

Configurar FlexVPN com integração com ISE

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Passo 1: Configuração do Hub](#)

[Passo 2: Configuração do raio](#)

[Passo 3: Configuração do ISE](#)

[Passo 3.1: Criar usuários, grupos e adicionar dispositivo de rede](#)

[Passo 3.2: Configurar Conjunto de Políticas](#)

[Passo 3.3: Configurar Diretiva de Autorização](#)

[Verificar](#)

[Troubleshooting](#)

[Cenário de trabalho](#)

Introdução

Este documento descreve como configurar o FlexVPN usando o Cisco Identity Services Engine (ISE) para atribuir dinamicamente configurações a spokes.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco Identity Services Engine (ISE)
- protocolo RADIUS
- Flex Virtual Private Network (FlexVPN)

Componentes Utilizados

Este documento é baseado nestas versões de software e hardware:

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

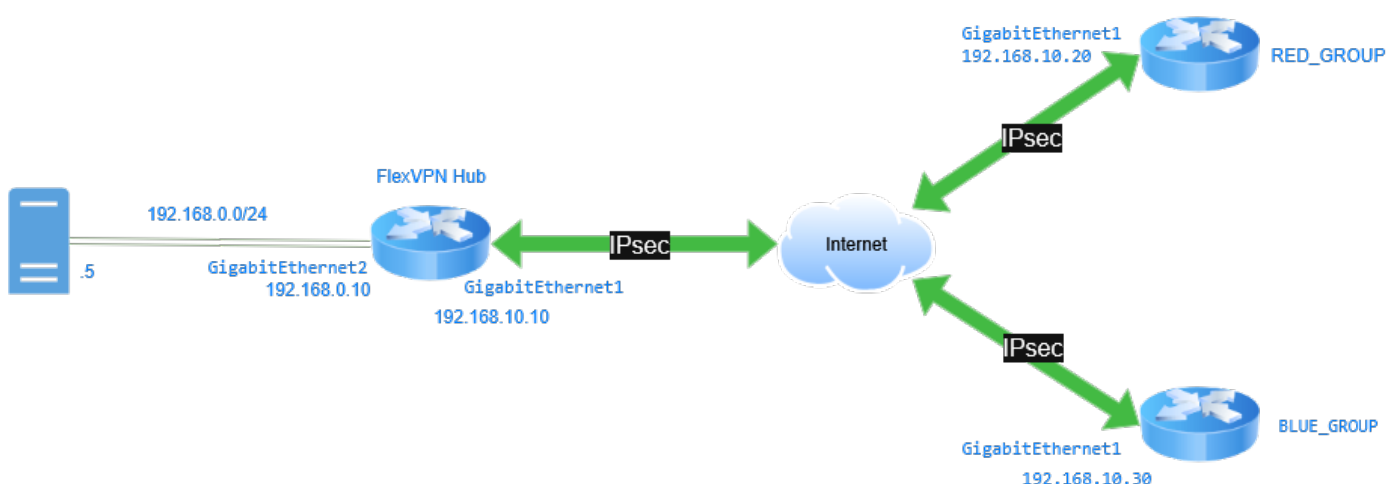
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Diagrama de Rede

O FlexVPN pode estabelecer uma conexão com spokes e atribuir determinadas configurações que permitem o gerenciamento de comunicação e tráfego. Referenciado no diagrama, isso demonstra como o FlexVPN se integra ao ISE para que, quando um spoke se conecta ao HUB, os parâmetros da origem do túnel e do pool DHCP sejam atribuídos, dependendo do grupo ou ramificação ao qual o spoke pertence. Ele está usando o certificado para autenticar os spokes, depois o ISE com Radius como servidor de autorização e tarifação.



FlexVPN com integração com ISE

Passo 1: Configuração do Hub

a. Configure um `trustpoint` para armazenar o certificado do roteador. Os certificados são usados para autenticar os 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 um `certificate map`. A finalidade do `certificate map` é identificar e corresponder certificados com base nas informações especificadas, caso o roteador tenha vários certificados instalados.

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

c. Configure um **RADIUS server** para autorização e tarifação no dispositivo:

