Konfiguration von FlexVPN mit ISE-Integration

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie FlexVPN mithilfe der Cisco Identity Services Engine (ISE) konfiguriert wird, um Stationen dynamisch Konfigurationen zuzuweisen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine (ISE)
- RADIUS-Protokoll
- Flex Virtual Private Network (FlexVPN)

Verwendete Komponenten

Dieses Dokument basiert auf den folgenden Software- und Hardwareversionen:

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

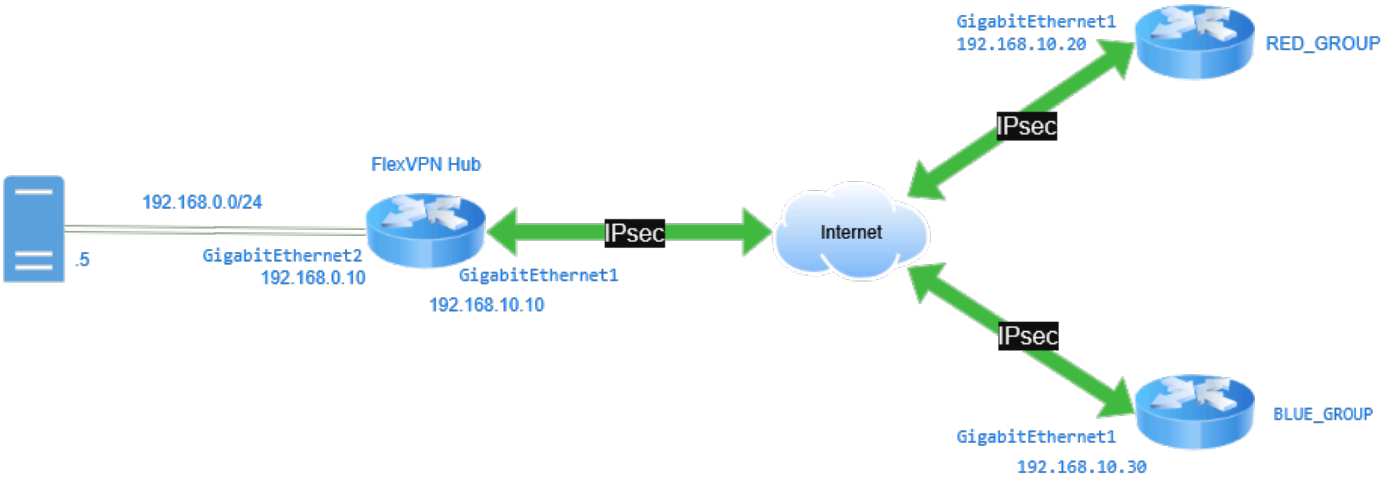
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm

FlexVPN kann eine Verbindung mit Stationen herstellen und bestimmte Konfigurationen zuweisen, die die Kommunikation und das Datenverkehrsmanagement ermöglichen. In dem Diagramm wird gezeigt, wie FlexVPN mit ISE integriert wird, sodass bei einer Verbindung einer Spoke mit dem HUB die Parameter der Tunnelquelle und des DHCP-Pools abhängig von der Gruppe oder dem Zweig zugewiesen werden, zu der die Spoke gehört. Es verwendet das Zertifikat, um die Stationen zu authentifizieren, dann ISE mit Radius als Autorisierungs- und Accounting-Server.



FlexVPN mit ISE-Integration

Schritt 1: Hub-Konfiguration

antwort: Konfigurieren Sie eine trustpoint, um das Router-Zertifikat zu speichern. Zertifikate werden verwendet, um die Stationen zu authentifizieren.

```
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. Konfigurieren eines **certificate map**. Der Zweck des certificate map besteht darin, Zertifikate anhand der angegebenen Informationen zu identifizieren und abzugleichen, falls auf dem Router mehrere Zertifikate installiert sind.

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

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

c. Konfigurieren Sie einer RADIUS server für Autorisierung und Abrechnung auf dem Gerät:

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

d. Definieren Sie die **RADIUS server group** mit ihrer IP-Adresse, ihren Kommunikations-Ports, ihrem gemeinsamen Schlüssel und ihrer Quellschnittstelle für den RADIUS-Datenverkehr.

```
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. Konfigurieren Sie die **loopback interfaces**. Die loopback interfaces werden als Quellverbindung für den Tunnel verwendet und abhängig von der verbundenen Gruppe dynamisch zugewiesen.

```
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
```

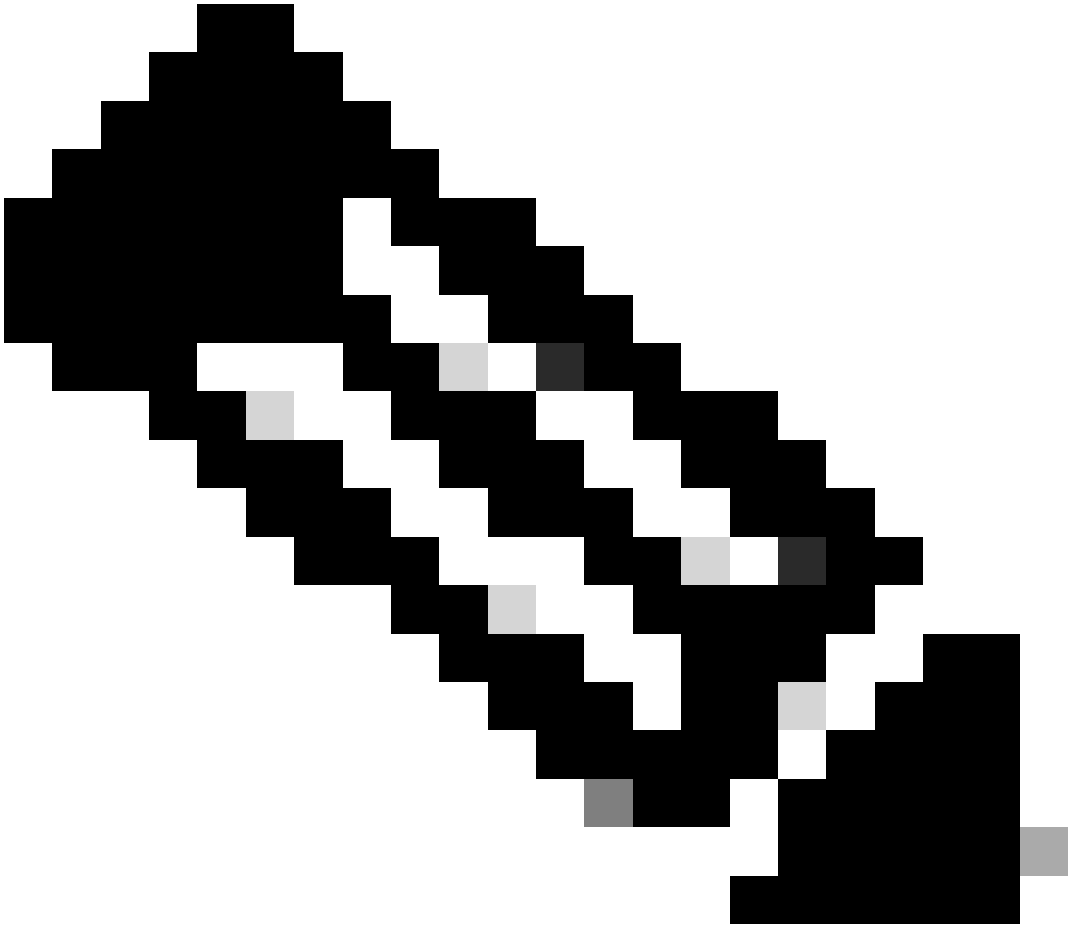
f. Definieren Sie einen **IP local pool** Wert für jede Gruppe.

```
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. Konfigurieren Sie EIGRP, und geben Sie die Netzwerke jeder Gruppe bekannt.

