配置FlexVPN与ISE集成

目录

简介

先决条件

- 要求
- 使用的组件

配置

- 网络图
- 步骤 1：中心配置
- 步骤 2：分支配置
- 步骤 3：ISE 配置
  - 第 3.1 步：创建用户、组并添加网络设备
  - 第 3.2 步：配置策略集
  - 第 3.3 步：配置授权策略

验证

故障排除

- 工作场景

简介

本文档介绍如何使用思科身份服务引擎(ISE)配置FlexVPN以动态地将配置分配给分支。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎(ISE)配置
- RADIUS协议
- Flex虚拟专用网络(FlexVPN)

使用的组件

本文档基于以下软件和硬件版本：

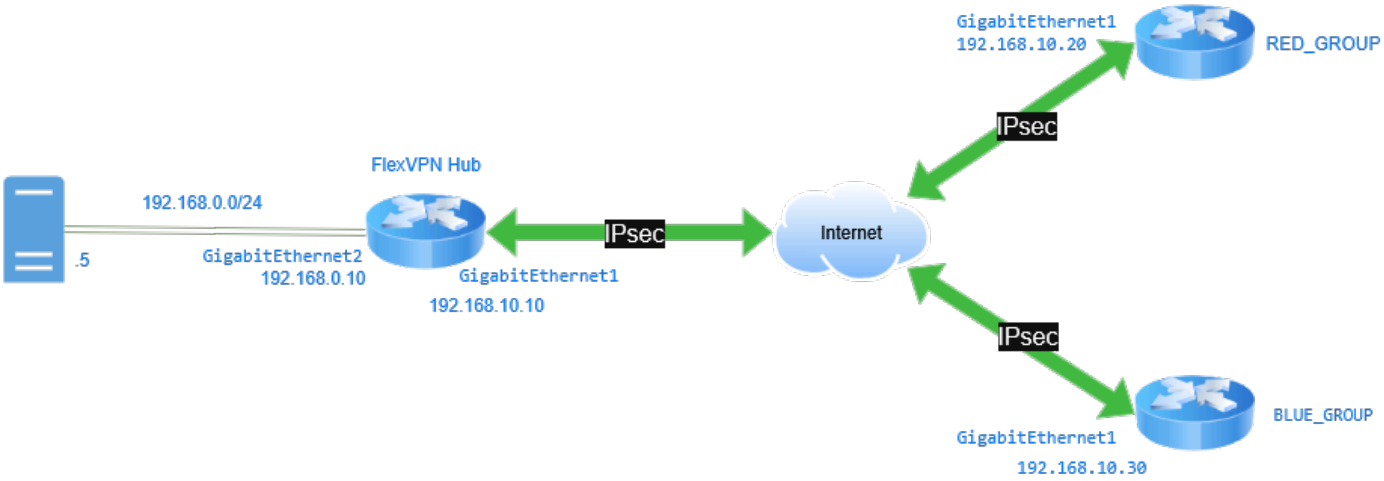
- 思科CSR1000V(VXE)- 17.03.04a版本
- 思科身份服务引擎(ISE)- 3.1

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图

FlexVPN可与分支建立连接，并分配启用通信和流量管理的特定配置。如图所示，这演示了FlexVPN如何与ISE集成，以便在分支连接到HUB时，根据分支所属的组或分支分配隧道源和DHCP池的参数。它使用证书对辐射点进行身份验证，然后使用Radius作为授权和记帐服务器的ISE。



集成ISE的FlexVPN

步骤 1：中心配置

a.配置trustpoint，以存储路由器证书。证书用于对辐射点进行身份验证。

```
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.配置**certificate map**。其目的是根据certificate map指定的信息识别和匹配证书，以便路由器安装多个证书。

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

c.在设备RADIUS server上配置用于授权和记帐的：

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

d.为RADIUS**RADIUS server group**流量定义其IP地址、通信端口、共享密钥和源接口。

```
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.配置**loopback interfaces**。将loopback interfaces用作隧道的源连接，并根据所连接的组进行动态分配。

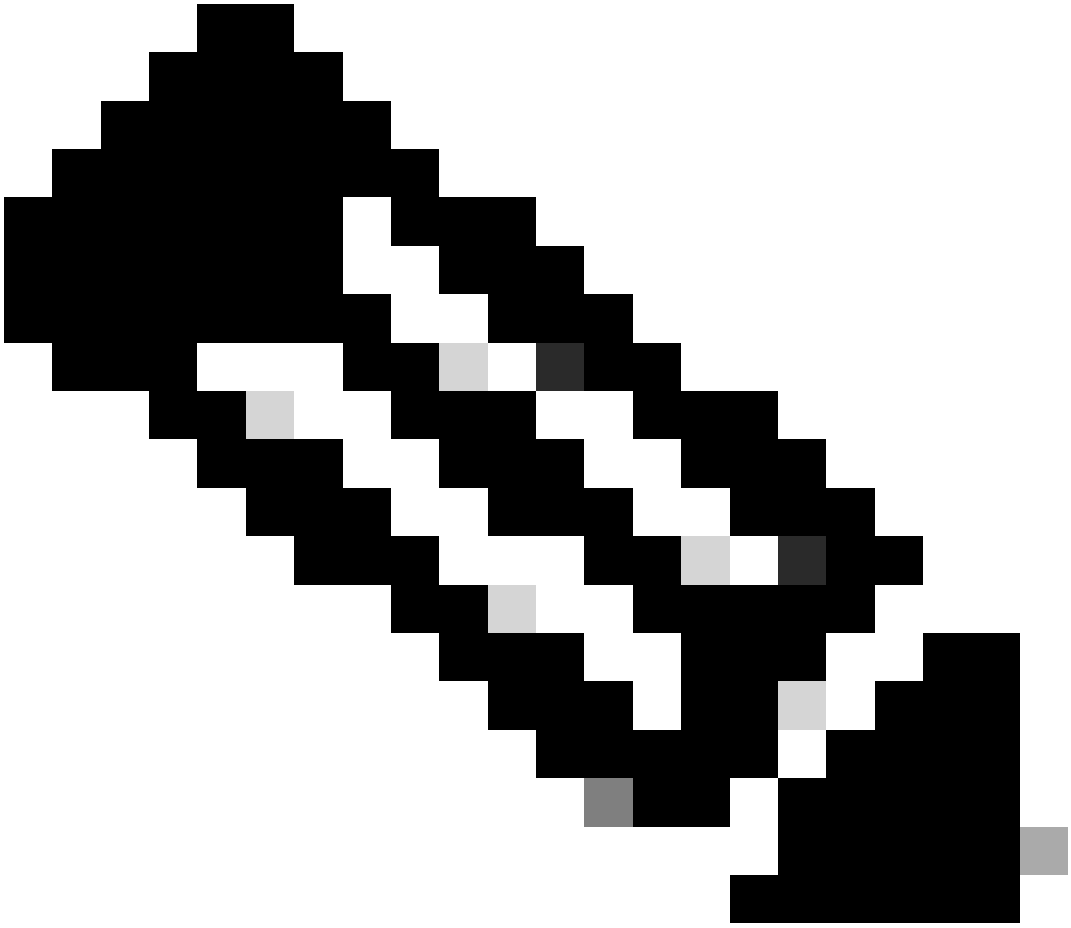
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f.为每个组**IP local pool**定义一个。

```
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.配置EIGRP并通告每个组的网络。

