

# Configuración de FlexVPN con integración de ISE

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Paso 1: Configuración del hub](#)

[Paso 2: Configuración de radio](#)

[Paso 3: Configuración de ISE](#)

[Paso 3.1: Crear usuarios, grupos y agregar dispositivos de red](#)

[Paso 3.2: Configurar conjunto de políticas](#)

[Paso 3.3: Configurar directiva de autorización](#)

[Verificación](#)

[Troubleshoot](#)

[Escenario de trabajo](#)

---

## 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:

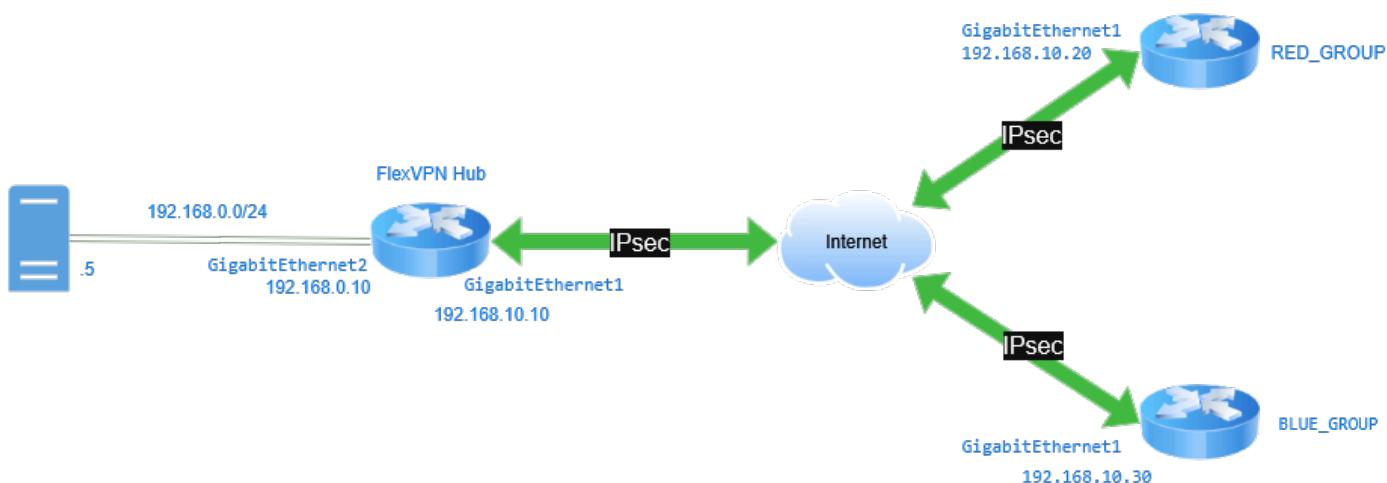
- Cisco CSR1000V (VXE), versión 17.03.04a
- Cisco Identity Services Engine (ISE) - 3.1

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

- 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
```

- 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 un **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
```

