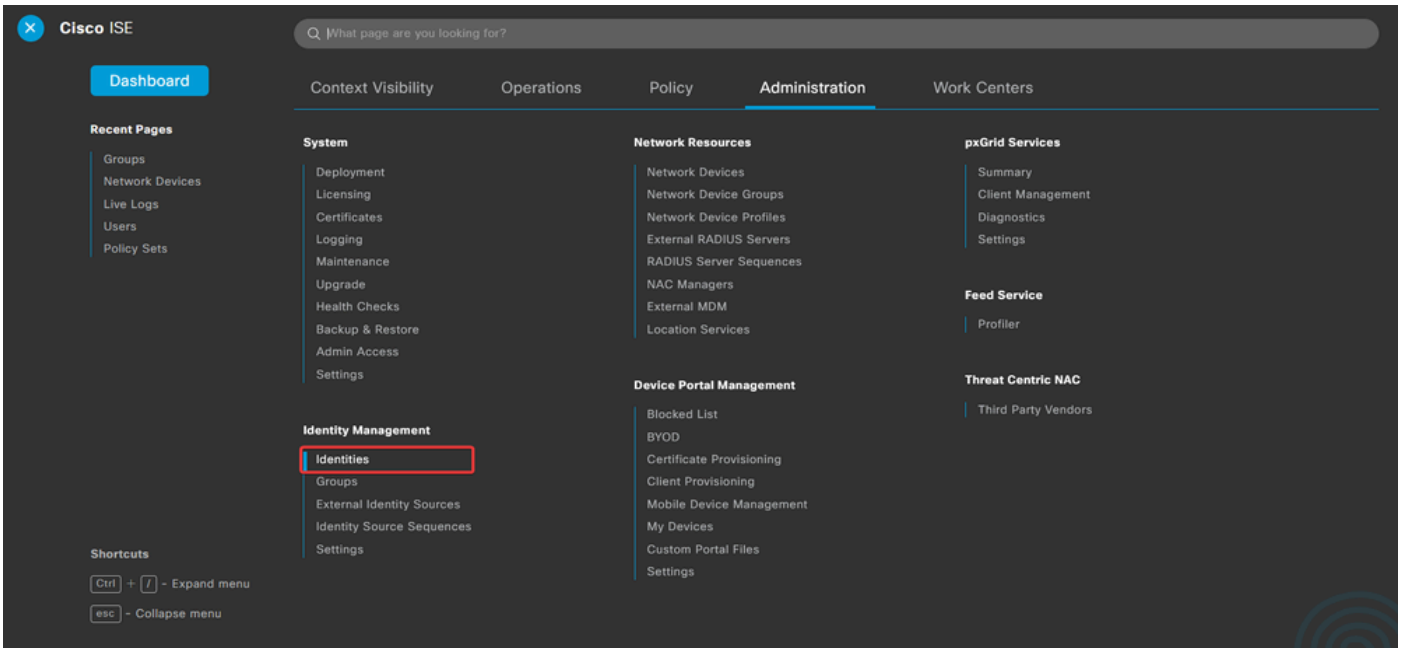
c. Voer de velden Netwerkapparaatnaam en IP-adres in en vink **RADIUS Authentication Settings** vervolgens het selectievakje aan en voeg het **Shared Secret**. gedeelde geheime wachtwoord toe dat is gebruikt toen de RADIUS-servergroep werd gemaakt op de FlexVPN-hub. Klik op de knop .Save

IP-adres netwerkapparaat



gedeelde netwerkapparaatsleutel

d. Navigeer naar **Administration** > **Identity Management** > **Identities**links.