```
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
```



> Anmerkung: FlexVPN unterstützt dynamische Routing-Protokolle wie OSPF, EIGRP und BGP über VPN-Tunnel. In diesem Leitfaden wird EIGRP verwendet.

---

h. Konfigurieren Sie die **crypto ikev2 name mangler**. Der IKEv2 name mangler wird verwendet, um den Benutzernamen für die IKEv2-Autorisierung abzuleiten. In diesem Fall ist es so konfiguriert, dass die Informationen der Organisationseinheit aus den Zertifikaten auf den Stationen als Benutzername für die Autorisierung verwendet werden.

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

i. Konfigurieren Sie die **IKEv2 profile**. Auf die certificate map, AAA server group, und name mangler wird im IKEv2-Profil verwiesen.

Die lokale und die Remote-Authentifizierung werden in diesem speziellen Szenario wie **RSA-SIG**konfiguriert.

Ein lokales Benutzerkonto muss auf dem RADIUS server mit einem Benutzernamen erstellt werden, der mit demorganization-unitCisco1234Wert und dem Kennwort übereinstimmt (wie in der unten stehenden Konfiguration angegeben).

```
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) Konfigurieren Sie dieIPsec profileund verweisen Sie auf die IKEv2 profile.

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

K. Erstellen Sie die virtual-template. Es wird verwendet, um eine zu erstellen virtual-access interface und die IPsec profile erstellt zu verknüpfen.

Legen Sie fest**virtual-template**, dass keine IP-Adresse vorhanden ist, da diese vom zugewiesen wird RADIUS server.

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

Konfigurieren Sie zweiloopbacks, um ein internes Netzwerk zu simulieren.

