Configuración de FlexVPN con integración de ISE

Contenido

Introducción

Este documento describe cómo configurar FlexVPN mediante Cisco Identity Services Engine (ISE) para asignar dinámicamente configuraciones a radios.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Cisco Identity Services Engine (ISE)
- protocolo RADIUS
- Red privada virtual flexible (FlexVPN)

Componentes Utilizados

Este documento se basa en las siguientes versiones de software y hardware:

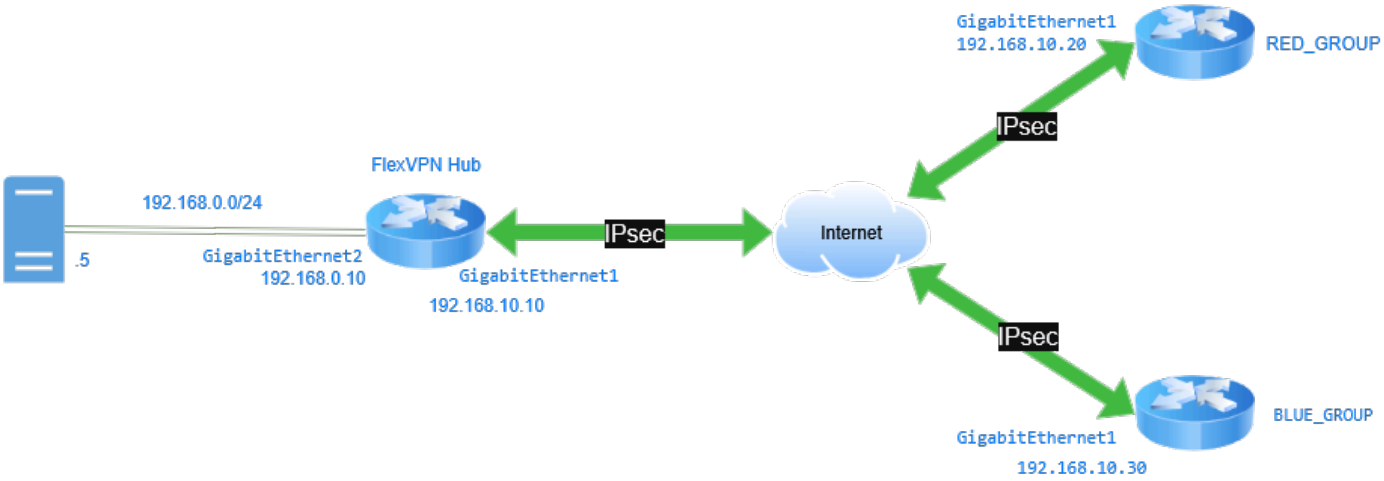
- Cisco CSR1000V (VXE), versión 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

FlexVPN puede establecer una conexión con radios y asignar determinadas configuraciones que permiten la comunicación y la gestión del tráfico. A lo que se hace referencia en el diagrama, esto demuestra cómo FlexVPN se integra con ISE de modo que, cuando un spoke se conecta al HUB, los parámetros del origen del túnel y del conjunto DHCP se asignan en función del grupo o la rama a la que pertenece el spoke. Está utilizando el certificado para autenticar los radios y, a continuación, ISE con Radius como servidor de autorización y contabilidad.



FlexVPN con integración de ISE

Paso 1: Configuración del hub

a. Configure una`trustpoint`para almacenar el certificado del router. Los certificados se utilizan para autenticar los radios.

```
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 un **certificate map**. El propósito de la certificate map es identificar y hacer coincidir los certificados en función de la información especificada, en caso de que el router tenga varios certificados instalados.

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

c. Configure una RADIUS server para la autorización y la contabilización en el dispositivo:

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

d. Defina el **RADIUS server group** con su dirección IP, puertos de comunicación, clave compartida e interfaz de origen para el tráfico 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. Configure el **loopback interfaces**. Los loopback interfaces se utilizan como la conexión de origen para el túnel y se asignan dinámicamente en función del grupo que esté conectado.

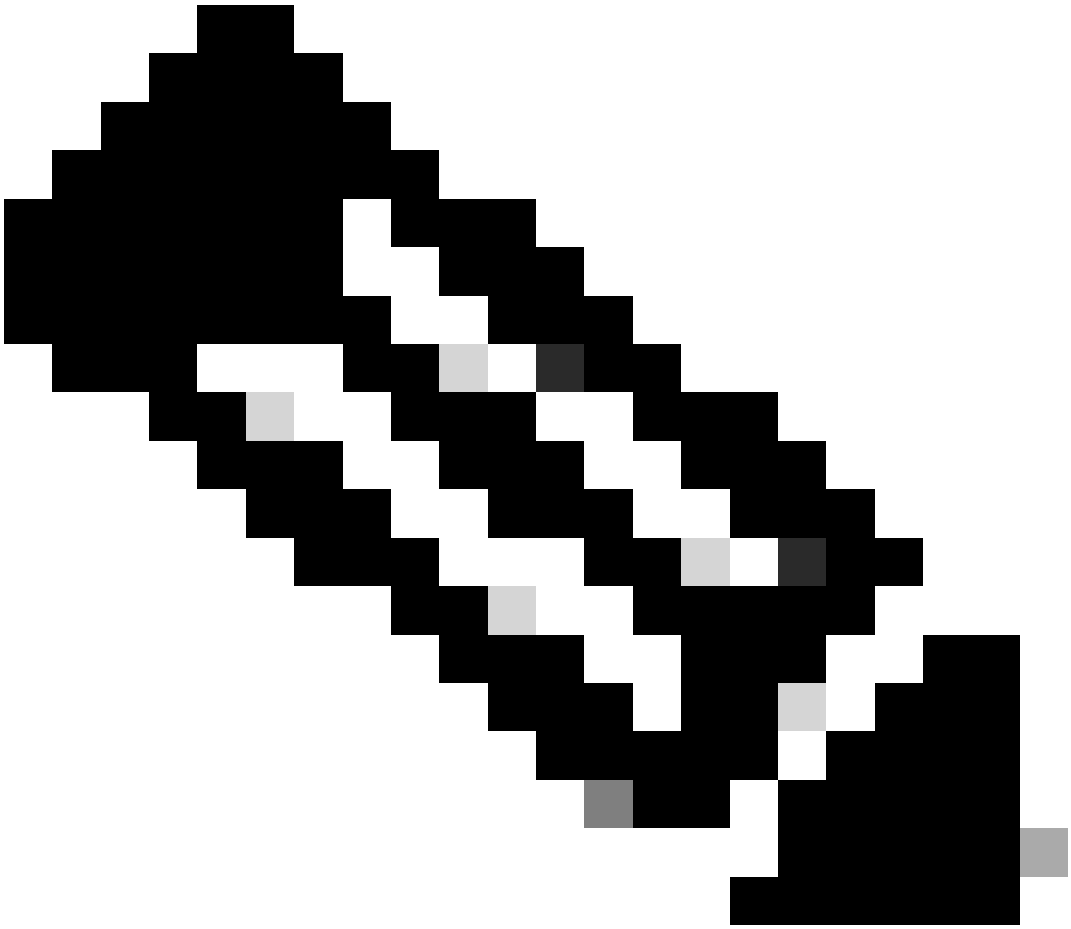
```
interface Loopback100
description RED TUNNEL SOURCE
ip address 10.100.100.1 255.255.255.255
!
interface Loopback200
description BLUE TUNNEL SOURCE
ip address 10.200.200.1 255.255.255.255
```

f. Defina una **IP local pool** para cada grupo.

