Configurazione di FlexVPN con l'integrazione ISE

Sommario

Introduzione

Questo documento descrive come configurare FlexVPN con Cisco Identity Services Engine (ISE) per assegnare dinamicamente le configurazioni agli spoke.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione Cisco Identity Services Engine (ISE)
- protocollo RADIUS
- Flex Virtual Private Network (FlexVPN)

Componenti usati

Questo documento si basa sulle seguenti versioni software e hardware:

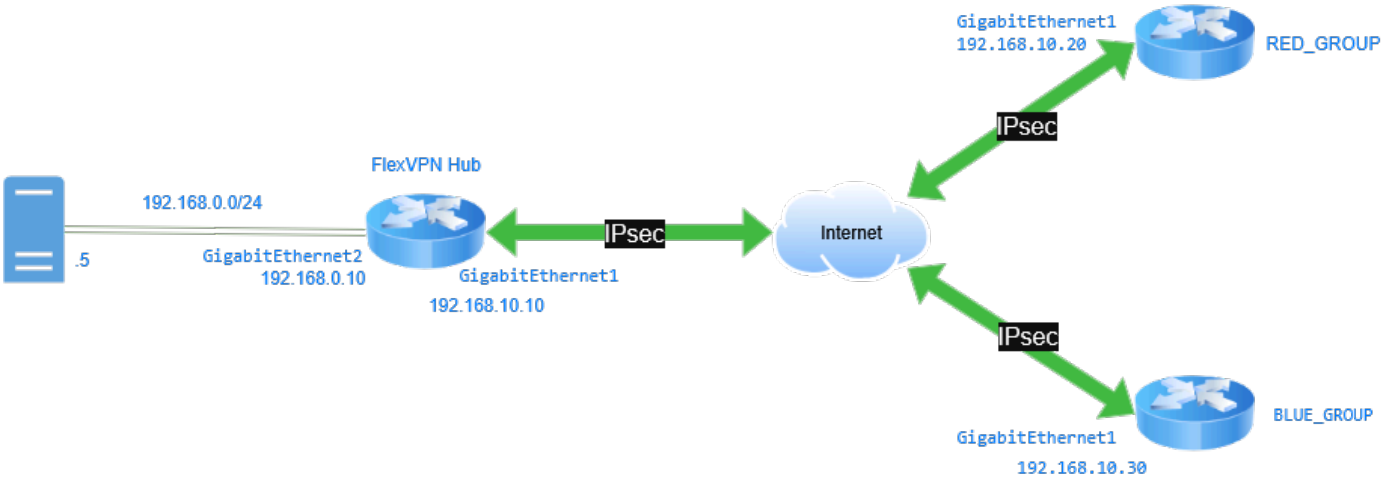
- Cisco CSR1000V (VXE) - Versione 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

FlexVPN può stabilire una connessione con gli spoke e assegnare alcune configurazioni che consentono la comunicazione e la gestione del traffico. Menzionato nel diagramma, questo mostra come FlexVPN si integra con ISE in modo che, quando un spoke si connette all'HUB, i parametri dell'origine del tunnel e del pool DHCP vengano assegnati a seconda del gruppo o della diramazione a cui appartiene il spoke. Sta utilizzando il certificato per autenticare gli spoke, quindi ISE con Radius come server di autorizzazione e accounting.



FlexVPN con integrazione ISE

Passaggio 1: Configurazione hub

r. Configurare un certificato`trustpoint`per l'archiviazione del router. I certificati vengono utilizzati per autenticare gli spoke.

```
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. Configurare un **certificate map**file. Lo scopo del `certificate map` comando è identificare e associare i certificati in base alle informazioni specificate, nel caso in cui nel router siano installati più certificati.

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

c. Configurare un RADIUS server per l'autorizzazione e l'accounting sul dispositivo:

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

d. Definire il **RADIUS server group** router con il relativo indirizzo IP, le porte di comunicazione, la chiave condivisa e l'interfaccia di origine per il traffico 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. Configurare il **loopback interfaces** file. I loopback interfaces parametri vengono utilizzati come connessione di origine per il tunnel e vengono assegnati dinamicamente a seconda del gruppo connesso.

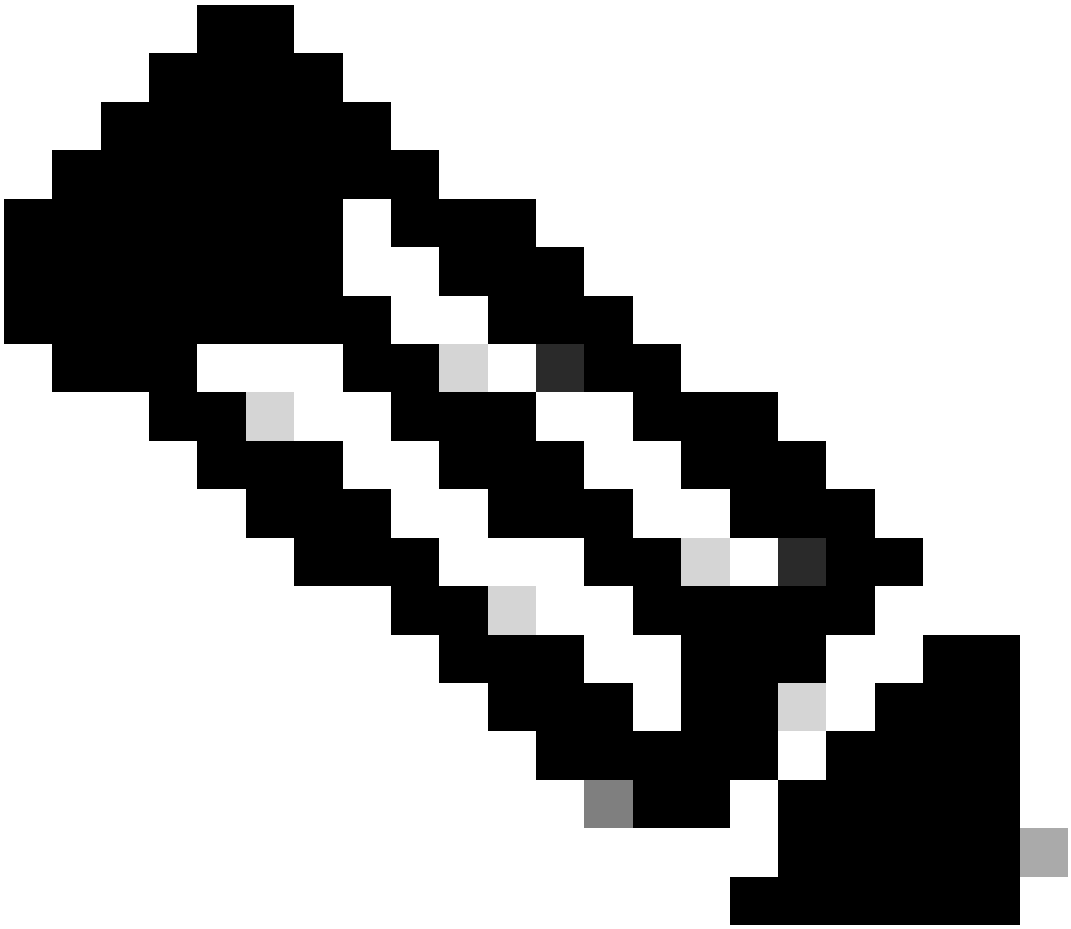
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f. Definire un'**IP local pool** associazione per ogni gruppo.