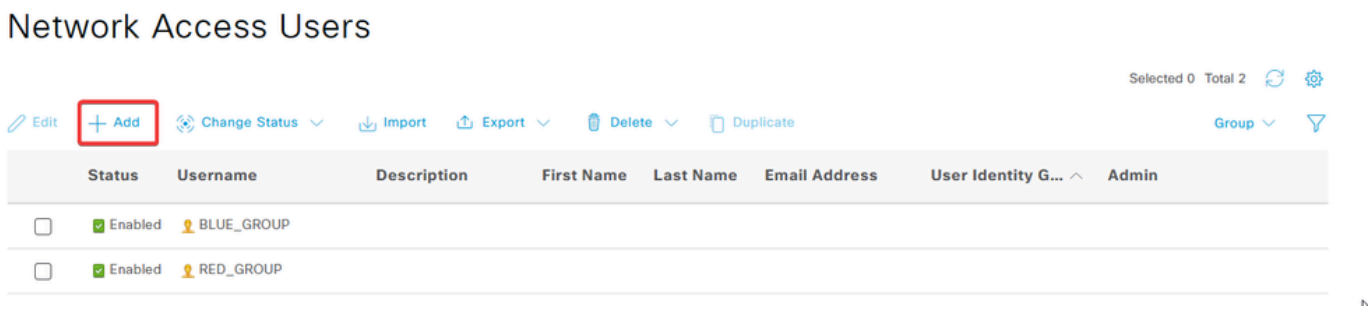


beheer-identificeer beheer-identificeert

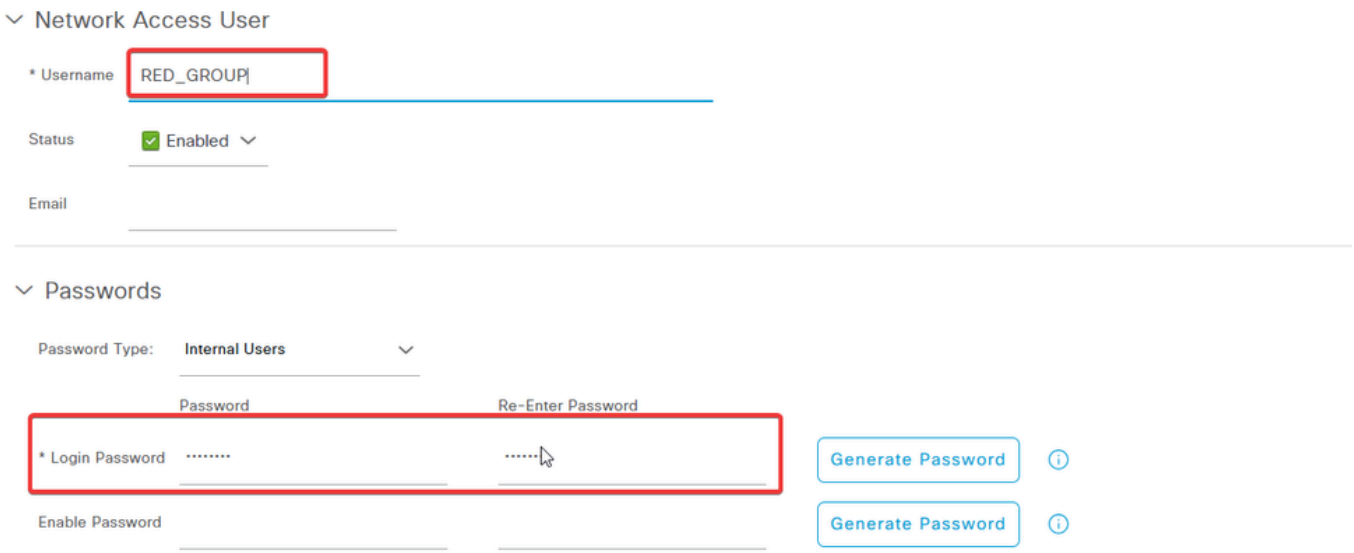
e. Klik hieropAddom een nieuwe gebruiker aan te maken in de lokale serverdatabase.

Voer deUsernameen **Login Password**. De gebruikersnaam is dezelfde naam die de certificaten hebben op de waarde van de organisatie-eenheid op het certificaat en het aanmeldingswachtwoord moet hetzelfde zijn als het wachtwoord dat is opgegeven in het IKev2-profiel.

Klik op de knop .**Save**



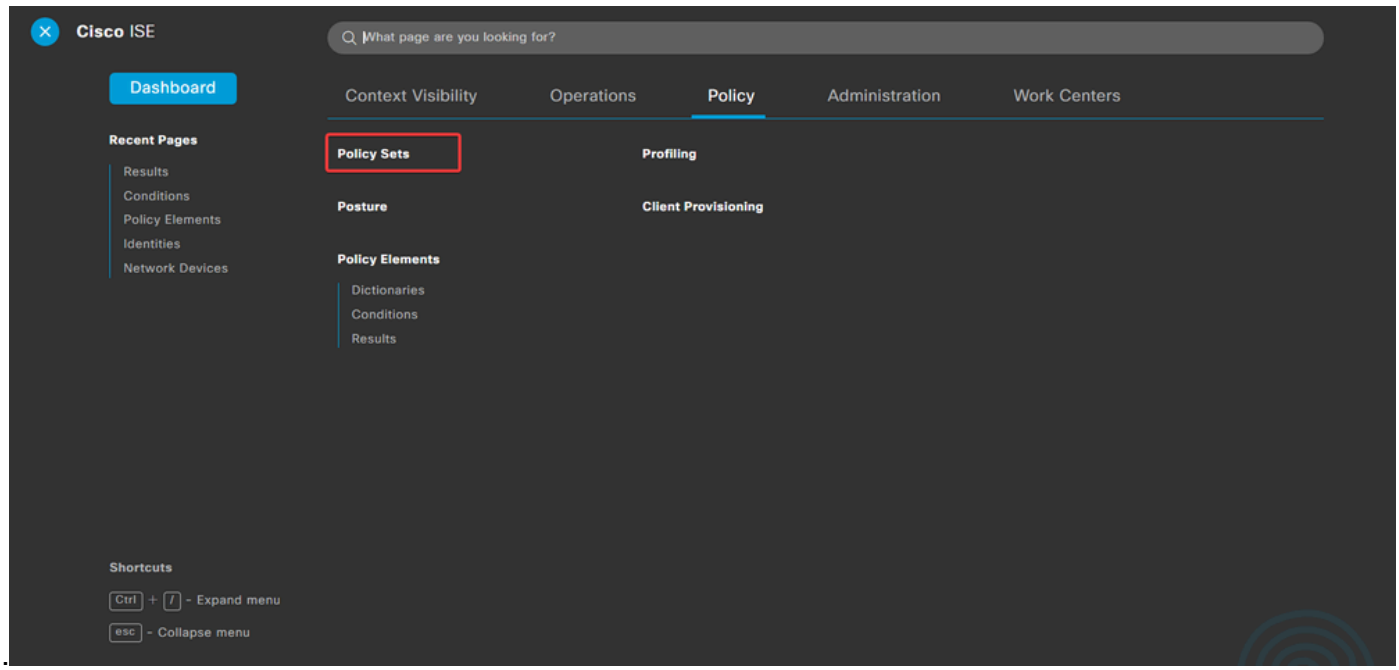
beheer-identificeer beheer-identificeert



