Configuration de FlexVPN avec intégration ISE

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configurer

- Diagramme du réseau
- Étape 1 : Configuration du concentrateur
- Étape 2 : Configuration du rayon
- Étape 3 : Configuration ISE
  - Étape 3.1 : Créer des utilisateurs, des groupes et ajouter un périphérique réseau
  - Étape 3.2 : Configurer le jeu de stratégies
  - Étape 3.3 : Configurer la stratégie d'autorisation

Vérifier

Dépannage

- Scénario de travail

Introduction

Ce document décrit comment configurer FlexVPN à l'aide de Cisco Identity Services Engine (ISE) pour attribuer dynamiquement des configurations aux rayons.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine (ISE)
- protocole RADIUS
- Flex Virtual Private Network (FlexVPN)

Composants utilisés

Ce document est basé sur les versions logicielles et matérielles suivantes :

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

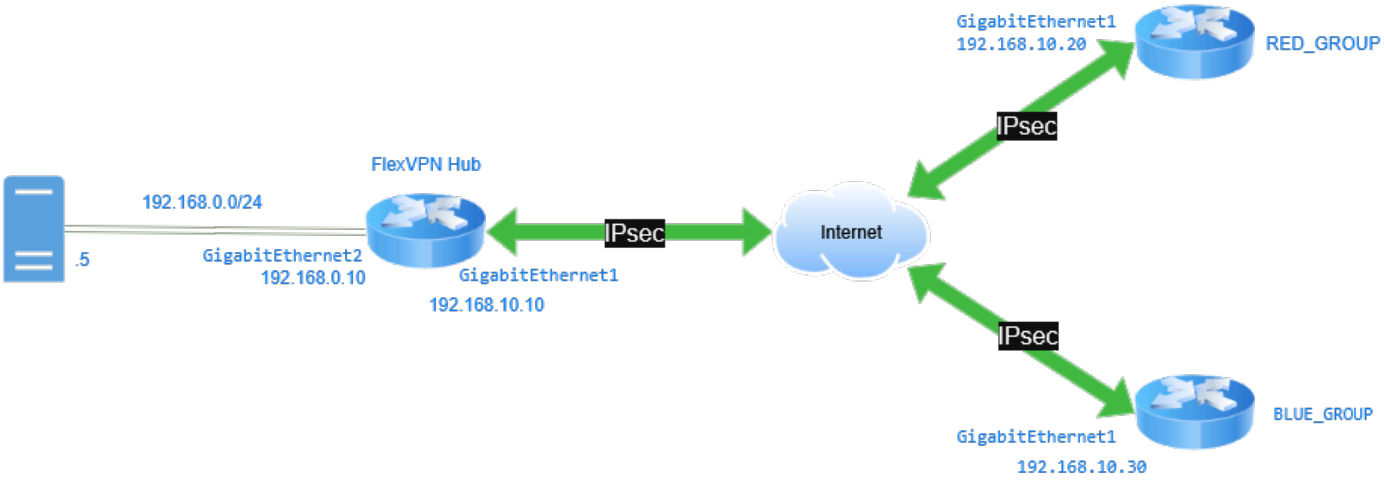
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau

est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Diagramme du réseau

FlexVPN peut établir une connexion avec des rayons et attribuer certaines configurations qui permettent la communication et la gestion du trafic. Référencé dans le schéma, ceci montre comment FlexVPN s'intègre avec ISE de sorte que, quand un rayon se connecte au HUB, les paramètres de la source du tunnel et du pool DHCP sont assignés selon le groupe ou la branche à laquelle le rayon appartient. Il utilise le certificat pour authentifier les rayons, puis ISE avec Radius comme serveur d'autorisation et de comptabilité.



FlexVPN avec intégration ISE

Étape 1 : Configuration du concentrateur

a. Configurez un trustpoint pour stocker le certificat du routeur. Les certificats sont utilisés pour authentifier les rayons.

```
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. Configurez un **certificate map**. L'objectif de l' certificate map est d'identifier et de faire correspondre les certificats en fonction des informations spécifiées, au cas où le routeur aurait plusieurs certificats installés.

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

c. Configurez unRADIUS serverpour l'autorisation et la comptabilité sur le périphérique :

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

d. Définissez le **RADIUS server group** avec son adresse IP, ses ports de communication, sa clé partagée et son interface source pour le trafic RADIUS.

```
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. Configurez le **loopback interfaces**. Les loopback interfaces sont utilisés comme connexion source pour le tunnel et sont affectés dynamiquement en fonction du groupe connecté.

```
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
```

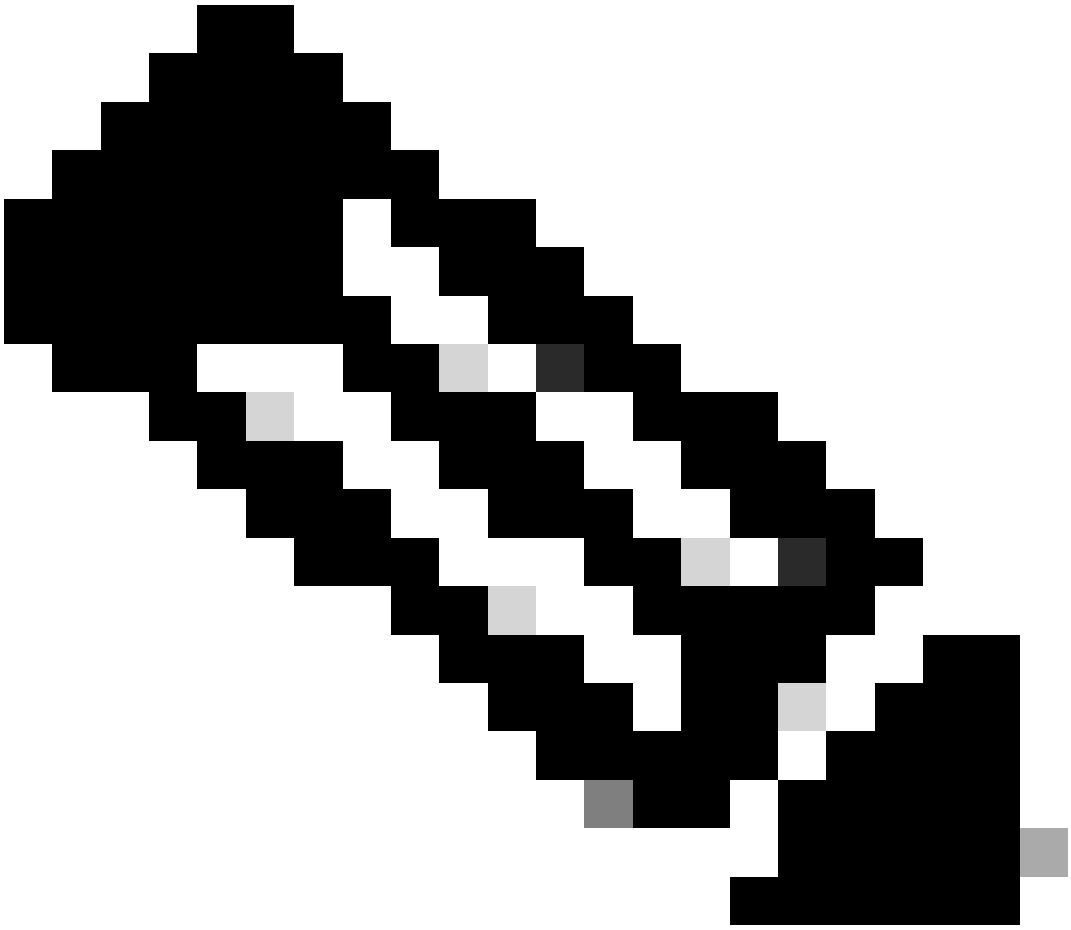
f. Définissez un **IP local pool** pour chaque groupe.

```
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. Configurez EIGRP et annoncez les réseaux de chaque groupe.