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

d. Defina o **RADIUS server group** com seu endereço IP, portas de comunicação, chave compartilhada e interface de origem para o tráfego 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 o **loopback interfaces**. Os **loopback interfaces** roteadores são usados como a conexão de origem para o túnel e são atribuídos dinamicamente, dependendo do grupo que está 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
```

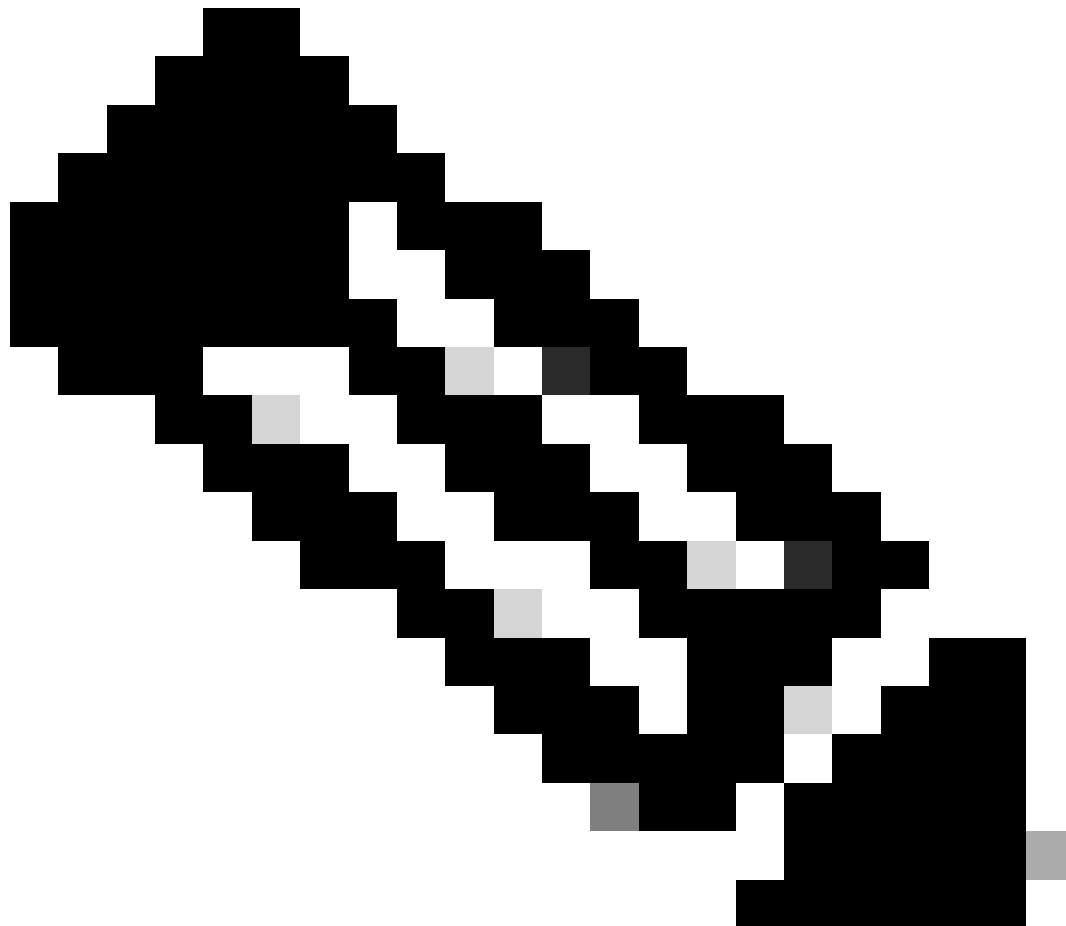
f. Defina um **IP local pool** para cada grupo.

```
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 o **EIGRP** e anuncie as 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
```



Note: O FlexVPN suporta protocolos de roteamento dinâmico como OSPF, EIGRP e BGP sobre túneis VPN. Neste guia, o EIGRP está sendo usado.

h. Configure o `crypto ikev2 name mangler`. O `ikev2 name mangler` é usado para derivar o nome de usuário para autorização IKEv2. Nesse caso, ele é configurado para usar as informações de Organização-Unidade dos certificados nos spokes como o nome de usuário para autorização.

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

i. Configure o **IKEv2 profile**. Os **certificate map**, **AAA server group**, e **name mangler** são referenciados no perfil **IKEv2**.

As autenticações local e remota são configuradas como **RSA-SIG**, neste cenário específico.

Uma conta de usuário local deve ser criada no **RADIUS server** com um nome de usuário que corresponda ao **organization-unit** valor e à senha **Cisco1234** (conforme especificado na configuração abaixo).

```
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 o **IPsec profile** e faça referência ao **IKEv2 profile**.

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

k) Crie o **virtual-template**. É usado para criar um **virtual-access interface** e vincular o **IPsec profile** criado.

Defina o **virtual-template** sem endereço IP, pois ele é atribuído pelo **RADIUS server**.