```
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
```



注意：FlexVPN支持动态路由协议，例如VPN隧道上的OSPF、EIGRP和BGP。本指南使用EIGRP。

---

h.配置**crypto ikev2 name mangler**。用IKEv2 name mangler于获取IKEv2授权的用户名。在这种情况下，它配置为使用分支上证书中的组织单元信息作为授权的用户名。

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

i.配置**IKEv2 profile**。在certificate mapIKEvAAA server group2配置文件中引用 name mangler、和。

在此特定场景中，本地和远**RSA-SIG**程身份验证配置为。

必须在上创建本地用户帐户RADIUS server，其用户名与值及密码organization-unit(如下面的配置中所指定Cisco1234)匹配。

```
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.配置IPsec profile，并参IKEv2 profile考。

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

k.创建virtual-template。它用于创建并链virtual-access interface接所创建IPsec profile的。

设置无**virtual-template**IP地址的，因为这是由分配的RADIUS server。

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

配置两loopbacks，以模拟内部网络。

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

步骤 2：分支配置

a.配置trustpoint，以存储分支路由器的证书。

```
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.配置certificate map。其目的是根据certificate map指定的信息识别和匹配证书，以便路由器安装多个证书。

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

c.配置AAA本地授权网络。

aaa authorization network命令用于授权与网络服务相关的访问请求。它包括验证用户在经过身份验证后是否有权访问请求的服务。

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

d.配置IKEv2 profile。中certificate map引用和AAA本地授IKEv2 profile权。

本地和远程身份验证配置为 **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.配置IPsec profile ，并参考 IKEv2 profile.

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

f.配置tunnel interface。配置tunnel interface为根据授权结果从集线器接收隧道IP地址。