```
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. Configurare EIGRP e annunciare le reti di ciascun gruppo.

```
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
```



> Nota: FlexVPN supporta protocolli di routing dinamico come OSPF, EIGRP e BGP su tunnel VPN. In questa guida viene utilizzato il protocollo EIGRP.

---

h. Configurare il **crypto ikev2 name mangler**file. Il IKEv2 name mangler nome utente viene utilizzato per derivare il nome utente per l'autorizzazione IKEv2. In questo caso, è configurato per utilizzare le informazioni dell'unità organizzativa dei certificati sugli spoke come nome utente per l'autorizzazione.

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

i. Configurare il **IKEv2 profile**file. certificate mapNel profilo IKEv2 viene fatto riferimento alle name mangler, AAA server groupe.

In questo scenario specifico, l'autenticazione locale e remota sono configurate come **RSA-SIG**.

È necessario creare un account utente locale sul RADIUS server computer con un nome utente che corrisponda al valore e allaorganization-unitpasswordCisco1234(come specificato nella configurazione seguente).

```
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. Configurare il fileIPsec profilee fare riferimento al IKEv2 profilefile.

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

k. Creare il virtual-templatefile. Viene utilizzato per creare un virtual-access interface e collegare il IPsec profile file creato.

Impostare l'**virtual-template**indirizzo senza indirizzo IP, in quanto assegnato dalla RADIUS serverfunzione.

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

Configurarne dueloopbacksper simulare una rete interna.

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

Passaggio 2: Configurazione spoke

r. Configurare untrustpointper archiviare il certificato del router spoke.

```
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. Configurare uncertificate mapdatabase. Lo scopo del certificate map comando è identificare e associare i certificati in base alle informazioni specificate, nel caso in cui nel router siano installati più certificati.

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

c. Configurare la rete di autorizzazione locale AAA.

Il comando aaa authorization network viene usato per autorizzare le richieste di accesso relative ai servizi di rete. Consente inoltre di verificare se un utente dispone dell'autorizzazione per accedere al servizio richiesto dopo l'autenticazione.

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

d. Configurare laIKEv2 profileporta. Le autorizzazioni locali certificate map e AAA sono referenziate nella IKEv2 profiledirectory.

L'autenticazione locale e remota è configurata come **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. Configurare il fileIPsec profilee fare riferimento alla IKEv2 profile.

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

f. Configurare latunnel interfaceporta. Il tunnel interface router è configurato per ricevere un indirizzo IP del tunnel dall'hub in base ai risultati dell'autorizzazione.

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

g. Configurare EIGRP, pubblicizzando la rete locale dello spoke e del tunnel interfacerouter.

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

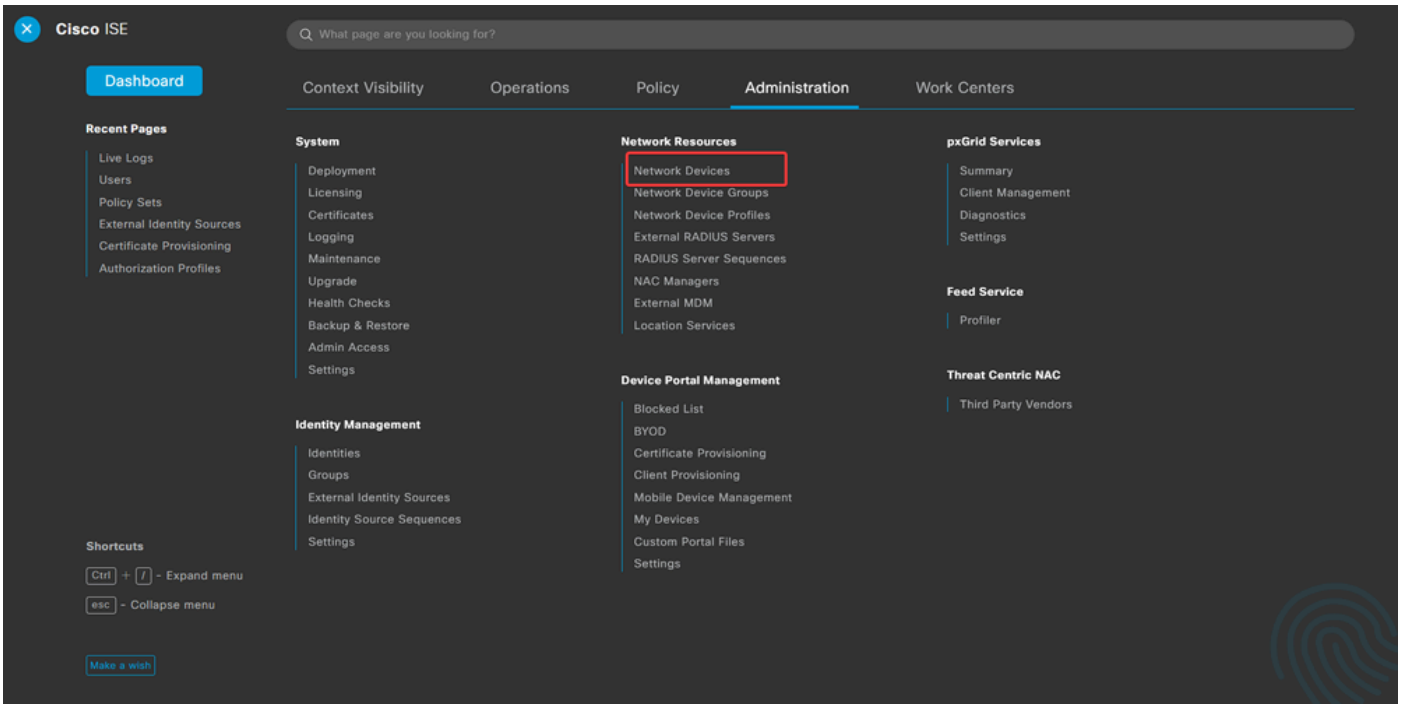
Configurare unaloopbackrete per simulare una rete interna.