```
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 y anuncie las redes de cada grupo.

```
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 admite protocolos de routing dinámico como OSPF, EIGRP y BGP a través de túneles VPN. En esta guía, se utiliza EIGRP.

---

h. Configure el **crypto ikev2 name mangler**. El IKEv2 name mangler se utiliza para derivar el nombre de usuario para la autorización IKEv2. En este caso, se configura para utilizar la información de la Unidad organizativa de los certificados en los radios como nombre de usuario para la autorización.

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

i. Configure el **IKEv2 profile**. En el perfil IKEv2 se hace referencia a certificate map, AAA server group, and name mangler.

La autenticación local y remota se configuran como **RSA-SIG**, en este escenario específico.

Se debe crear una cuenta de usuario local en el RADIUS server con un nombre de usuario que coincida con elorganization-unitvalor y la contraseñaCisco1234(como se especifica en la siguiente configuración).

```
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 elIPsec profiley haga referencia al IKEv2 profile.

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

k. Cree el virtual-template. Se utiliza para crear un vínculo virtual-access interface y crear el IPsec profile creado.

Establezca el **virtual-template** sin dirección IP, ya que se lo asigna el RADIUS server.

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

Configure dosloopbackspara simular una red 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
```

Paso 2: Configuración de radio

a. Configure un trustpoint para almacenar el certificado 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. Configure un certificate map. El propósito de la certificate map es identificar y hacer coincidir los certificados en función de la información especificada, en caso de que el router tenga varios certificados instalados.

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

c. Configure la red de autorización local AAA.

El comando aaa authorization network se utiliza para autorizar las solicitudes de acceso relacionadas con los servicios de red. Incluye la comprobación de si un usuario tiene permiso para acceder al servicio solicitado después de su autenticación.

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

d. Configure el IKEv2 profile. Se hace referencia a la autorización local certificate map y AAA en la IKEv2 profile.