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

Phase 2: Spoke-Konfiguration

antwort: Konfigurieren Sie einetrustpoint, um das Zertifikat des Spoke-Routers zu speichern.

```
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. Konfigurieren einescertificate map. Der Zweck des certificate map besteht darin, Zertifikate anhand der angegebenen Informationen zu identifizieren und abzugleichen, falls auf dem Router mehrere Zertifikate installiert sind.

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

c. Konfigurieren Sie das lokale AAA-Autorisierungsnetzwerk.

Der Befehl aaa Authorization Network wird verwendet, um Zugriffsanforderungen für Netzwerkdienste zu autorisieren. Dazu gehört auch die Überprüfung, ob ein Benutzer nach der Authentifizierung über die Berechtigung für den Zugriff auf den angeforderten Dienst verfügt.

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

d. Konfigurieren Sie dieIKEv2 profile. Auf die certificate map und die lokale AAA-Autorisierung wird im IKEv2 profileverwiesen.

Die lokale und die Remote-Authentifizierung werden konfiguriert 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. Konfigurieren Sie die IPsec profile und verweisen Sie auf die IKEv2 profile.

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

f. Konfigurieren Sie die tunnel interface. Der tunnel interface wird so konfiguriert, dass er eine Tunnel-IP-Adresse vom Hub basierend auf den Autorisierungsergebnissen erhält.

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

g. Konfigurieren Sie EIGRP, und geben Sie das lokale Netzwerk des Spoke und des tunnel interface an.