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

Passaggio 3: Configurazione di ISE

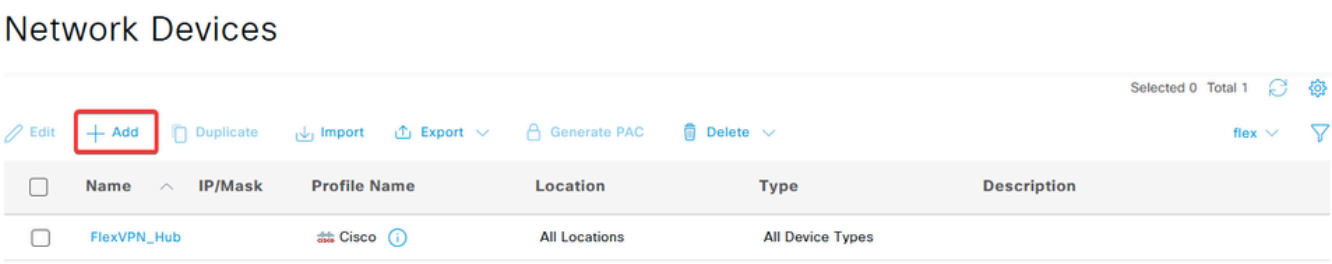
Passaggio 3.1: Creare utenti, gruppi e aggiungere dispositivi di rete

r. Accedere al server ISE e selezionare **Administration** > **Network Resources** > **Network Devices**.



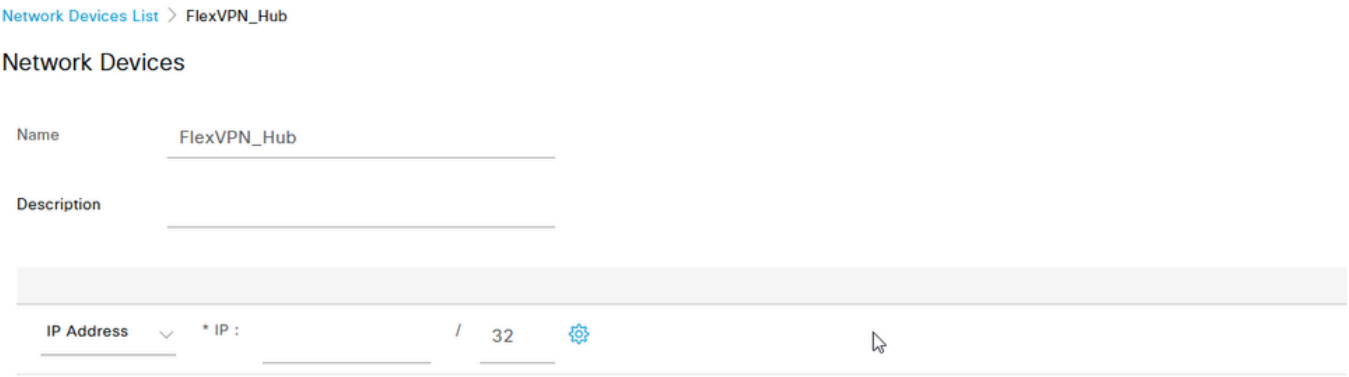
Amministrazione-Risorse di rete-Dispositivi di rete

b. Fare clic **Add** per configurare l'hub FlexVPN come client AAA.

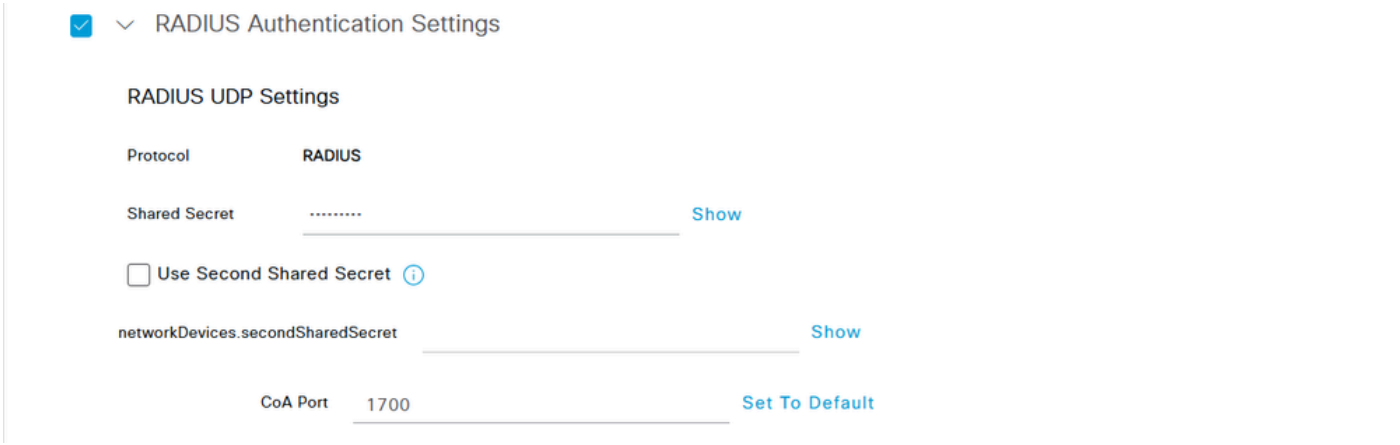


Aggiunta del router FlexVPN come client AAA

c. Immettere i campi Nome dispositivo di rete e Indirizzo IP, quindi selezionare la casella di controllo **RADIUS Authentication Settings** e aggiungere la **Shared Secret**. Password segreta condivisa che deve essere la stessa utilizzata quando il gruppo di server RADIUS è stato creato sull'hub FlexVPN. Fare clic su .Save