```
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
```



> Remarque : FlexVPN prend en charge les protocoles de routage dynamique tels que OSPF, EIGRP et BGP sur les tunnels VPN. Dans ce guide, le protocole EIGRP est utilisé.

---

h. Configurez le **crypto ikev2 name mangler**. Le IKEv2 name mangler est utilisé pour dériver le nom d'utilisateur pour l'autorisation IKEv2. Dans ce cas, il est configuré pour utiliser les informations Organization-Unit des certificats sur les rayons comme nom d'utilisateur pour l'autorisation.

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

i. Configurez le **IKEv2 profile**. Les certificate map, AAA server groupet les name mangler sont référencés dans le profil IKEv2.

Dans ce scénario spécifique, les authentifications locale et distante sont configurées comme **RSA-SIG**.

Un compte d'utilisateur local doit être créé sur le RADIUS server avec un nom d'utilisateur qui correspond à la valeur et au motorganization-unitde passeCisco1234(comme spécifié dans la configuration ci-dessous).

```
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. Configurez leIPsec profileet référencez le IKEv2 profile.

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

k. Créez le virtual-template. Il permet de créer un virtual-access interface et de lier le IPsec profile créé.

Définissez le **virtual-template** sans adresse IP, car il est attribué par le RADIUS server.

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

Configurez deuxloopbackspour simuler un réseau interne.

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

```
interface Loopback1020
ip address 10.10.2.10 255.255.255.255
```