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

Konfigurieren Sie eine loopback, um ein internes Netzwerk zu simulieren.

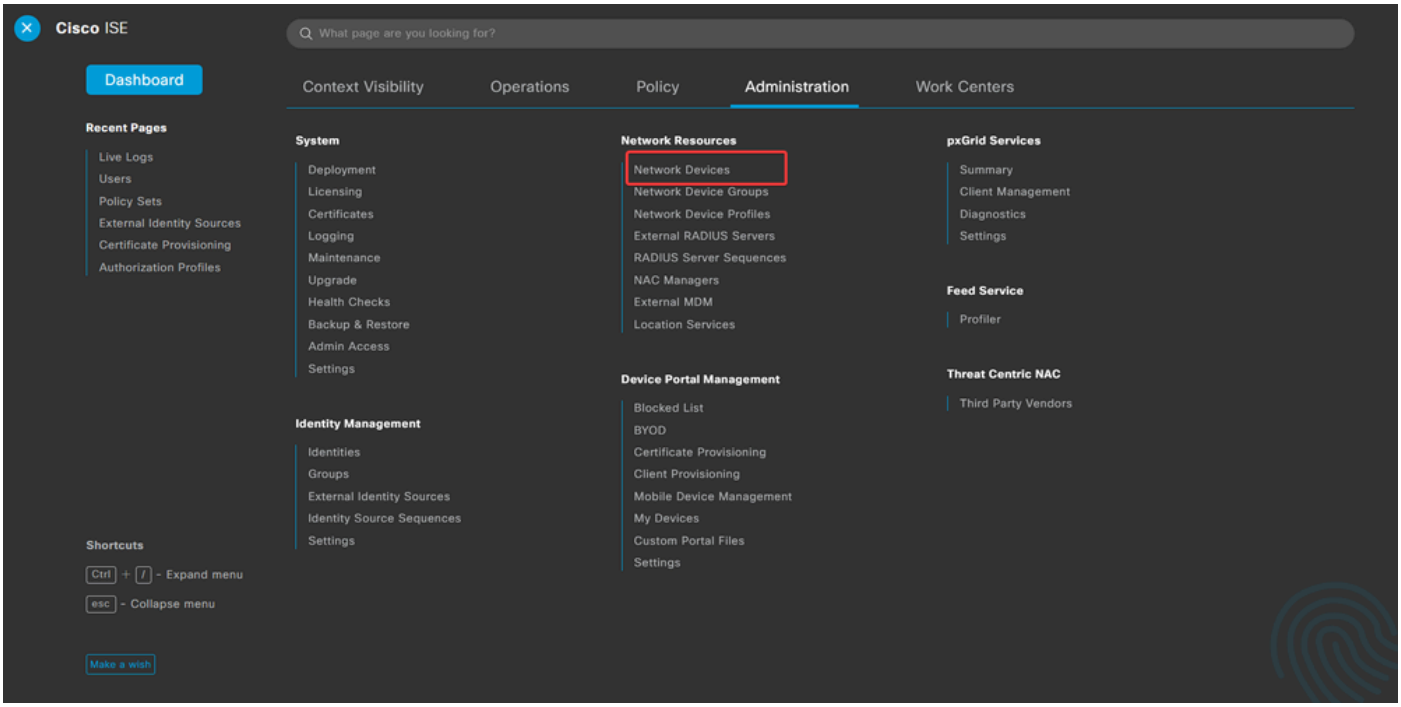
```
interface Loopback2010
ip address 10.20.1.10 255.255.255.255
```

Schritt 3: ISE-Konfiguration

Phase 3.1: Erstellen von Benutzern und Gruppen sowie Hinzufügen von Netzwerkgeräten

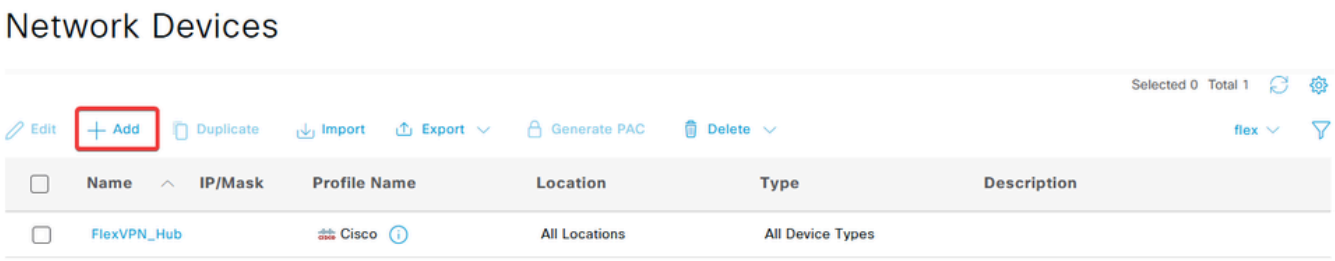
antwort: Melden Sie sich beim ISE-Server an, und navigieren Sie zu **Administration** > **Network Resources** >

Network Devices.



Administration - Netzwerkressourcen - Netzwerkgeräte

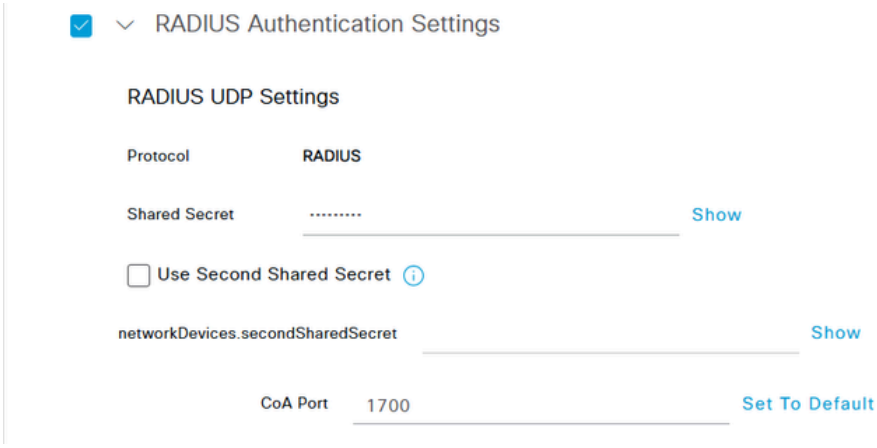
b. Klicken Sie hier, **Add** um den FlexVPN Hub als AAA-Client zu konfigurieren.



FlexVPN-Router als AAA-Client hinzufügen

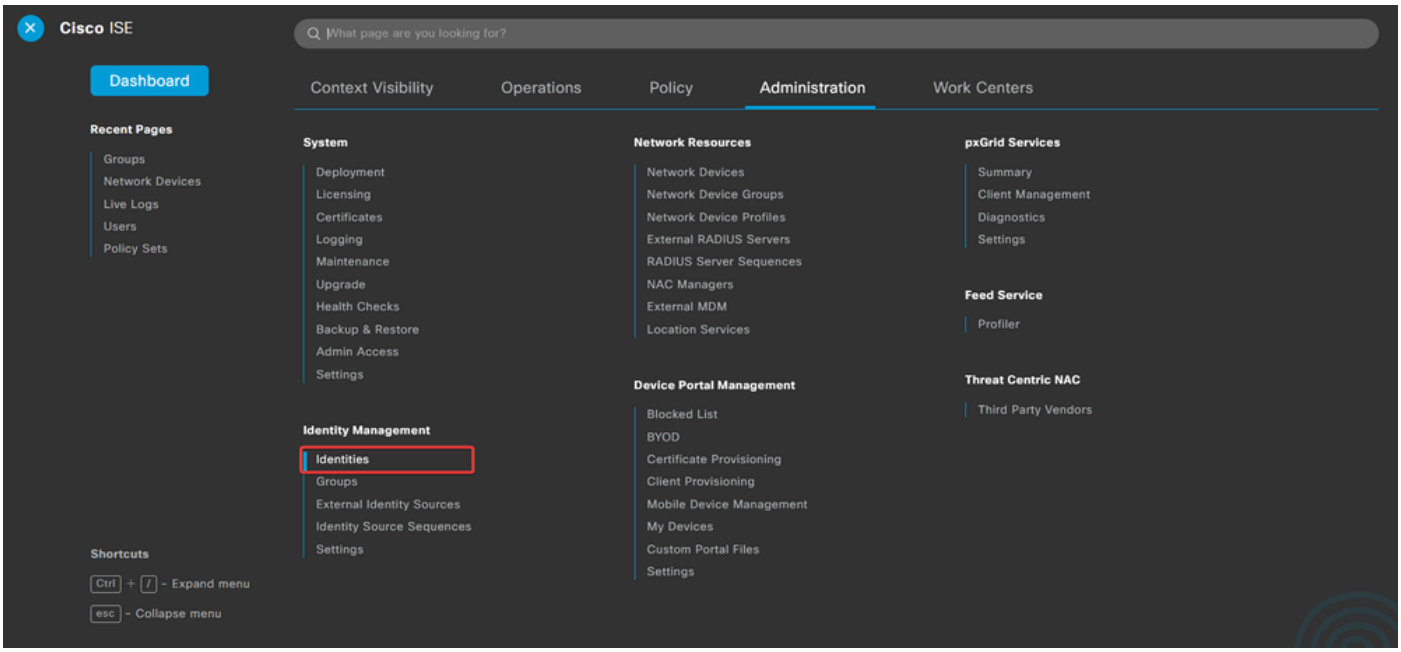
c. Geben Sie die Felder für den Netzwerkgerätenamen und die IP-Adresse ein, aktivieren Sie dann das **RADIUS Authentication Settings** Kontrollkästchen, und fügen Sie das **Shared Secret**. Kennwort für den gemeinsamen geheimen Zugriff hinzu. Dieses Kennwort muss mit dem identisch sein, das bei der Erstellung der RADIUS-Servergruppe auf dem FlexVPN-Hub verwendet wurde. Klicken Sie auf .Save

IP-Adresse des Netzwerkgeräts



Gemeinsam genutzter Netzwerkgeräteschlüssel

d. Navigieren Sie zu **.Administration > Identity Management > Identities**



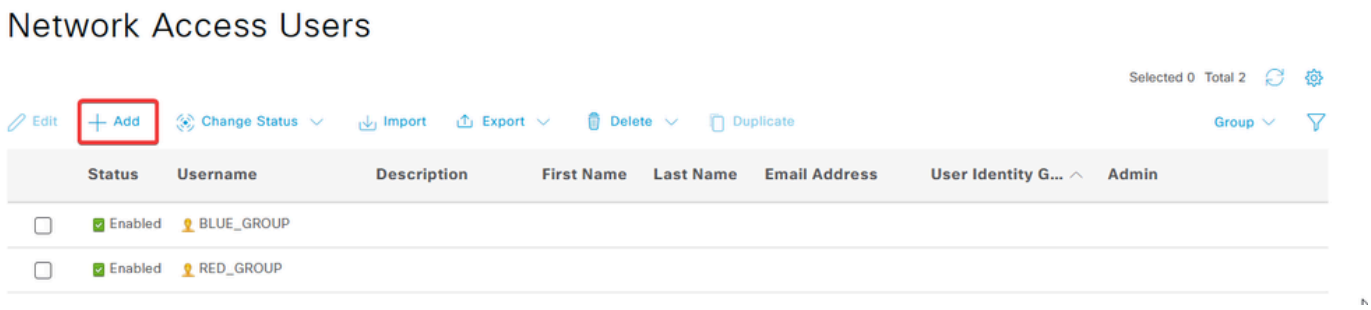
Administration - Identifizierung des Managements - Identifizierung

e. Klicken Sie aufAdd, um einen neuen Benutzer in der lokalen Serverdatenbank zu erstellen.

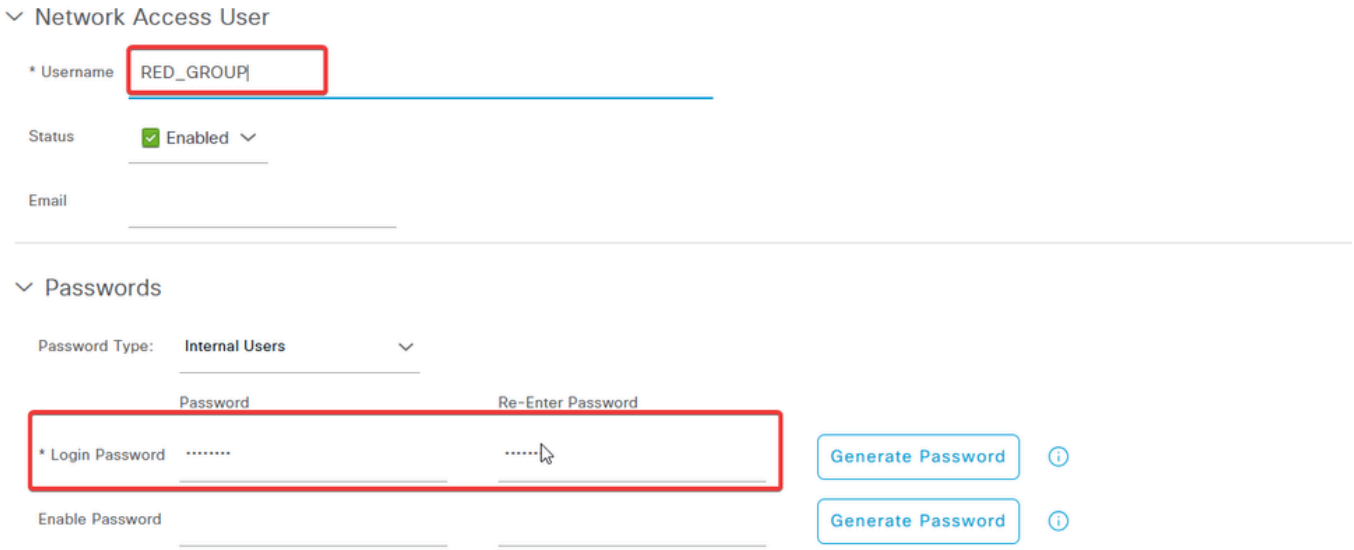