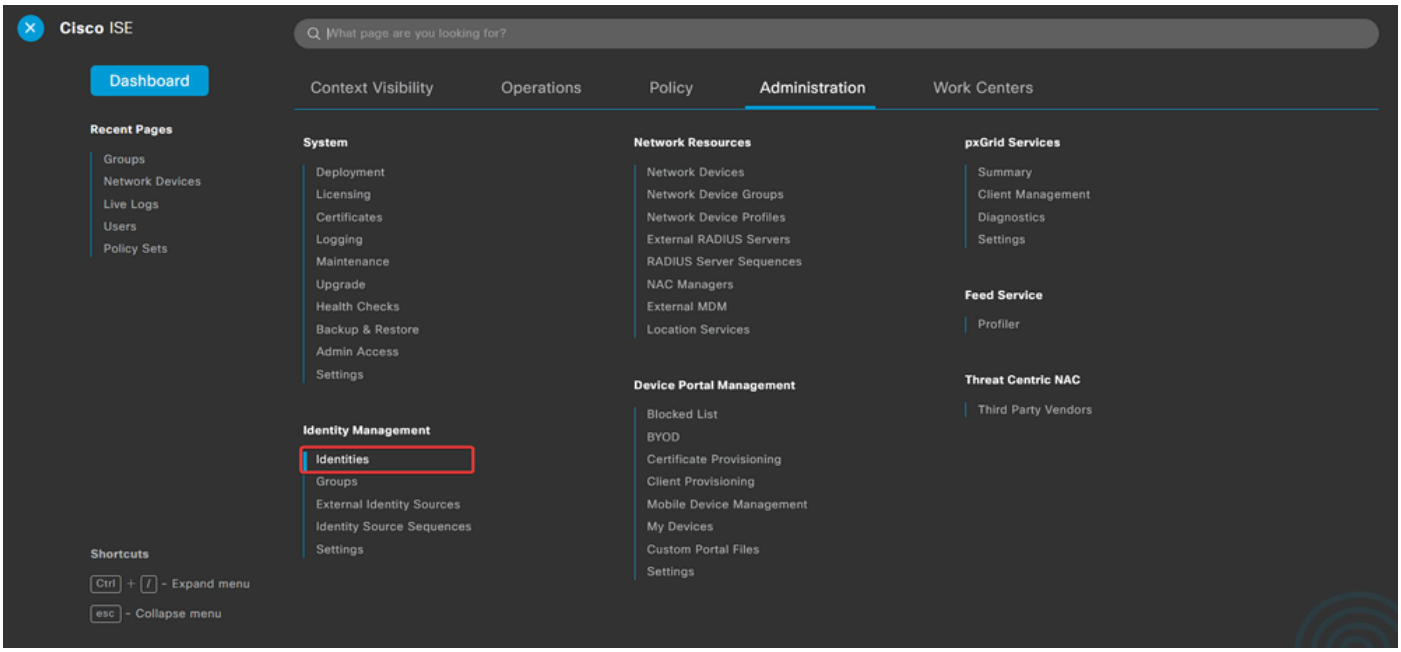


Indirizzo IP dispositivo di rete



Chiave condivisa dispositivo di rete

d. Passare a **Administration** > **Identity Management** > **Identities**.

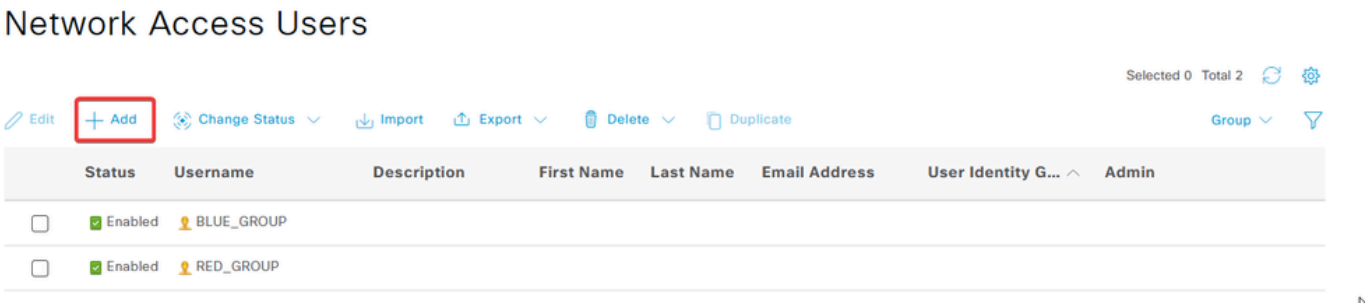


Amministrazione-Identifica gestione-Identifica

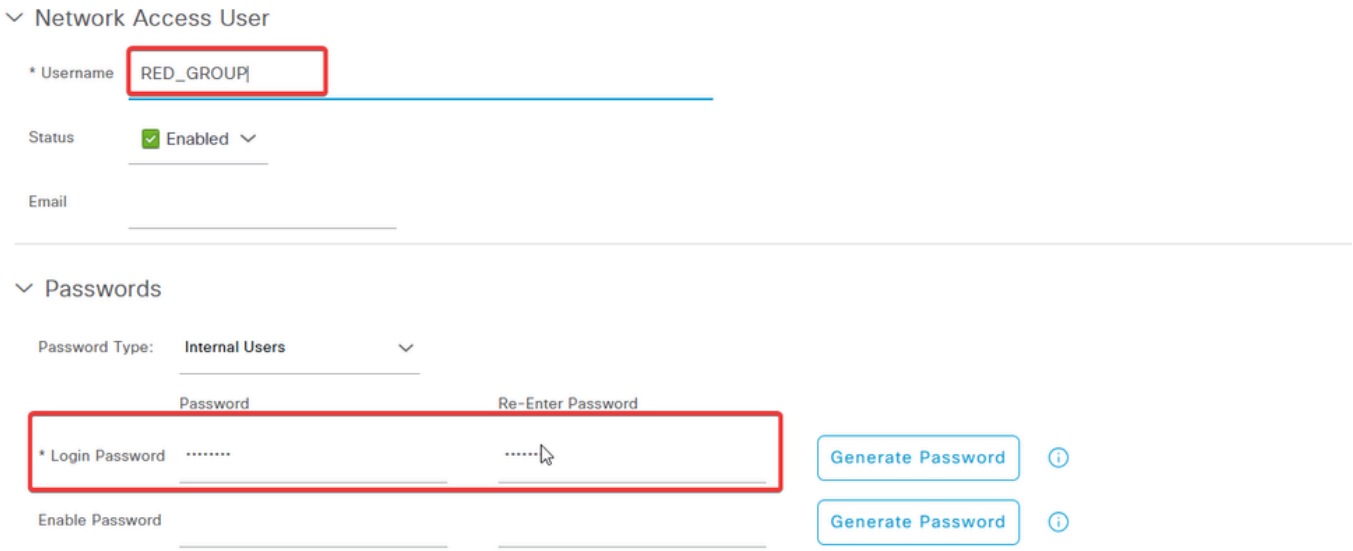
e. Fare clic su**Add**per creare un nuovo utente nel database locale del server.

Immettere il valore**Username**e **Login Password**. Il nome utente è lo stesso che i certificati non hanno un valore di unità organizzativa nel certificato e la password di accesso deve essere la stessa specificata nel profilo IKev2.

Fare clic su .**Save**



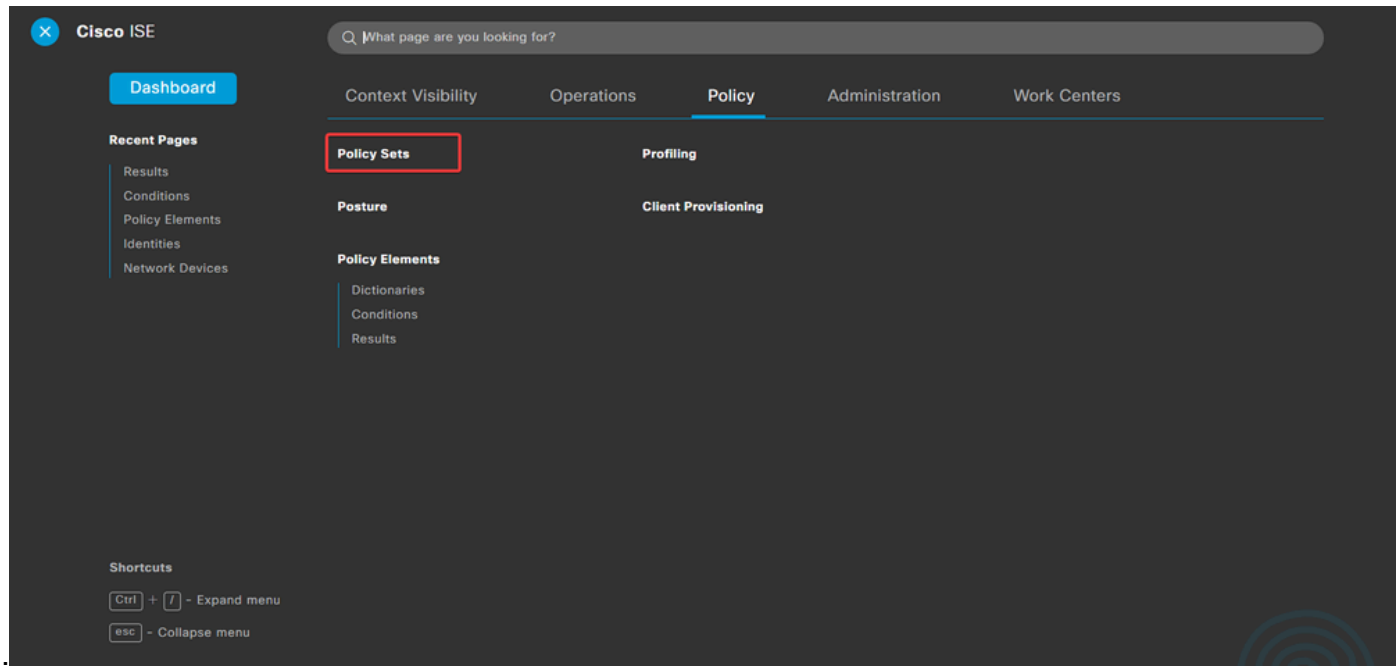
Amministrazione-Identifica gestione-Identifica