```
interface Tunnel0
```

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

g.配置EIGRP，通告分支和的本地网tunnel interface络。

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

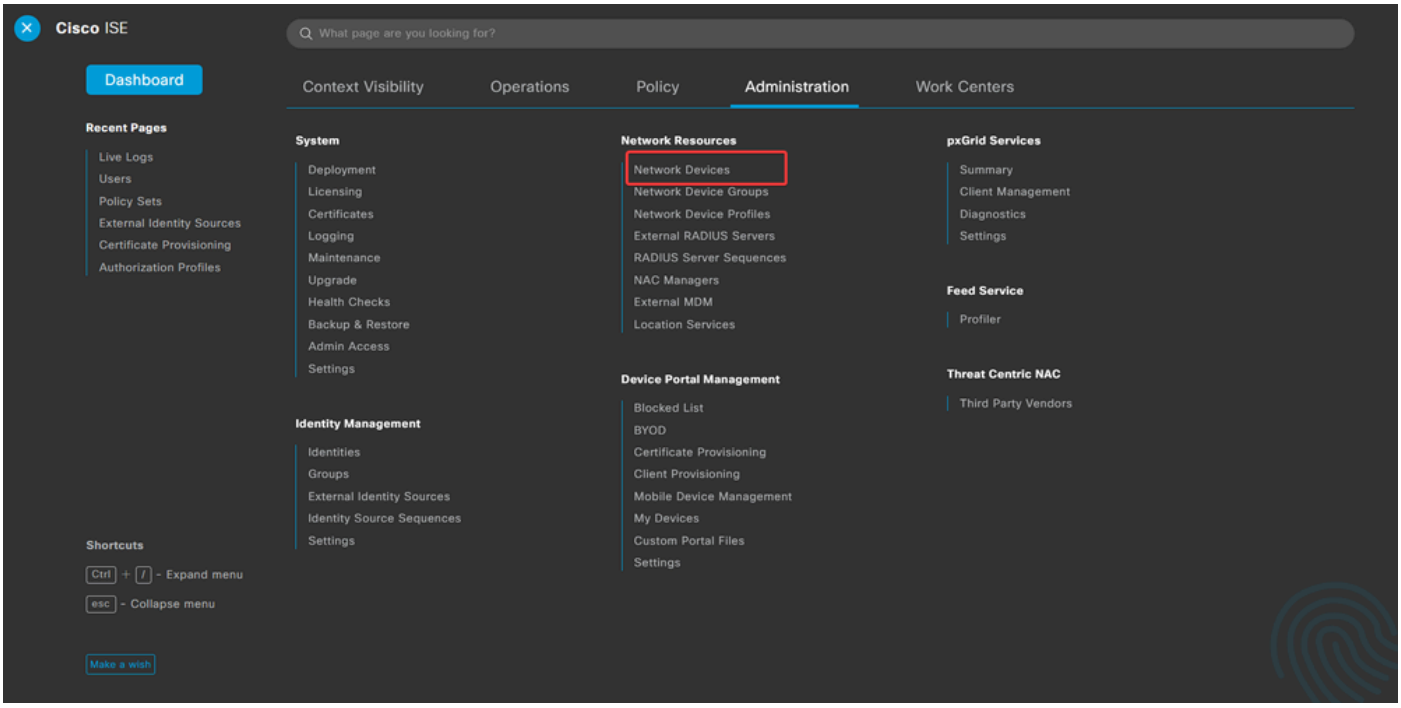
配置loopback，以模拟内部网络。

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

步骤 3：ISE 配置

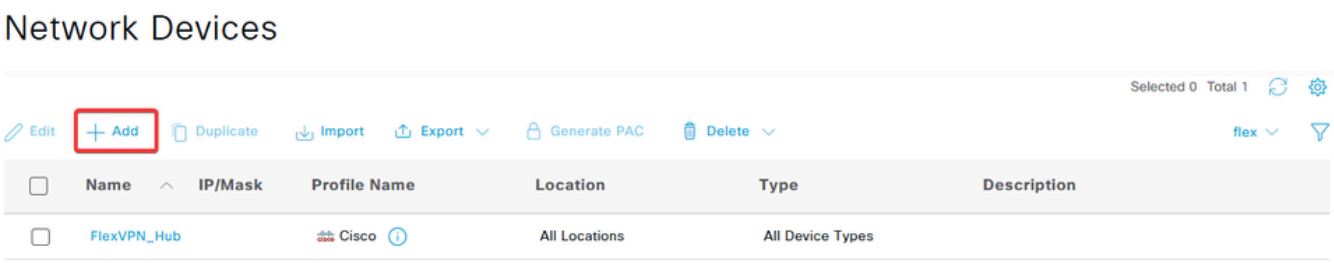
第 3.1 步：创建用户、组并添加网络设备

a.登录ISE服务器并导航至**Administration** > **Network Resources** > **Network Devices**。



管理 — 网络资源 — 网络设备

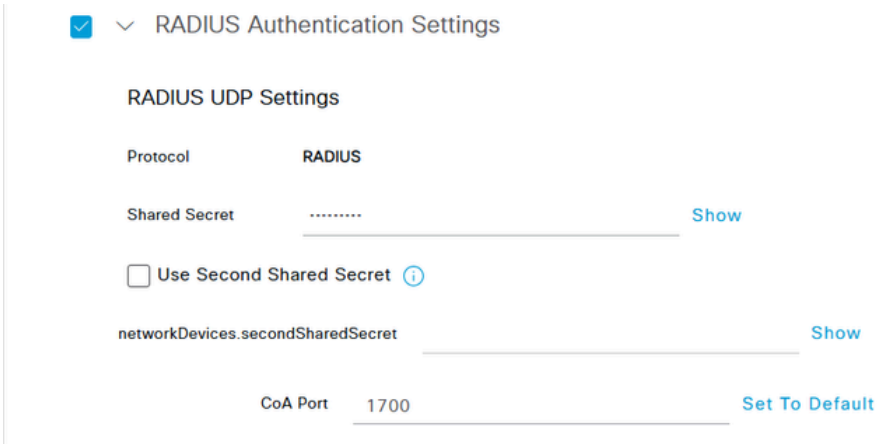