Geben Sie dasUsernameund **Login Password**ein. Der Benutzername ist derselbe, den die Zertifikate auf

dem Zertifikat als Organisationseinheit haben, und das Anmeldekennwort muss mit dem identisch sein, das im IKev2-Profil angegeben wurde.

Klicken Sie auf .**Save**



Administration - Identifizierung des Managements - Identifizierung

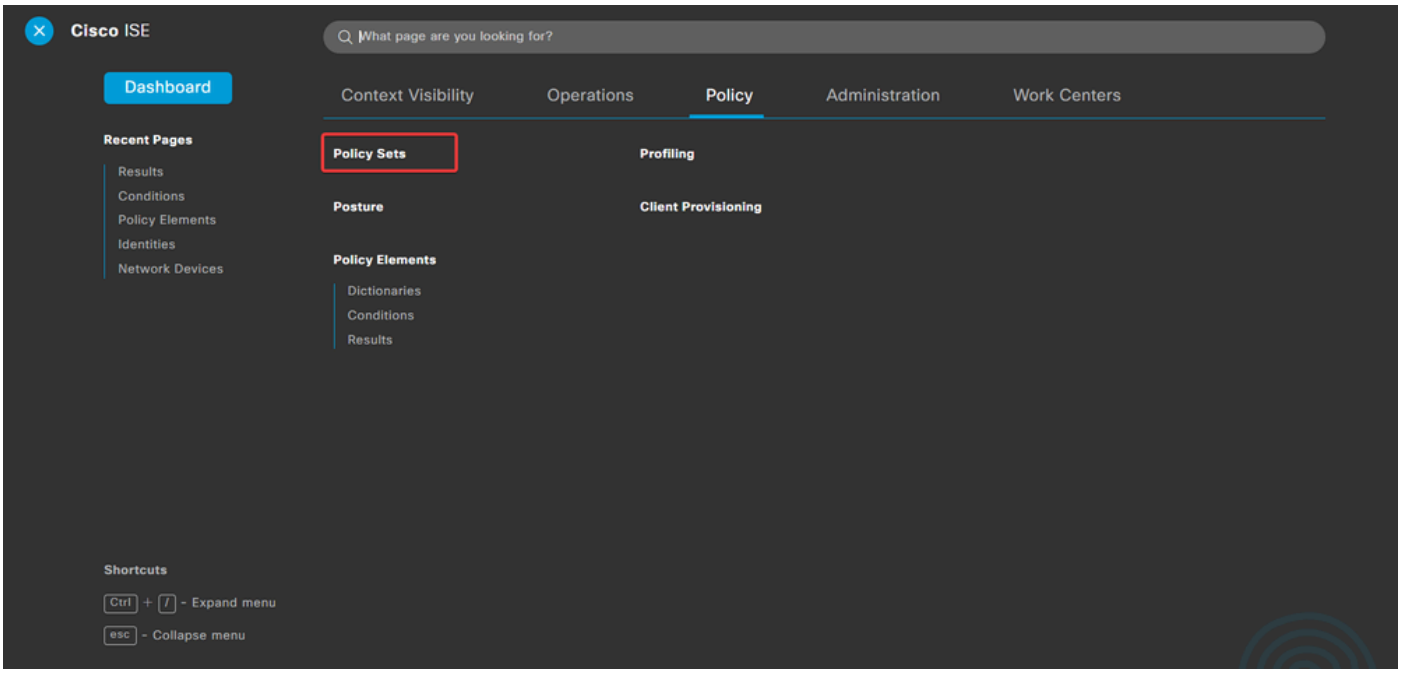


Gruppe erstellt wie Organisationseinheitswert

Phase 3.2: Policy Set konfigurieren

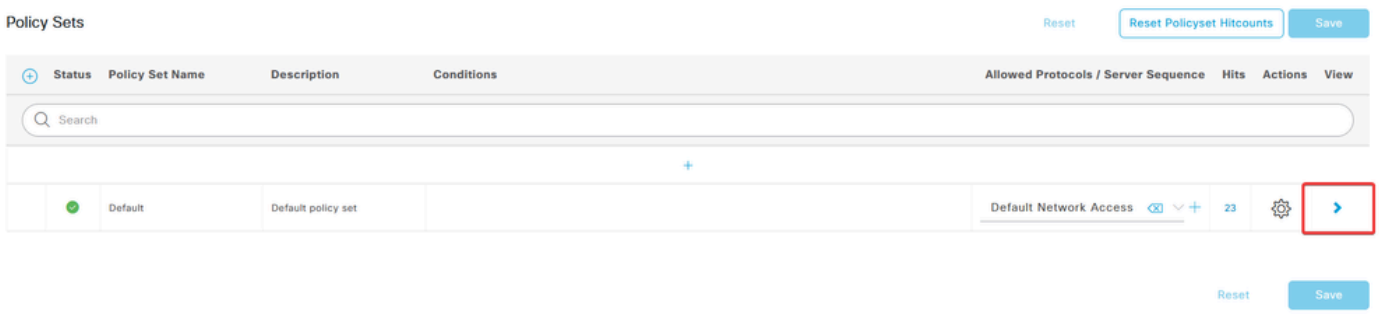
antwort: Navigieren Sie zu .**Policy > Policy Sets**

.



Richtlinien-Sets

b. Wählen Sie die Standard-Autorisierungsrichtlinie aus, indem Sie auf den Pfeil rechts im Bildschirm klicken:



Standardrichtlinie bearbeiten

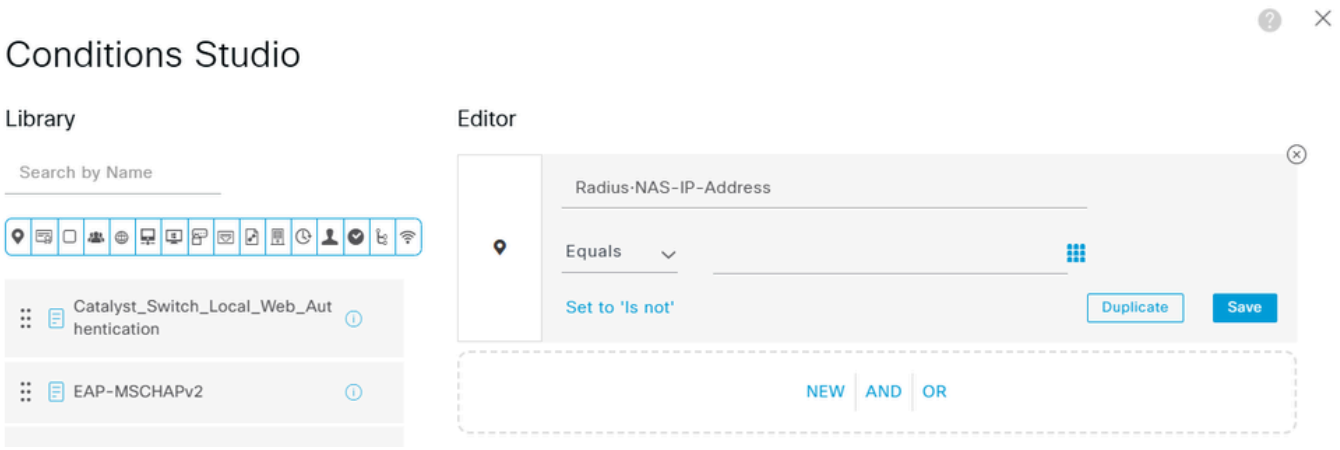
c. Klicken Sie auf den Dropdown-Menüpfeil nebenAuthentication Policy, um ihn zu erweitern. Klicken Sie dann auf das **add (+)** Symbol, um eine neue Regel hinzuzufügen.

Authentifizierungsrichtlinie hinzufügen

d. add (+)Geben Sie den Namen für die Regel ein, und wählen Sie das Symbol in der Spalte Bedingungen aus.

Authentifizierungsrichtlinie erstellen

e. Klicken Sie auf das Textfeld Attribute-Editor und anschließend auf dasNAS-IP-AddressSymbol. Geben Sie die IP-Adresse (192.168.0.10) des FlexVPN Hub ein.

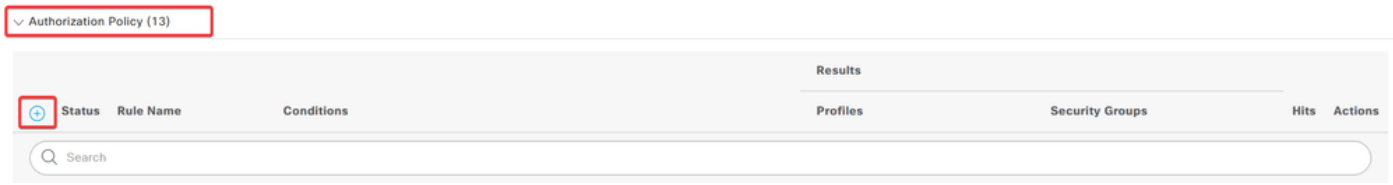


Authenticate FlexVPN Hub

Authentifizierungsrichtlinie

Phase 3.3: Autorisierungsrichtlinie konfigurieren

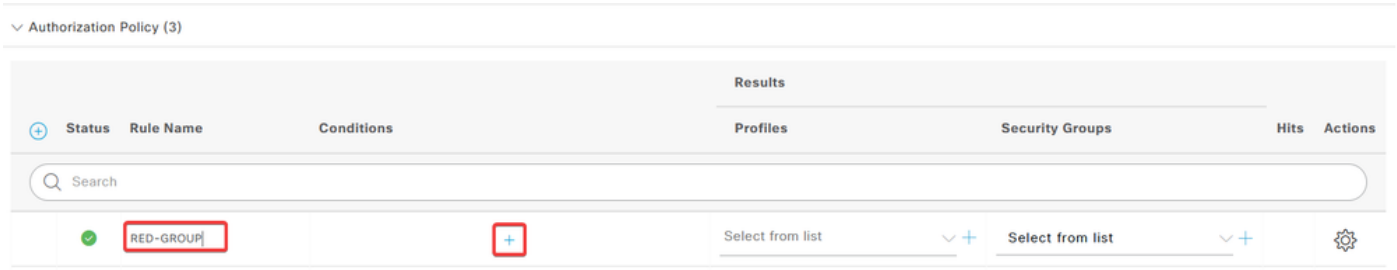
antwort: Klicken Sie auf den Dropdown-Menüpfeil neben, um ihnAuthorization Policyzu erweitern. Klicken Sie dann auf das **add (+)** Symbol, um eine neue Regel hinzuzufügen.