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

Configure dois **loopbacks** para simular uma rede 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
```

Passo 2: Configuração do raio

a. Configure um `trustpoint` para armazenar o certificado do roteador 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 um `certificate map`. A finalidade do `certificate map` é identificar e corresponder certificados com base nas informações especificadas, caso o roteador tenha vários certificados instalados.

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

c. Configure a rede de autorização local AAA.

O comando `aaa authorization network` é usado para autorizar solicitações de acesso relacionadas aos serviços de rede. Isso inclui verificar se um usuário tem permissão para acessar o serviço solicitado após ser autenticado.

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

d. Configure o `IKEv2 profile`. O local de autorização `certificate map` e AAA são referenciados no `IKEv2 profile`.

As autenticações local e remota são configuradas 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 o IPsec profile e consulte o IKEv2 profile.

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

f. Configure o tunnel interface. O tunnel interface é configurado para receber um endereço IP de túnel do hub com base nos resultados da autorização.

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

g. Configure o EIGRP, anunciando a rede local do spoke e do tunnel interface.

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

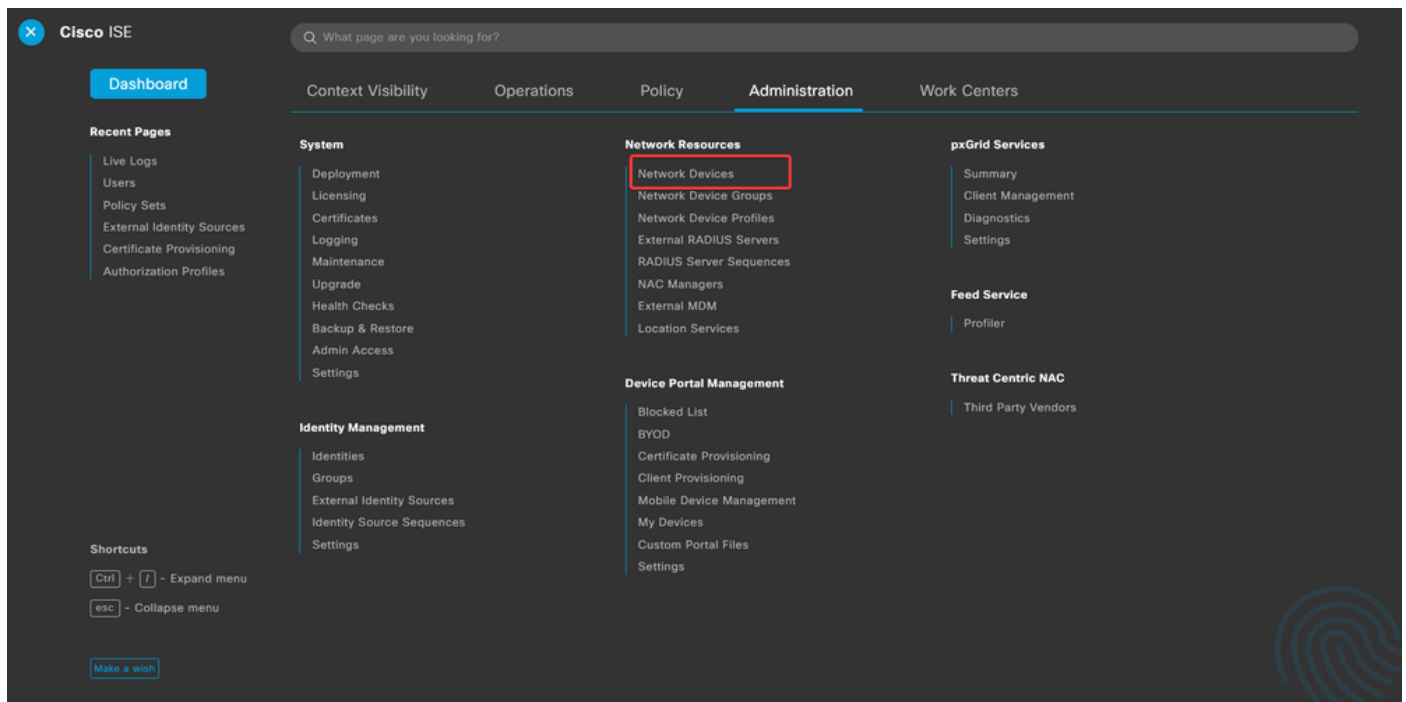
Configure um loopback para simular uma rede interna.

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

Passo 3: Configuração do ISE