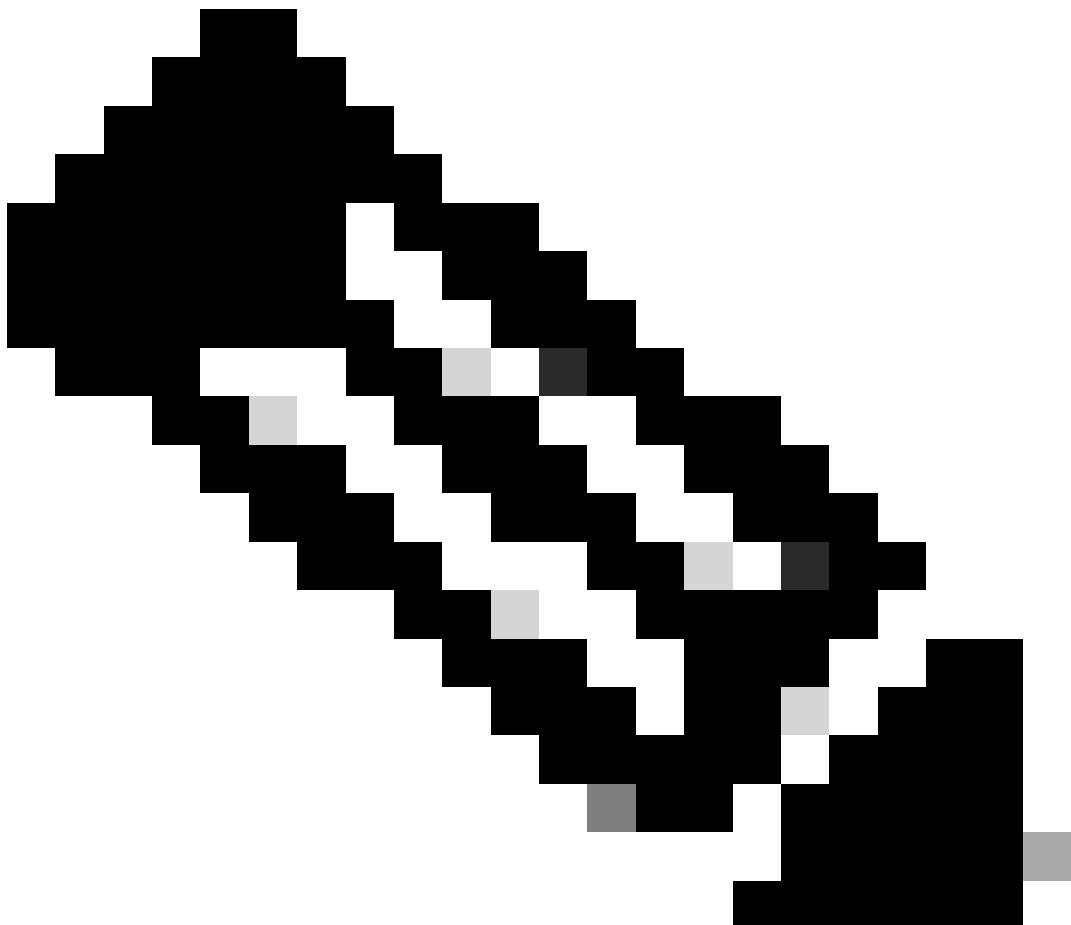
f. Defina una **IP local pool** para cada grupo.

```
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 coincide con el **organization-unit** valor y la contraseña **Cisco1234** (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 el **IPsec profile** y 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 dos **loopbacks** para 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

- 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
```

- 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
```

- 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
```

- 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 el IPsec profile y haga referencia al IKEv2 profile.

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

f. Configure el tunnel 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 un loopback para 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**.

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Cisco ISE', a search bar, and tabs for 'Dashboard', 'Context Visibility', 'Operations', 'Policy', 'Administration' (which is currently selected), and 'Work Centers'. On the left, there's a sidebar with 'Recent Pages' (Live Logs, Users, Policy Sets, etc.), 'System' (Deployment, Licensing, Certificates, etc.), 'Identity Management' (Identities, Groups, External Identity Sources, etc.), and 'Shortcuts' (Ctrl + [ ] - Expand menu, esc - Collapse menu). The main content area is titled 'Network Resources' and contains a list of items: Network Devices (highlighted with a red box), Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, and Location Services. To the right are sections for 'pxGrid Services' (Summary, Client Management, Diagnostics, Settings), 'Feed Service' (Profiler), and 'Threat Centric NAC' (Third Party Vendors). A large blue circular icon with a fingerprint pattern is on the right side.

Administración-Recursos de red-Dispositivos de red

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

## Network Devices

Selected 0 Total 1						
	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	FlexVPN_Hub	Cisco		All Locations	All Device Types	

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**.