b.点击**Add**以将FlexVPN中心配置为AAA客户端。



将FlexVPN路由器添加为AAA客户端

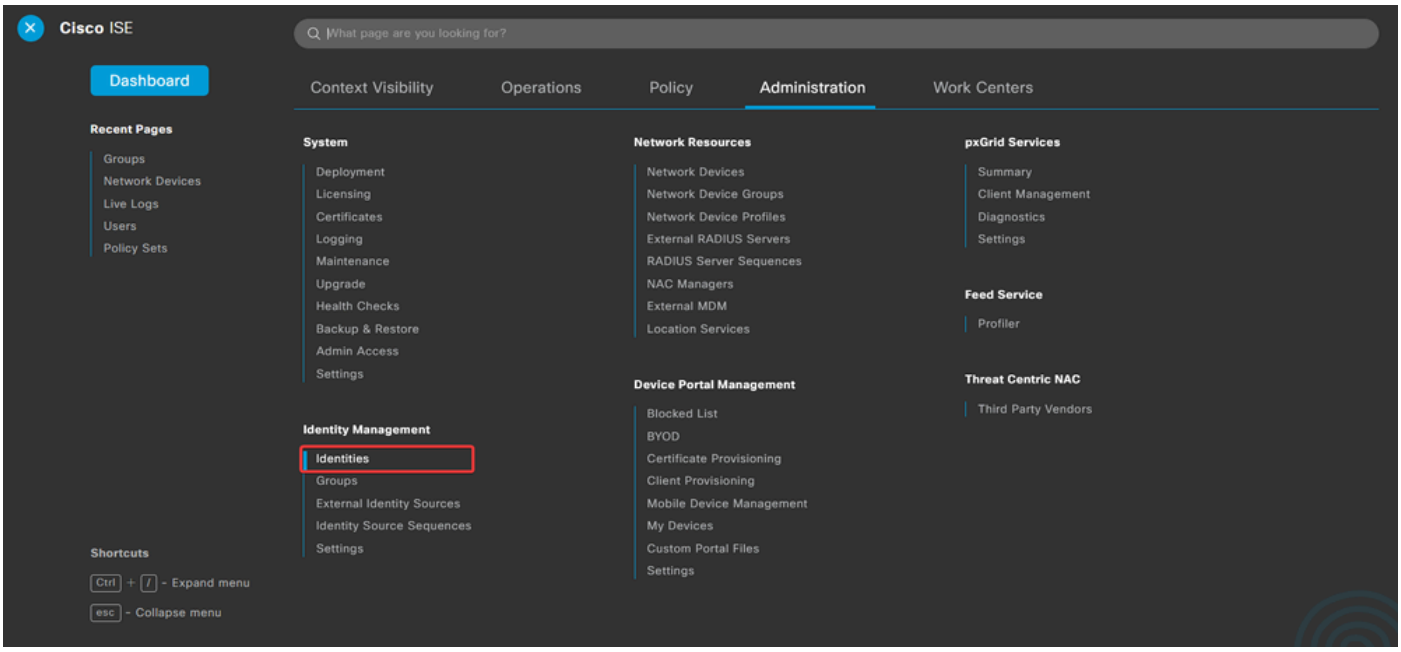
RADIUS Authentication Settings c.输入网络设备名称和IP地址字段，然后选中此复选框，然后添加**Shared Secret**.“共享密钥密码必须与FlexVPN中心上创建RADIUS服务器组时使用的密码相同”。单击。Save

网络设备IP地址



网络设备共享密钥

d.导航至**Administration** > **Identity Management** > **Identities**中。

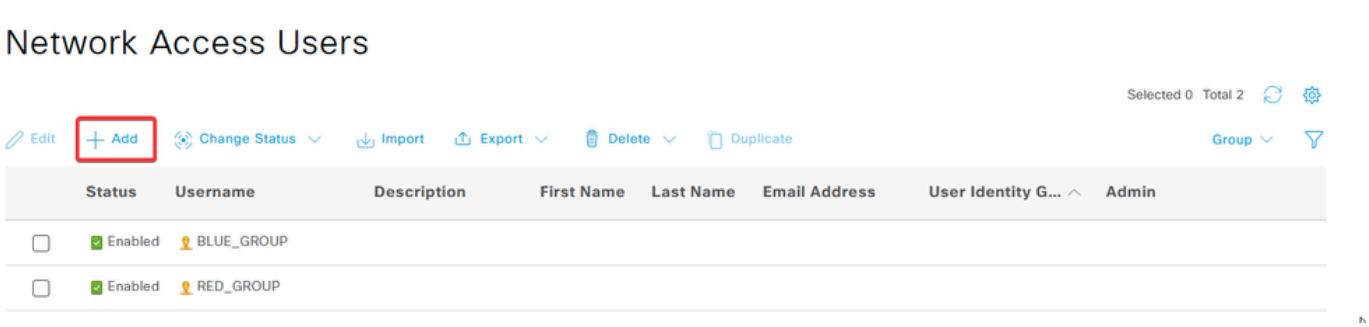


Administration-Identify Management-Identify

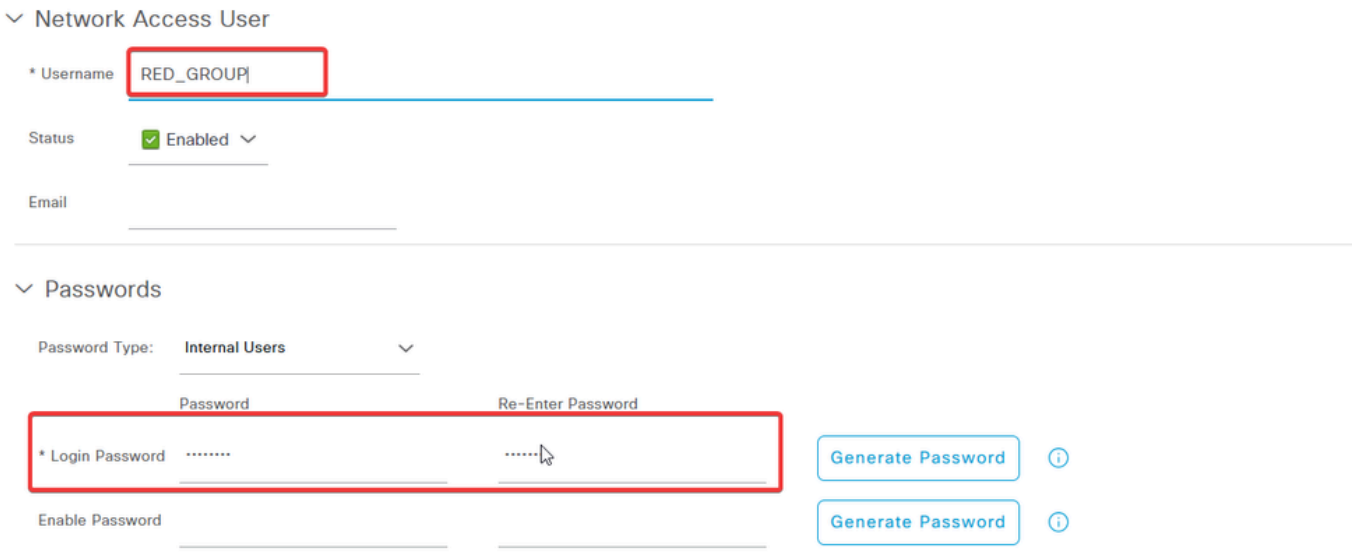
e.单击Add，以便在服务器本地数据库中创建新用户。