Étape 2 : Configuration du rayon

a. Configurez untrustpointpour stocker le certificat du routeur en étoile.

```
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. Configurez uncertificate map. L'objectif de l' certificate map est d'identifier et de faire correspondre les certificats en fonction des informations spécifiées, au cas où le routeur aurait plusieurs certificats installés.

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

c. Configurez le réseau d'autorisation local AAA.

La commande aaa authorization network est utilisée pour autoriser les demandes d'accès liées aux services réseau. Elle consiste à vérifier si un utilisateur est autorisé à accéder au service demandé après avoir été authentifié.

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

d. Configurez leIKEv2 profile. Les autorisations certificate map et AAA locales sont référencées dans le IKEv2 profile.

Les authentifications locale et distante sont configurées en tant que **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. Configurez leIPsec profileet référencez le IKEv2 profile.

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

f. Configurez letunnel interface. Le tunnel interface est configuré pour recevoir une adresse IP de tunnel du concentrateur en fonction des résultats d'autorisation.

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

g. Configurez le protocole EIGRP, annonçant le réseau local du rayon et du tunnel interfacesatellite.

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

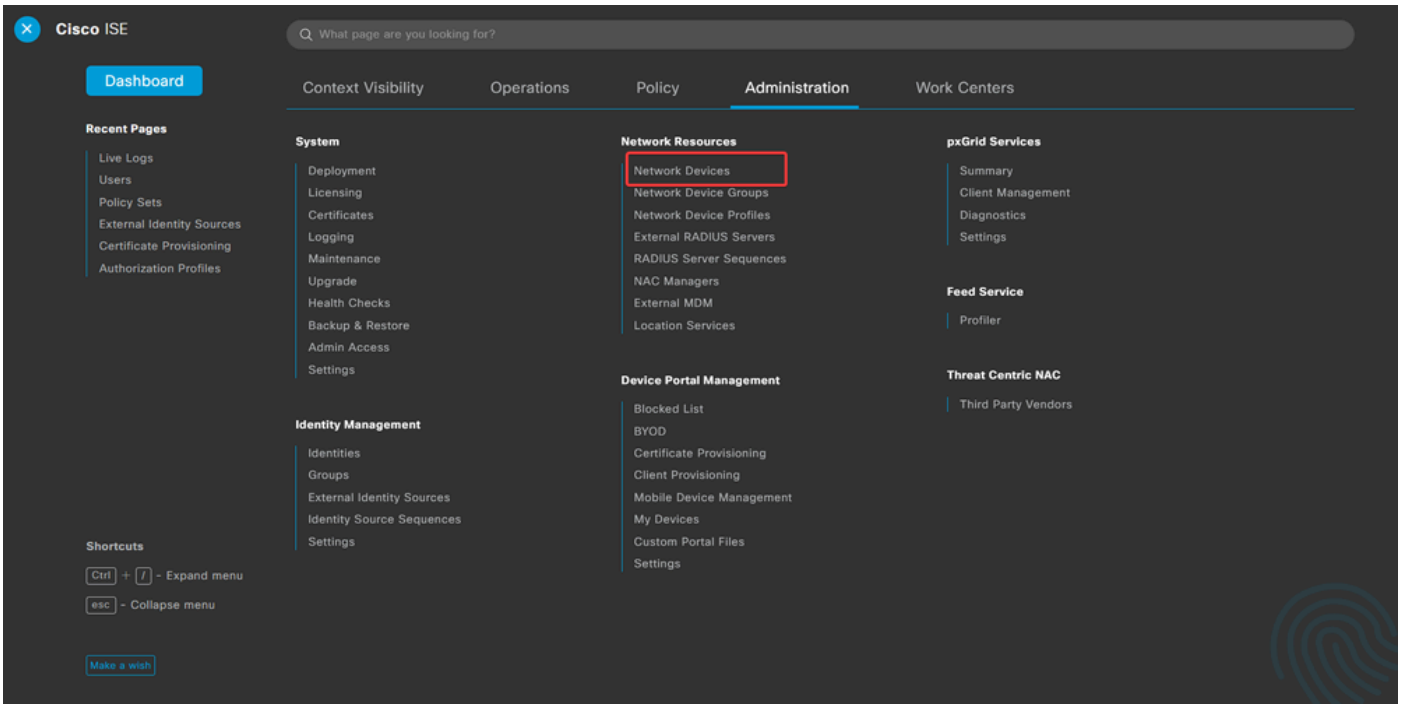