Groep gemaakt op dezelfde manier als de waarde van de organisatie-eenheid

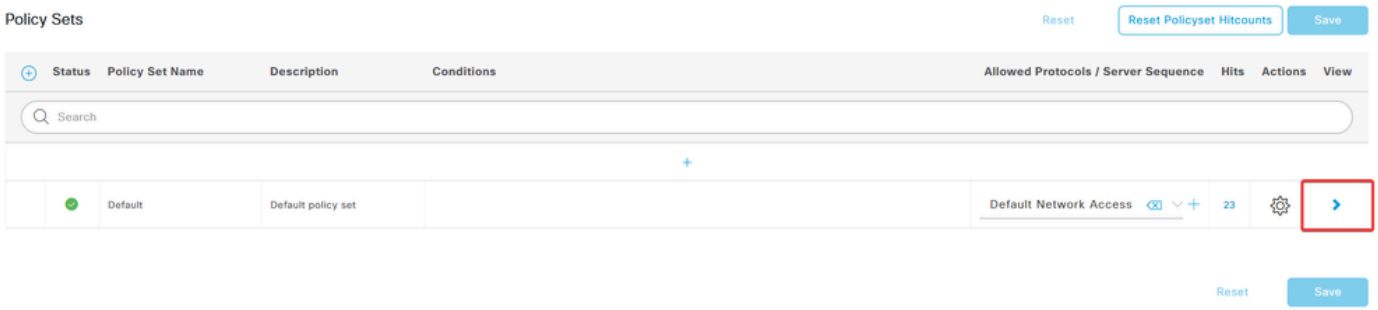
Stap 3.2: Beleidsset configureren

a. Navigeer naar **Policy** > **Policy Sets**.



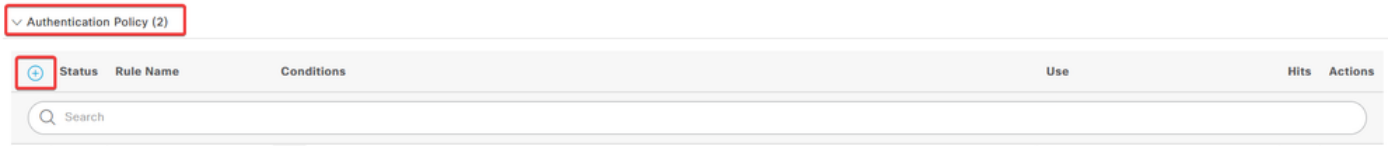
beleidssets

b. Selecteer het standaardautorisatiebeleid door op de pijl aan de rechterkant van het scherm te klikken:



Standaardbeleid bewerken

c. Klik op de pijl in het vervolgkeuzemenu naastAuthentication Policydeze om deze uit te vouwen. Klik vervolgens op het **add (+)** pictogram om een nieuwe regel toe te voegen.

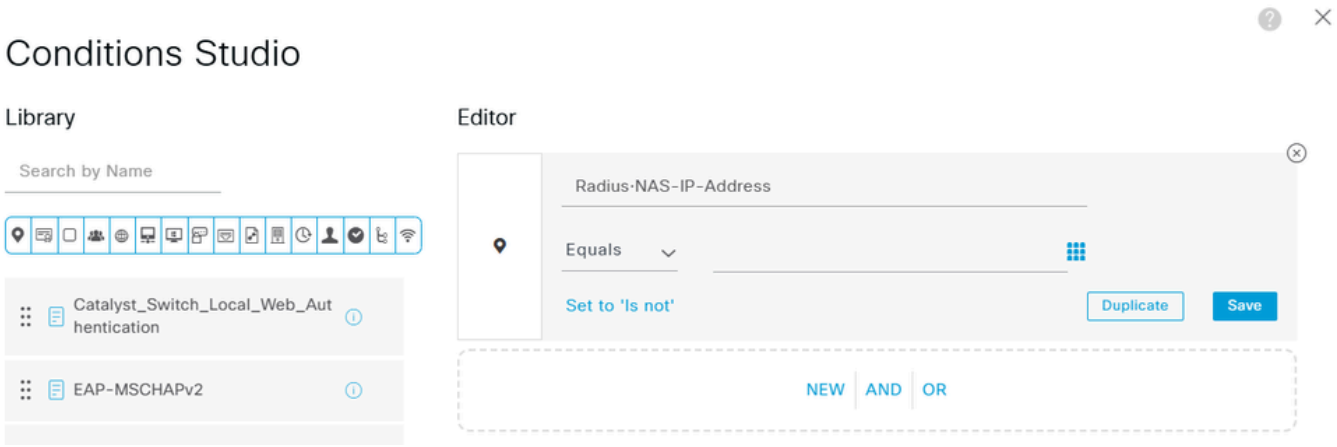


Verificatiebeleid toevoegen

d. Voer de naam voor de regel in en selecteer het pictogramadd (+)onder de kolom Voorwaarden.

Verificatiebeleid maken

e. Klik op het tekstvak Attribuuteditor en klik op hetNAS-IP-Addresspictogram. Voer het IP-adres (192.168.0.10) van de FlexVPN-hub in.