输入和Username**Login Password**。用户名与证书在证书上的organization-unit值上的名称相同，且登录密码必须与IKev2配置文件中指定的密码相同。

单击。**Save**



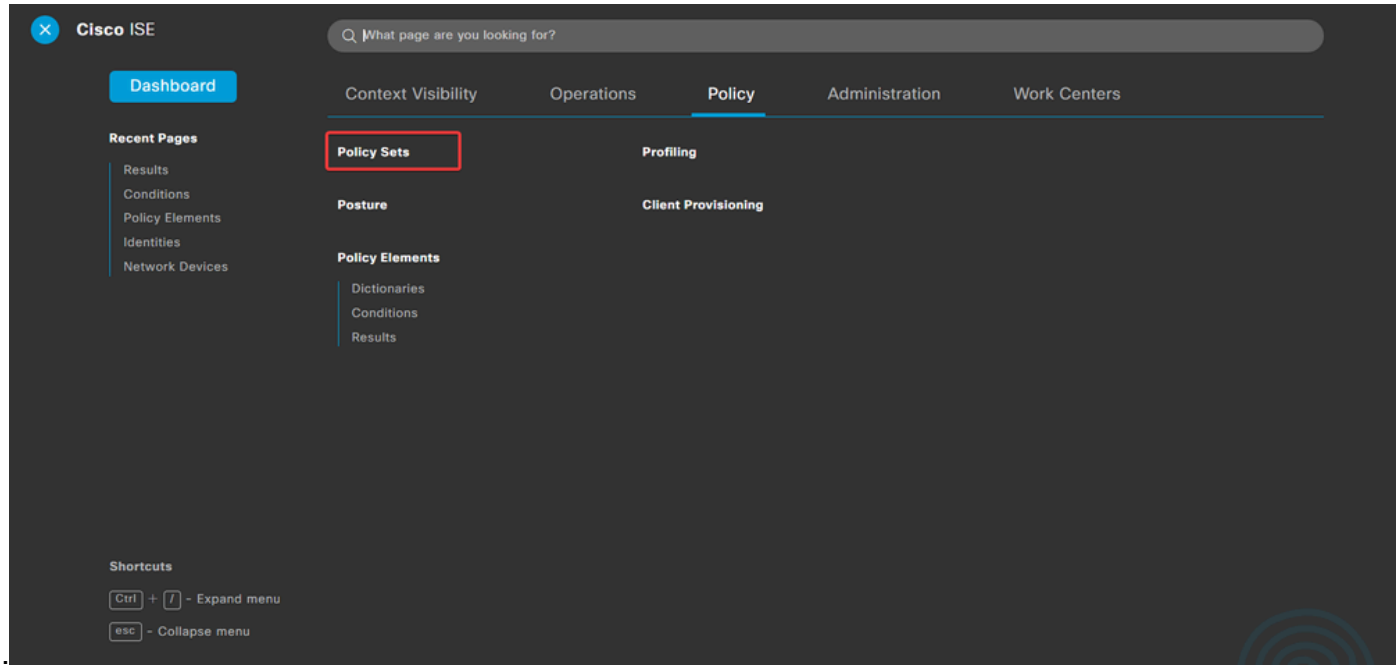
Administration-Identify Management-Identify



创建的组与组织单位值相同

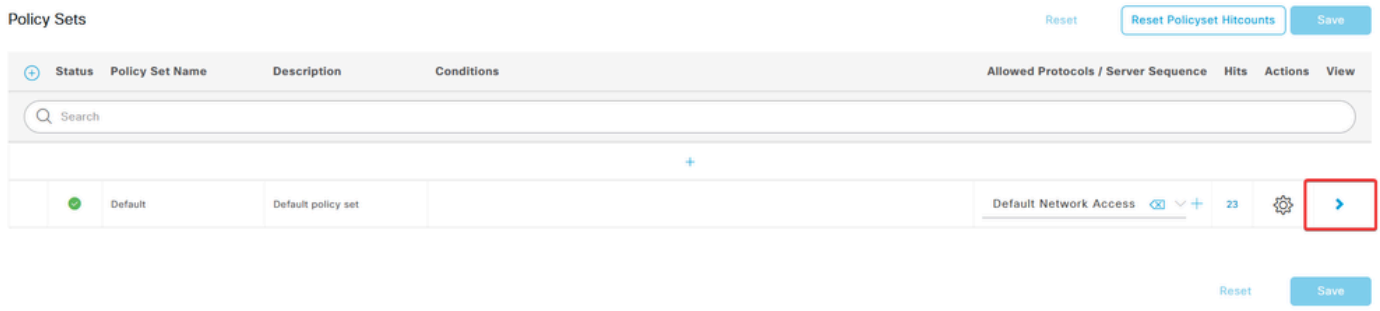
第 3.2 步：配置策略集

a.导航至**Policy > Policy Sets**中。



策略 — 策略集

b.通过点击屏幕右侧的箭头选择默认授权策略：

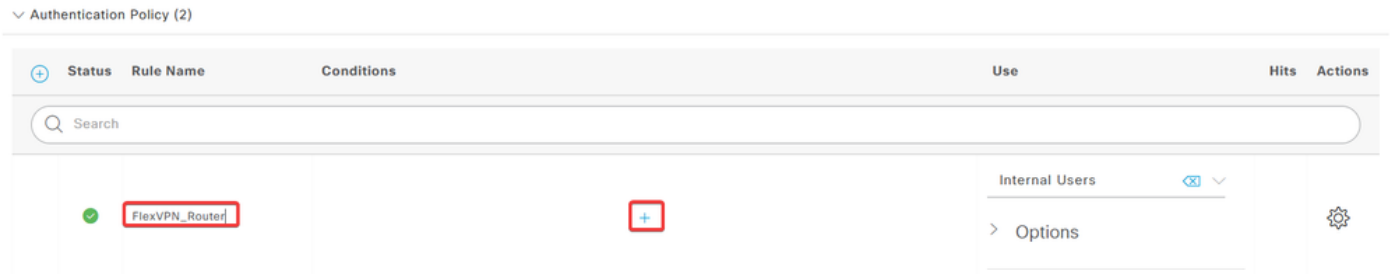


编辑默认策略

c.点击旁边的下拉菜单箭头Authentication Policy，展开它。然后，点击**add (+)**图标以添加新规则。

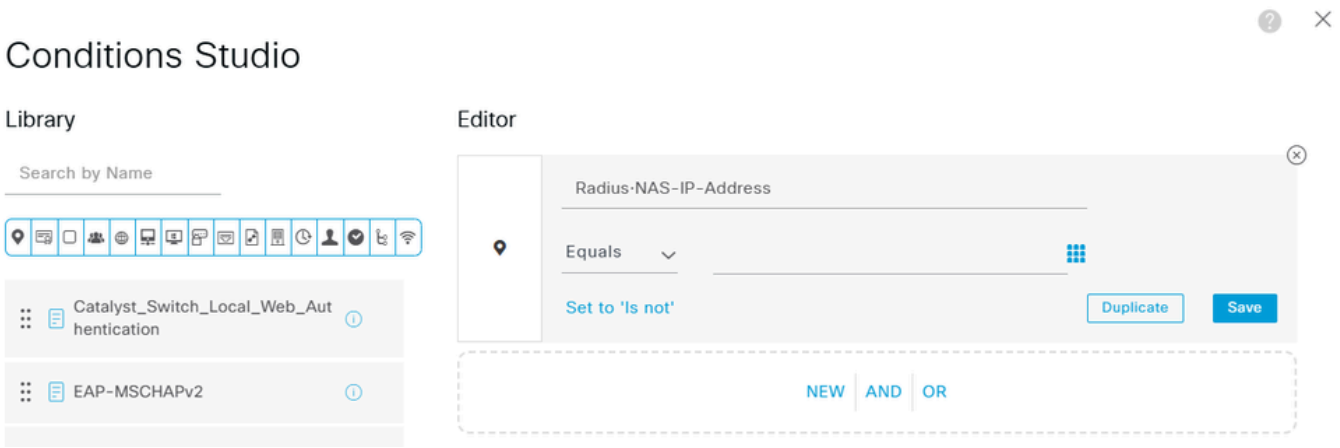
添加身份验证策略

d.输入规则的名称，然后在“条件add (+)”列下选择图标。