Configurez unloopbackpour simuler un réseau interne.

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

Étape 3 : Configuration ISE

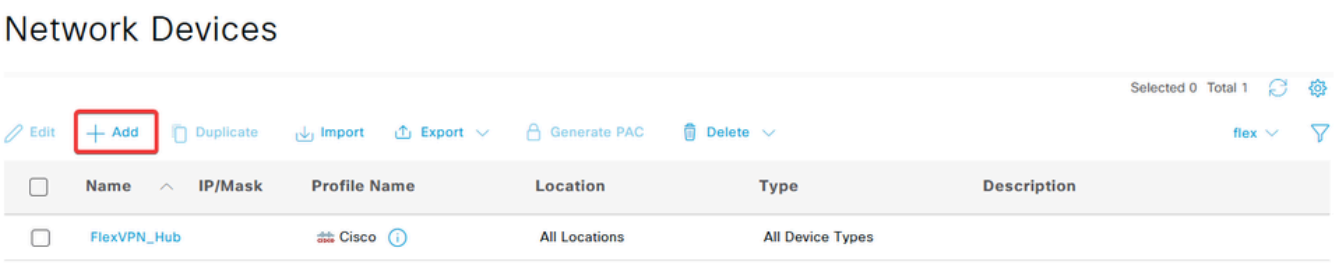
Étape 3.1 : Créer des utilisateurs, des groupes et ajouter un périphérique réseau

a. Connectez-vous au serveur ISE et accédez à **Administration** > **Network Resources** > **Network Devices**.



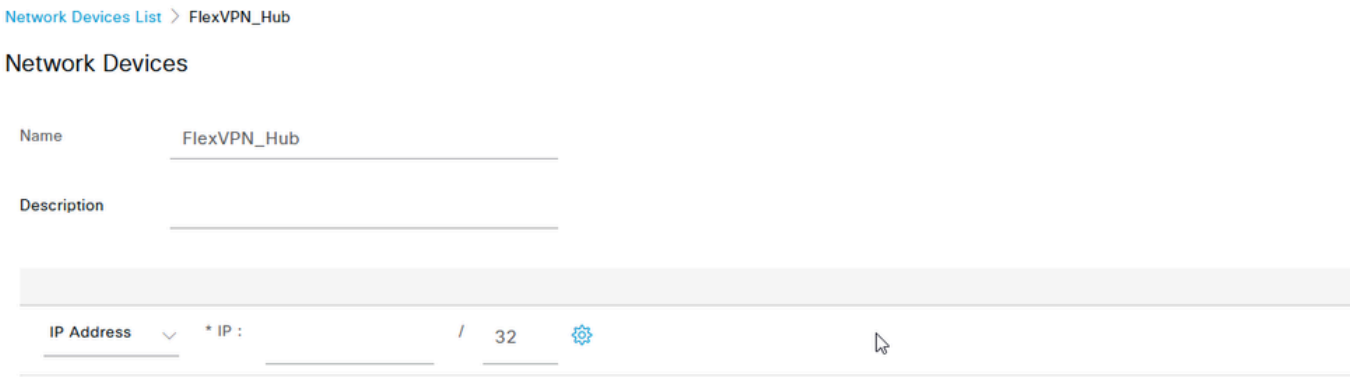
Administration-Ressources réseau-Périphériques réseau

b. Cliquez **Add** pour configurer le concentrateur FlexVPN en tant que client AAA.

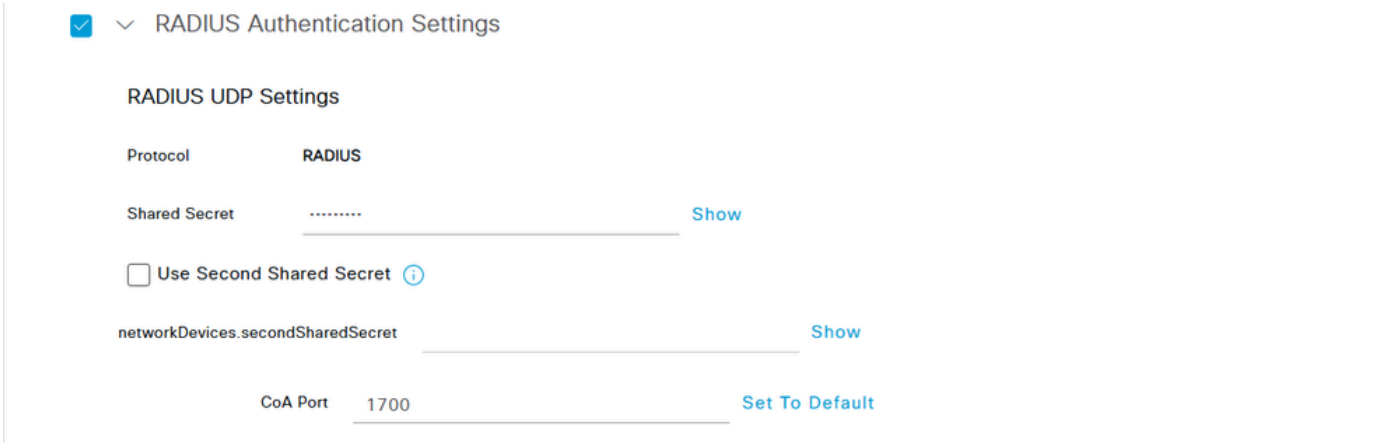


Ajouter un routeur FlexVPN en tant que client AAA

c. Entrez les champs Nom du périphérique réseau et Adresse IP, puis cochez la **RADIUS Authentication Settings** case et ajoutez **Shared Secret**. Le mot de passe secret partagé doit être le même que celui qui a été utilisé lors de la création du groupe de serveurs RADIUS sur le concentrateur FlexVPN. Cliquez surSave.

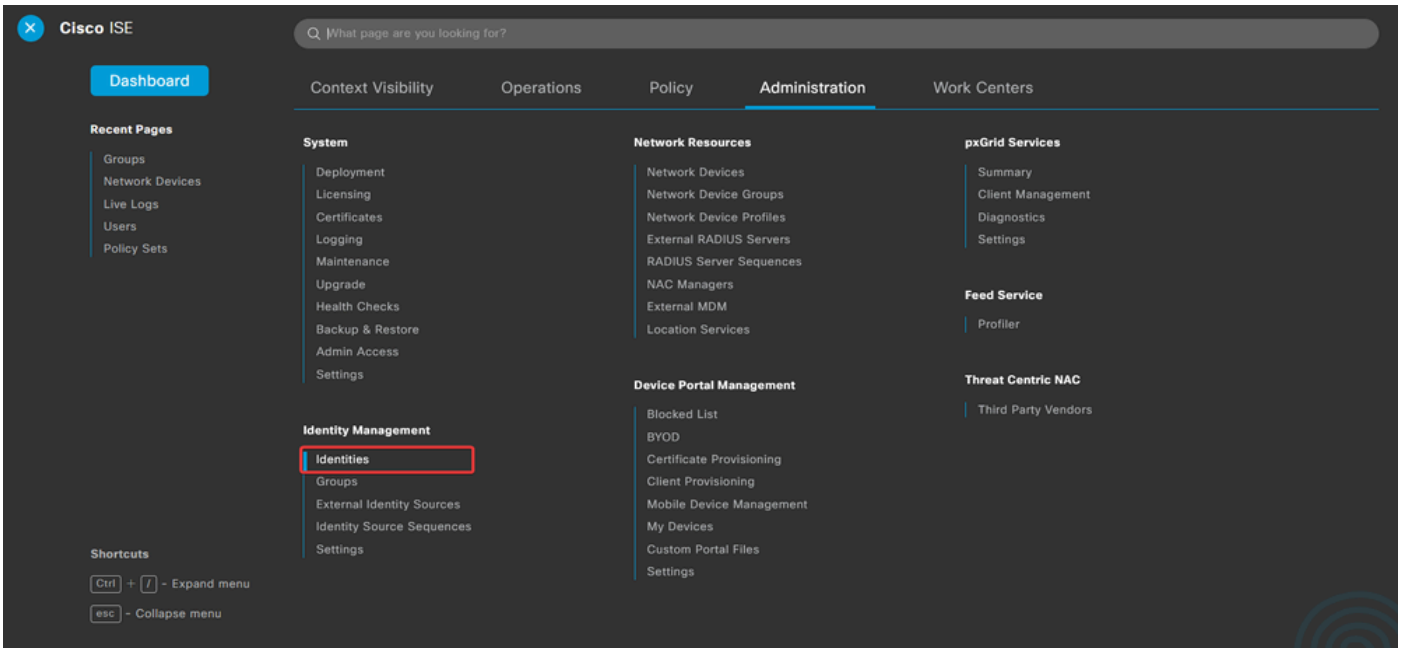


Adresse IP du périphérique réseau



Clé partagée du périphérique réseau

d. Accédez à **Administration** > **Identity Management** > **Identities**.

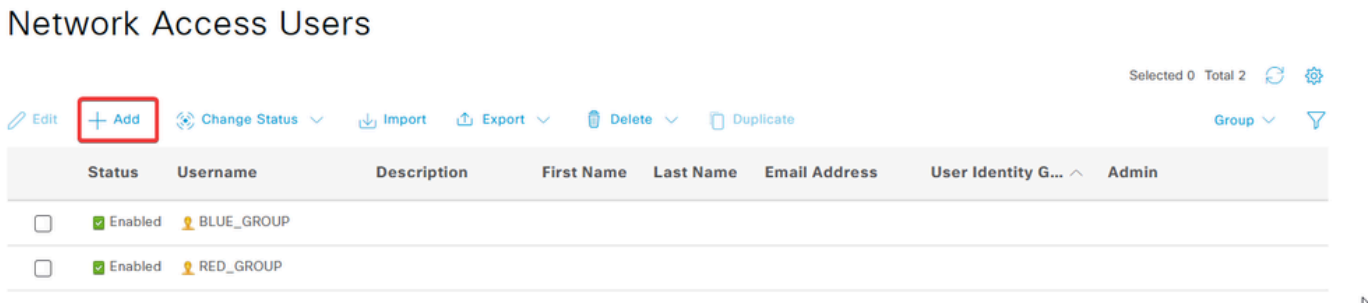


Administration-Identifier la gestion-Identifie

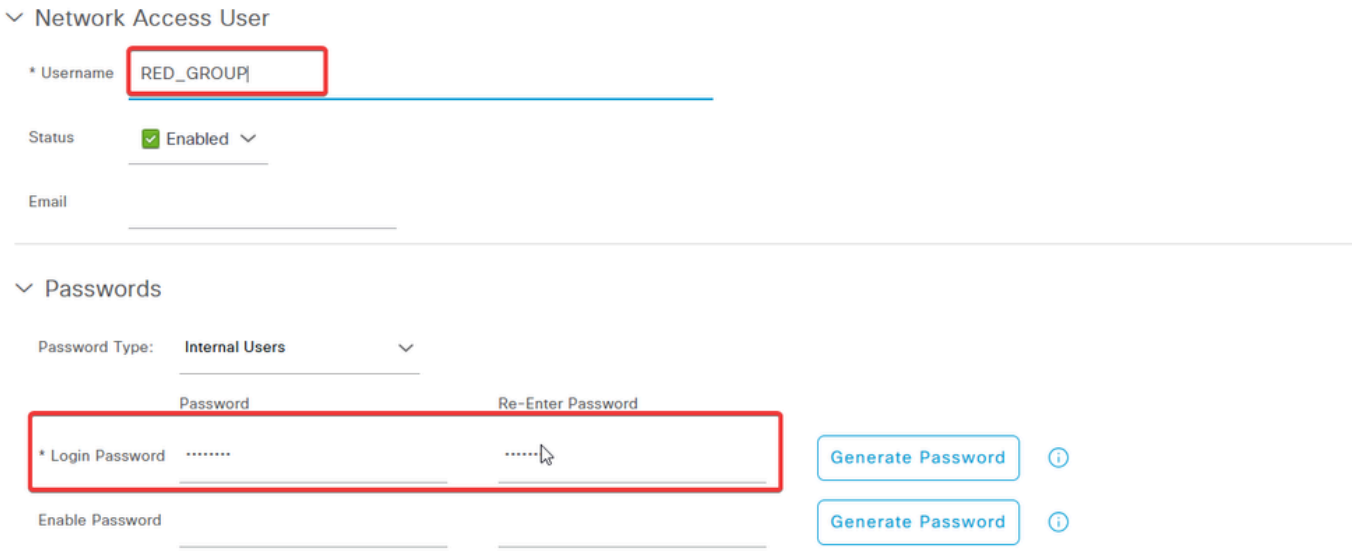
e. Cliquez surAddafin de créer un nouvel utilisateur dans la base de données locale du serveur.

Saisissez lesUsernameet **Login Password**. Le nom d'utilisateur est le même que celui que les certificats ont sur la valeur d'unité d'organisation sur le certificat et le mot de passe de connexion doit être le même que celui spécifié sur le profil IKev2.