Network Devices List > FlexVPN\_Hub

### Network Devices

Name	FlexVPN_Hub
Description	
IP Address	* IP :

Dirección IP del dispositivo de red

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol	RADIUS
Shared Secret	*****
<input type="checkbox"/> Use Second Shared Secret <a href="#">(i)</a>	
networkDevices.secondSharedSecret	<a href="#">Show</a>
CoA Port	1700
<a href="#">Set To Default</a>	

Clave compartida de dispositivo de red

d. Vaya a .Administration > Identity Management > Identities

The screenshot shows the Cisco ISE Administration interface. The top navigation bar has tabs for Dashboard, Context Visibility, Operations, Policy, Administration (which is selected), and Work Centers. On the left, there's a sidebar with 'Recent Pages' (Groups, Network Devices, Live Logs, Users, Policy Sets) and 'Shortcuts' (Ctrl + / - Expand menu, esc - Collapse menu). The main content area is divided into several sections: System (Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Health Checks, Backup & Restore, Admin Access, Settings), Network Resources (Network Devices, Network Device Groups, Network Device Profiles, External RADIUS Servers, RADIUS Server Sequences, NAC Managers, External MDM, Location Services), pxGrid Services (Summary, Client Management, Diagnostics, Settings), Feed Service (Profiler), Device Portal Management (Blocked List, BYOD, Certificate Provisioning, Client Provisioning, Mobile Device Management, My Devices, Custom Portal Files, Settings), Threat Centric NAC (Third Party Vendors), and Identity Management (Groups, External Identity Sources, Identity Source Sequences, Settings). The 'Identities' option under Identity Management is highlighted with a red box.

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**.

## Network Access Users

The screenshot shows a table with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity G..., and Admin. Two rows are present:

Status	Username	Description	First Name	Last Name	Email Address	User Identity G...	Admin
<input type="checkbox"/>	Enabled	BLUE_GROUP					
<input type="checkbox"/>	Enabled	RED_GROUP					

Administración-Identificar Gestión-Identifica

### Network Access User

\* Username:  (highlighted with a red box)

Status:  Enabled

Email: \_\_\_\_\_

### Passwords

Password Type: Internal Users

Password	Re-Enter Password
* Login Password: ..... (highlighted with a red box)	.....

Enable Password: \_\_\_\_\_

(i)

(i)

Grupo creado igual que valor unitario de organización

## Paso 3.2: Configurar conjunto de políticas

### a. Vaya a .Policy > Policy Sets

The screenshot shows the Cisco ISE dashboard with the Policy tab selected. On the left, there is a sidebar with Recent Pages: Results, Conditions, Policy Elements, Identities, and Network Devices. The Policy Sets link under Policy Elements is highlighted with a red box.

## Conjuntos de políticas

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

The screenshot shows the 'Policy Sets' interface. At the top, there are buttons for 'Reset', 'Reset Policyset Hitcounts', and 'Save'. Below is a search bar with a magnifying glass icon and the word 'Search'. The main table has columns for '+', 'Status', 'Policy Set Name', 'Description', 'Conditions', 'Allowed Protocols / Server Sequence', 'Hits', 'Actions', and 'View'. A row for 'Default' is selected, showing 'Default policy set' in the 'Description' column. In the 'Conditions' column, there is a section titled 'Default Network Access' with a dropdown menu, a minus sign, a plus sign, the number '23', a gear icon, and a red box highlighting the right-pointing arrow icon. At the bottom, there are 'Reset' and 'Save' buttons.

## Editar política predeterminada

c. Haga clic en la flecha del menú desplegable junto a Authentication Policy para expandirlo. Luego, haga clic en el add (+) ícono para agregar una nueva regla.

The screenshot shows the 'Authentication Policy' interface. At the top, there is a red box around the 'Authentication Policy (2)' section. Below is a search bar with a magnifying glass icon and the word 'Search'. The main table has columns for '+', 'Status', 'Rule Name', 'Conditions', 'Use', 'Hits', and 'Actions'. The first row, labeled 'FlexVPN\_Router', has its 'Conditions' column highlighted with a red box around the '+' icon. At the bottom, there are 'Reset' and 'Save' buttons.