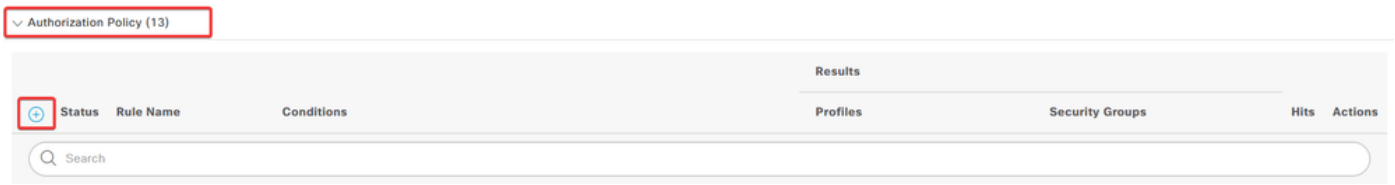


Authenticate FlexVPN Hub

Authenticatiebeleid

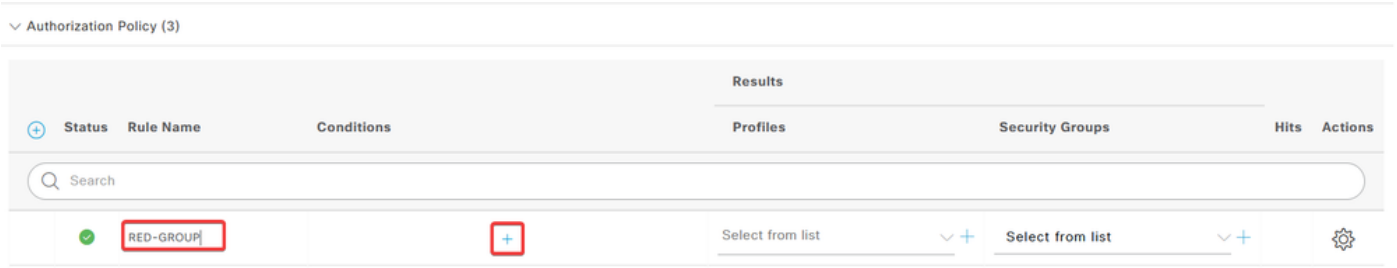
Stap 3.3: Autorisatiebeleid configureren

a. Klik op de pijl in het vervolgkeuzemenu naastAuthorization Policyom deze uit te vouwen. Klik vervolgens op het **add (+)** pictogram om een nieuwe regel toe te voegen.



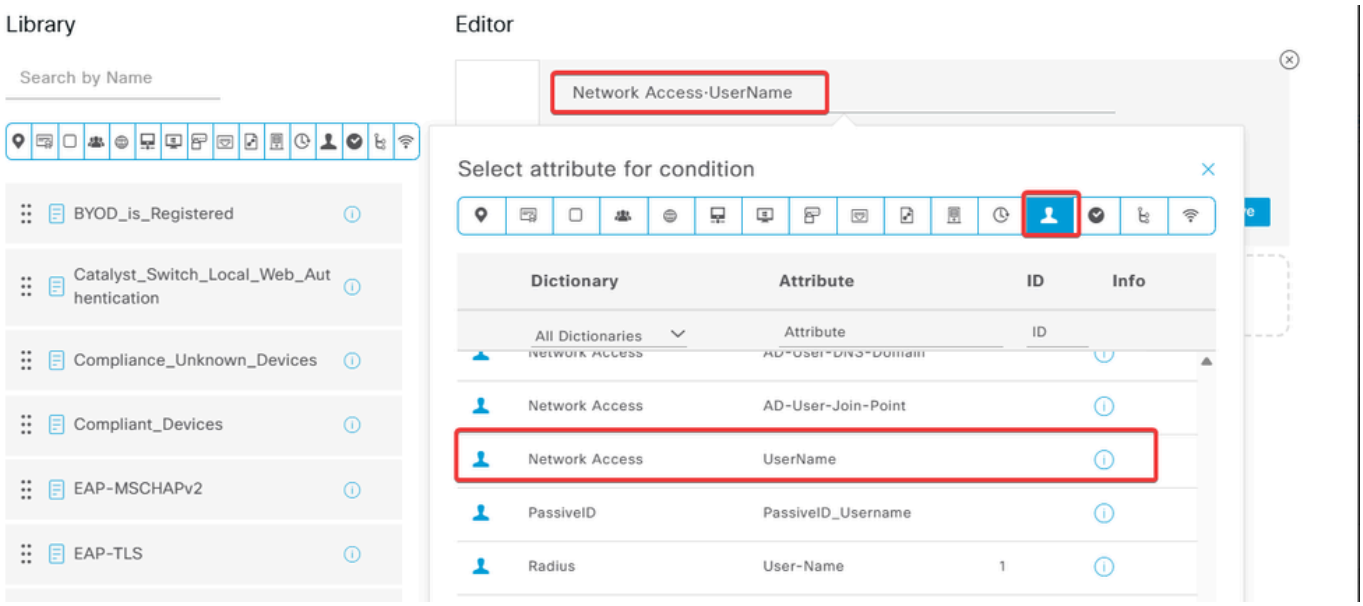
Nieuw machtigingsbeleid maken

b. Voer de naam voor de regel in en selecteer het **add (+)** pictogram onder de kolom Voorwaarden.