Cliquez sur **Save**.



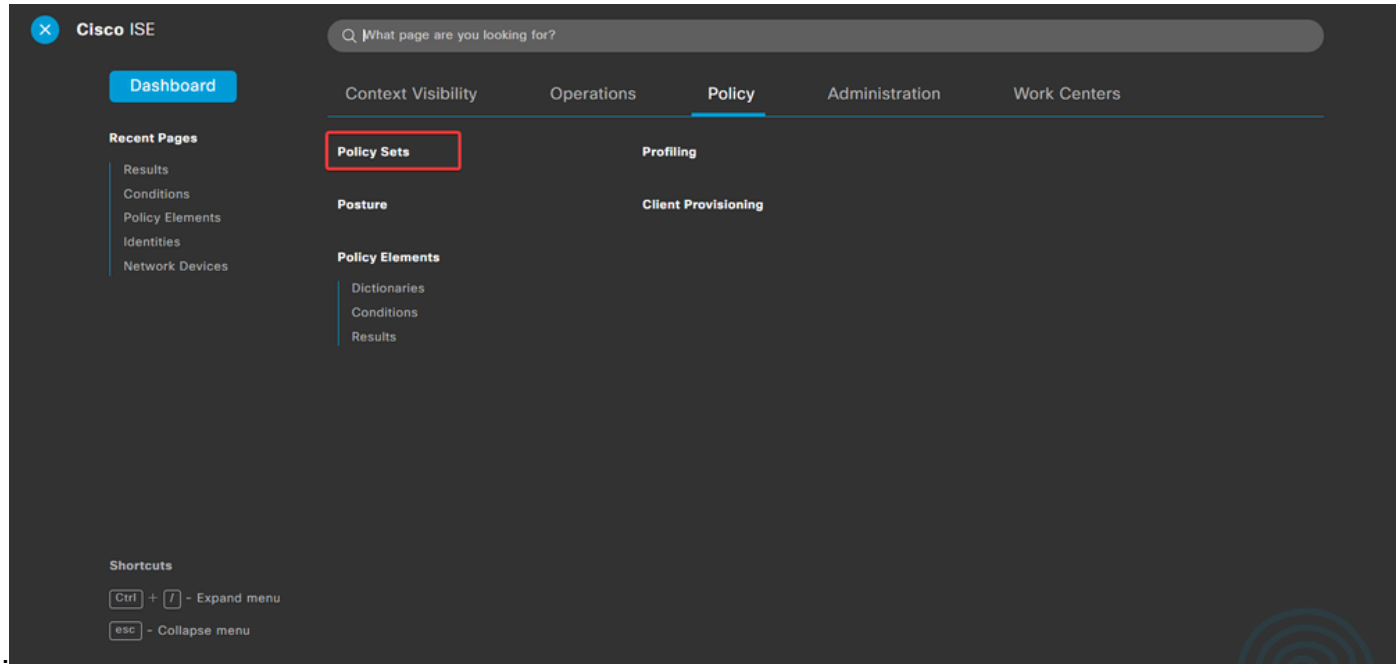
Administration-Identifier la gestion-Identifie



Groupe créé identique à la valeur unitaire de l'organisation

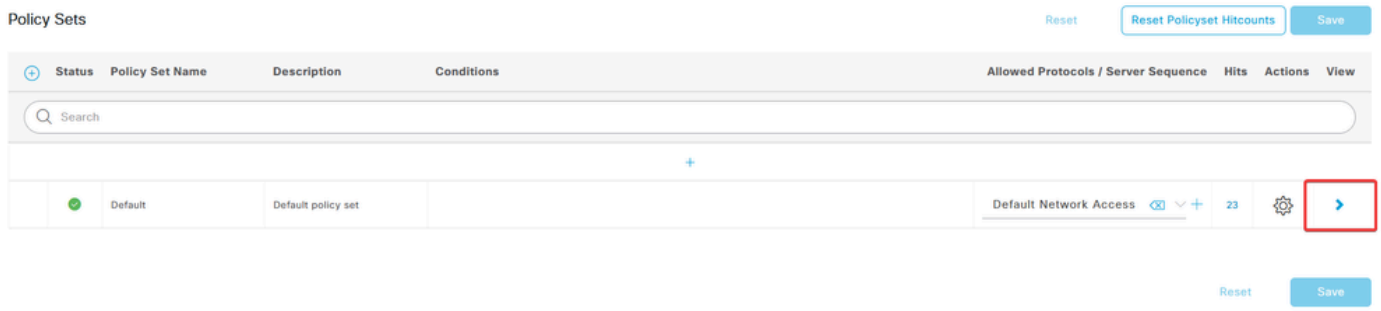
Étape 3.2 : Configurer le jeu de stratégies

a. Accédez à **Policy** > **Policy Sets**.



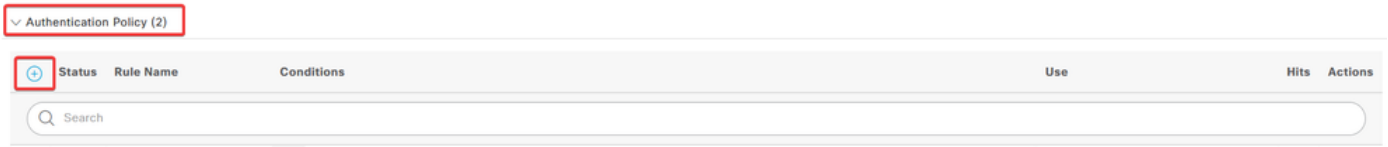
Ensembles de stratégies-stratégies

b. Sélectionnez la stratégie d'autorisation par défaut en cliquant sur la flèche à droite de l'écran :



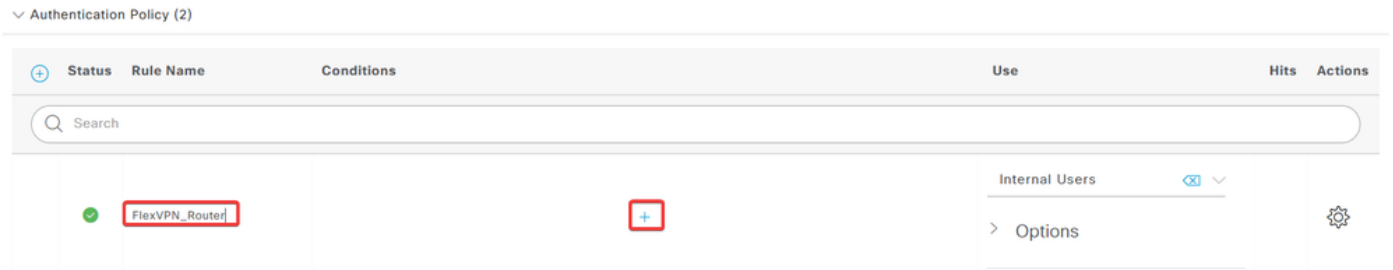
Modifier la stratégie par défaut

c. Cliquez sur la flèche du menu déroulant en regard de pour`Authentication Policy`la développer. Cliquez ensuite sur l'**add (+)**icône afin d'ajouter une nouvelle règle.



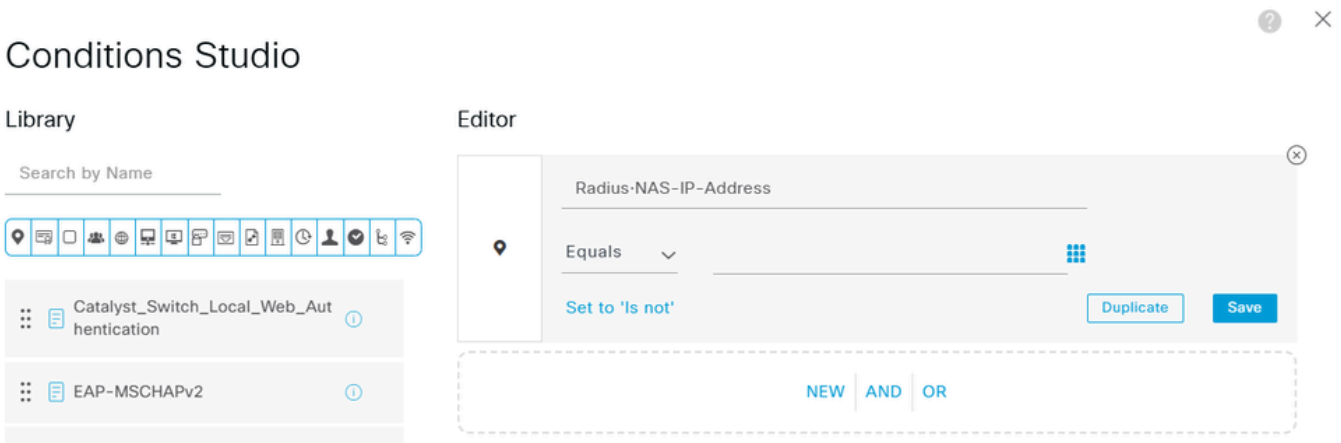
Ajouter une stratégie d'authentification

d. Entrez le nom de la règle et sélectionnez l'icône`add (+)`dans la colonne Conditions.

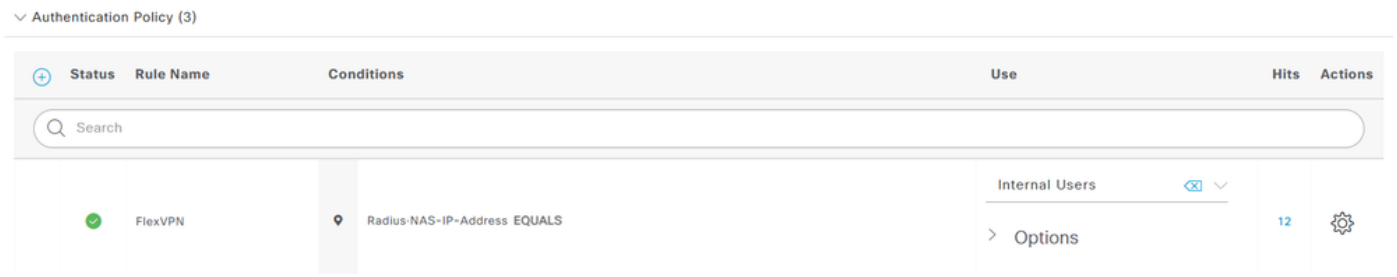


Créer une stratégie d'authentification

e. Cliquez sur la zone de texte Éditeur d'attributs et cliquez sur l'`NAS-IP-Address`icône. Saisissez l'adresse IP (192.168.0.10) du concentrateur FlexVPN.



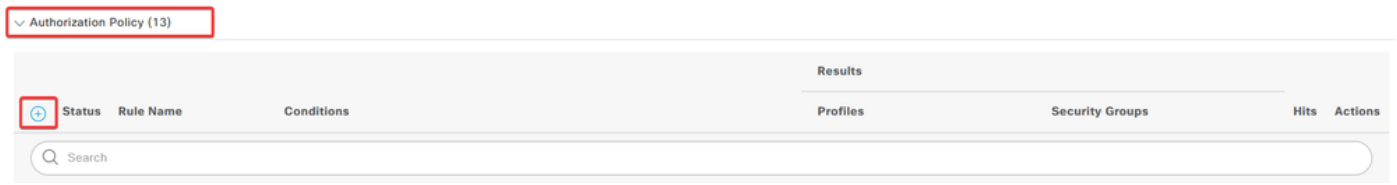
Authenticate FlexVPN Hub



Stratégie d'authentification

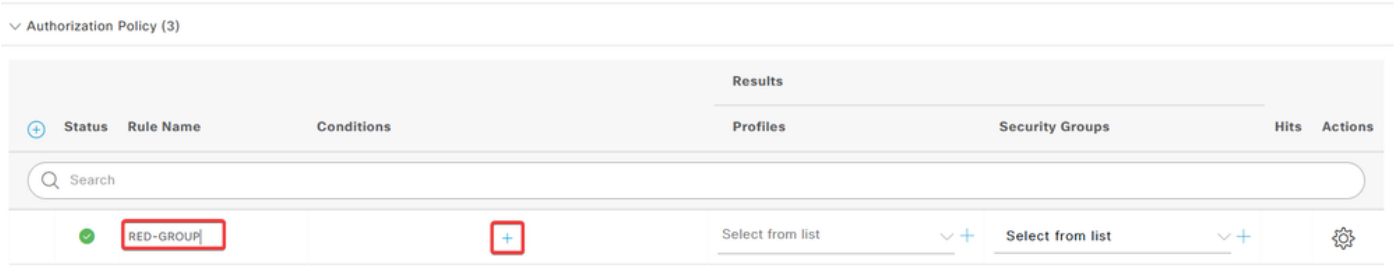
Étape 3.3 : Configurer la stratégie d'autorisation

a. Cliquez sur la flèche du menu déroulant en regard de Authorization Policy pour la développer. Cliquez ensuite sur l'**add (+)** icône afin d'ajouter une nouvelle règle.