## Agregar política de autenticación

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

The screenshot shows the 'Create authentication policy' interface. At the top, there is a red box around the 'Authentication Policy (2)' section. Below is a search bar with a magnifying glass icon and the word 'Search'. The main table has columns for '+', 'Status', 'Rule Name', 'Conditions', 'Use', 'Hits', and 'Actions'. A new rule is being created with the name 'FlexVPN\_Router' in the 'Rule Name' column. The 'Conditions' column for this new rule is highlighted with a red box around the '+' icon. At the bottom, there are 'Internal Users' dropdown menus, an 'Options' button, and a red box highlighting the '+' icon in the 'Conditions' column. There is also a gear icon at the bottom right.

## Crear política de autenticación

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

# Conditions Studio

The screenshot shows the Conditions Studio interface. On the left is the 'Library' section, which contains a search bar and a grid of icons representing various conditions. Below the grid are two items listed: 'Catalyst\_Switch\_Local\_Web\_Authentication' and 'EAP-MSCHAPv2'. On the right is the 'Editor' section, which displays a condition being built: 'Radius-NAS-IP-Address Equals Set to 'Is not''. There are buttons for 'Duplicate' and 'Save' at the bottom right.

Authenticate FlexVPN Hub

The screenshot shows the 'Authentication Policy' list view. It includes columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is at the top. One policy is visible: 'FlexVPN' with the condition 'Radius-NAS-IP-Address EQUALS'. The 'Actions' column for this row shows 'Internal Users' and 'Options'.

Política de autenticación

## Paso 3.3: Configurar directiva de autorización

- Haga clic en la flecha del menú desplegable junto a Authorization Policy para expandirlo. Luego, haga clic en el add (+) icono para agregar una nueva regla.

The screenshot shows the 'Authorization Policy' list view. It includes columns for Status, Rule Name, Conditions, Results, Profiles, Security Groups, Hits, and Actions. A search bar is at the top. One policy is visible: 'RED-GROUP' with the condition 'Radius-NAS-IP-Address EQUALS'. The 'Actions' column for this row shows 'Internal Users' and 'Options'.

Crear nueva directiva de autorización

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

The screenshot shows the 'Authorization Policy' list view. It includes columns for Status, Rule Name, Conditions, Results, Profiles, Security Groups, Hits, and Actions. A search bar is at the top. A new rule is being created with the name 'RED-GROUP'. The 'Conditions' column for this rule has an 'add +' icon highlighted with a red box. The 'Profiles' and 'Security Groups' columns also have 'Select from list' dropdowns with '+' icons.

Crear nueva regla

- Haga clic en el cuadro de texto Attribute Editor y haga clic en el Subject icono. Seleccione el Network Access - UserName atributo.

**Library**

Search by Name

**Editor**

Network Access-UserName

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Network Access	AD-User-Join-Point		
Network Access	UserName		
PassiveID	PassiveID_Username		
Radius	User-Name	1	

Seleccione Network Access - UserName

d. Seleccione **Contains** como operador y, a continuación, agregue el valor **Organization-Unit** de los certificados.

## Conditions Studio

**Library**

Search by Name

**Editor**

Network Access-UserName

Contains RED\_GROUP

Set to 'Is not'

Save

NEW AND OR

Agregar nombre de grupo

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

Authorization Policy (3)

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
+						
✓	RED-GROUP	Network Access-UserName CONTAINS RED_GROUP	Select from list	Select from list	122	

Agregar nuevo perfil de autorización

f. Ingrese el perfil **Name**.