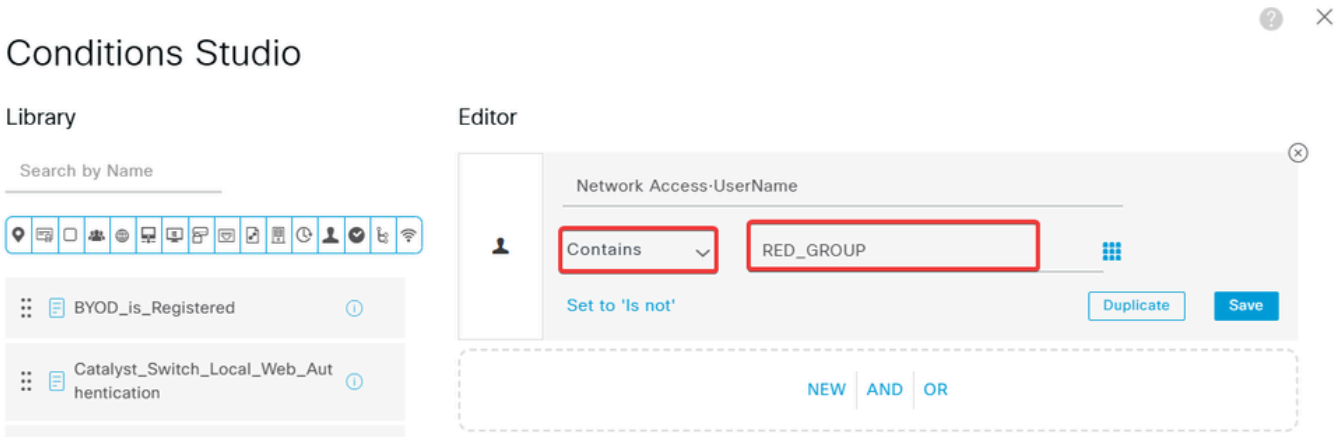
Nieuwe regel maken

c. Klik op het tekstvak Attribuuteditor en klik op hetSubjectpictogram. Selecteer het **Network Access - UserName** attribuut.



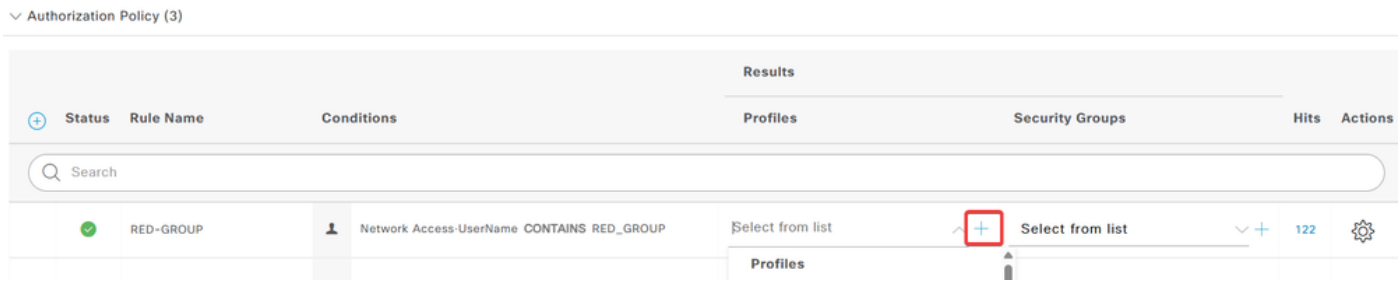
Selecteer Netwerktoegang - gebruikersnaam

d. Selecteer**Contains**als operator en voeg vervolgens de Organisatie-eenheid-waarde van de certificaten toe.



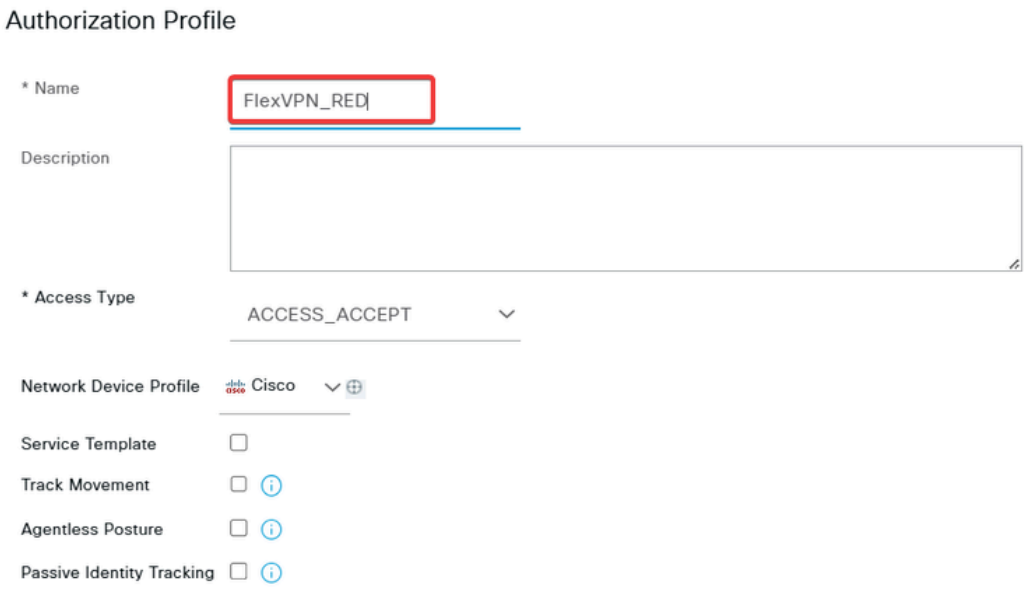
Groepsnaam toevoegen

e. Klik in de kolom Profielen op het pictogram**add (+)**en kies **Create a New Authorization Profile**Profielen.



Nieuw machtigingsprofiel toevoegen

f. Voer het profiel **Name**in.