Neue Autorisierungsrichtlinie erstellen

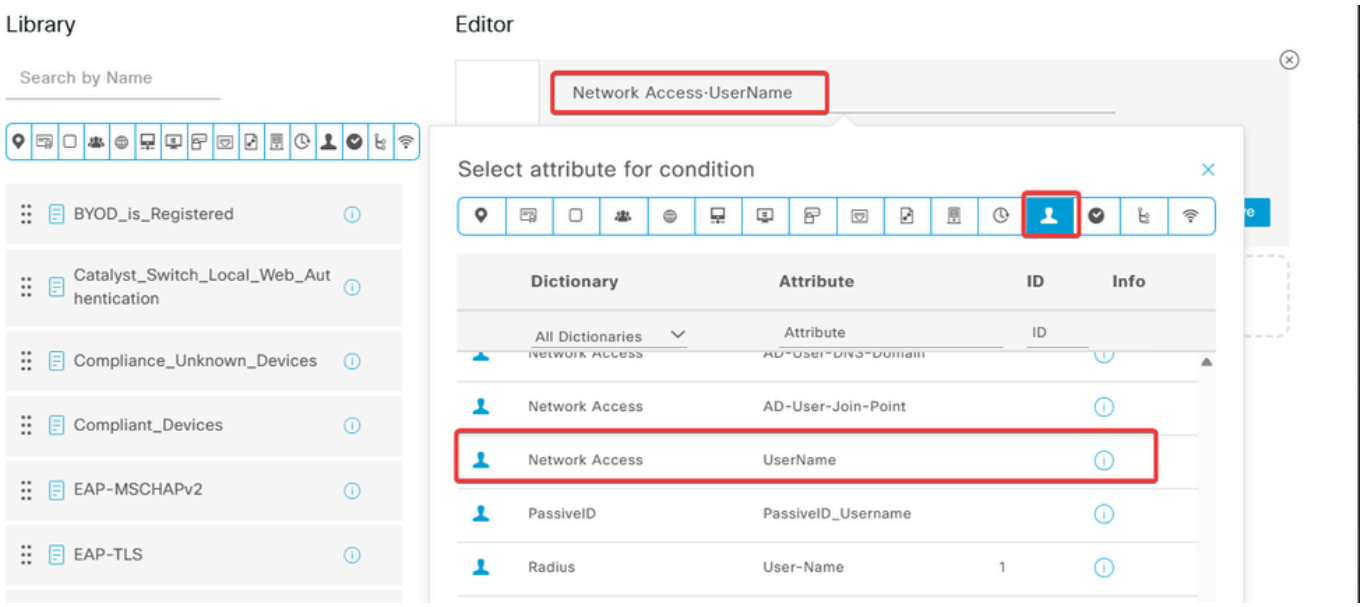
b. Geben Sie den Namen für die Regel ein, und wählen Sie das **add (+)** Symbol in der Spalte

Bedingungen aus.



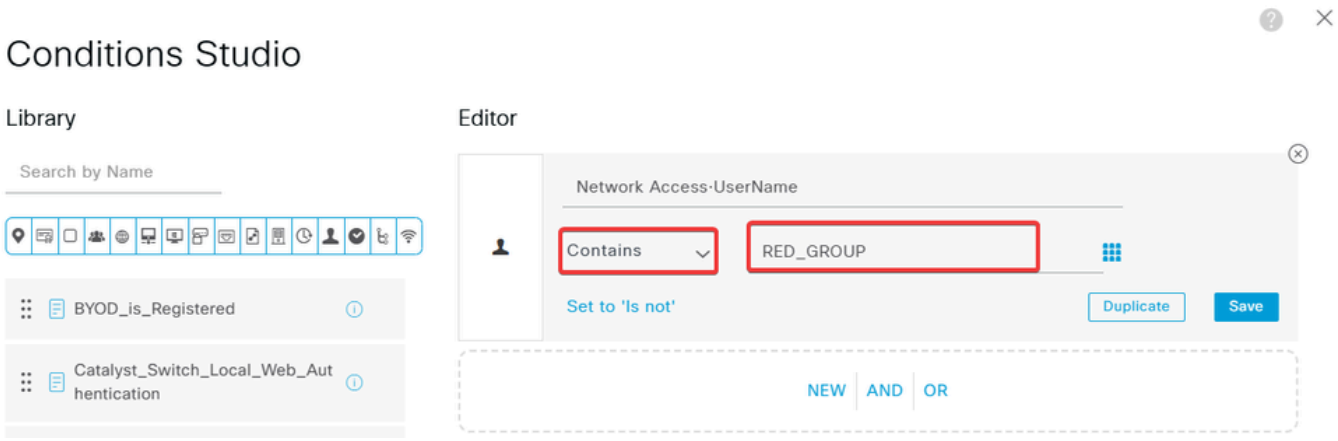
Neue Regel erstellen

c. Klicken Sie auf das Textfeld Attribute-Editor und anschließend auf dasSubjectSymbol. Wählen Sie das **Network Access - UserName** Attribut aus.



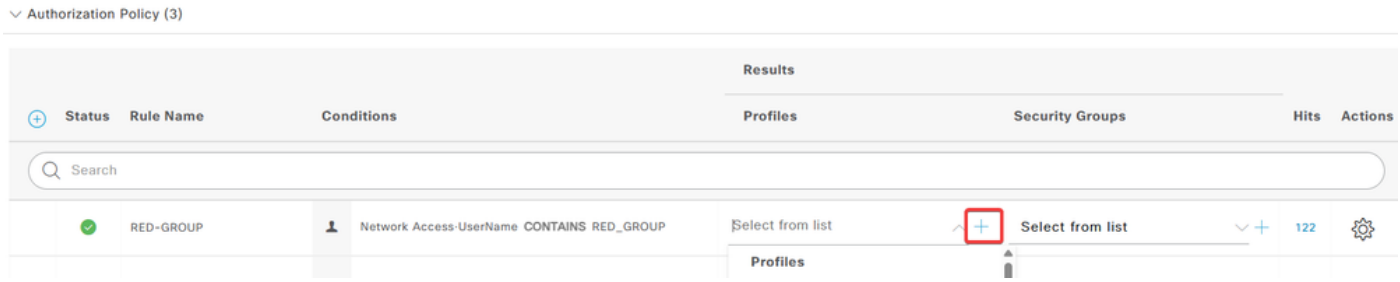
Netzwerkzugriff auswählen - Benutzername

d. Wählen SieContainsals Operator aus, und fügen Sie dann den Wert Organization-Unit der Zertifikate hinzu.



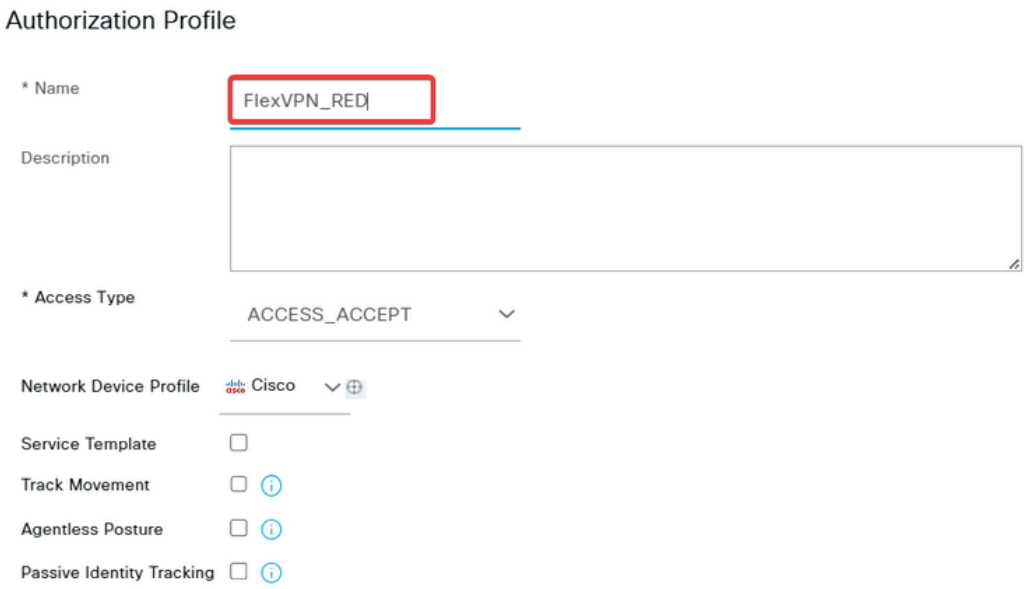
Gruppennamen hinzufügen

e. Klicken Sie in der Spalte Profile auf dasadd (+)Symbol, und wählen Sie **Create a New Authorization Profile**.



Neues Autorisierungsprofil hinzufügen

f. Geben Sie das Profil **Name**ein.



Autorisierungsprofil benennen

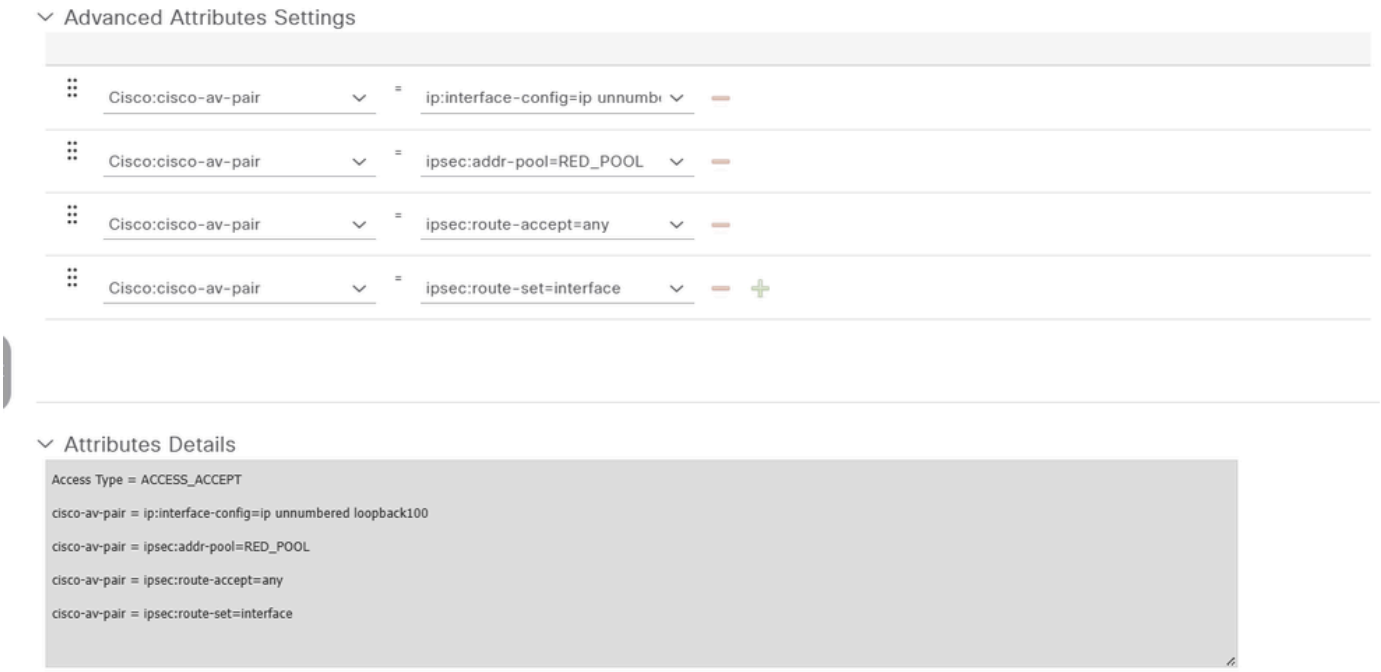
g. Navigieren Sie zu **.Advanced Attributes Settings** Wählen Sie dann das cisco-av-pairAttribut aus dem Dropdown-Menü auf der linken Seite aus, und fügen Sie das Attribut hinzu, das je nach Gruppe der FlexVPN-Spoke zugewiesen wird.

Zu den Attributen, die für dieses Beispiel zugewiesen werden sollen, gehören:

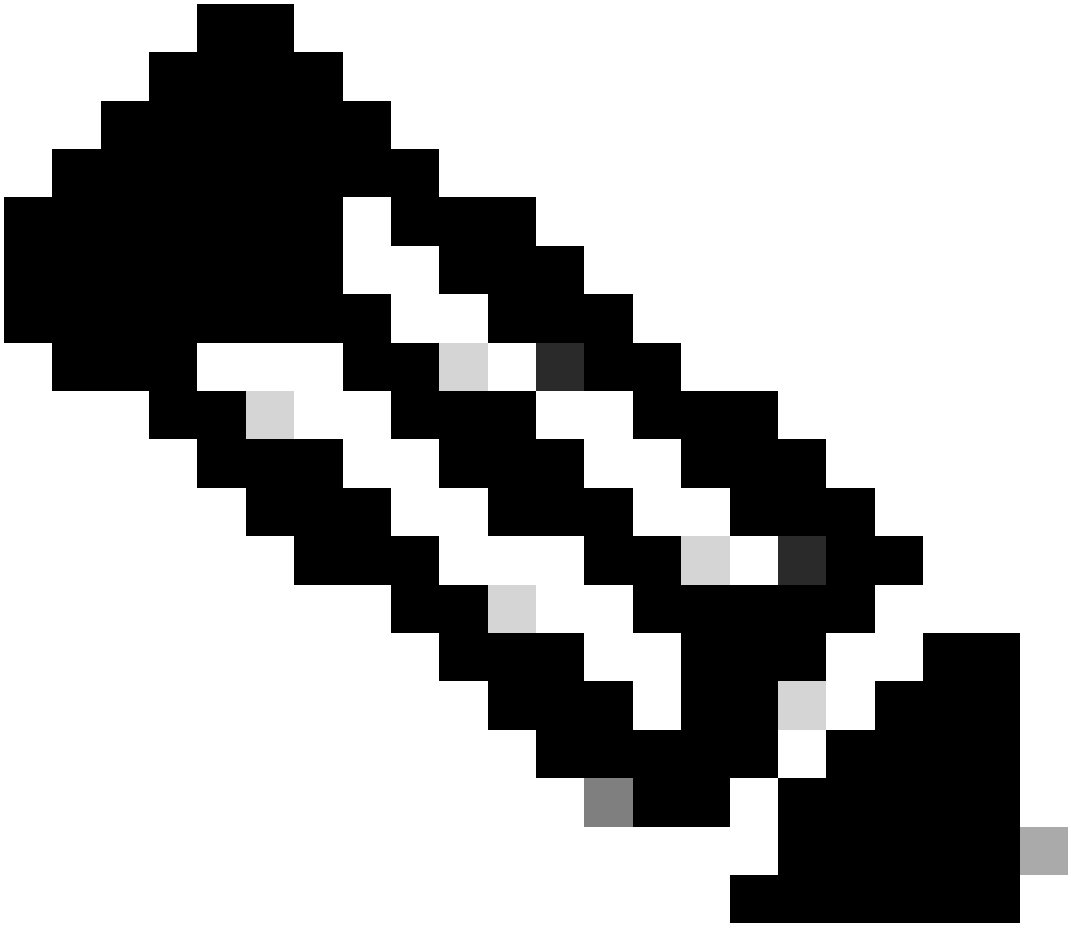
- Zuweisen der Loopback-Schnittstelle als Quelle
- Den Pool angeben, von dem die Stationen eine IP-Adresse erhalten.

Die route accept any und -route set interfaceAttribute sind erforderlich, da die Routen ohne sie den Stationen nicht ordnungsgemäß angekündigt werden.