La autenticación local y remota se configuran como **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 elIPsec profiley haga referencia al IKEv2 profile.

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

f. Configure eltunnel interface. El tunnel interface está configurado para recibir una dirección IP de túnel del hub según los resultados de la autorización.

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

g Configure EIGRP, anunciando la red local del spoke y el tunnel interface.

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

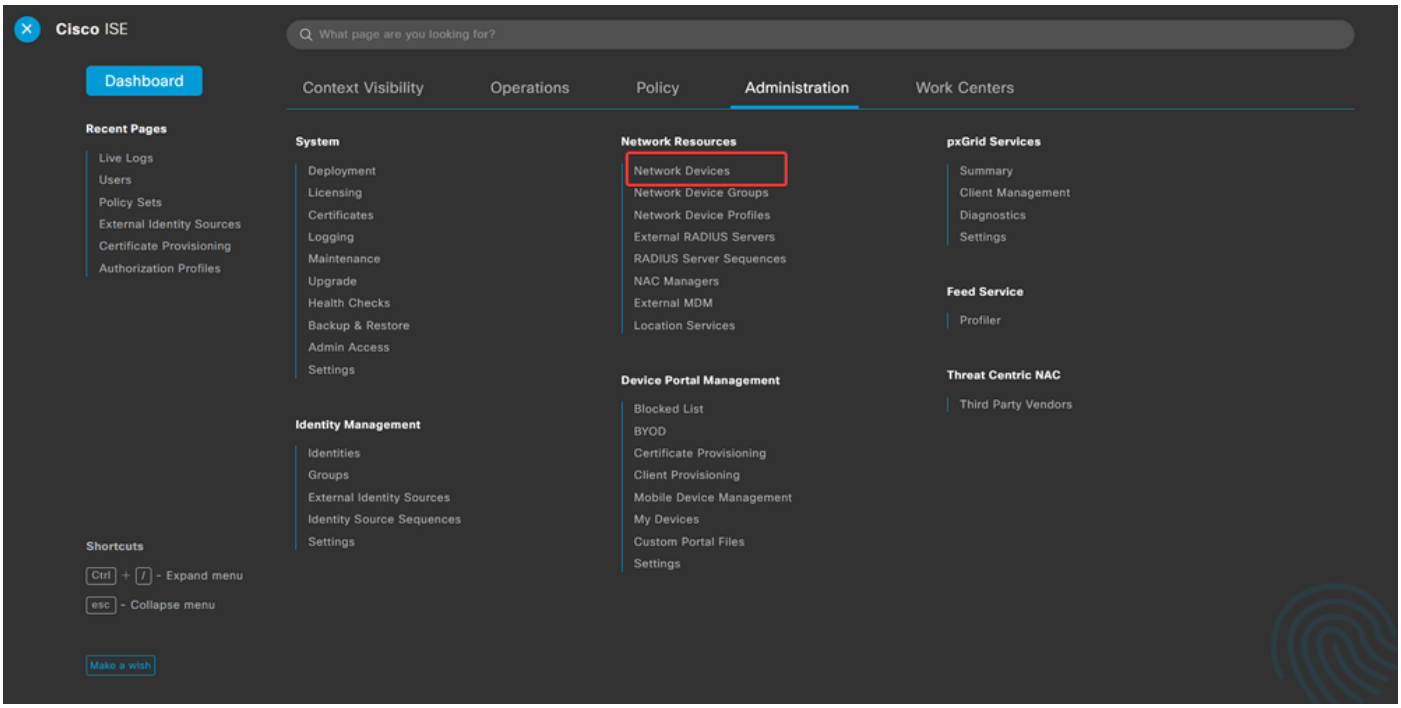
Configure unloopbackpara simular una red interna.

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

Paso 3: Configuración de ISE

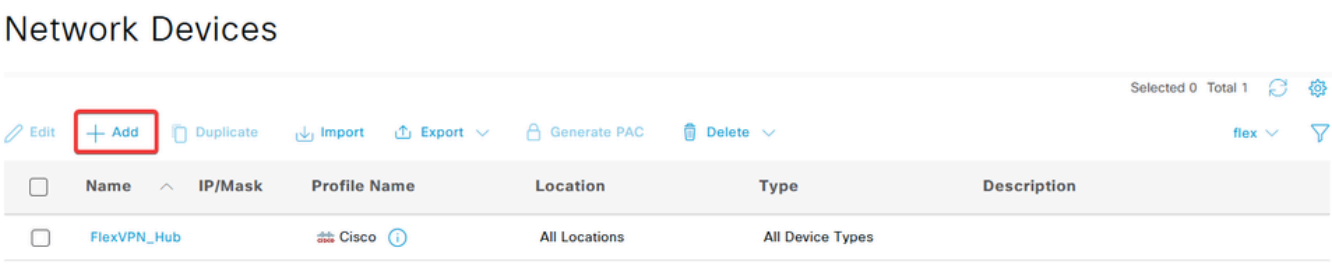
Paso 3.1: Crear usuarios, grupos y agregar dispositivos de red

a. Inicie sesión en el servidor ISE y navegue hasta **Administration** > **Network Resources** > **Network Devices.**



Administración-Recursos de red-Dispositivos de red

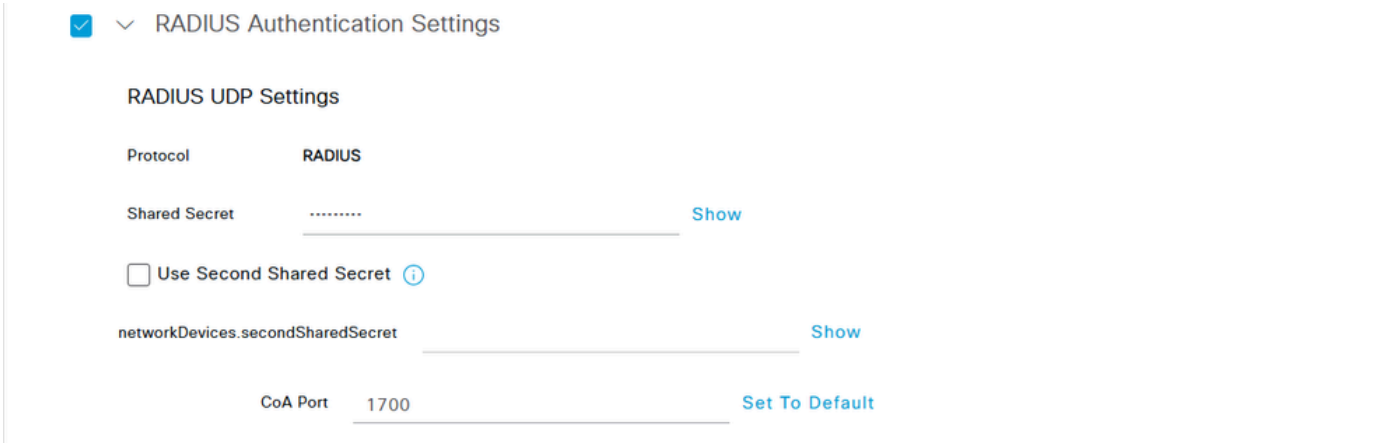
b. Haga clic **Add** para configurar el FlexVPN Hub como cliente AAA.



Adición de un router FlexVPN como cliente AAA

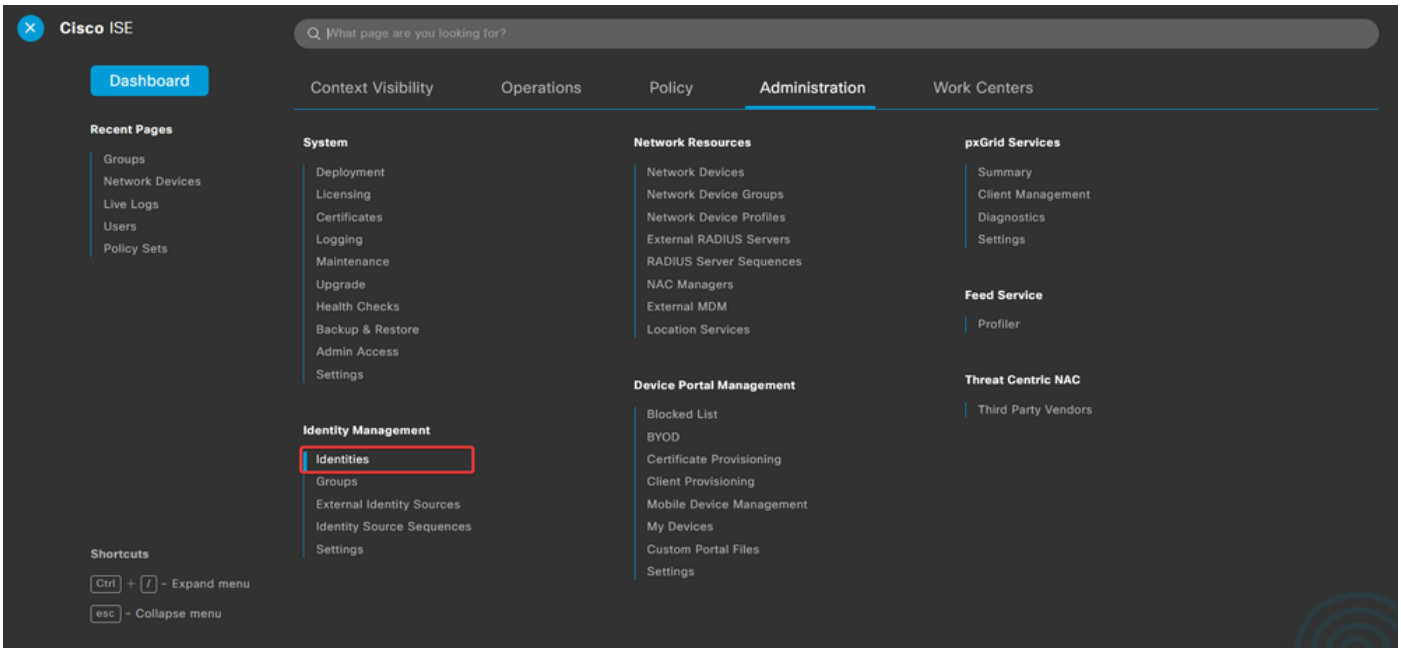