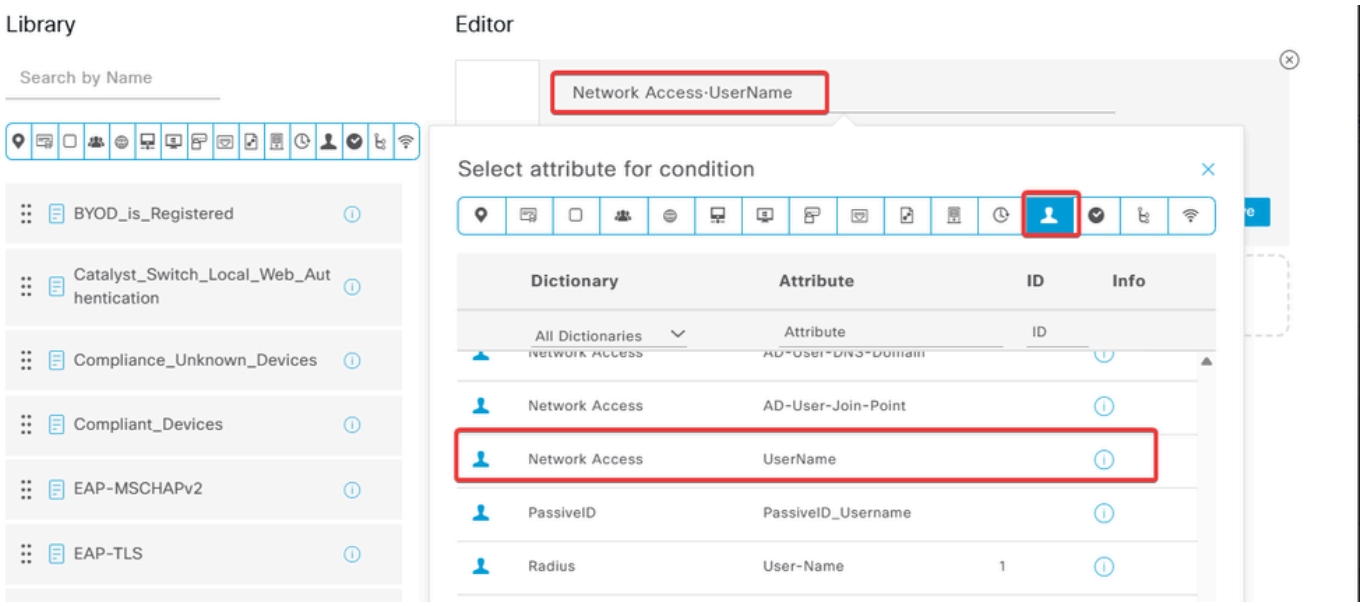
Créer une nouvelle stratégie d'autorisation

b. Entrez le nom de la règle et sélectionnez l'**add (+)** icône dans la colonne Conditions.



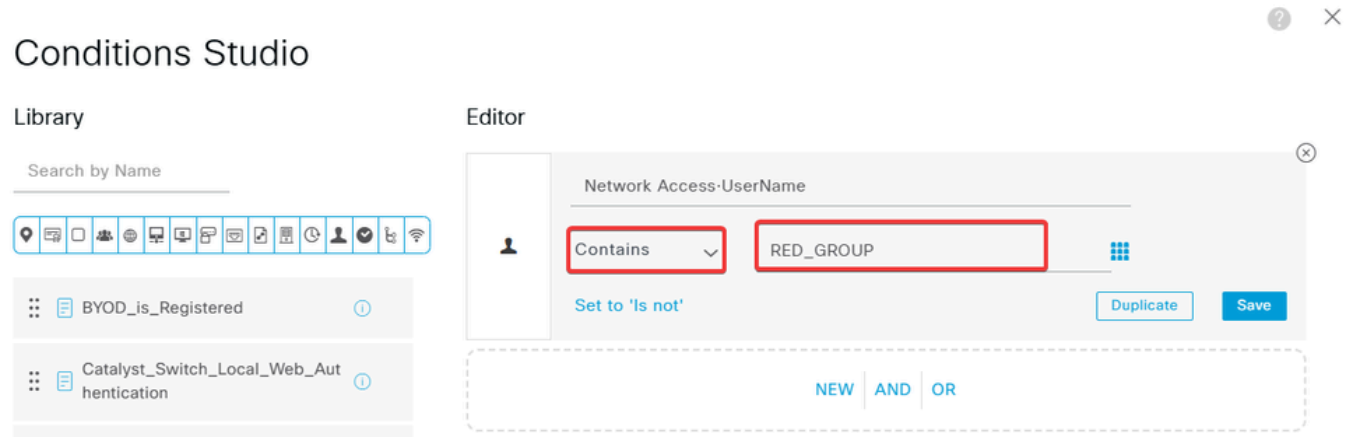
Créer une règle

c. Cliquez sur la zone de texte Éditeur d'attributs et cliquez sur l'Subject icône. Sélectionnez l'**Network Access - UserName** attribut.



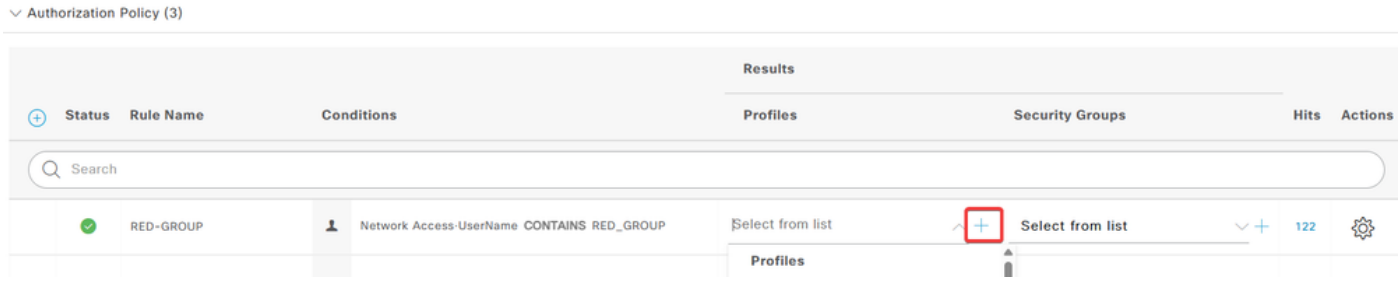
Sélectionnez Accès réseau - NomUtilisateur

d. Sélectionnez`Contains`l'opérateur, puis ajoutez la valeur Unité d'organisation des certificats.



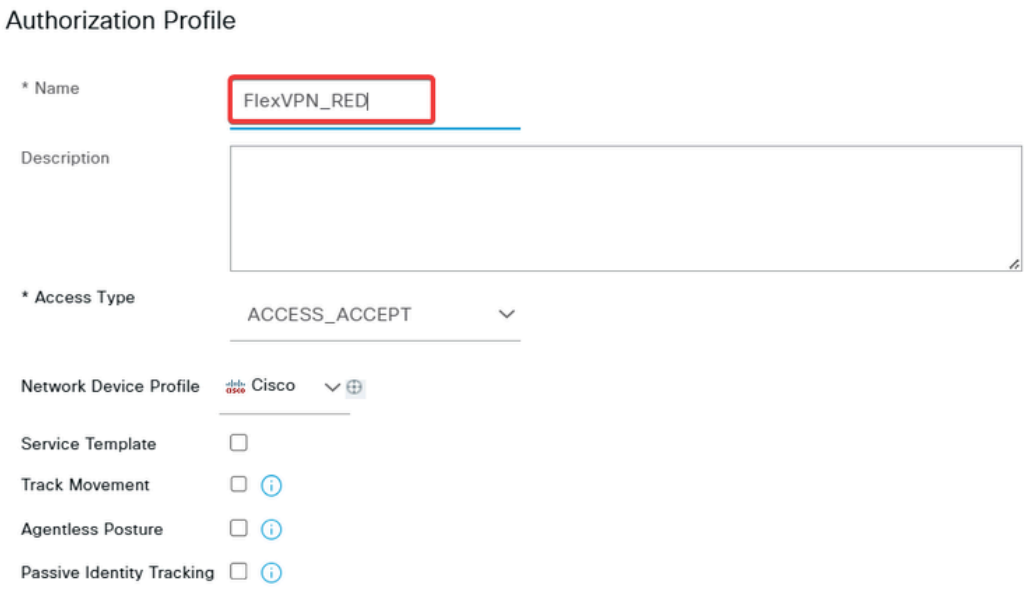
Ajouter un nom de groupe

e. Dans la colonne Profiles, cliquez sur l'`add (+)`icône et choisissez **Create a New Authorization Profile**.



Ajouter un nouveau profil d'autorisation

f. Saisissez le profil **Name**.



Nommer le profil d'autorisation

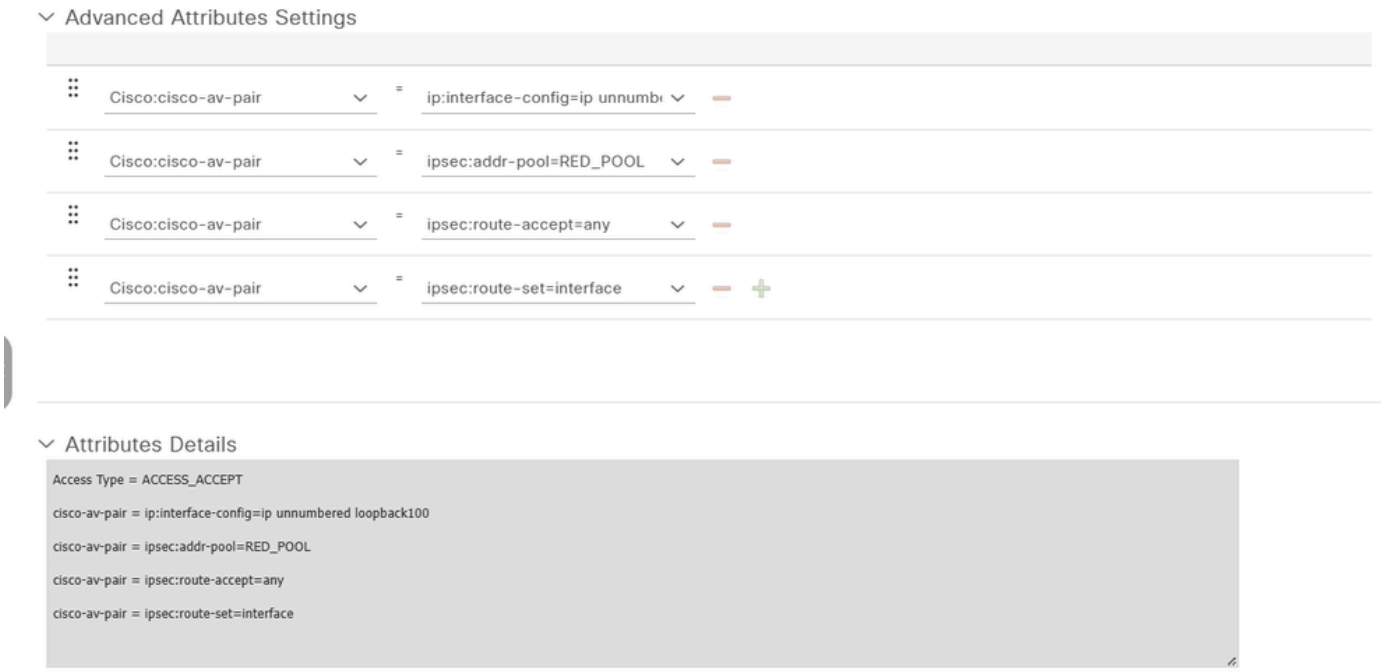
g. Accédez à **Advanced Attributes Settings**. Ensuite, sélectionnez l'cisco-av-pairattribut dans le menu déroulant sur le côté gauche, et ajoutez l'attribut qui est affecté à l'étoile FlexVPN en fonction du groupe.

Les attributs à affecter à cet exemple sont les suivants :

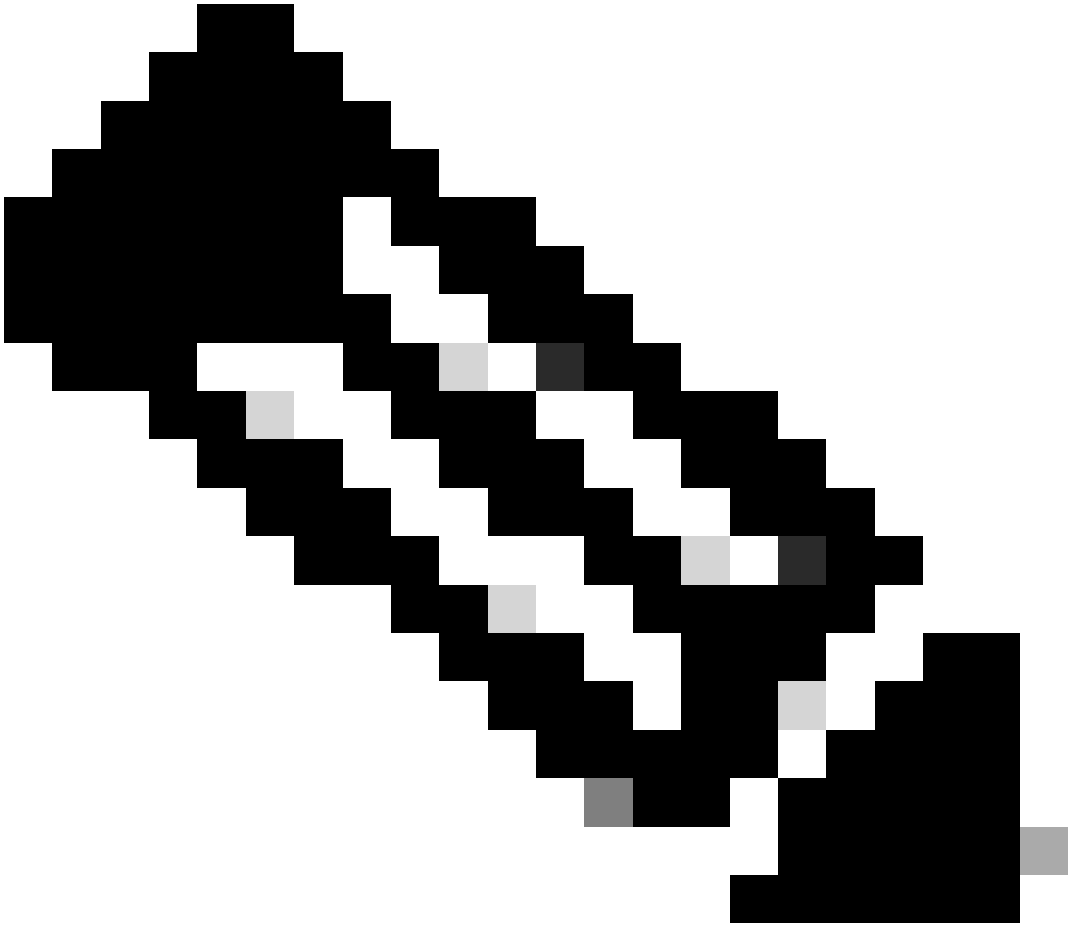
- Attribution de l'interface de bouclage comme source.
- Spécification du pool à partir duquel les rayons obtiennent une adresse IP.

Les route accept any attributs et route set interface sont requis car, sans eux, les routes ne sont pas annoncées correctement aux rayons.