Passo 3.1: Criar usuários, grupos e adicionar dispositivo de rede

a. Faça login no servidor ISE e navegue até **Administration > Network Resources > Network Devices**.



Administração-Recursos de rede-Dispositivos de rede

b. Clique **Add** para configurar o FlexVPN Hub como um cliente AAA.

Network Devices

Edit + Add Duplicate Import Export Generate PAC Delete						
Selected 0 Total 1 flex						
☐	Name	IP/Mask	Profile Name	Location	Type	Description
☐	FlexVPN_Hub		Cisco	All Locations	All Device Types	

Adicione o roteador FlexVPN como cliente AAA

c. Insira os campos Network device Name e IP Address e marque **RADIUS Authentication Settings** a caixa de seleção e adicione a senha **Shared Secret**. The shared secret deve ser a mesma que foi usada quando o RADIUS Server Group foi criado no FlexVPN Hub. Clique em **.Save**

Network Devices List > FlexVPN_Hub

Network Devices

Name

Description

IP Address / 32 ☐

Endereço IP do dispositivo de rede

☒ **RADIUS Authentication Settings**

RADIUS UDP Settings

Protocol **RADIUS**

Shared Secret [Show](#)

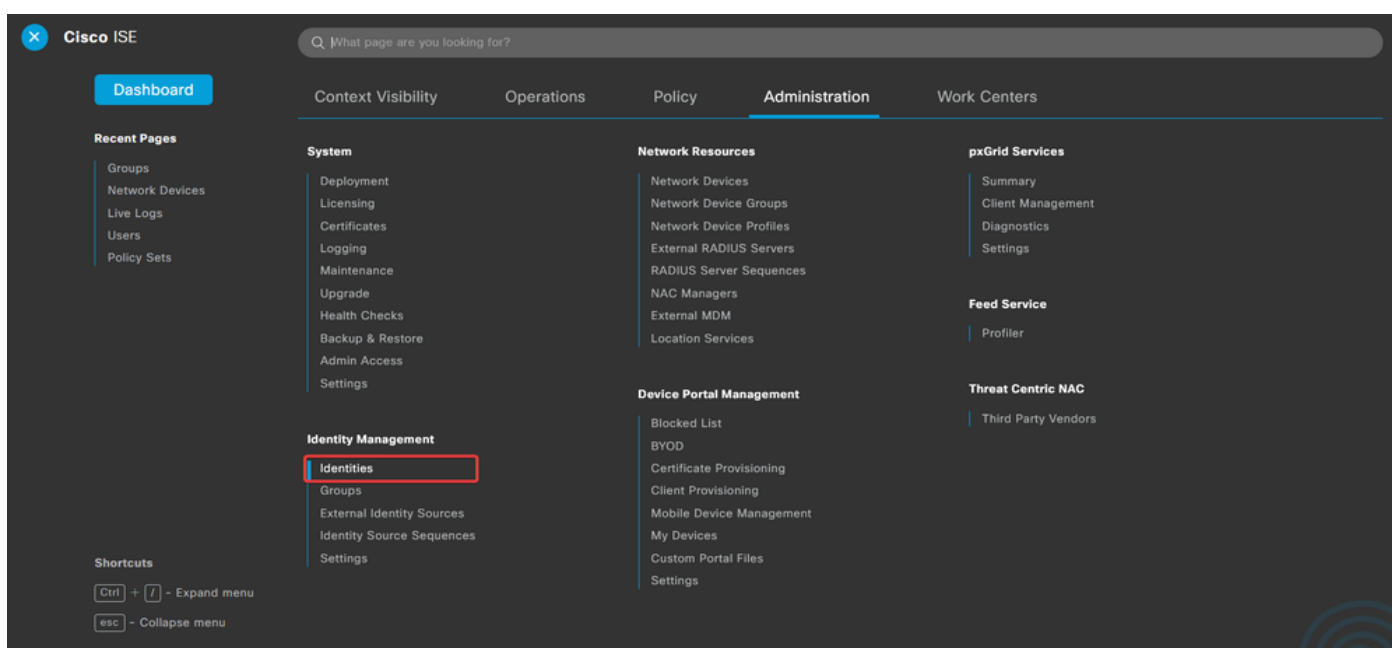
☐ Use Second Shared Secret ⓘ

networkDevices.secondSharedSecret [Show](#)

CoA Port [Set To Default](#)

Chave Compartilhada do Dispositivo de Rede

d. Navegue até **Administration > Identity Management > Identities**.



Administração-Identificar Gerenciamento-Identifica

e. Clique **Add** para criar um novo usuário no banco de dados local do servidor.

Insira o **Username** e **Login Password**. O nome de usuário é o mesmo nome que os certificados têm em valor de unidade organizacional no certificado e a senha de login deve ser a mesma que foi especificada no perfil **Ikev2**.

Clique em **.Save**