```
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
```



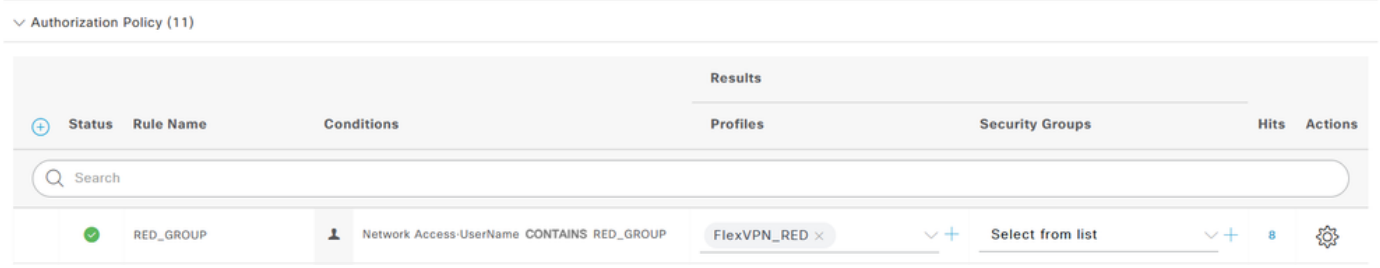
Erweiterte Attributeinstellungen



Anmerkung: Attributspezifikationen (Name, Syntax, Beschreibung, Beispiel usw.) finden Sie im Konfigurationsleitfaden für FlexVPN RADIUS-Attribute:

FlexVPN and Internet Key Exchange Version 2 Configuration Guide, Cisco IOS XE Gibraltar 16.12.x

h. Weisen Sie die **authorization profile** in der Profilspalte zu.



Autorisierungsregel

i. Klicken Sie auf **Save**.

Überprüfung

- Verwenden Sie den Befehl, **show ip interface brief** um den Status "Tunnel", "Virtual-Template" und "Virtual-Access" zu überprüfen.

Auf dem Hub hat die virtuelle Vorlage den Status "up/down", was normal ist, und für jeden Spoke, der eine Verbindung mit dem Hub hergestellt hat, wird ein virtueller Zugriff erstellt, der einen Status "up/up" anzeigt.

<#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
```

