Configure FlexVPN with ISE Integration

Contents

Introduction

This document describes how to configure FlexVPN using Cisco Identity Services Engine (ISE) to dynamically assign configurations to spokes.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

This document is based on these software and hardware versions:

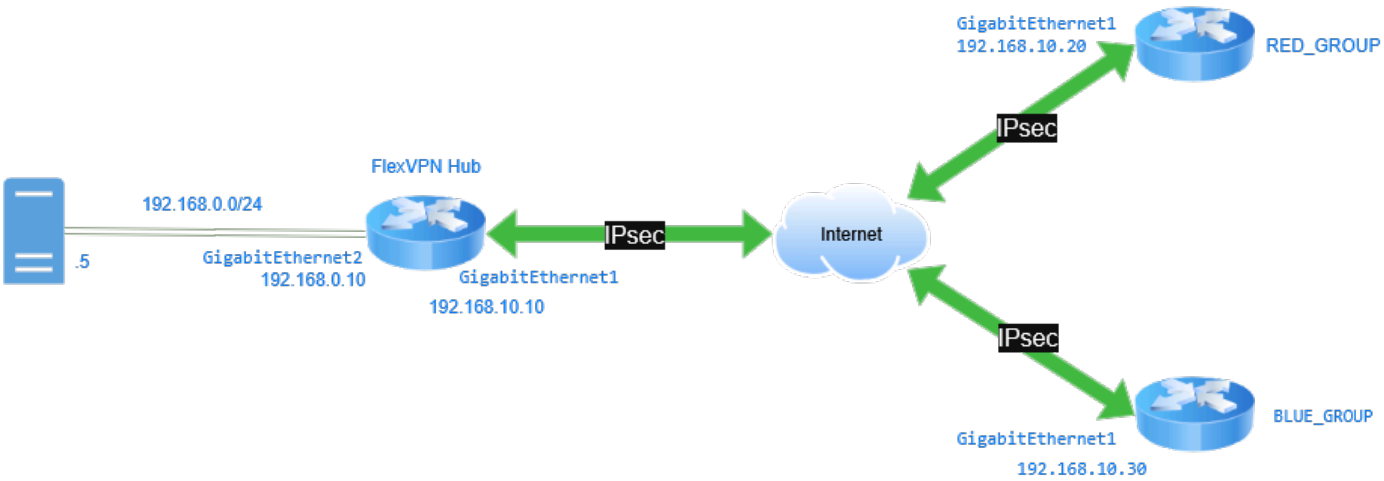
- Cisco CSR1000V (VXE) - Version 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram

FlexVPN can establish a connection with spokes and assign certain configurations that enable communication and traffic management. Referenced in the diagram, this demonstrates how FlexVPN integrates with ISE so that, when a spoke connects to the HUB, the parameters of tunnel source and DHCP pool are assigned depending on the group or branch to which the spoke belongs to. It is using the certificate to authenticate the spokes, then ISE with Radius as authorization and accounting server.



FlexVPN with ISE Integration

Step 1: Hub Configuration

a. Configure a trustpoint to store the router certificate. Certificates are used to authenticate the spokes.

```
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. Configure a **certificate map**. The purpose of the certificate map is to identify and match certificates based on the specified information, in case the router has multiple certificates installed.

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

c. Configure a RADIUS server for authorization and accounting on the device:

```
aaa new-model
!
aaa authorization network FLEX group ISE
```

```
aaa accounting network FLEX start-stop group ISE
```

d. Define the **RADIUS server group** with its IP address, communication ports, shared key, and source interface for the RADIUS traffic.

```
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. Configure the **loopback interfaces.** The loopback interfaces are used as the source connection for the tunnel and are dynamically assigned depending on the group that is connected.

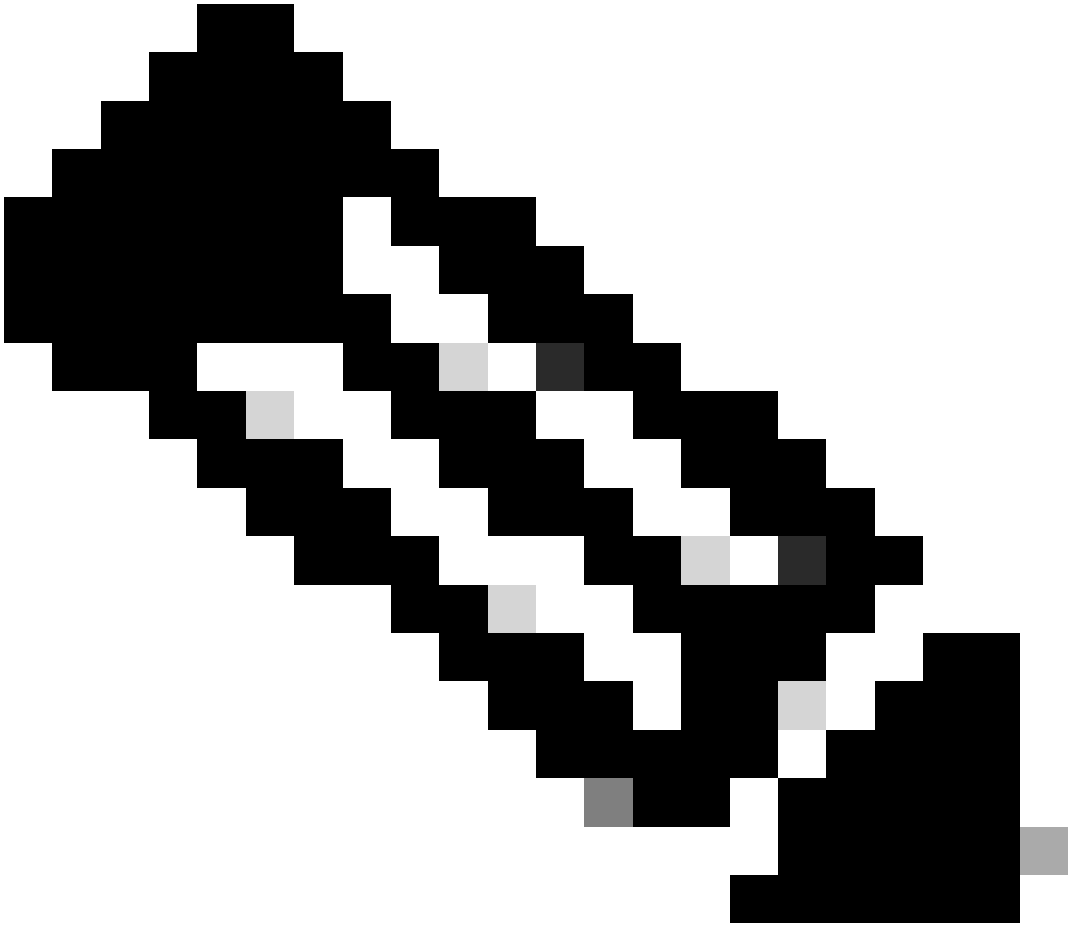
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f. Define an **IP local pool** for each group.

```
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. Configure **EIGRP** and advertise the networks of each group.