```
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
```



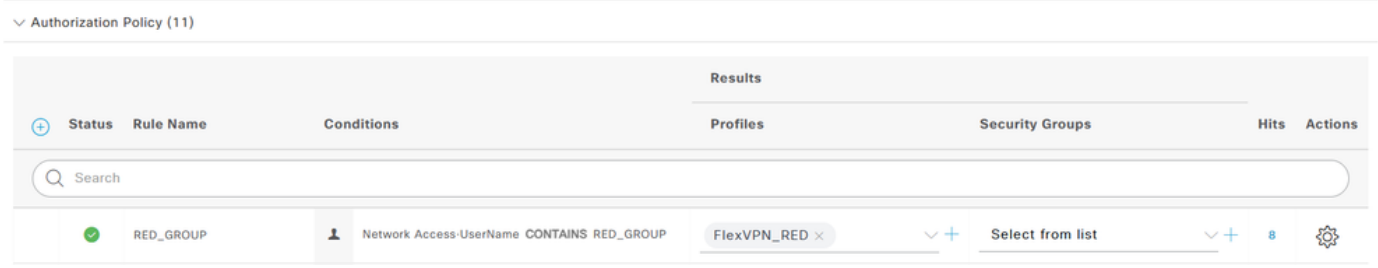
Paramètres d'attributs avancés



Remarque : Pour connaître les spécifications d'attribut (nom, syntaxe, description, exemple, etc.), consultez le guide de configuration des attributs RADIUS FlexVPN :

Guide de configuration FlexVPN et Internet Key Exchange version 2, Cisco IOS XE Gibraltar 16.12.x

h. Attribuez le **authorization profile** dans la colonne des profils.



Règle D'Autorisation

i. Cliquez sur **Save**.

Vérifier

- Utilisez la commande **show ip interface brief** pour vérifier l'état du tunnel, du modèle virtuel et de l'accès virtuel.

Sur le concentrateur, le modèle virtuel a un état up/down qui est normal, et un accès virtuel est créé pour chaque satellite qui a établi une connexion avec le concentrateur et affiche un état up/up.

<#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
```