c. Ingrese los campos Network Device Name y IP Address y luego marque la **RADIUS Authentication Settings** casilla y agregue la **Shared Secret**. contraseña secreta compartida debe ser la misma que se utilizó cuando se creó el Grupo de servidores RADIUS en el FlexVPN Hub. Haga clic en**Save**.

Dirección IP del dispositivo de red



Clave compartida de dispositivo de red

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

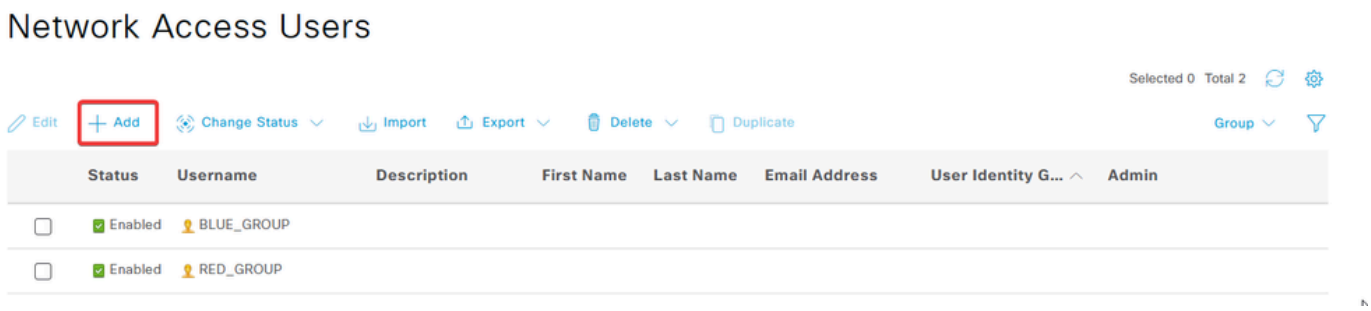


Administración-Identificar Gestión-Identifica

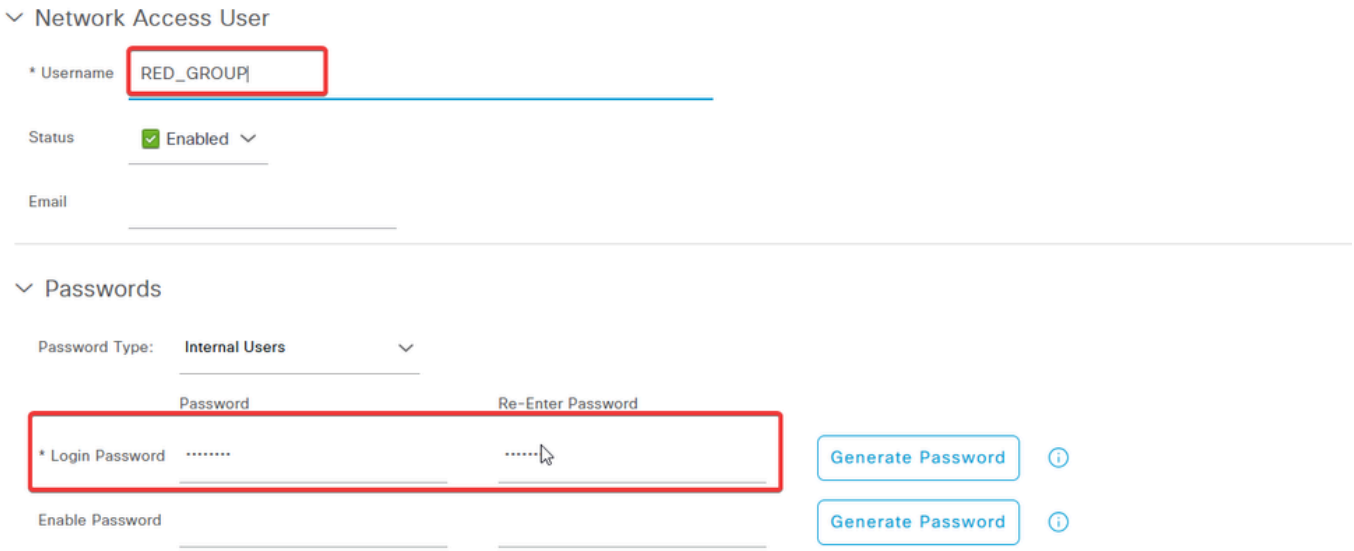
e. Haga clic**Add**para crear un nuevo usuario en la base de datos local del servidor.

Introduzca el**Username**y **Login Password**. El nombre de usuario es el mismo nombre que los certificados tienen en el valor de unidad de organización del certificado y la contraseña de inicio de sesión debe ser la misma que se especificó en el perfil IKev2.

Haga clic en **Save**.



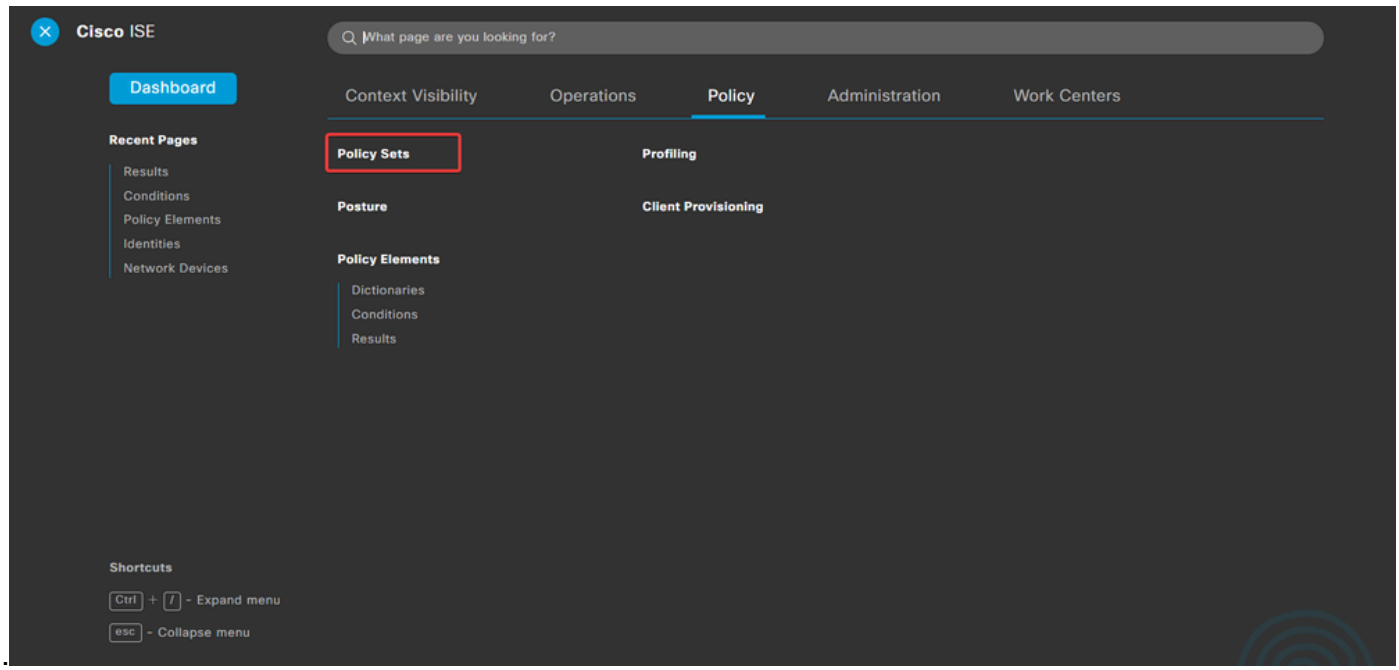
Administración-Identificar Gestión-Identifica



Grupo creado igual que valor unitario de organización

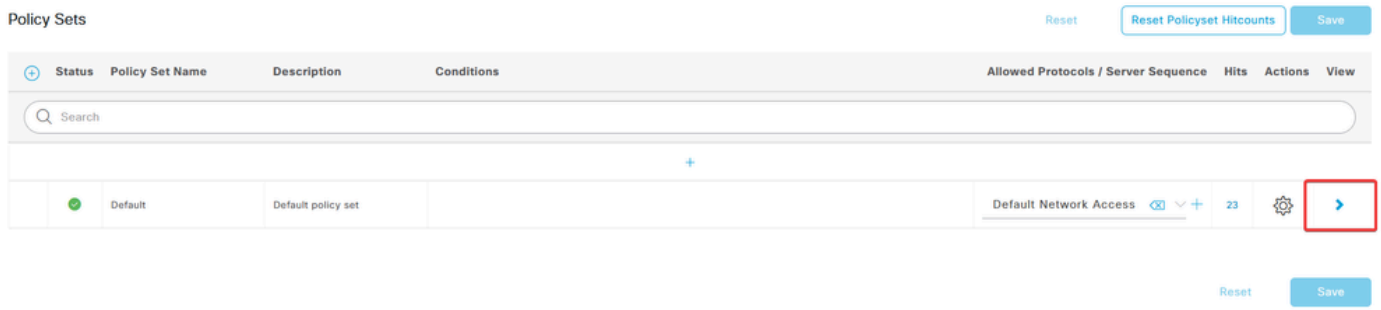
Paso 3.2: Configurar conjunto de políticas

a. Vaya a .**Policy** > **Policy Sets**



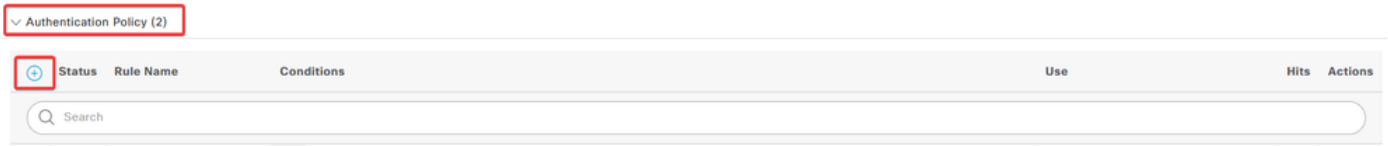
Conjuntos de políticas