```
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
```



Note: FlexVPN supports dynamic routing protocols such as OSPF, EIGRP, and BGP over VPN tunnels. In this guide, EIGRP is being used.

---

h. Configure the **crypto ikev2 name mangler**. The IKEv2 name mangler is used to derive the username for IKEv2 authorization. In this case, it is configured to use the Organization-Unit information from the certificates on the spokes as the username for authorization.

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

i. Configure the **IKEv2 profile**. The certificate map, AAA server group, and name mangler are referenced in the IKEv2 profile.

The local and remote authentication are configured as **RSA-SIG**, in this specific scenario.

A **local user account** must be created on the RADIUS server with a username that matches the organization-unit value and the password Cisco1234 (as specified in the configuration below).

```
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. Configure the IPsec profile and reference the IKEv2 profile.

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

k. Create the virtual-template. It is used to create a virtual-access interface and link the IPsec profile created.

Set the **virtual-template** with no IP address, as this is assigned by the RADIUS server.

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

Configure two loopbacks to simulate an internal network.

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

Step 2: Spoke configuration

a. Configure a trustpoint to store the certificate of the spoke router..

```
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. Configure a certificate map. The purpose of the certificate map is to identify and match certificates based on the specified information, in case the router has multiple certificates installed.

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

c. Configure **AAA local authorization network**.

The **aaa authorization network** command is used to authorize access requests related to network services. It includes verifying whether a user has permission to access the requested service after being authenticated.

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

d. Configure the IKEv2 profile. The certificate map and AAA authorization local are referenced in the IKEv2 profile.

The local and remote authentication are configured as **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. Configure the IPsec profile and reference the IKEv2 profile.

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

f. Configure the tunnel interface. The tunnel interface is configured to receive a tunnel IP address from the Hub based on the authorization results.

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

g. Configure **EIGRP**, advertising the local network of the spoke and the tunnel interface.