创建身份验证策略

e.单击Attribute Editor文本框并点击图NAS-IP-Address标。输入FlexVPN集线器的IP地址(192.168.0.10)。



Authenticate FlexVPN Hub

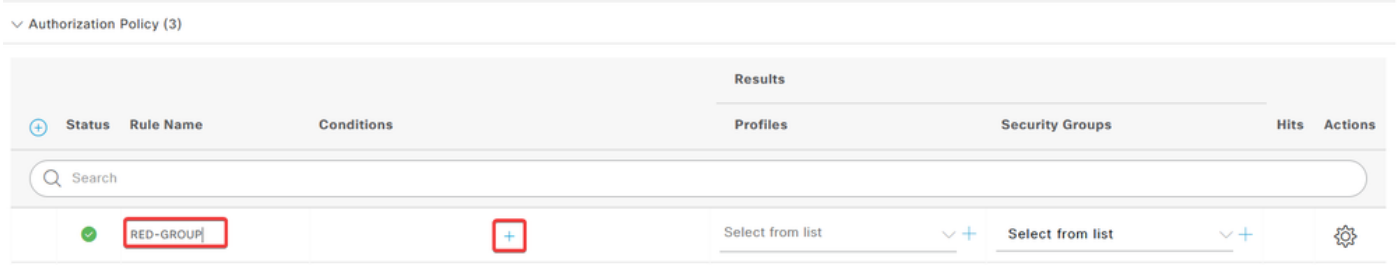
验证策略

第 3.3 步：配置授权策略

a.点击旁边的下拉菜单箭Authorization Policy头将其展开。然后，点击**add (+)**图标以添加新规则。

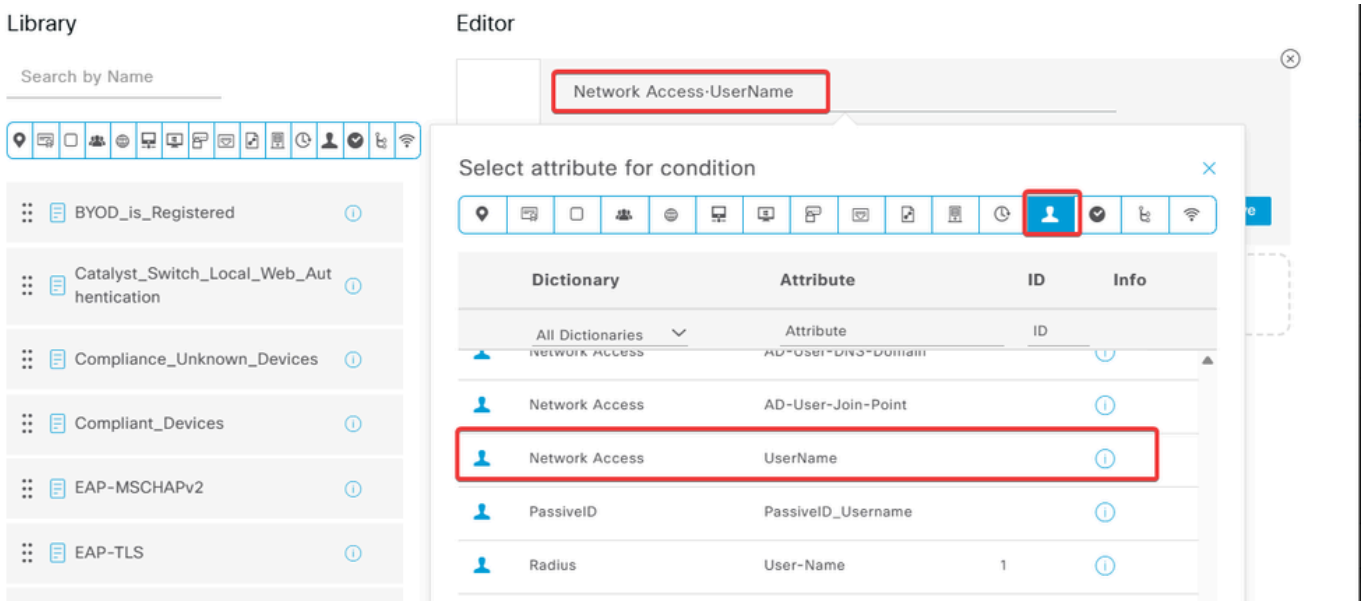
创建新授权策略

b.输入规则的名称，并在Conditions**add (+)**列下选择图标。



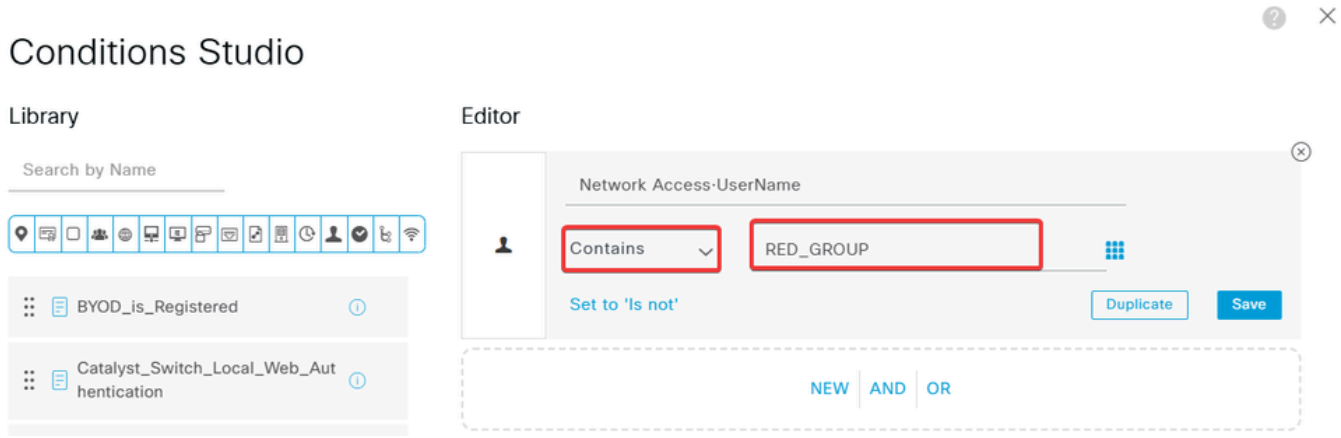
创建新规则

c.单击“属性编辑器”文本框，然后单击图Subject标。选择属**Network Access - UserName**性。



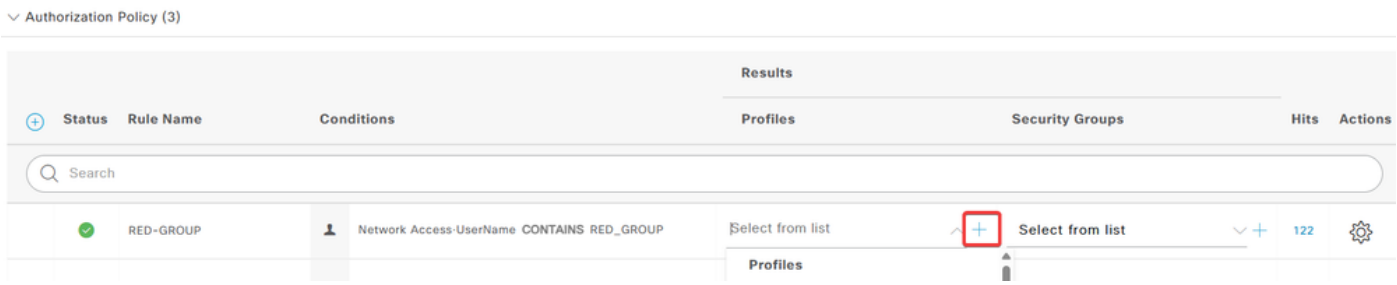
选择Network Access - UserName