b. Seleccione la política de autorización predeterminada haciendo clic en la flecha en el lado derecho de la pantalla:



Editar política predeterminada

c. Haga clic en la flecha del menú desplegable juntoAuthentication Policya para expandirlo. Luego, haga clic en el **add (+)** icono para agregar una nueva regla.

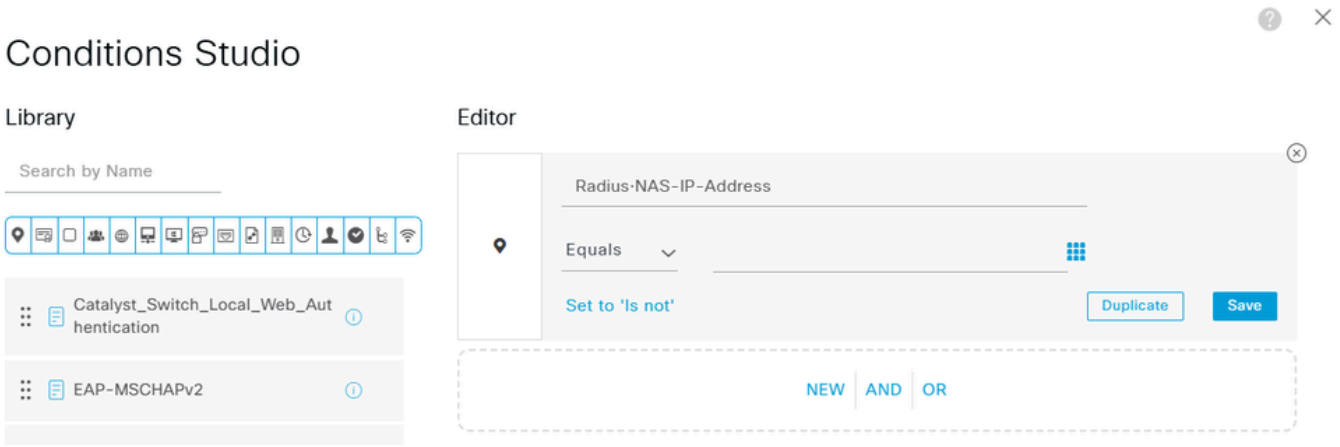


Agregar política de autenticación

d. Introduzca el nombre de la regla y seleccione eladd (+)icono en la columna Condiciones.

Crear política de autenticación

e. Haga clic en el cuadro de texto Attribute Editor y haga clic en elNAS-IP-Addressicono. Introduzca la dirección IP (192.168.0.10) del FlexVPN Hub.

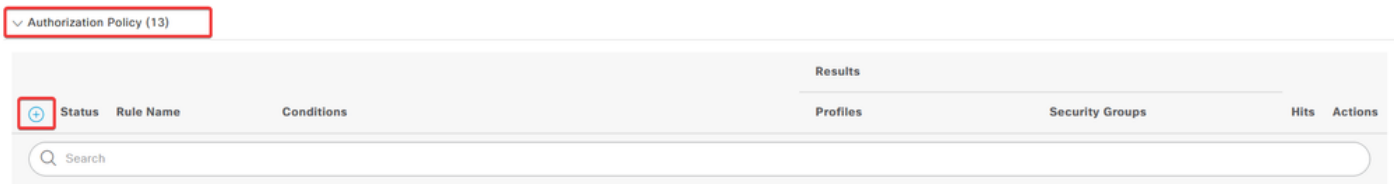


Authenticate FlexVPN Hub

Política de autenticación

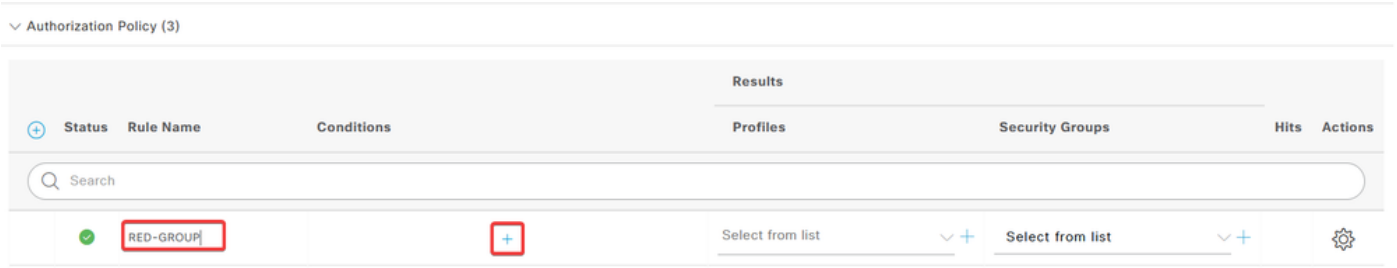
Paso 3.3: Configurar directiva de autorización

a. Haga clic en la flecha del menú desplegable juntoAuthorization Policya para expandirlo. Luego, haga clic en el **add (+)** icono para agregar una nueva regla.



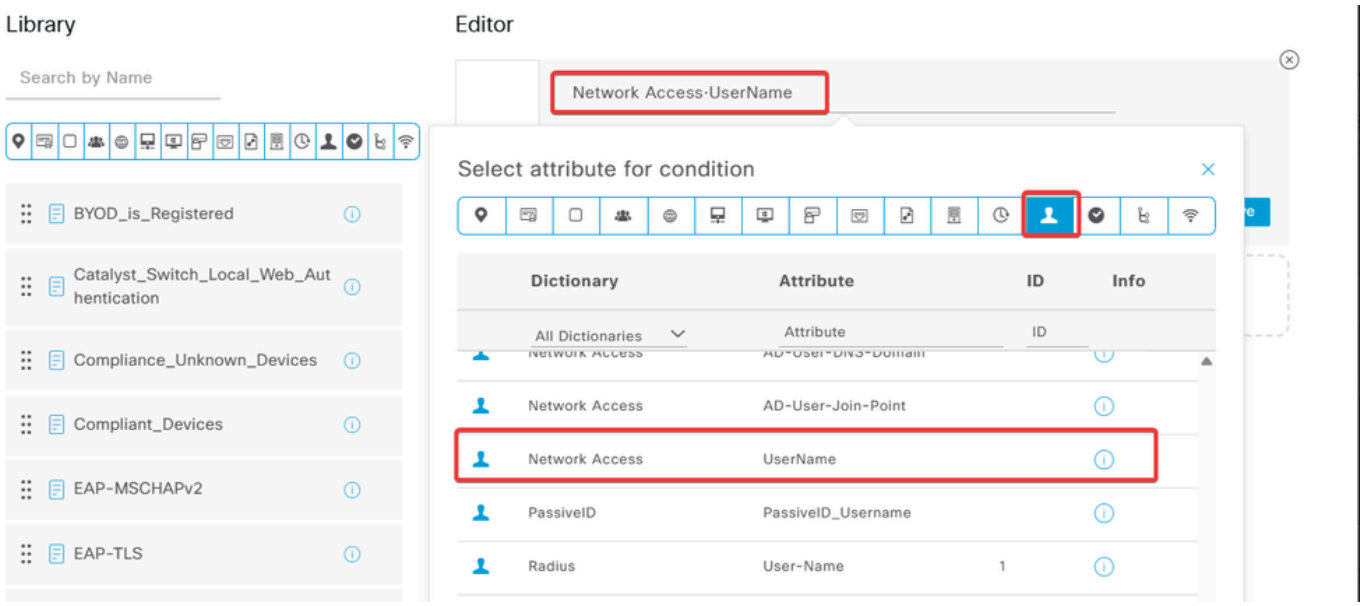
Crear nueva directiva de autorización

b. Introduzca el nombre de la regla y seleccione el **add (+)** icono en la columna Condiciones.



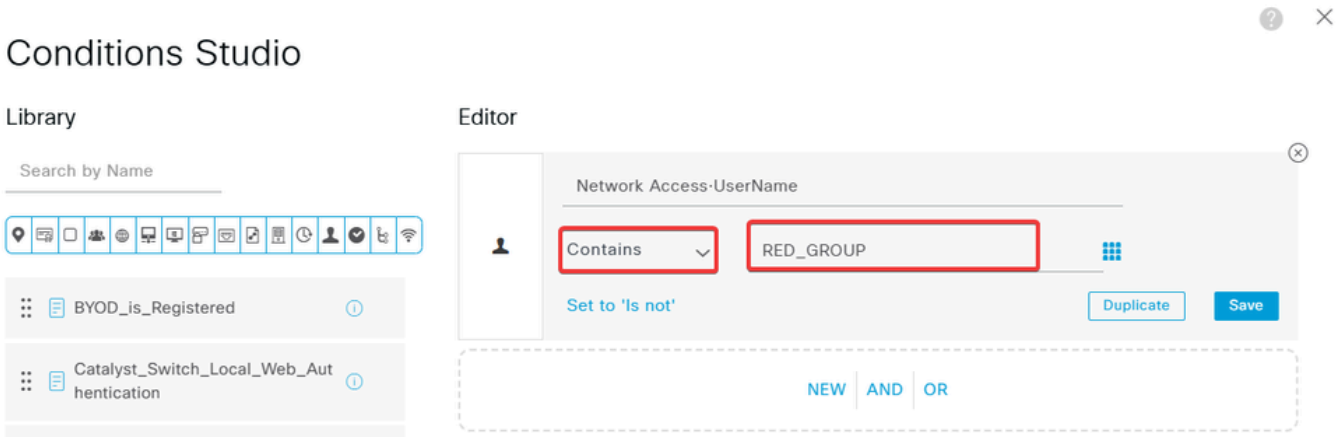
Crear nueva regla