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

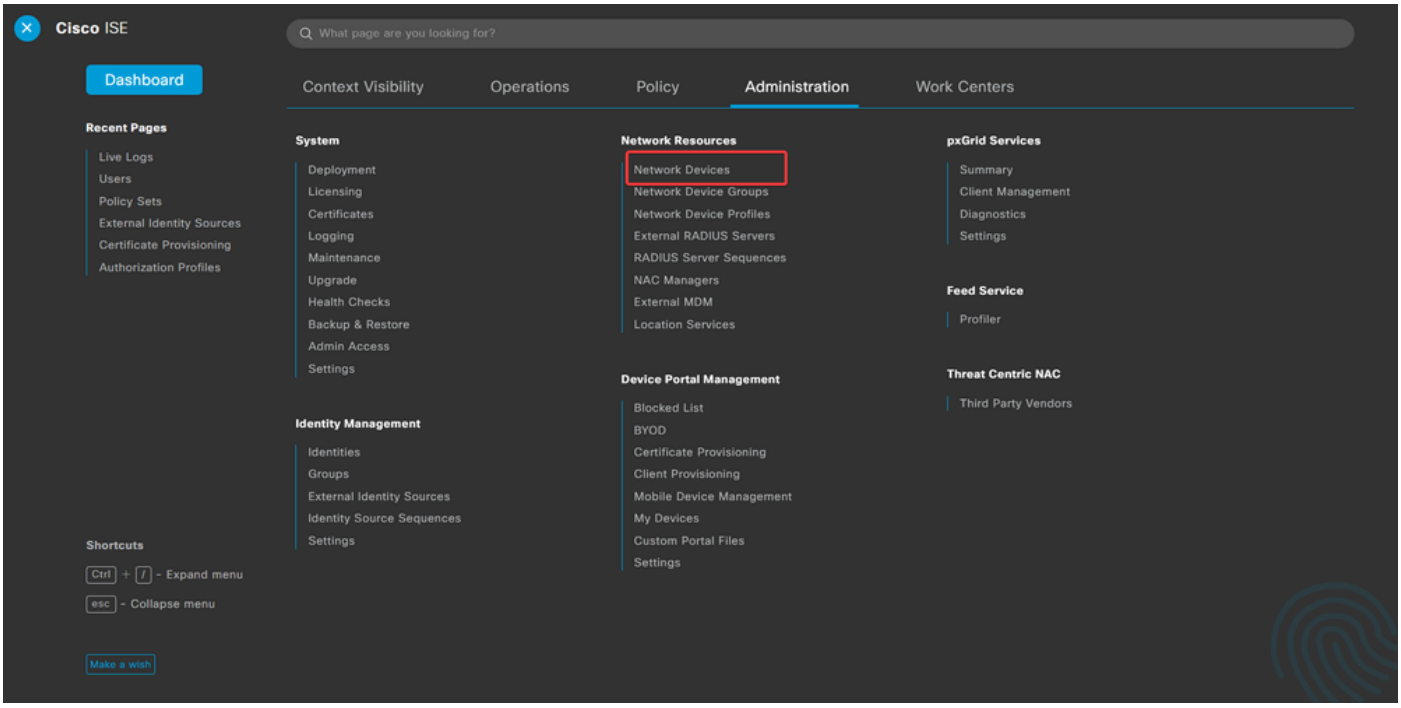
Configure a loopback to simulate an internal network.

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

Step 3: ISE Configuration

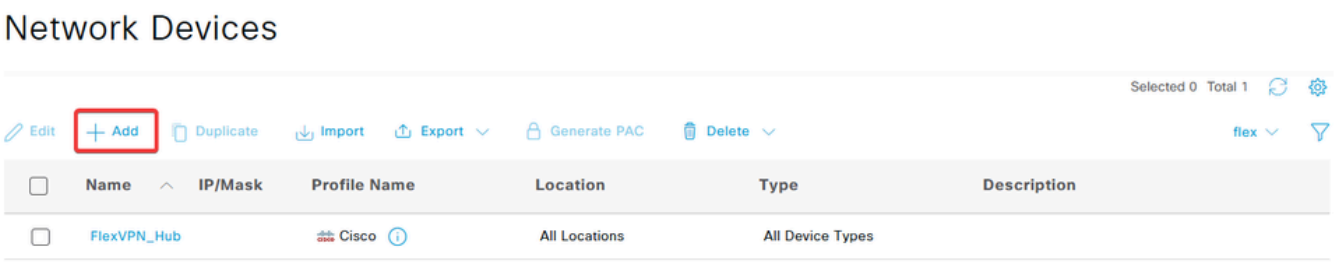
Step 3.1: Create Users, Groups, and add Network Device

a. Log into the **ISE server** and navigate to **Administration > Network Resources > Network Devices.**



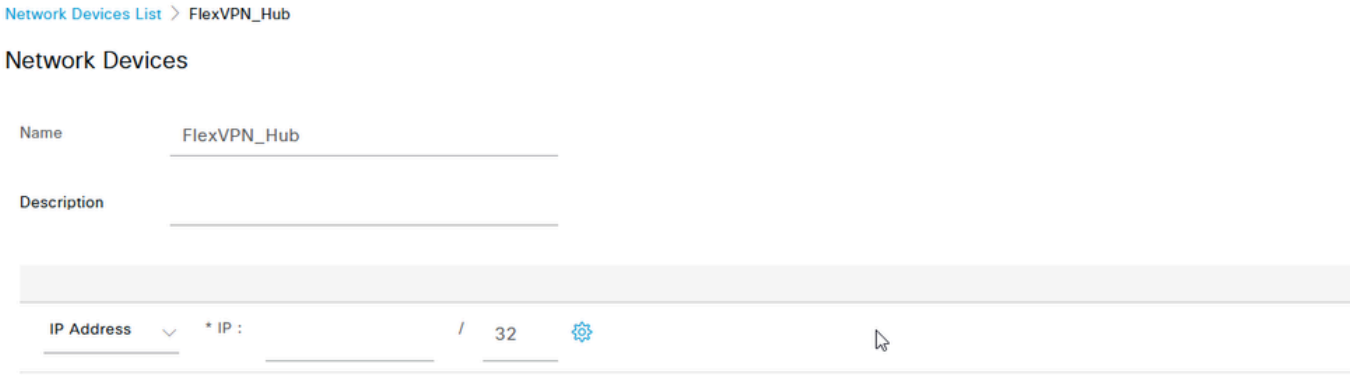
Administration-Network Resources-Network Devices

b. Click **Add** to configure the FlexVPN Hub as a AAA client.

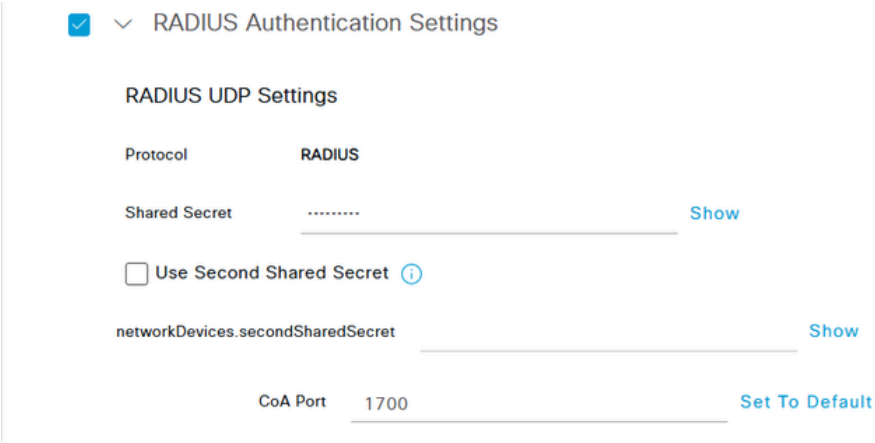


Add FlexVPN Router as AAA Client

c. Enter the **network device Name** and **IP Address fields** and then check **RADIUS Authentication Settings** box and add the **Shared Secret**. The shared secret password must be the same one that was used when the RADIUS Server Group was created on the FlexVPN Hub. Click Save.

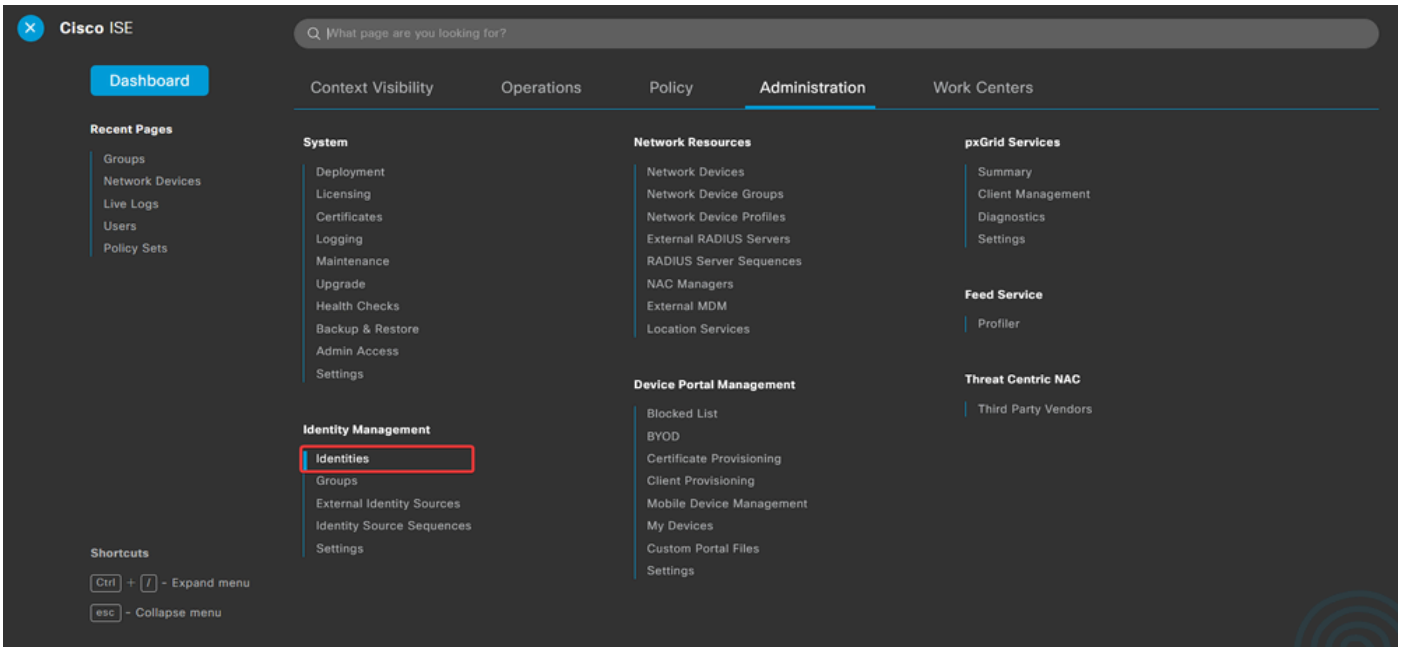


Network Device IP Address



Network Device Shared Key

d. Navigate to **Administration > Identity Management > Identities.**

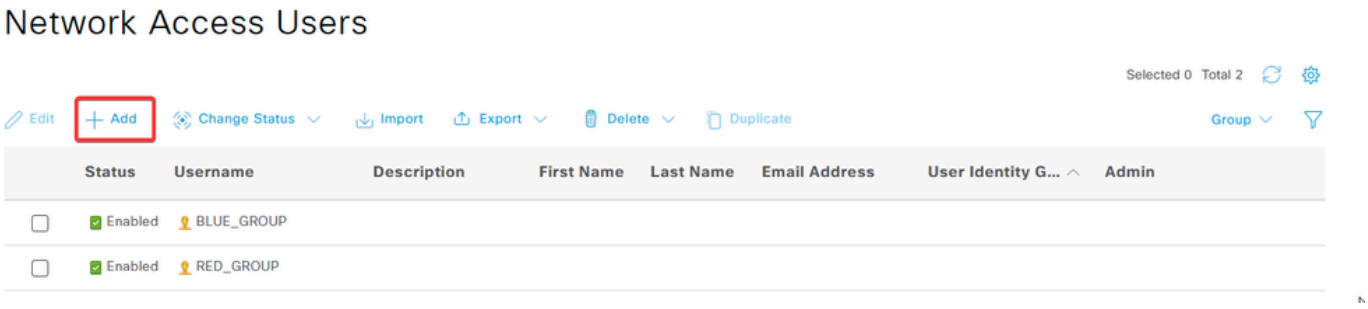


Administration-Identify Management-Identifies

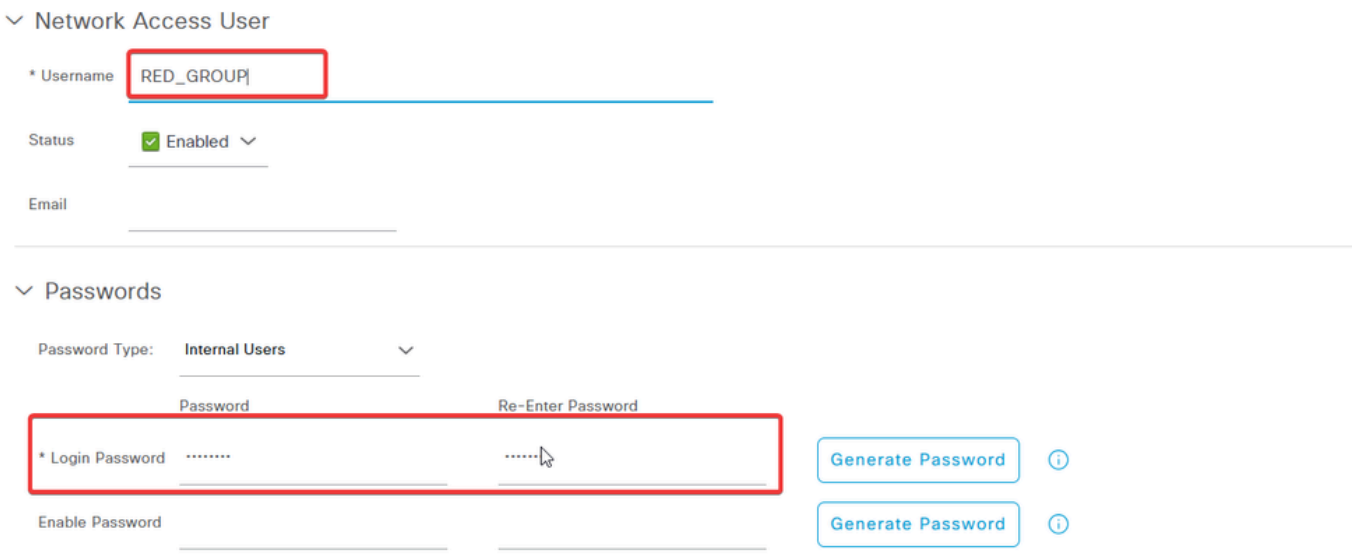
e. Click Add in order to create a new user in the server local database.