Network Access Users

Selected 0 Total 2  

 Edit  Add  Change Status  Import  Export  Delete  Duplicate Group  

Status	Username	Description	First Name	Last Name	Email Address	User Identity G...	Admin
☐	 Enabled  BLUE_GROUP						
☐	 Enabled  RED_GROUP						

Administração-Identificar Gerenciamento-Identifica

Network Access User

* Username

Status  Enabled 

Email

Passwords

Password Type: **Internal Users** 

Password

Re-Enter Password

* Login Password

.....

[Generate Password](#)



Enable Password

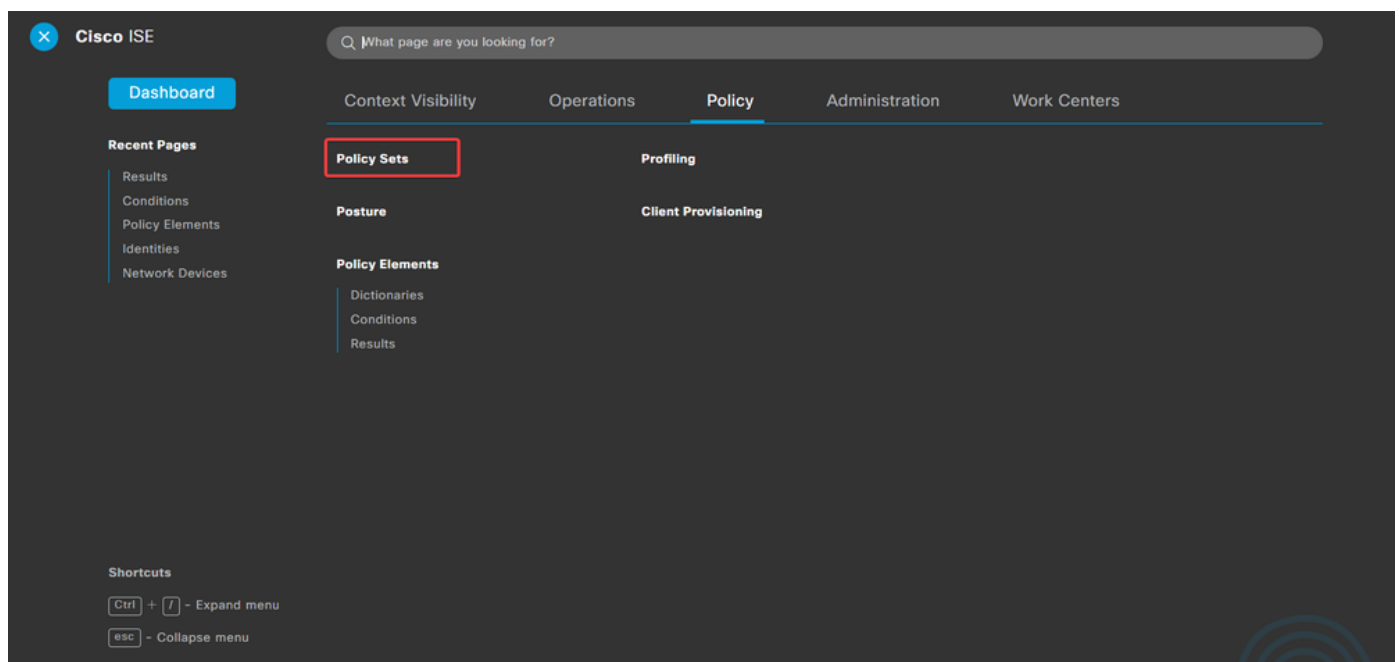
[Generate Password](#)



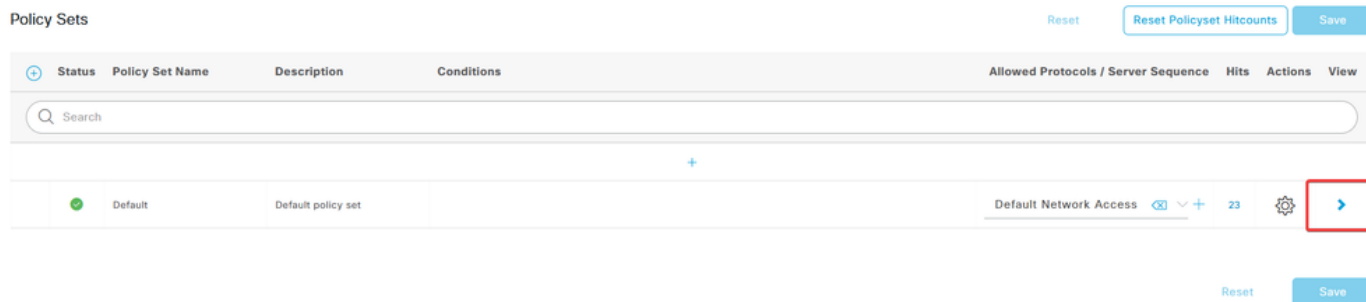
Grupo criado igual ao valor da unidade organizacional

Passo 3.2: Configurar Conjunto de Políticas

a. Navegue até **Policy > Policy Sets**.



b. Selecione a política de autorização padrão clicando na seta no lado direito da tela:



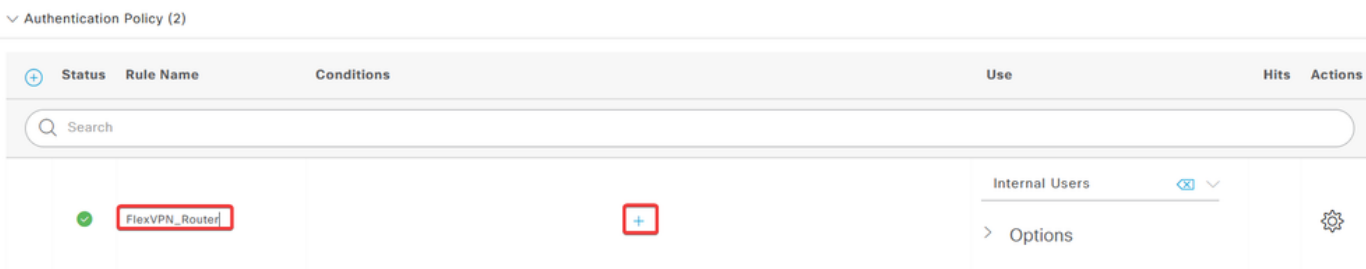
Editar política padrão

c. Clique na seta do menu suspenso ao lado de Authentication Policy para expandi-lo. Em seguida, clique no ícone para adicionar uma nova regraadd (+).



Adicionar política de autenticação

d. Insira o nome da regra e selecione o íconeadd (+)na coluna Condições.



Criar Política de Autenticação

e. Clique na caixa de texto Editor de atributos e clique noNAS-IP-Addressícone. Insira o endereço IP (192.168.0.10) do FlexVPN Hub.

Conditions Studio

Library

Search by Name



- Catalyst_Switch_Local_Web_Authentication
- EAP-MSCHAPv2

Editor

Radius·NAS-IP-Address

Equals

Set to 'Is not'

Duplicate

Save

NEW

AND

OR

Authentication Policy (3)

+	Status	Rule Name	Conditions	Use	Hits	Actions
	✓	FlexVPN	Radius-NAS-IP-Address EQUALS	Internal Users > Options	12	⚙️

Política de autenticação