d.选择Contains，作为运算符，然后添加证书的Organization-Unit值。



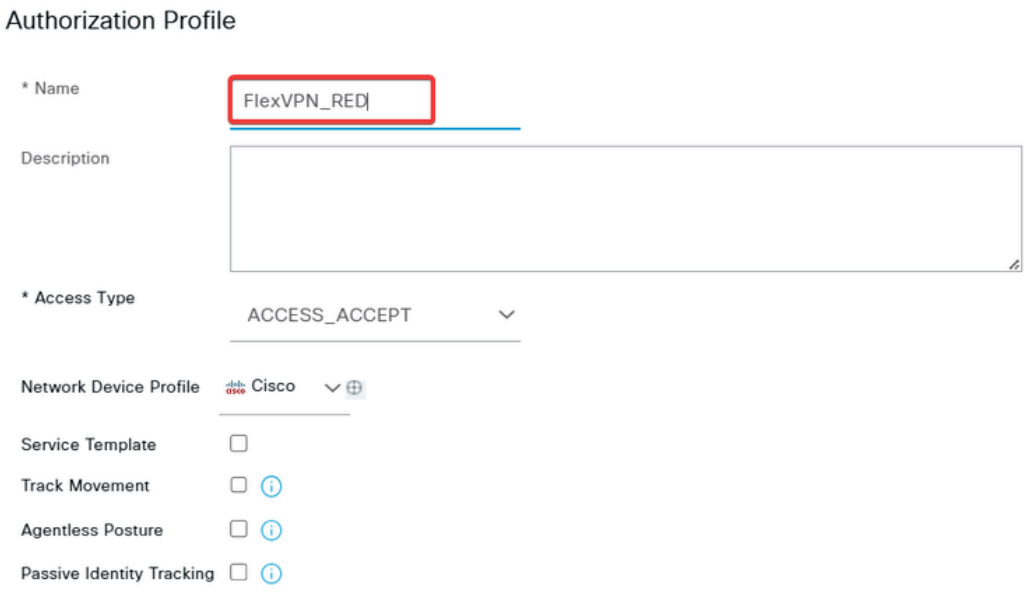
添加组名称

e.在Profiles列中，点击图标add (+)，然后选**Create a New Authorization Profile**择。



添加新授权配置文件

f.输入profile**Name**。



命名授权配置文件

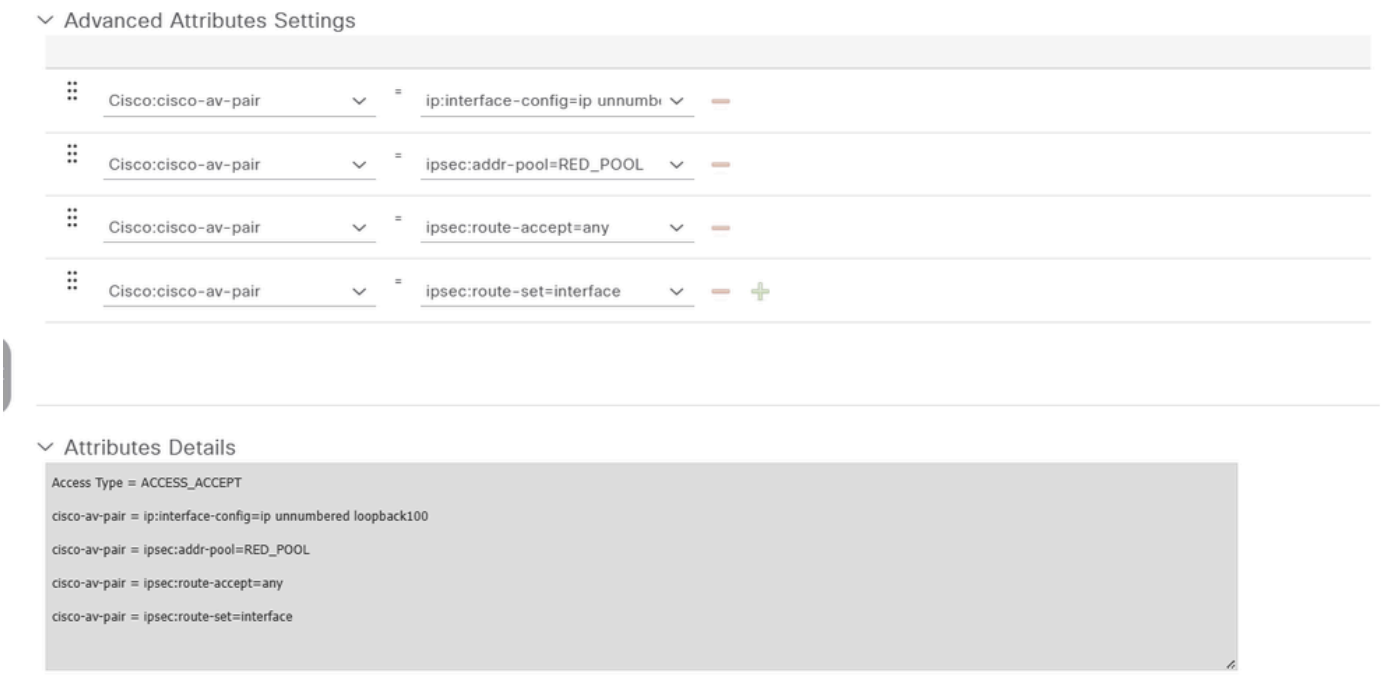
g.导航至**Advanced Attributes Settings**中。然后，从左侧的下拉菜单中选择cisco-av-pair属性，并根据组添加分配给FlexVPN分支的属性。

要为此示例分配的属性包括：

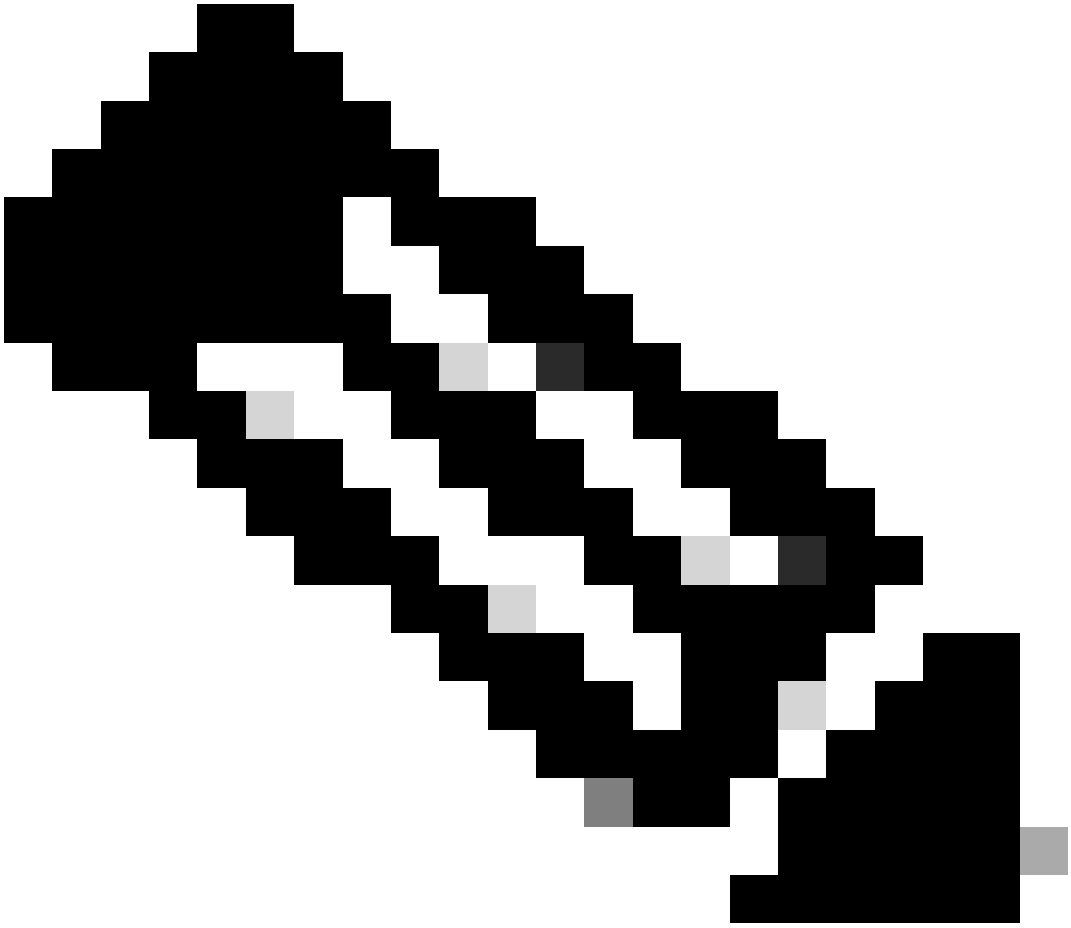
- 将环回接口分配为源。
- 指定辐条从中获取IP地址的池。

和route accept any属route set interface性是必需的，因为没有它们，路由将无法正确通告到分支。