Enter the Username and **Login Password.** The username is the same name that the certificates has on organization-unit value on the certificate and the log in password must be the same that it was specify on the IKev2 profile.

Click **Save.**



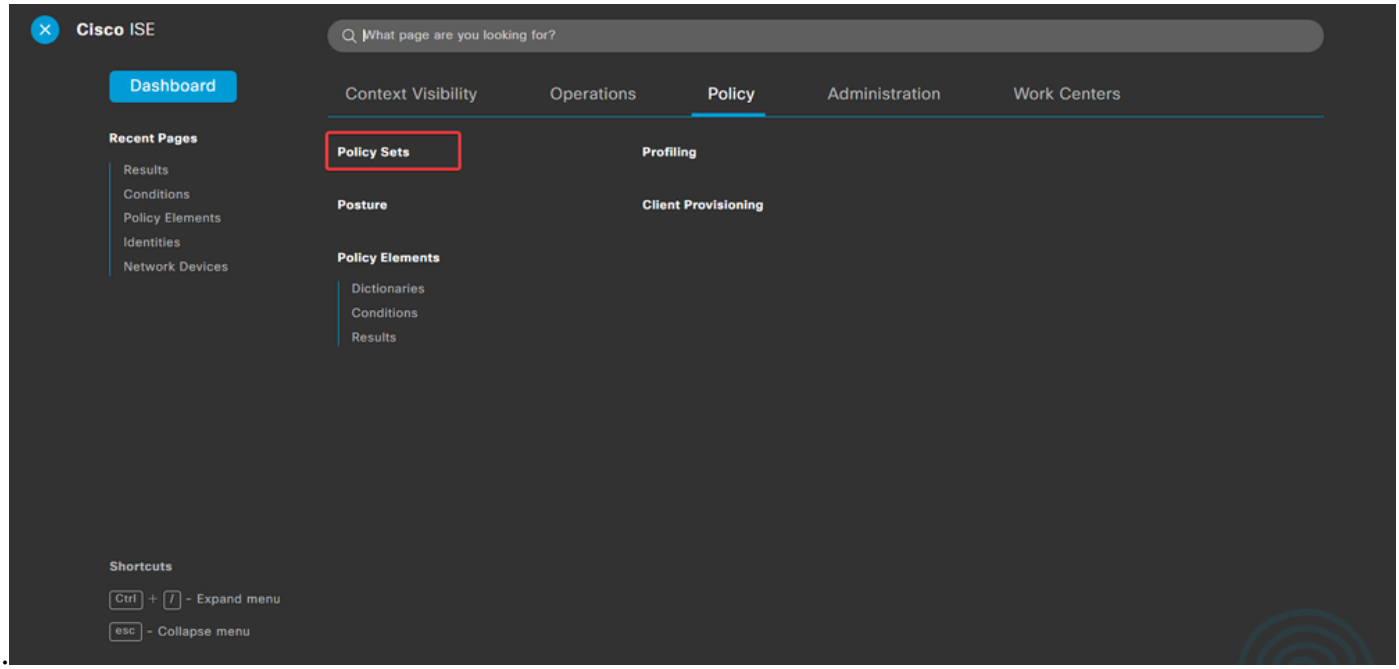
Administration-Identify Management-Identifies



Group Created Same as Organization Unit Value

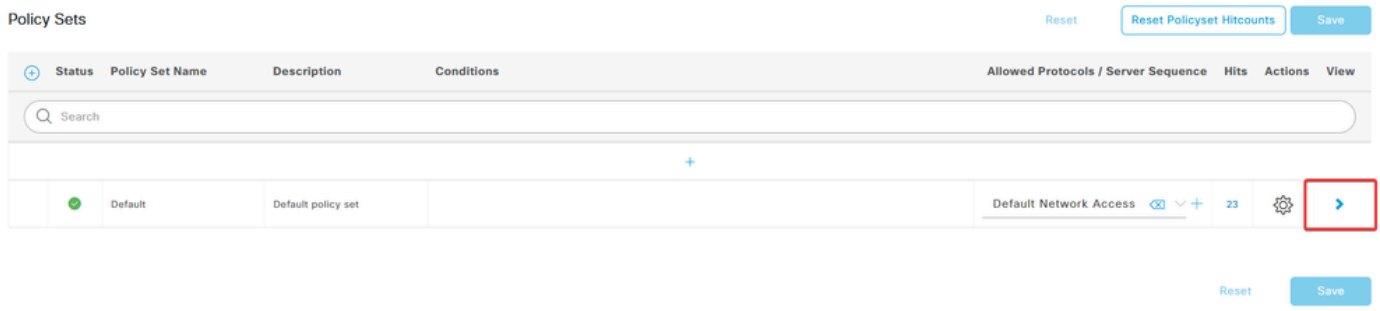
Step 3.2: Configure Policy Set

a. Navigate to **Policy > Policy Sets.**



Policy-Policy Sets

b. Select the **default authorization policy** by clicking the **arrow** on the right side of the screen:

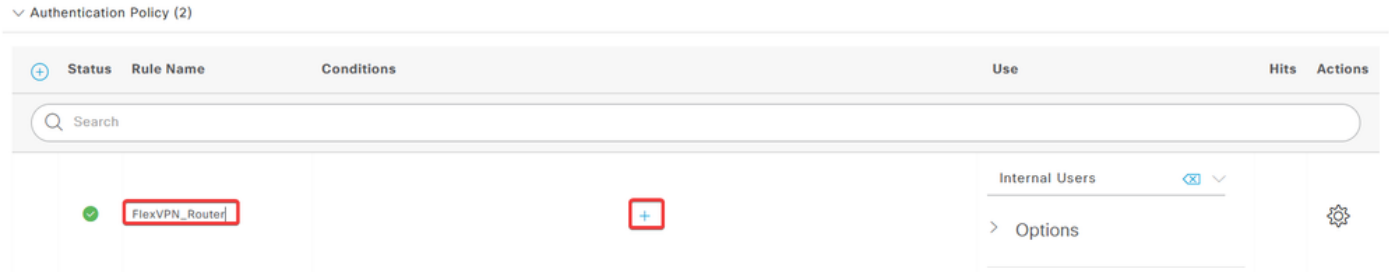


Edit Default Policy

c. Click the **drop-down menu arrow** next to Authentication Policy to expand it. Then, click the **add (+)** icon in order to add a new rule.

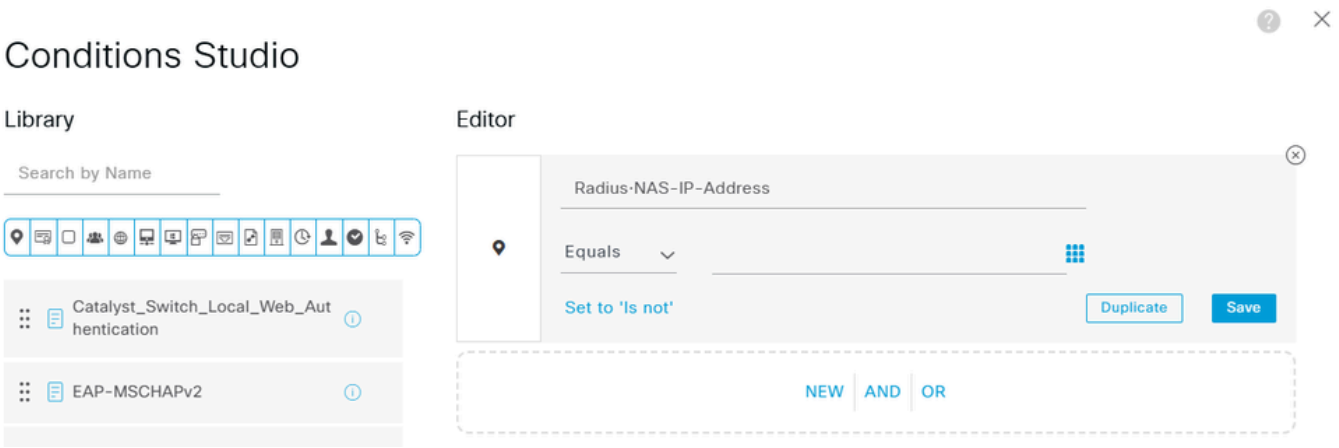
Add Authentication Policy

d. Enter the **name** for the rule and select the add (+) icon under **Conditions** column.



Create Authentication Policy

e. Click the **Attribute Editor** textbox and click the NAS-IP-Address icon. Enter the **IP address** (**192.168.0.10**) of the FlexVPN Hub.



Authenticate FlexVPN Hub

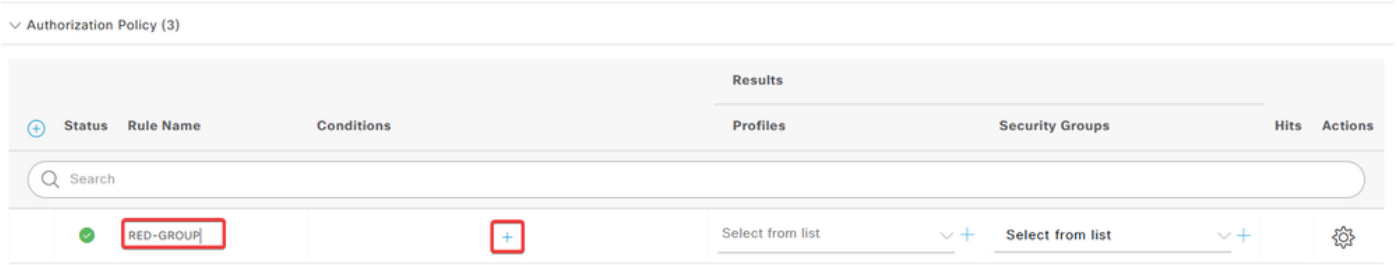
Authentication Policy

Step 3.3: Configure Authorization Policy

a. Click the **drop-down menu arrow** next to Authorization Policyto expand it. Then, click the **add (+)** icon in order to add a new rule.