c. Haga clic en el cuadro de texto Attribute Editor y haga clic en elSubjecticono. Seleccione el **Network Access - UserName** atributo.



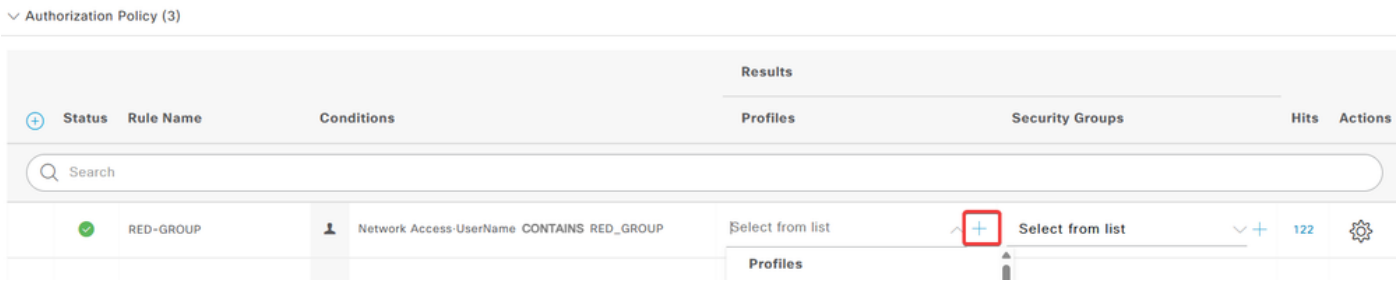
Seleccione Network Access - UserName

d. SeleccioneContainscomo operador y, a continuación, agregue el valor Organization-Unit de los certificados.



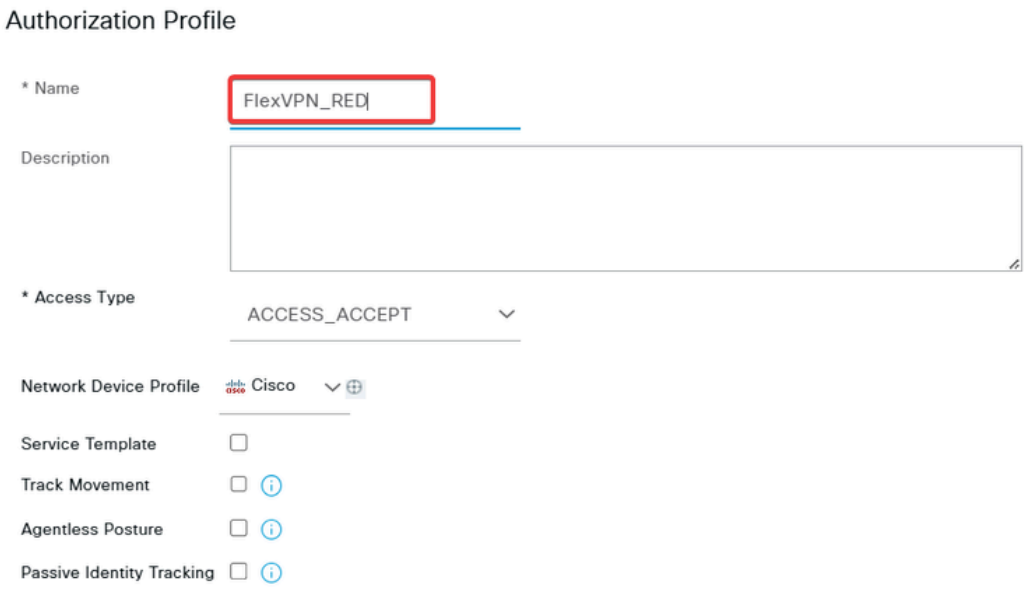
Agregar nombre de grupo

e. En la columna Profiles, haga clic en eladd (+)icono y elija **Create a New Authorization Profile**.



Agregar nuevo perfil de autorización

f. Ingrese el perfil**Name**.



Nombre el perfil de autorización

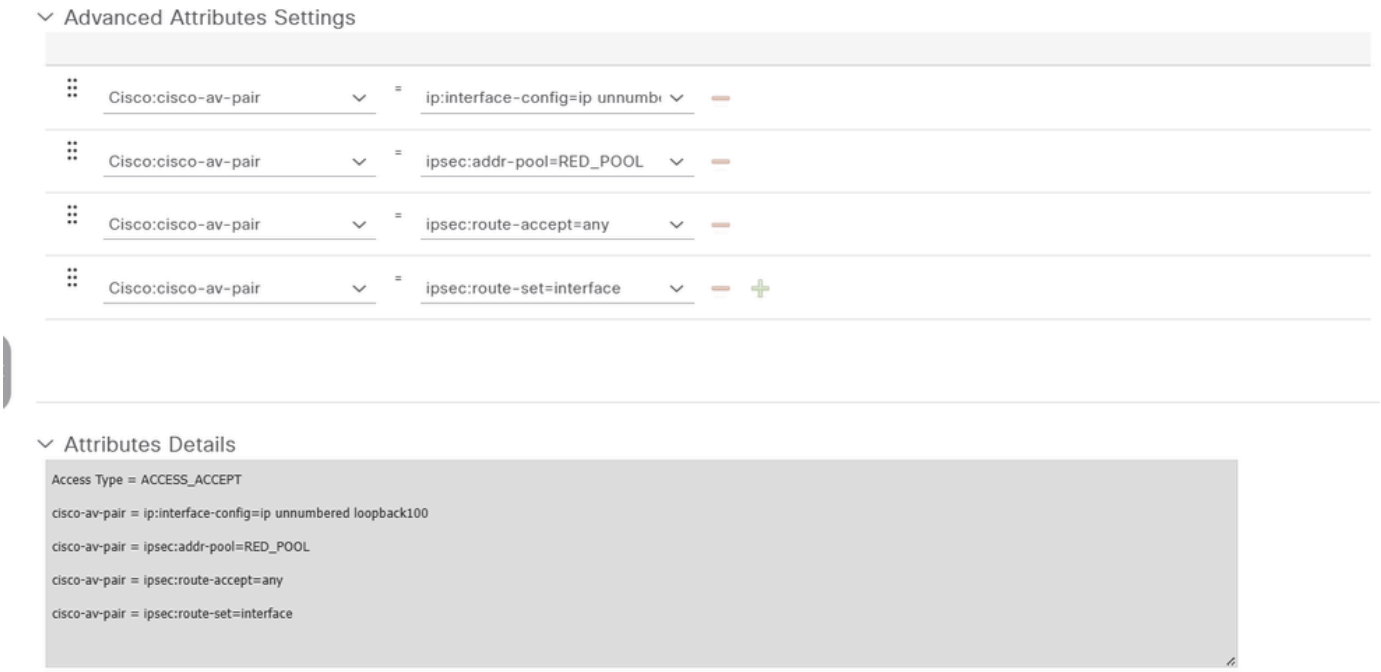
g Vaya a .**Advanced Attributes Settings** A continuación, seleccione el cisco-av-pairatributo en el menú desplegable del lado izquierdo y agregue el atributo que se asigna al radio de FlexVPN en función del grupo.

Los atributos que se asignarán para este ejemplo incluyen:

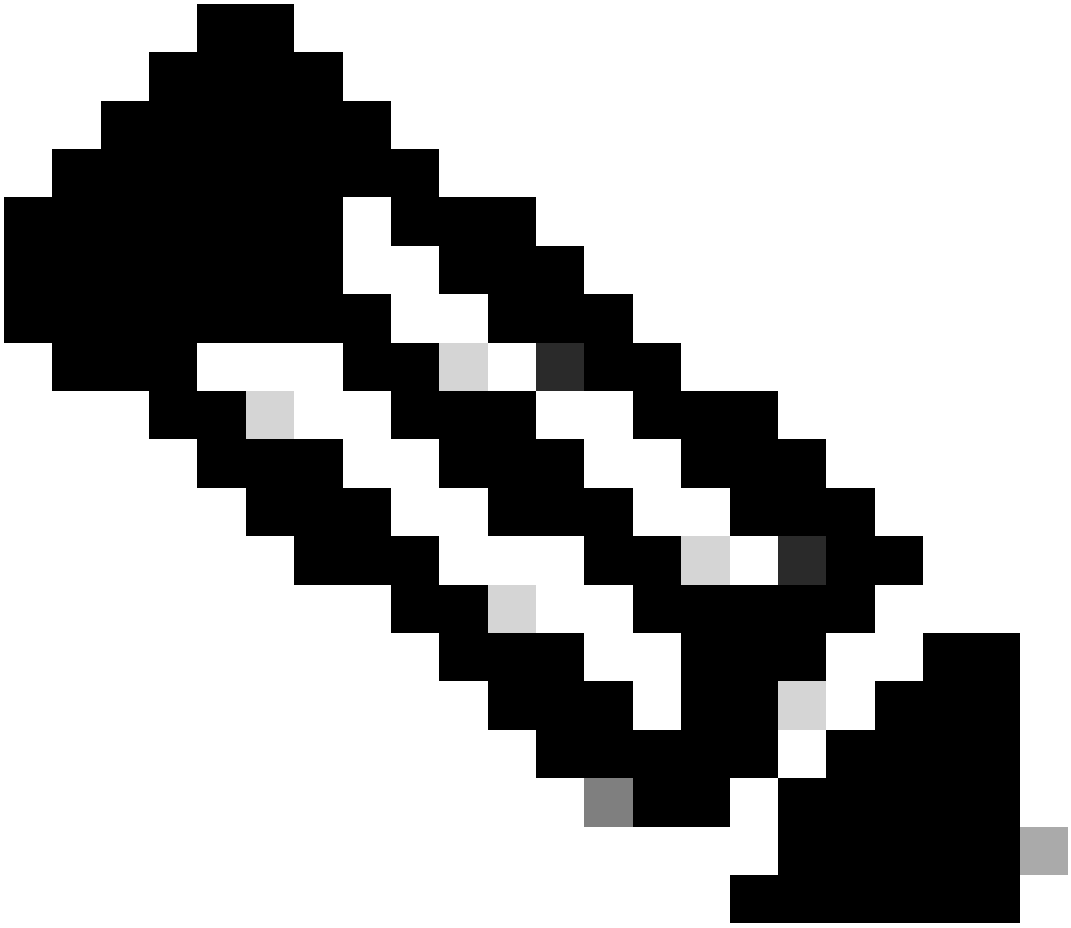
- Asignación de la interfaz de loopback como origen.
- Especificando el conjunto del que los radios obtienen una dirección IP.

Los atributos route accept any y route set interface son necesarios porque, sin ellos, las rutas no se anuncian correctamente a los 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
```