Passo 3.3: Configurar Diretiva de Autorização

a. Clique na seta do menu suspenso ao lado de Authorization Policy para expandi-lo. Em seguida, clique no ícone para adicionar uma nova regra add (+).

Authorization Policy (13)

+	Status	Rule Name	Conditions	Results	Hits	Actions
				Profiles	Security Groups	

Criar Nova Diretiva de Autorização

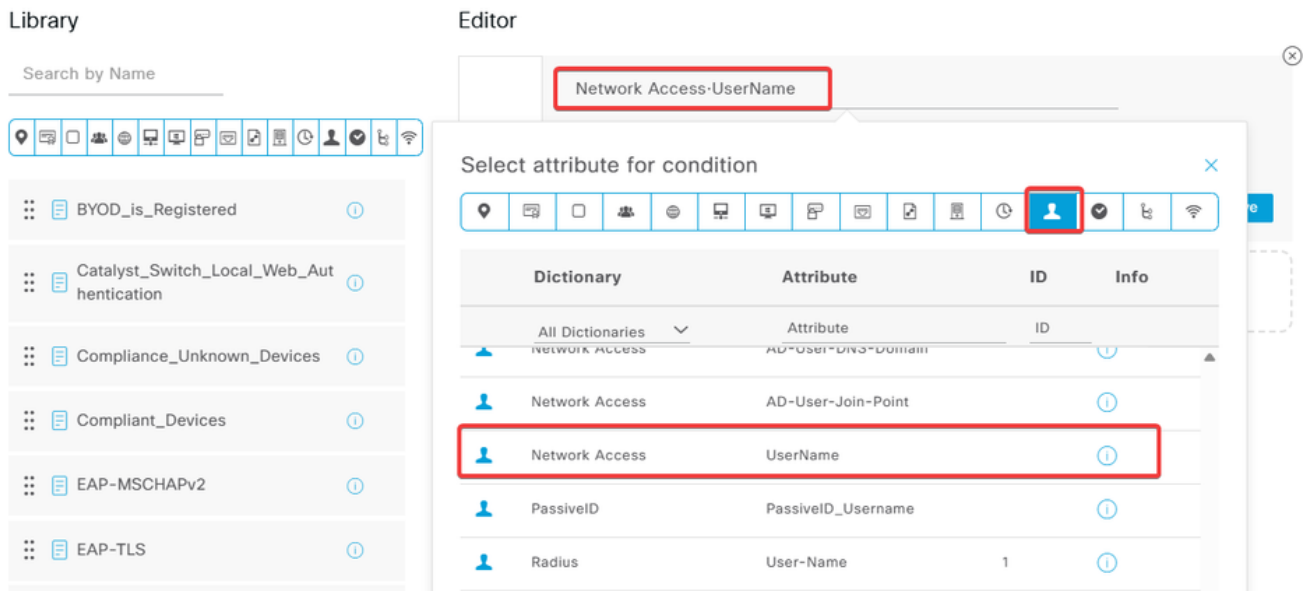
b. Insira o nome da regra e selecione o ícone add (+) na coluna Condições.

Authorization Policy (3)

+	Status	Rule Name	Conditions	Results	Hits	Actions
	✓	RED-GROUP	+	Profiles	Security Groups	
				Select from list	Select from list	

Criar nova regra

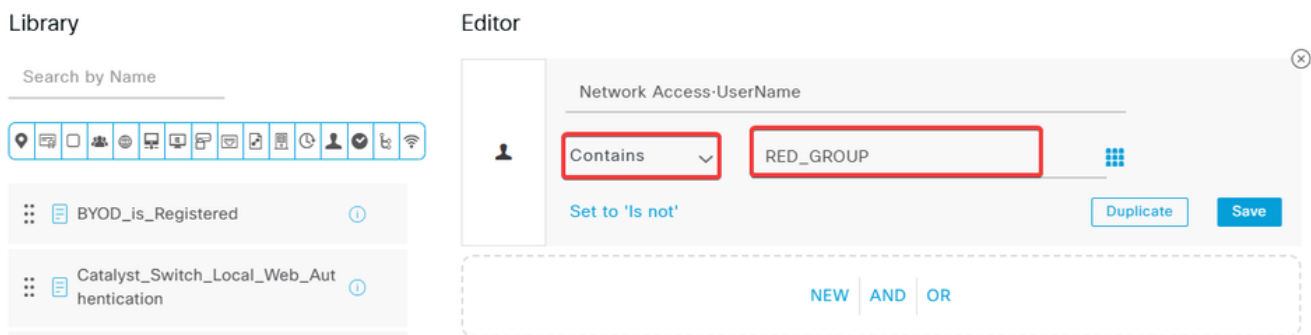
c. Clique na caixa de texto Editor de atributos e clique no Subject ícone. Selecione o Network Access - UserName atributo.



Selecionar Acesso à Rede - Nome de Usuário

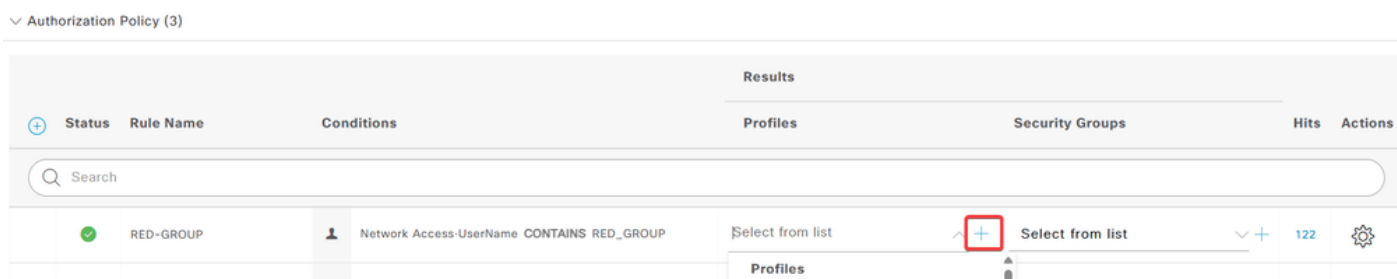
d. Selecione **Contains** como o operador e, em seguida, adicione o valor **Organization-Unit** dos certificados.

Conditions Studio



Adicionar nome do grupo

e. Na coluna **Profiles**, clique no **add (+)** ícone e escolha **Create a New Authorization Profile**.



Adicionar novo perfil de autorização

f. Digite o **perfilName**.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template ☐

Track Movement ☐

Agentless Posture ☐

Passive Identity Tracking ☐

Nomear o Perfil de Autorização

g. Navegue até **Advanced Attributes Settings**. Em seguida, selecione o `cisco-av-pair` atributo no menu suspenso no lado esquerdo e adicione o atributo que é atribuído ao FlexVPN Spoke, dependendo do grupo.

Os atributos a serem designados para este exemplo incluem:

- Atribuindo a interface de loopback como origem.