```
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
```



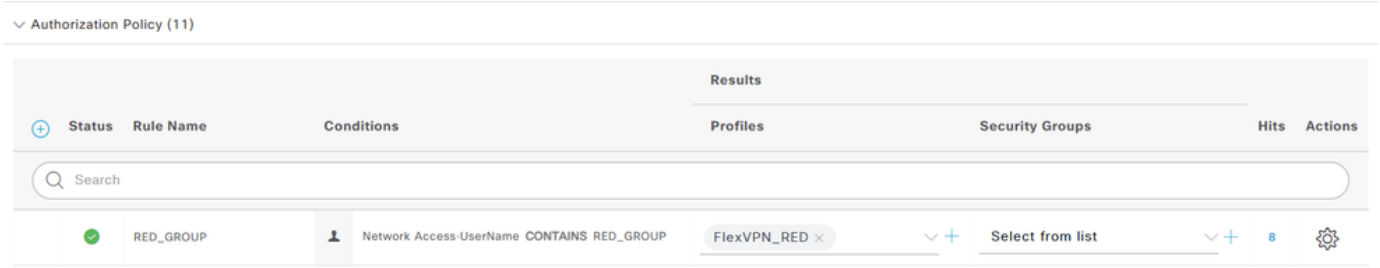
高级属性设置



注意：有关属性规范（名称、语法、说明、示例等），请参阅FlexVPN RADIUS属性配置指南：

FlexVPN和Internet密钥交换版本2配置指南，Cisco IOS XE Gibraltar 16.12.x

h.在配置**authorization profile**文件列中分配。



授权规则

i.单击**Save**。

验证

- 使用命**show ip interface brief**令查看隧道、虚拟模板和虚拟访问状态。

在集线器上，虚拟模板具有正常的up/down状态，并且为与集线器建立连接并显示打开/up状态的每个分支创建了虚拟访问。

<#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
```

在分支上，隧道接口从分配给组的池中接收到IP地址并显示打开/打开状态。

<#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
```

- 使用命令**.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
```

- 使用命令**show crypto session** 确认路由器之间已建立安全连接。

```
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
```

- 使用命令show ip eigrp neighbors，确认已与其他站点建立了EIGRP邻接关系。

```
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
```

- 使用命令show ip route，检验路由是否已推送到分支。
  - 分支上10.20.1.10环回接口的路由已由集线器通过EIGRP获取，并可通过虚拟访问访问

<#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
```

- 10.10.1.10和10.10.2.10的路由是通过EIGRP获取的，可通过RED_GROUP的源IP(10.100.100.1)到达，RED_GROUP的源IP可通过Tunnel0访问。

<#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
```

故障排除

本节提供可用于对此部署类型进行故障排除的信息。使用以下命令调试隧道协商过程：

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和RADIUS调试有助于分支授权故障排除。

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

Working Scenario

此日志显示授权过程和参数的指定。

```
     <#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
```

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。