Naam van het autorisatieprofiel

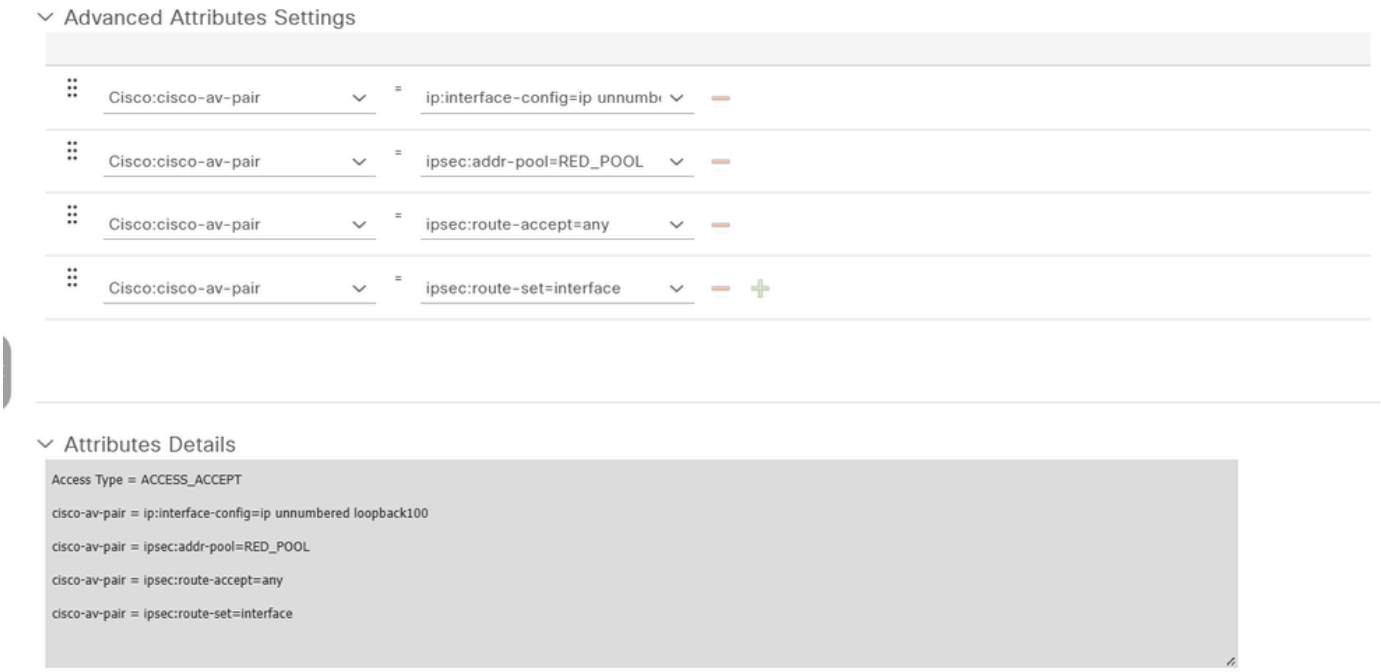
g. Navigeer naar **Advanced Attributes Settings**links. Selecteer vervolgens het cisco-av-pairkenmerk in het vervolgkeuzemenu aan de linkerkant en voeg het kenmerk toe dat afhankelijk van de groep is toegewezen aan de FlexVPN Spoke.

De attributen die voor dit voorbeeld moeten worden toegewezen, zijn onder meer:

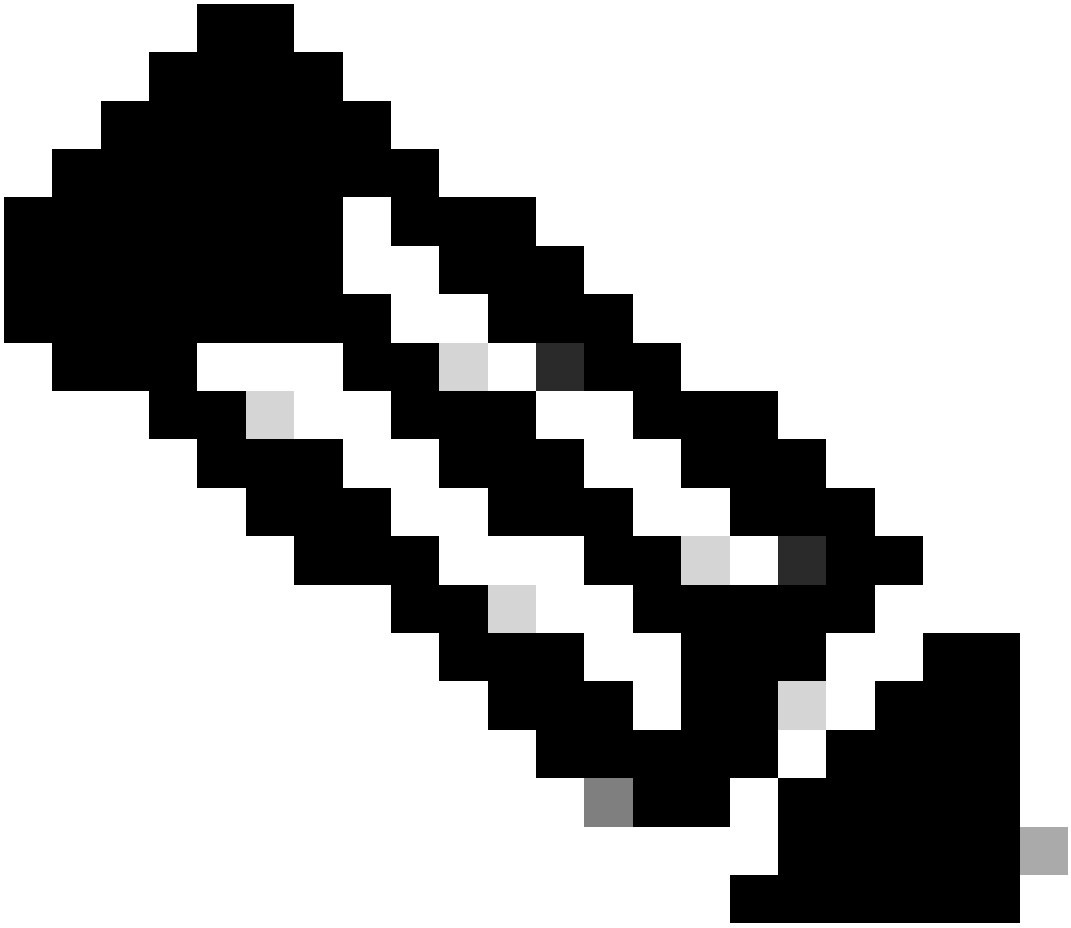
- De loopback-interface als bron toewijzen.
- De pool opgeven waaruit de spaken een IP-adres verkrijgen.