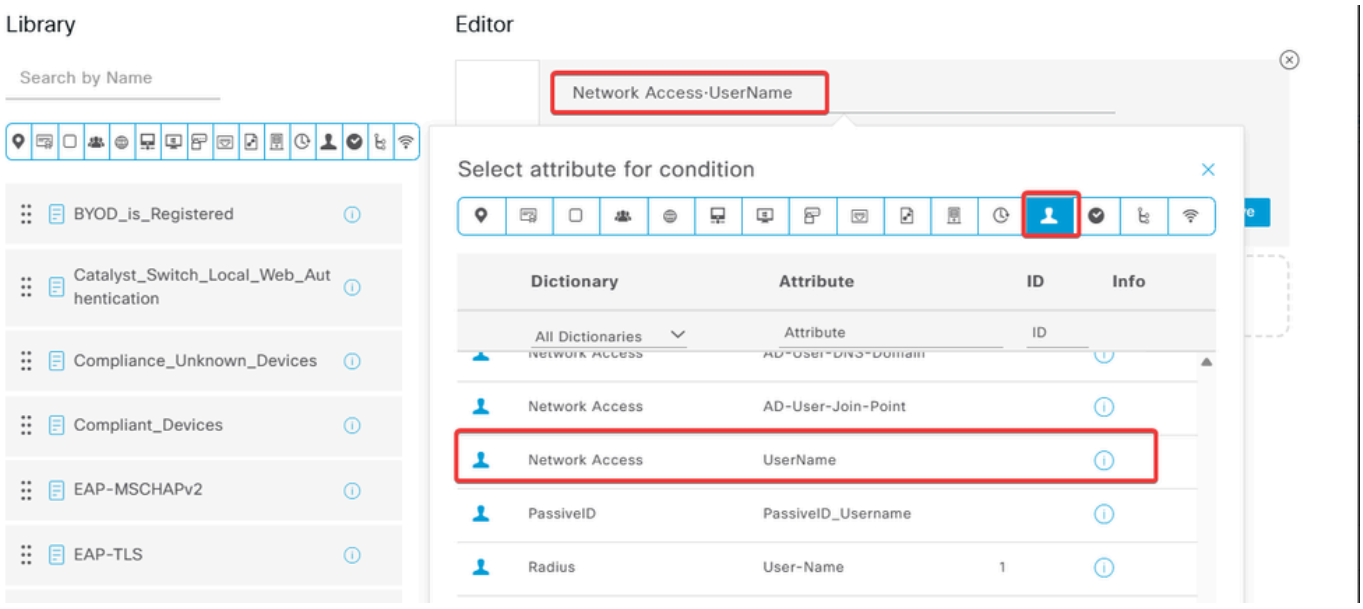
Create New Authorization Policy

b. Enter the **name** for the rule and select the **add (+)** icon under **Conditions** column.



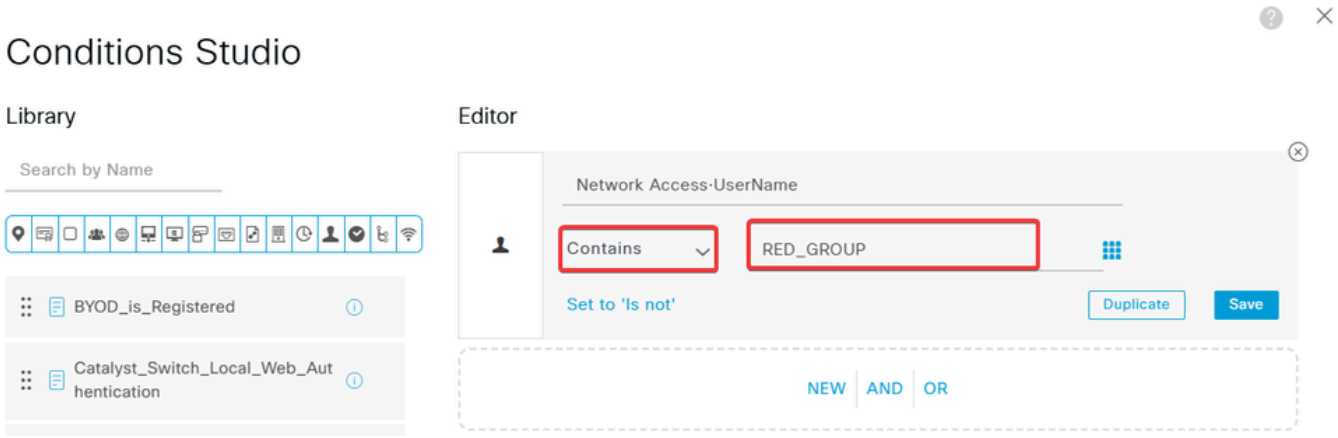
Create New Rule

c. Click the **Attribute Editor** textbox and click the Subject icon. Select the **Network Access - UserName** attribute.



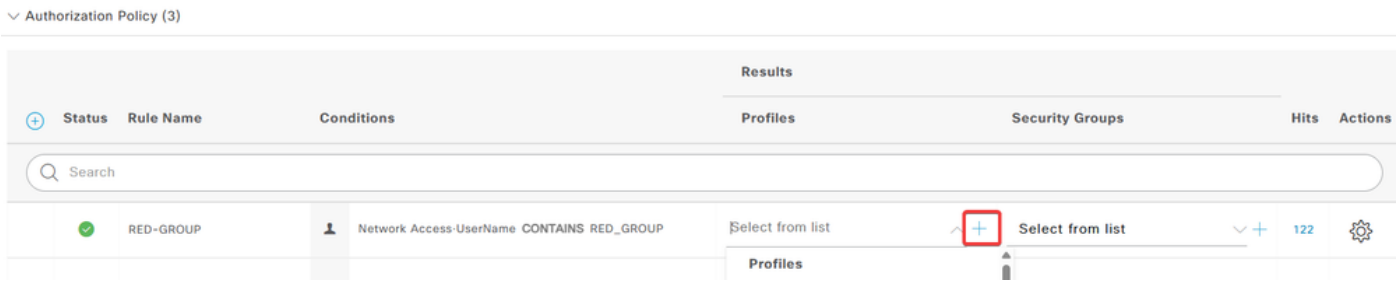
Select Network Access - UserName

d. Select Contains as the operator, then add the **Organization-Unit** value of the certificates.



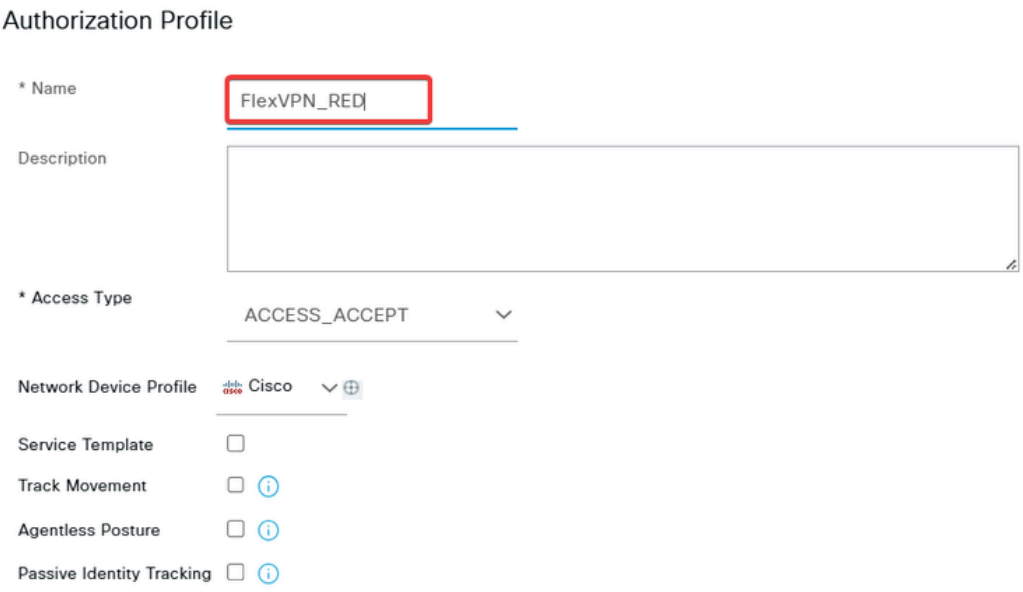
Add Group Name

e. In the **Profiles** column, click the add (+) icon and choose **Create a New Authorization Profile.**



Add New Authorization Profile

f. Enter the **profile Name.**



Name the Authorization Profile

g. Navigate to **Advanced Attributes Settings.** Then, select the cisco-av-pair **attribute** from the drop-down menu on

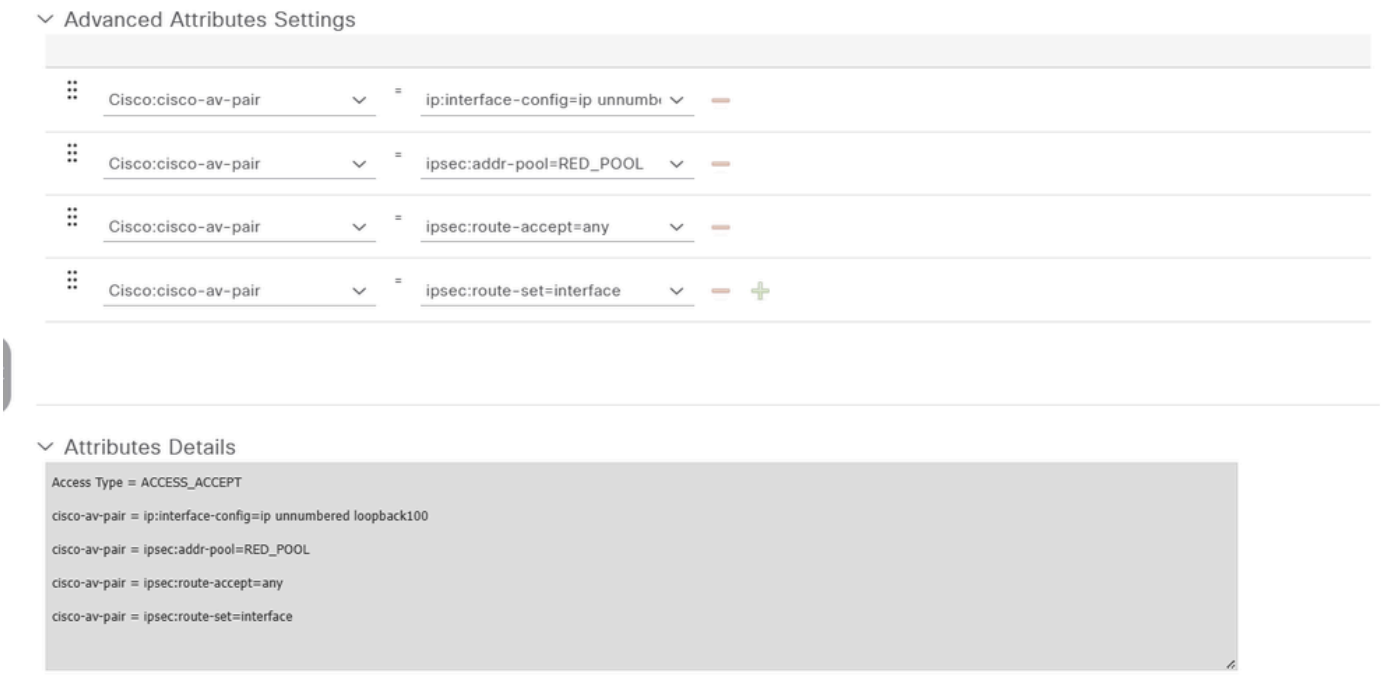
the left side, and add the **attribute** that is assigned to the **FlexVPN Spoke** depending on the group.

The attributes to be assigned for this example include:

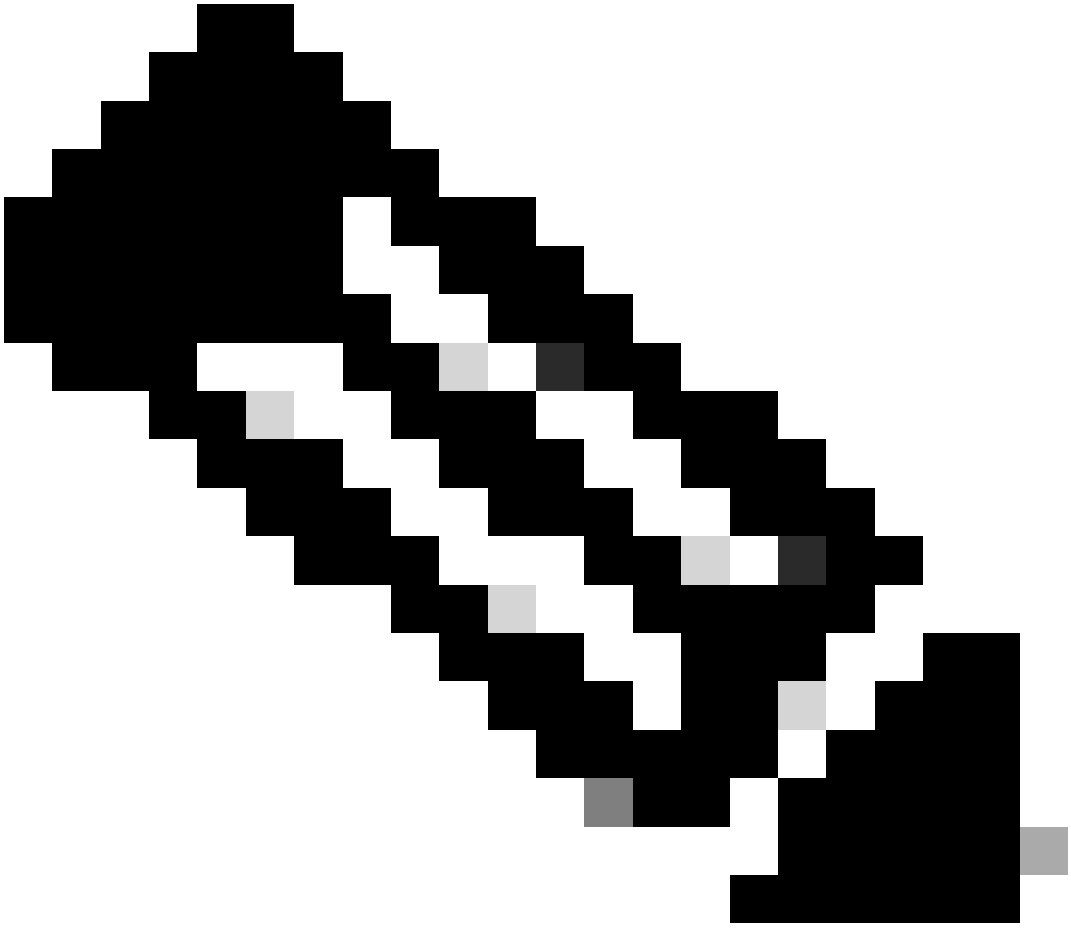
- Assigning the loopback interface as the source.
- Specifying the pool from which the spokes obtain an IP address..

The route accept any and route set interface attributes are required because, without them, the routes are not advertised properly to the spokes.