Gruppo creato uguale al valore dell'unità organizzativa

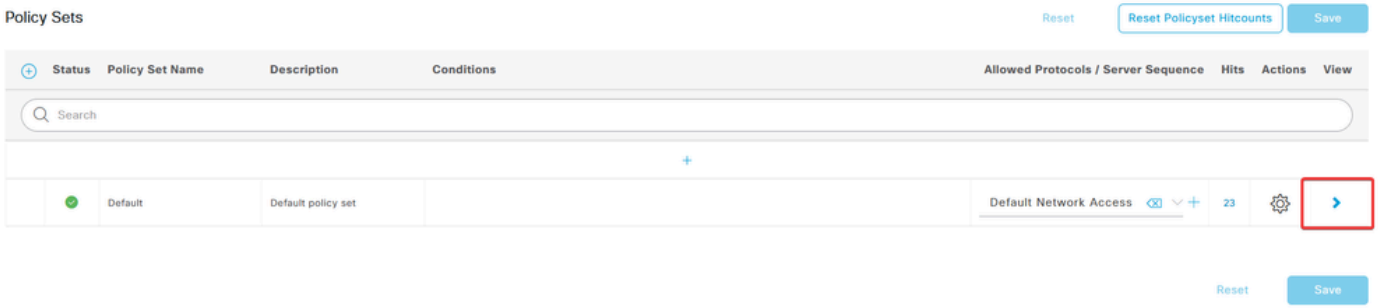
Passaggio 3.2: Configura set di criteri

r. Passare a **Policy** > **Policy Sets**.



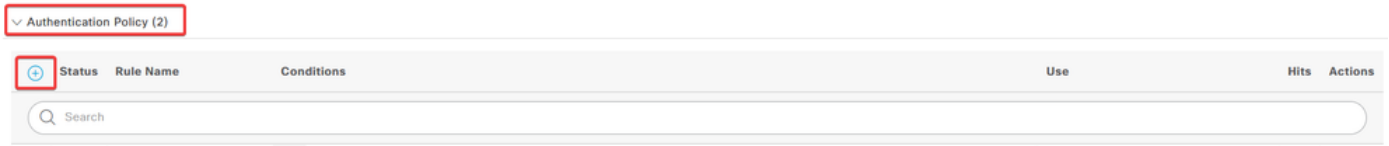
Set di criteri

b. Selezionare il criterio di autorizzazione predefinito facendo clic sulla freccia sul lato destro della schermata:



Modifica criterio predefinito

c. Fare clic sulla freccia del menu a discesa accantoAuthentication Policya per espanderlo. Quindi, fare clic sulladd (+)'icona per aggiungere una nuova regola.

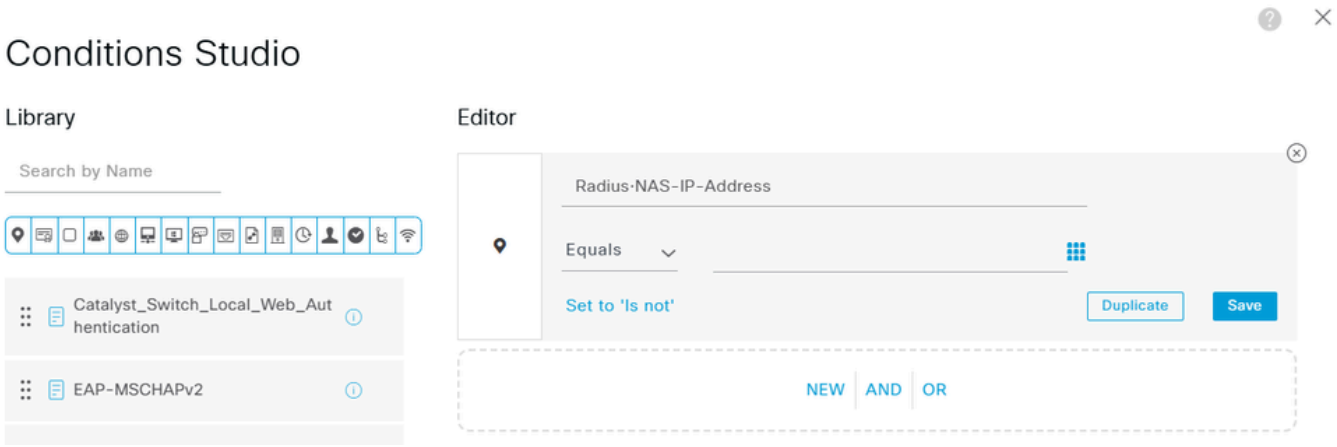


Aggiungi criterio di autenticazione

d. Immettere il nome della regola e selezionare l'iconaadd (+)nella colonna Condizioni.

Crea criterio di autenticazione

e. Fare clic sulla casella di testo Editor attributi e fare clic sullNAS-IP-Address' icona. Immettere l'indirizzo IP (192.168.0.10) dell'hub FlexVPN.