Sur le satellite, l'interface du tunnel a reçu une adresse IP du pool attribué au groupe et affiche un état up/up.

<#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
```

- Utilisez la commande.**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
```

- Utilisez la commande **show crypto session** pour confirmer que la connexion sécurisée entre les routeurs est établie.

```
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
```

- Utilisez la commande show ip eigrp neighbors pour confirmer que la contiguïté EIGRP est établie avec l'autre 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
```

- Utilisez la commande show ip route pour vérifier que les routes ont été transmises aux rayons.
  - La route pour l'interface de bouclage 10.20.1.10 sur le rayon a été apprise par le concentrateur par EIGRP et elle est accessible via l'accès virtuel


```
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
```

- Les routes pour 10.10.1.10 et 10.10.2.10 ont été apprises via EIGRP et sont accessibles via l'IP source de RED_GROUP (10.100.100.1), qui est accessible 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner ce type de déploiement. Utilisez ces commandes pour déboguer le processus de négociation de tunnel :

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

Les débogages AAA et RADIUS peuvent aider au dépannage de l'autorisation des rayons.

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

Working Scenario

Ce journal indique le processus d'autorisation et l'attribution des paramètres.

```
     <#root>


RADIUS(000001A7): Received from id 1645/106
AAA/BIND(000001A8): Bind i/f
AAA/AUTHOR (0x1A8): Pick method list 'FLEX'
RADIUS/ENCODE(000001A8):Orig. component type = VPN IPSEC



RADIUS(000001A8): Config NAS IP: 192.168.0.10



vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(000001A8): Config NAS IPv6: ::
RADIUS/ENCODE(000001A8): acct_session_id: 4414
RADIUS(000001A8): sending
RADIUS(000001A8): 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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.