- Especificando o pool do qual os spokes obtêm um endereço IP.

Os atributos `route accept any` e `route set interface` são necessários porque, sem eles, as rotas não são anunciadas corretamente aos 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 loopback100		
	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

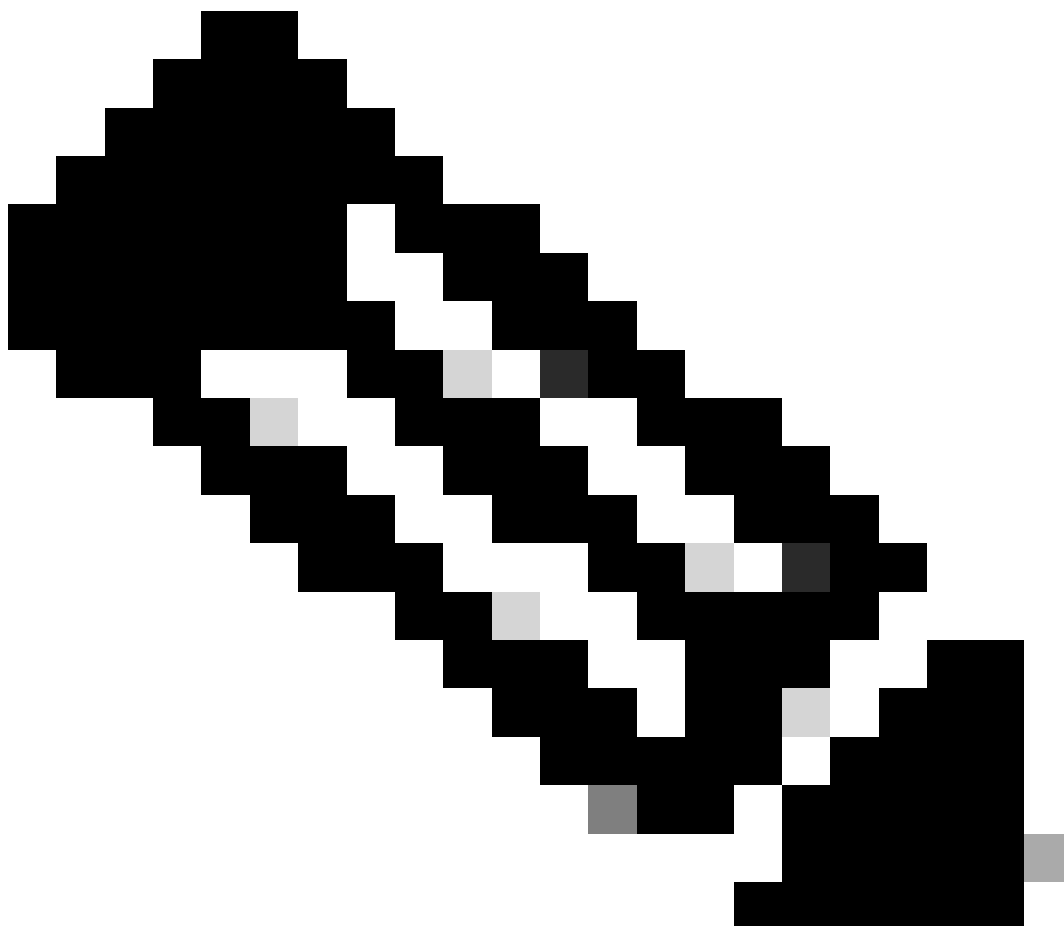
cisco-av-pair = ip:interface-config=ip unnumbered loopback100

cisco-av-pair = ipsec:addr-pool=RED_POOL

cisco-av-pair = ipsec:route-accept=any

cisco-av-pair = ipsec:route-set=interface

Configurações avançadas de atributos



Note: Para especificações de atributos (nome, sintaxe, descrição, exemplo e assim por diante), consulte o Guia de configuração de atributos RADIUS FlexVPN:

[Guia de configuração do FlexVPN e do Internet Key Exchange versão 2, Cisco IOS XE Gibraltar 16.12.x](#)

h. Atribua o **authorization profile** na coluna **Perfis**.

Authorization Policy (11)

				Results			
+ Status	Rule Name	Conditions		Profiles	Security Groups	Hits	Actions
Search							
	RED_GROUP	Network Access-UserName CONTAINS RED_GROUP		FlexVPN_RED	+ Select from list	+ 8	

Regra de autorização

i. Clique em **save**.

Verificar

- Use o comando `show ip interface brief` para revisar o status do túnel, modelo virtual e acesso virtual.

No Hub, o Modelo Virtual tem um status up/down, que é normal, e um Acesso Virtual é criado para cada Spoke que estabelece uma conexão com o Hub e mostra um status up/up.

<#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

No spoke, a interface de túnel recebeu um endereço IP do pool atribuído ao grupo e mostra um status 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 o 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
```