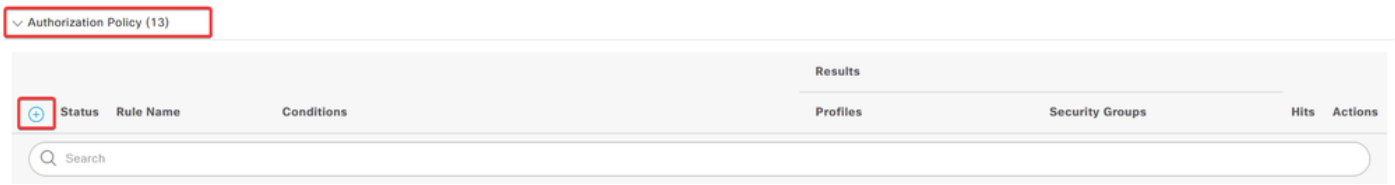


Authenticate FlexVPN Hub

Criterio di autenticazione

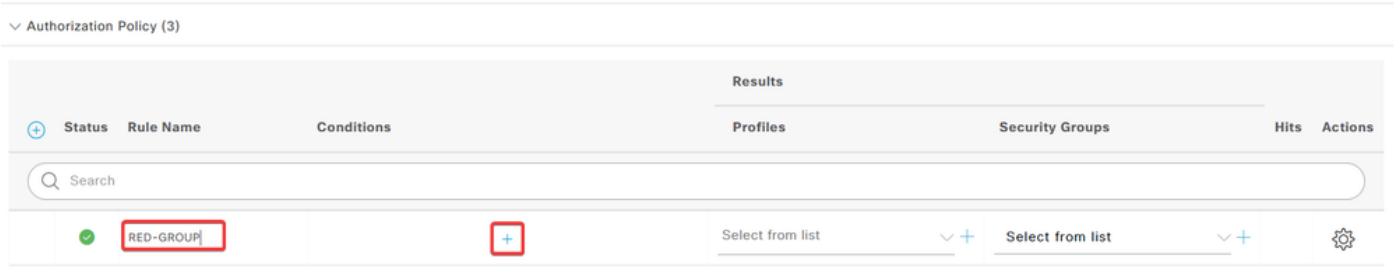
Passaggio 3.3: Configura criteri di autorizzazione

r. Fare clic sulla freccia del menu a discesa accantoAuthorization Policya per espanderlo. Quindi, fare clic sull**add (+)**'icona per aggiungere una nuova regola.



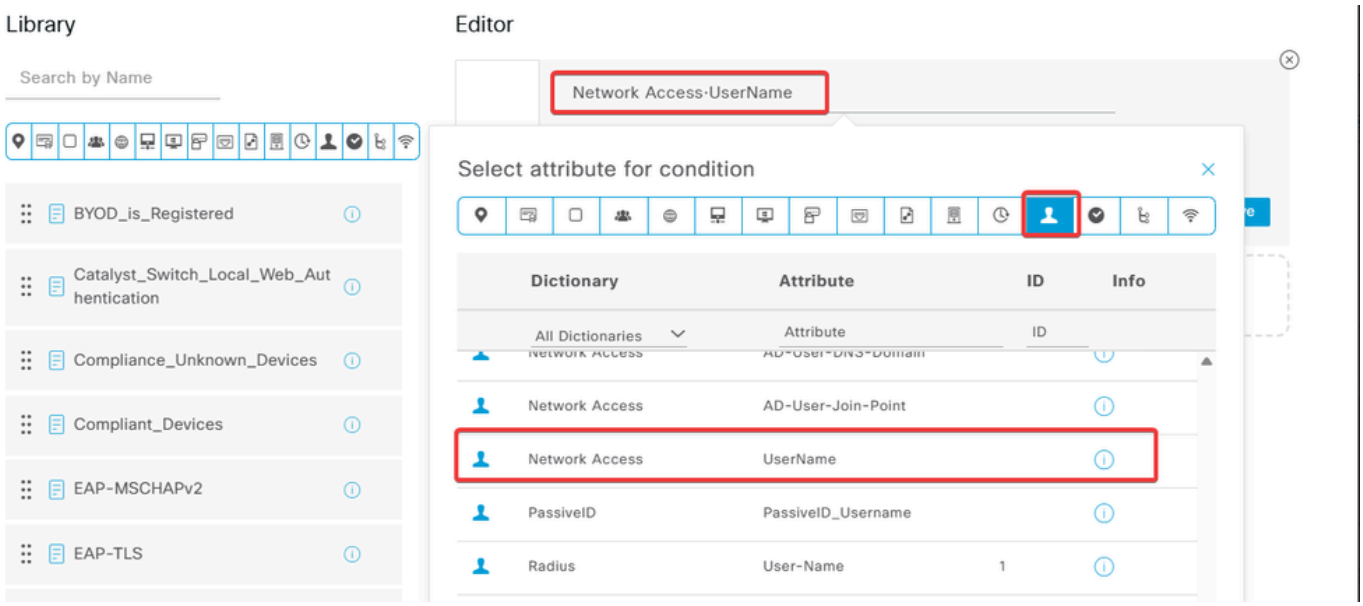
Crea nuovo criterio di autorizzazione

b. Immettere il nome della regola e selezionare l'**add (+)**icona nella colonna Condizioni.



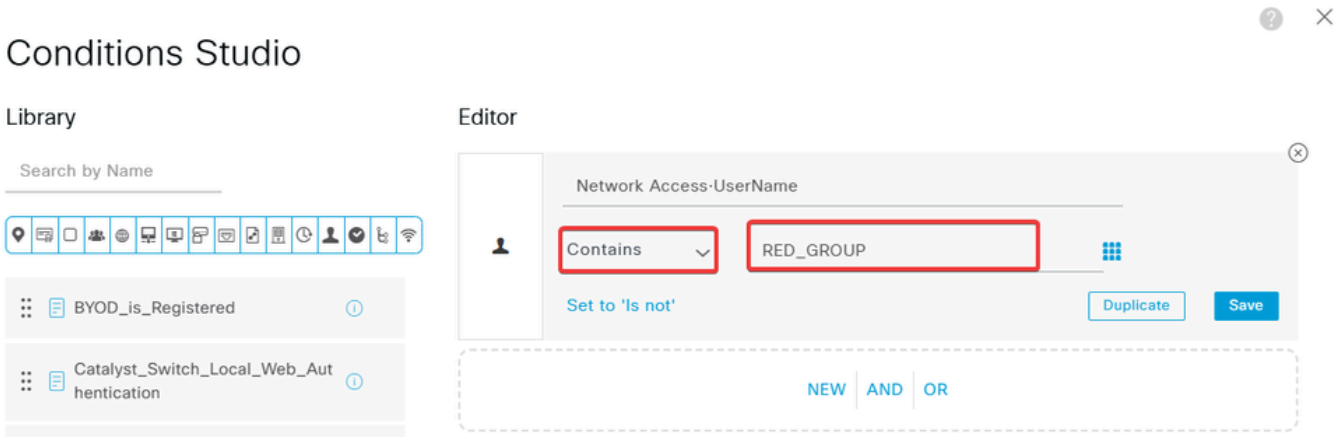
Crea nuova regola

c. Fare clic sulla casella di testo Editor attributi e fare clic sullSubject' icona. Selezionare l'**Network Access - UserName**attributo.