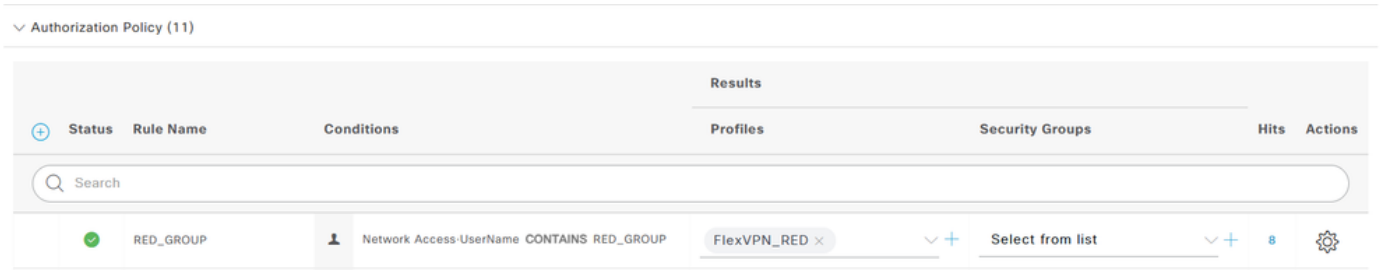
Configuración avanzada de atributos



Nota: Para obtener información sobre las especificaciones de atributos (nombre, sintaxis, descripción, ejemplo, etc.), consulte la guía de configuración de atributos RADIUS de FlexVPN:

Guía de Configuración de FlexVPN e Intercambio de Claves de Internet Versión 2, Cisco IOS XE Gibraltar 16.12.x

h. Asigne el **authorization profile** en la columna de perfiles.



Regla de autorización

i. Haga clic en **Save**.

Verificación

- Utilice el comando **show ip interface brief** para revisar el estado del túnel, la plantilla virtual y el acceso virtual.

En el concentrador, la plantilla virtual tiene un estado activo/inactivo que es normal, y se crea un acceso virtual para cada radio que estableció una conexión con el concentrador y muestra un estado activo/activo.

<#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
```

En el spoke, la interfaz de túnel recibió una dirección IP del conjunto asignado al grupo y muestra un estado up/up.

<#root>

```
FlexVPN_RED_SPOKE#show ip interface brief
Interface                  IP-Address      OK?  Method   Status          Protocol
GigabitEthernet1           192.168.10.20    YES  NVRAM    up              up
Loopback2                  10.20.1.10      YES  manual   up              up

Tunnel0                    172.16.10.107   YES  manual   up              up
```

- Use el 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
```

- Utilice el comando **show crypto session** para confirmar que se ha establecido la conexión segura entre los routers.

```
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
```

- Utilice el comando show ip eigrp neighbors para confirmar que la adyacencia EIGRP se ha establecido con el otro sitio.

```
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
```

- Utilice el comando show ip route para verificar que las rutas se han enviado a los radios.
    - EIGRP ha aprendido la ruta para la interfaz de loopback 10.20.1.10 en el spoke y se puede acceder a ella a través del acceso virtual


```
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
```

- Las rutas para 10.10.1.10 y 10.10.2.10 se aprendieron a través de EIGRP y se pueden alcanzar a través de la IP de origen del RED_GROUP (10.100.100.1), al que se puede acceder a través del túnel0.

<#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

Esta sección proporciona información que puede utilizar para solucionar problemas de este tipo de implementación. Utilice estos comandos para depurar el proceso de negociación de túnel:

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

Los debugs AAA y RADIUS pueden ayudar con la resolución de problemas de la autorización de los Spokes.

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

Working Scenario

Este registro muestra el proceso de autorización y la asignación de los parámetros.

```
     <#root>


RADIUS(OOOOO1A7): Received from id 1645/106
AAA/BIND(OOOOO1A8): Bind i/f
AAA/AUTHOR (Ox1A8): Pick method list 'FLEX'
RADIUS/ENCODE(OOOOO1A8):Orig. component type = VPN IPSEC



RADIUS(000001A8): Config NAS IP: 192.168.0.10




vrfid: [65535]  ipv6 tableid : [0]
idb is NULL
RADIUS(OOOOO1A8): Config NAS IPv6: ::
RADIUS/ENCODE(OOOOO1A8): acct_session_id: 4414
RADIUS(OOOOO1A8): sending
RADIUS(OOOOO1A8): Send Access-Request to 192.168.0.5:1645 id 1645/107, len 138
RADIUS:  authenticator 7A B5 97 5O F2 6E FO O9 - 3D BO 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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).