- Use o comando `show crypto session` para confirmar que a conexão segura entre os roteadores está estabelecida.

```
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 o comando `show ip eigrp neighbors` para confirmar se a adjacência EIGRP está estabelecida com o outro site.

```
FlexVPN_HUB#show ip eigrp neighbors
EIGRP-IPv4 VR(Flexvpn) Address-Family Neighbors for AS(10)
H   Address                Interface          Hold Uptime      SRTT   RTT    Q    Seq
                               (sec)            (ms)              Cnt    Num
0   172.16.10.107           Vi1                10 00:14:00       8   1494   0    31
```

- Use o comando `show ip route` para verificar se as rotas foram enviadas aos Spokes.
 - A rota para 10.20.1.10, interface de loopback no spoke foi aprendida pelo hub pelo EIGRP e é acessível por meio do acesso 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

```

- As rotas para 10.10.1.10 e 10.10.2.10 foram aprendidas por EIGRP e podem ser alcançadas por meio do IP de origem do RED_GROUP (10.100.100.1), que é acessível por meio do 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

```

Troubleshooting

Esta seção fornece informações que você pode usar para solucionar problemas desse tipo de implantação. Use estes comandos para depurar o processo de negociação do 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
```

As depurações de AAA e RADIUS podem ajudar na identificação e solução de problemas da autorização dos Spokes.

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

Working Scenario

Esse registro mostra o processo de autorização e a atribuição dos parâmetros.

```
<#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
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.