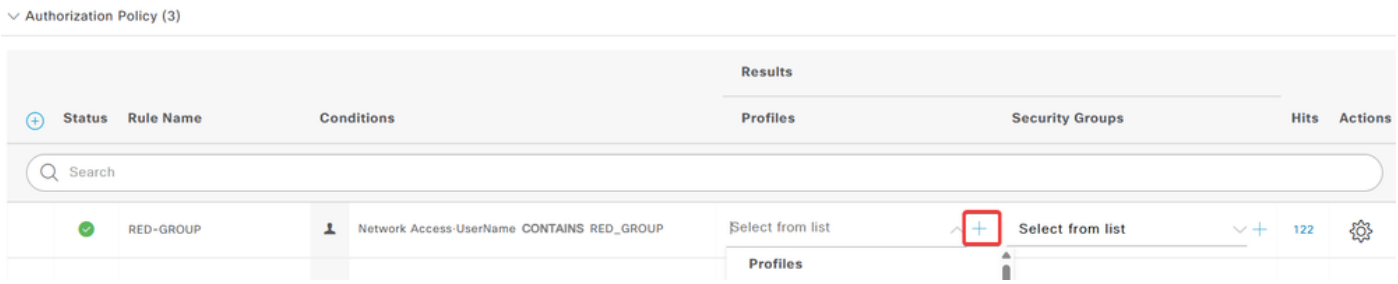
Seleziona accesso alla rete - NomeUtente

d. Selezionare**Contains**come operatore, quindi aggiungere il valore Organizzazione-Unità dei certificati.



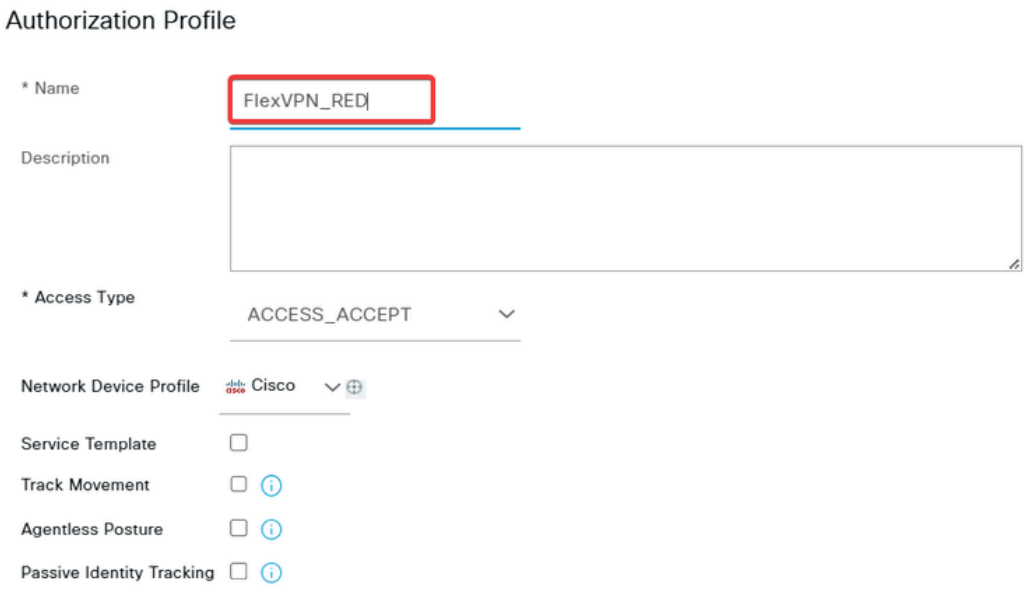
Aggiungi nome gruppo

e. Nella colonna Profili, fare clic sull**add (+)**'icona e scegliere **Create a New Authorization Profile.**



Aggiungi nuovo profilo di autorizzazione

f. Immettere il profilo**Name.**



Denominazione profilo di autorizzazione

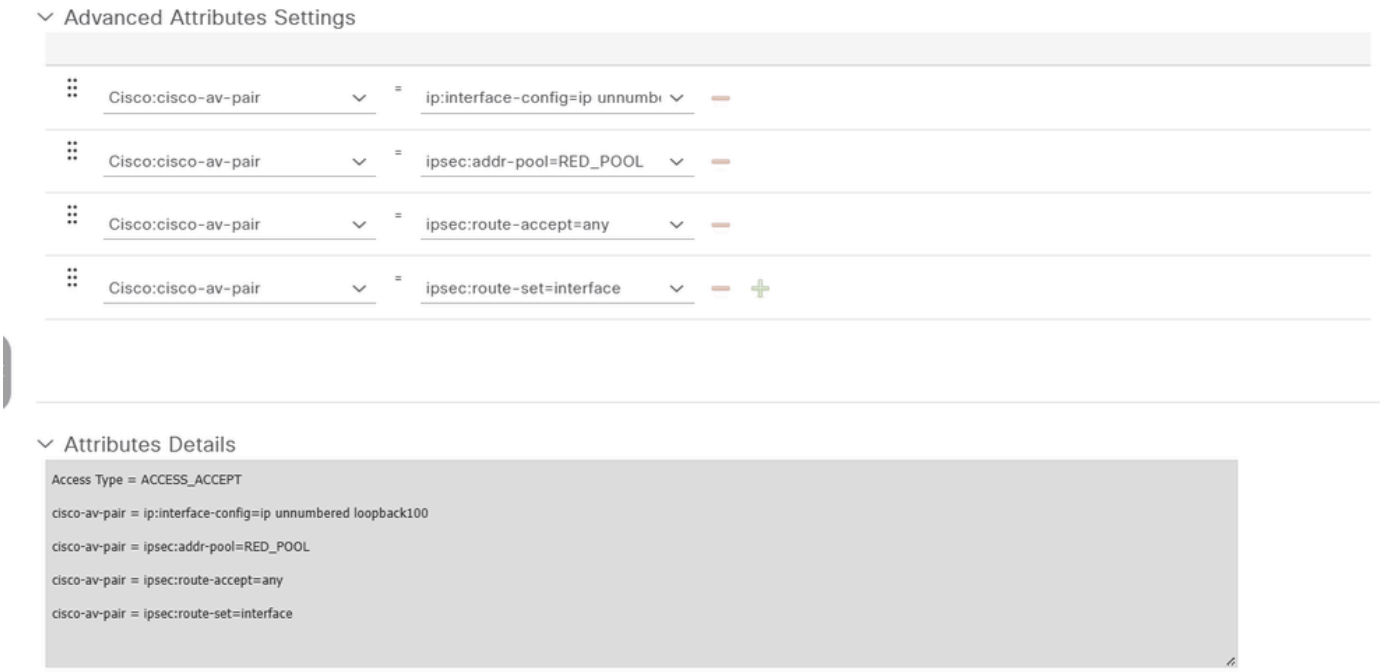
g. Passare a **Advanced Attributes Settings**. Quindi, selezionare l'cisco-av-pair'attributo dal menu a discesa sul lato sinistro e aggiungere l'attributo che è assegnato a FlexVPN Spoke a seconda del gruppo.