De route accept any en route set interface attributen zijn vereist omdat, zonder hen, de routes niet goed worden geadverteerd aan de spaken.

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:interface-config=ip unnumbered loopback100
cisco-av-pair = ipsec:addr-pool=RED_POOL
cisco-av-pair = ipsec:route-accept=any
cisco-av-pair = ipsec:route-set=interface
```



Geavanceerde instellingen voor kenmerken

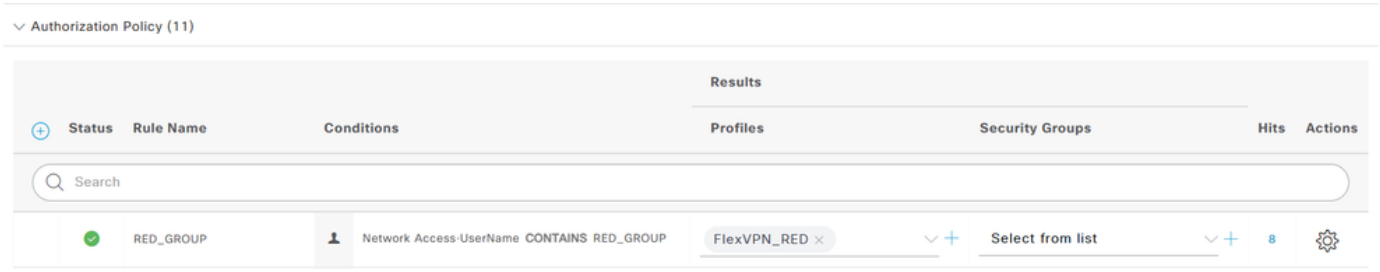


Opmerking: Raadpleeg de configuratiehandleiding van de FlexVPN RADIUS-kenmerken voor specificaties van kenmerken (naam, syntaxis, beschrijving, voorbeeld, enzovoort):

Configuratiehandleiding FlexVPN en Internet Key Exchange versie 2, Cisco IOS XE Gibraltar 16.12.x

---

h. Wijs de naam toe **authorization profile** in de kolom Profielen.



autorisatieregel

i. Klik **Save**op.

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 normale up/down-status en wordt er een Virtual-Access gemaakt voor elke Spoke die een verbinding met de Hub tot stand heeft gebracht en een up/up-status toont.

<#root>

```
FlexVPN_HUB#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.10   YES  NVRAM    up              up
GigabitEthernet2           192.168.0.10    YES  manual   up              up
Loopback100                10.100.100.1    YES  manual   up              up
Loopback200                10.200.200.1    YES  manual   up              up
Loopback1010               10.10.1.10      YES  manual   up              up
Loopback1020               10.10.2.1       YES  manual   up              up

Virtual-Access1            10.100.100.1    YES  unset    up              up


Virtual-Template2          unassigned      YES  unset    up              dow
```

Op de Spoke heeft de Tunnel-interface een IP-adres ontvangen van de pool die aan de groep is toegewezen en toont deze een up/up-status.

<#root>

```
FlexVPN_RED_SPOKE#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.20    YES  NVRAM    up              up
Loopback2                  10.20.1.10      YES  manual   up              up

Tunnel0                    172.16.10.107   YES  manual   up              up
```

- Gebruik de opdracht.**show interfaces virtual-access**

configuration

```
FlexVPN_HUB#show interfaces virtual-access 1 configuration
Virtual-Access1 is in use, but purpose is unknown
Derived configuration : 232 bytes
!
interface Virtual-Access1
 ip unnumbered Loopback100
```

```
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination dynamic
 tunnel protection ipsec profile IPSEC_FlexPROFILE
 no tunnel protection ipsec initiate
end
```

- Gebruik de opdracht **show crypto session** om te bevestigen dat de beveiligde verbinding tussen de routers tot stand is gebracht.

```
FlexVPN_HUB#show crypto session
Crypto session current status
Interface: Virtual-Access1
Profile: Flex_PROFILE
Session status: UP-ACTIVE
Peer: 192.168.10.20 port 500
  Session ID: 306
  IKEv2 SA: local 192.168.10.10/500 remote 192.168.10.20/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

- Gebruik de opdracht show ip eigrp neighbors om te bevestigen dat de EIGRP-nabijheid is vastgesteld met de andere site.

```
FlexVPN_HUB#show ip eigrp neighbors
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)
H   Address                 Interface              Hold Uptime     SRTT   RTO   Q   Seq
                                                   (sec)           (ms)       Cnt  Num
0   172.16.10.107           Vi1                      10 00:14:00      8  1494   0   31
```

- Gebruik de opdracht show ip route om te controleren of de routes naar de Spokes zijn geduwd.
  - De route voor 10.20.1.10, loopback-interface op de spaak is door de hub geleerd door EIGRP en is toegankelijk via de virtuele toegang


```
FlexVPN_HUB#show ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
C        10.10.1.10 is directly connected, Loopback1010
C        10.10.2.10 is directly connected, Loopback1020

D        10.20.1.10 [90/79360000] via 172.16.10.107, 00:24:42, Virtual-Access1
```

```
C        10.100.100.1 is directly connected, Loopback100
C        10.200.200.1 is directly connected, Loopback200
      172.16.0.0/32 is subnetted, 1 subnets
S        172.16.10.107 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, GigabitEthernet2
L        192.168.0.10/32 is directly connected, GigabitEthernet2
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.10/32 is directly connected, GigabitEthernet1
```

- De routes voor 10.10.1.10 en 10.10.2.10 werden aangeleerd via EIGRP en zijn bereikbaar via de bron-IP van de RED_GROUP (10.100.100.1), die toegankelijk is via Tunnel0.