## Authorization Profile

\* Name  FlexVPN\_RED

Description

\* Access Type  ▼

Network Device Profile  Cisco ▼ ⊕

Service Template

Track Movement  (i)

Agentless Posture  (i)

Passive Identity Tracking  (i)

Nombre el perfil de autorización

g Vaya a .Advanced Attributes Settings A continuación, seleccione el `cisco-av-pair` atributo 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
```

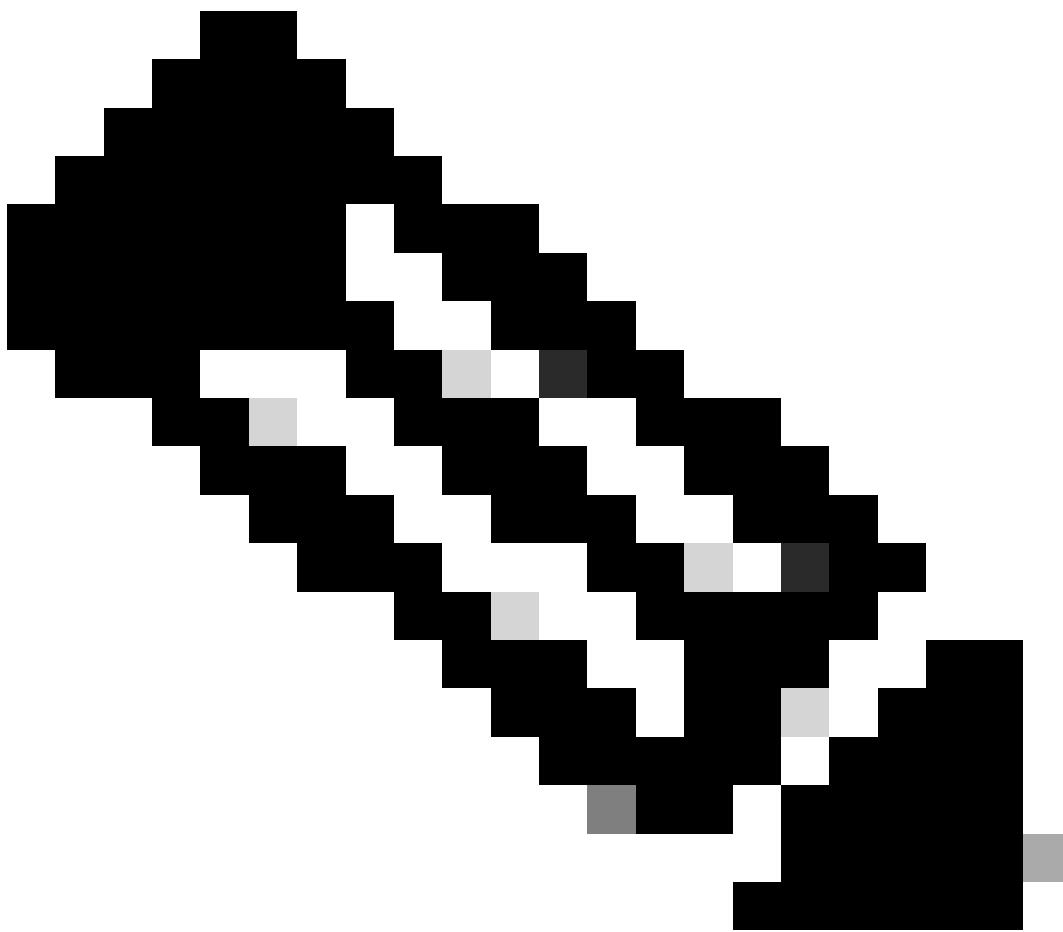
## ✓ Advanced Attributes Settings

Cisco:cisco-av-pair	▼	=	ip:interface-config=ip unnumbered	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=RED_POOL	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:route-accept=any	▼	-
Cisco:cisco-av-pair	▼	=	ipsec:route-set=interface	▼	- +

## ✓ Attributes Details

```
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 **profiles**.

✓ Authorization Policy (11)

Conditions		Profiles	Security Groups	Hits	Actions
<input type="checkbox"/> RED_GROUP	Network Access-UserName CONTAINS RED_GROUP	FlexVPN_RED	Select from list	8	

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        down
```

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    RT0     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

<#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

```

- 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

C     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(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]  
fdb 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
```

## 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).