Gli attributi da assegnare a questo esempio includono:

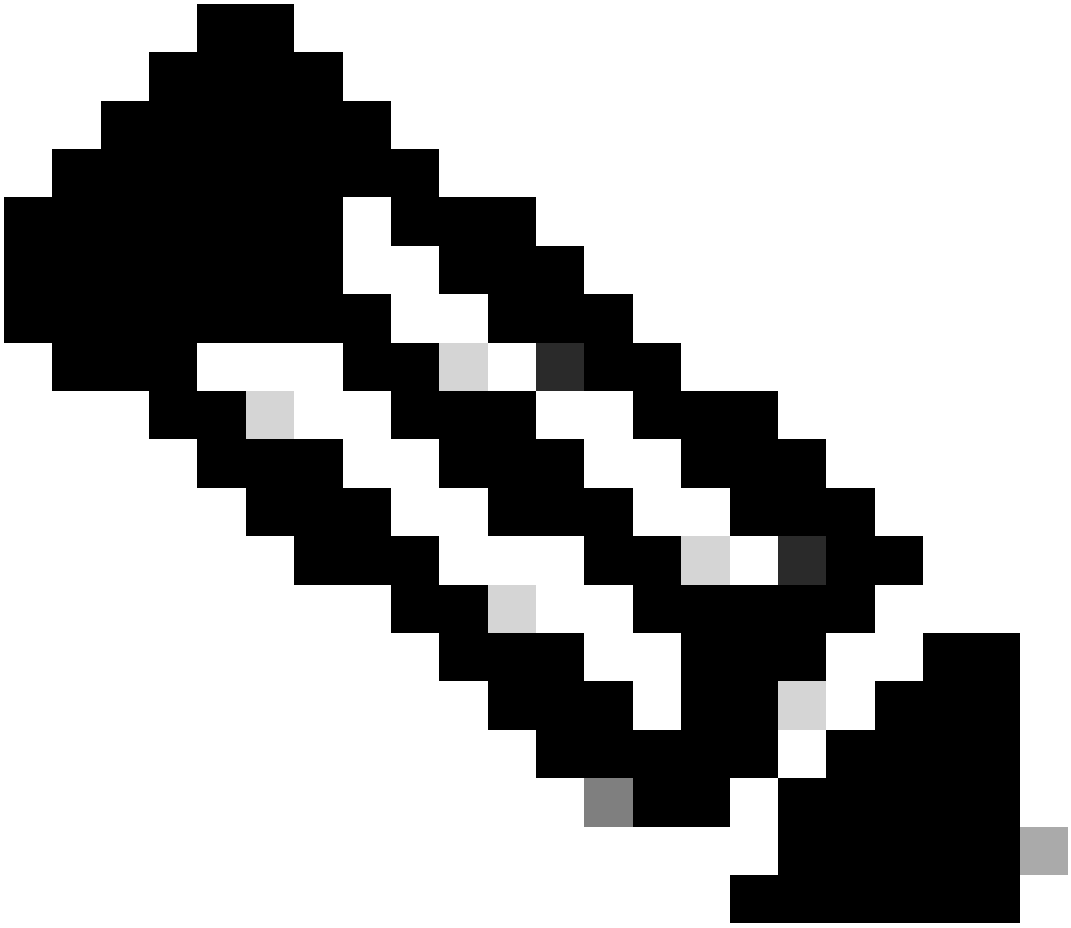
- Assegnazione dell'interfaccia di loopback come origine.
- Specifica del pool da cui gli spoke ottengono un indirizzo IP.

Gli attributi route accept any e route set interface sono obbligatori perché, senza di essi, i cicli di lavorazione non vengono pubblicizzati correttamente nei raggi.

```
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
```



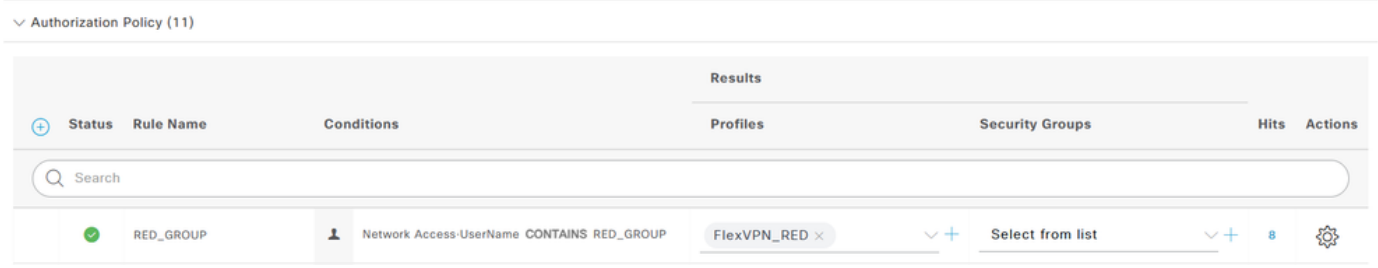
Impostazioni avanzate attributi



Nota: Per le specifiche degli attributi (nome, sintassi, descrizione, esempio e così via), consultare la guida alla configurazione di FlexVPN RADIUS Attributes:

Guida alla configurazione di FlexVPN e Internet Key Exchange versione 2, Cisco IOS XE Gibraltar 16.12.x

h. Assegnare il **authorization profile** nella colonna dei profili.



Regola di autorizzazione

i. Fare clic su **Save**.

Verifica

- Utilizzare il comando **show ip interface brief** per esaminare lo stato Tunnel, Virtual-Template e Virtual-Access.

Nell'hub, il modello virtuale ha uno stato attivo/inattivo normale e viene creato un accesso virtuale per ogni spoke che stabilisce una connessione con l'hub e mostra uno stato attivo/attivo.

<#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
```

Nello Spoke, l'interfaccia del tunnel ha ricevuto un indirizzo IP dal pool assegnato al gruppo e mostra uno stato attivo/attivo.

<#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
```

- Utilizzare il comando.**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
```

- Per verificare che **show crypto session** la connessione protetta tra i router sia stata stabilita, usare il comando.

```
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
```

- Utilizzare il comando`show ip eigrp neighbors`per verificare che l'adiacenza EIGRP sia stabilita con l'altro sito.

```
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
```

- Utilizzare il comando`show ip route`per verificare che le route siano state spostate nello Spoke.
  - Il percorso per la versione 10.20.1.10, interfaccia di loopback sullo spoke è stato appreso dall'Hub da EIGRP ed è accessibile attraverso l'accesso virtuale

<#root>

```
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
```

- Le route per le versioni 10.10.1.10 e 10.10.2.10 sono state apprese tramite EIGRP e sono raggiungibili tramite l'indirizzo IP di origine del gruppo RED (10.100.100.1), accessibile tramite il 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
```

Risoluzione dei problemi

In questa sezione vengono fornite informazioni utili per la risoluzione dei problemi relativi a questo tipo di distribuzione. Utilizzare questi comandi per eseguire il debug del processo di negoziazione del 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

I debug AAA e RADIUS possono essere utili per la risoluzione dei problemi relativi all'autorizzazione degli spoke.

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

Working Scenario

In questo registro vengono illustrati il processo di autorizzazione e l'assegnazione dei parametri.

```
     <#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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).