<#root>

```
FlexVPN_RED_SPOKE#sh ip route
<<<<< Output Ommitted >>>>>

Gateway of last resort is 192.168.10.1 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 192.168.10.1
      10.0.0.0/32 is subnetted, 5 subnets
D        10.10.1.10 [90/26880032] via 10.100.100.1, 00:00:00


D        10.10.2.10 [90/26880032] via 10.100.100.1, 00:00:00


C        10.20.1.10 is directly connected, Loopback2
S        10.100.100.1 is directly connected, Tunnel0


D        10.200.200.1 [90/26880032] via 10.100.100.1, 00:00:00


      172.16.0.0/32 is subnetted, 1 subnets
C        172.16.10.107 is directly connected, Tunnel0
      192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet1
L        192.168.10.20/32 is directly connected, GigabitEthernet1
```

Problemen oplossen

In dit gedeelte vindt u informatie die u kunt gebruiken om dit type implementatie op te lossen. 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

AAA- en RADIUS-debugs kunnen helpen bij het oplossen van problemen met de autorisatie van de Spokes.

debug aaa authentication
debug aaa authorization
debug aaa protocol radius
debug radius authentication

Working Scenario

Dit logboek toont het autorisatieproces en de toewijzing van de parameters.

```
     <#root>


RADIUS(OOOOO1A7): Received from id 1645/106
AAA/BIND(OOOOO1A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(OOOOO1A8):Orig. component type = VPN IPSEC



RADIUS(000001A8): Config NAS IP: 192.168.0.10



vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(OOOOO1A8): Config NAS IPv6: ::
RADIUS/ENCODE(OOOOO1A8): acct_session_id: 4414
RADIUS(OOOOO1A8): sending
RADIUS(OOOOO1A8): Send Access-Request to 192.168.0.5:1645 id 1645/107, len 138
RADIUS:  authenticator 7A B5 97 50 F2 6E F0 09 - 3D B0 54 B4 1A DB BA BA



RADIUS:  User-Name           [1]   11  "RED_GROUP"
```

```
RADIUS:  User-Password       [2]   18  *

RADIUS:  Calling-Station-Id  [31]  14  "192.168.10.20"

RADIUS:  Vendor, Cisco       [26]  63

RADIUS:   Cisco AVpair       [1]   57  "audit-session-id=L2L496130A2ZP2L496130A21ZI1F401F4ZM134"

RADIUS:  Service-Type        [6]   6   Outbound                 [5]

RADIUS:  NAS-IP-Address      [4]   6   192.168.0.10
```

```
RADIUS(000001A8): Sending a IPv4 Radius Packet


RADIUS(000001A8): Started 5 sec timeout


RADIUS: Received from id 1645/107 192.168.0.5:1645, Access-Accept, len 248


RADIUS:  authenticator BE F4 FC FF 7C 41 97 A7 - 3F 02 A7 A3 A1 96 91 38
RADIUS:  User-Name           [1]   11  "RED_GROUP"
RADIUS:  Class               [25]  69
RADIUS:   43 41 43 53 3A 4C 32 4C 34 39 36 31 33 30 41 32  [CACS:L2L496130A2]
RADIUS:   5A 50 32 4C 34 39 36 31 33 30 41 32 31 5A 49 31  [ZP2L496130A21ZI1]
RADIUS:   46 34 30 31 46 34 5A 4D 31 33 34 3A 49 53 45 42  [F401F4ZM134:ISEB]
RADIUS:   75 72 67 6F 73 2F 35 33 34 36 34 30 33 32 39 2F  [urgos/534640329/]
RADIUS:   32 39 31               [ 291]


RADIUS:  Vendor, Cisco       [26]  53


RADIUS:   Cisco AVpair       [1]   47  "ip:interface-config=ip unnumbered loopback100"


RADIUS:  Vendor, Cisco       [26]  32


RADIUS:   Cisco AVpair       [1]   26  "ipsec:addr-pool=RED_POOL"
```

```
RADIUS:  Vendor, Cisco       [26]  33

RADIUS:   Cisco AVpair       [1]   27  "ipsec:route-set=interface"

RADIUS:  Vendor, Cisco       [26]  30

RADIUS:   Cisco AVpair       [1]   24  "ipsec:route-accept=any"

RADIUS(000001A8): Received from id 1645/107
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to down
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001A9): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console
AAA/BIND(000001AA): Bind i/f
INFO: AAA/AUTHOR: Processing PerUser AV interface-config
%SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as console

%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up

AAA/BIND(000001AB): Bind i/f
RADIUS/ENCODE(000001AB):Orig. component type = VPN IPSEC
```

```
RADIUS(000001AB): Config NAS IP: 192.168.0.10
vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(000001AB): Config NAS IPv6: ::
RADIUS(000001AB): Sending a IPv4 Radius Packet
RADIUS(000001AB): Started 5 sec timeout
RADIUS: Received from id 1646/23 192.168.0.5:1646, Accounting-response, len 20



%DUAL-5-NBRCHANGE: EIGRP-IPv4 10: Neighbor 172.16.10.109 (Virtual-Access1) is up: new adjacency
```

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.