```
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
```



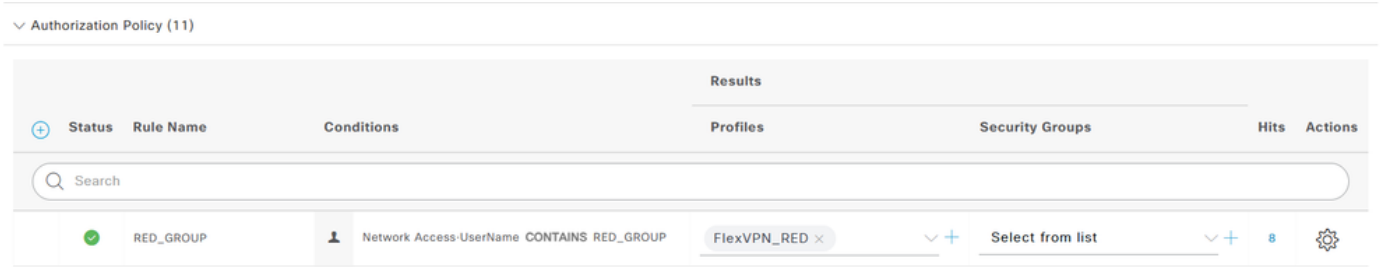
Advanced Attributes Settings



Note: For attribute specifications (name, syntax, description, example, and so on), please consult the FlexVPN RADIUS Attributes configuration guide:

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

h. Assign the **authorization profile** in the profiles column.



Authorization Rule

i. Click **Save.**

Verify

- Use the command **show ip interface brief** to review the Tunnel, Virtual-Template, and Virtual-Access status.

On the Hub, the Virtual-Template has an up/down status which is normal, and a Virtual-Access is created for each Spoke that established a connection with the Hub and shows an up/up status.

<#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
```