Auf dem Spoke hat die Tunnelschnittstelle eine IP-Adresse von dem Pool erhalten, der der Gruppe zugewiesen ist, und zeigt den Status "up/up" an.

<#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
```

- Verwenden Sie den Befehl.**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
```

- Verwenden Sie den Befehl, **show crypto session** um sicherzustellen, dass die sichere Verbindung zwischen den Routern hergestellt ist.

```
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
```

- Bestätigen Sie mit dem Befehl show ip eigrp neighbors, dass die EIGRP-Adjacency für den anderen Standort eingerichtet wurde.

```
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
```

- Verwenden Sie den Befehl show ip route, um zu überprüfen, ob die Routen zu den Spokes weitergeleitet wurden.
    - Die Route für die Loopback-Schnittstelle 10.20.1.10 am Spoke wurde vom Hub per EIGRP erfasst, und sie ist über den virtuellen Zugriff zugänglich.


```
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
```

- Die Routen für 10.10.1.10 und 10.10.2.10 wurden über EIGRP erfasst und sind über die Quell-IP der RED_GROUP (10.100.100.1) erreichbar, die über Tunnel0 erreichbar ist.

<#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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen, die Sie zur Fehlerbehebung bei diesem Bereitstellungstyp verwenden können. Verwenden Sie die folgenden Befehle, um den Tunnelaushandlungsprozess zu 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- und RADIUS-Debugging-Verfahren können bei der Fehlerbehebung bei der Autorisierung der Spokes helfen.

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

Working Scenario

Dieses Protokoll zeigt den Autorisierungsprozess und die Zuweisung der Parameter.

```
     <#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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.