On the Spoke, the Tunnel interface received an IP address from the pool assigned to the group and shows an 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
```

- Use the command **show interfaces virtual-access <interface-number> 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
```

- Use the command **show crypto session** to confirm that the secure connection between the routers is established.

```
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
```

- Use the command show ip eigrp neighbors to confirm that the EIGRP adjacency is established with the other 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
```

- Use the command show ip route to verify that the routes have pushed to the Spokes.
  - The route for 10.20.1.10, loopback interface on the spoke has been learned by the Hub by EIGRP and it is accessible through the virtual-access

<#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
```

- The routes for 10.10.1.10 and 10.10.2.10 were learned via EIGRP and are reachable through the source IP of the RED_GROUP (10.100.100.1), which is 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
```

Troubleshoot

This section provides information you can use to troubleshoot this type of deployment. Use these commands to debug the tunnel negotiation process:

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 and RADIUS debugs can help with the troubleshooting of the authorization of the Spokes.

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

Working Scenario

This logs shows the authorization process, and assigment of the parameters..

```
     <#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(OOOOO1A8): 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(OOOOO1A9): 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(OOOOO1AA): 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(OOOOO1AB): Bind i/f
RADIUS/ENCODE(OOOOO1AB):Orig. component type = VPN IPSEC
RADIUS(OOOOO1AB): Config NAS IP: 192.168.0.10
vrfid: [65535]  ipv6 tableid : [O]
idb is NULL
RADIUS(OOOOO1AB): Config NAS IPv6: ::
RADIUS(OOOOO1AB): Sending a IPv4 Radius Packet
RADIUS(OOOOO1AB): 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
```