

Configurar o mapeamento de atributos RADIUS para usuários remotos do FlexVPN

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações](#)

[Configuração do roteador](#)

[Configuração do Identity Services Engine \(ISE\)](#)

[Configuração do Cliente](#)

[Verificar](#)

[Troubleshooting](#)

[Depurações e logs](#)

[Cenário de trabalho](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o FlexVPN usando o Cisco Identity Services Engine (ISE) para verificar identidades e executar o mapeamento do grupo de atributos.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Rede Virtual Privada de Acesso Remoto (RAVPN - Remote Access Virtual Private Network) com configuração IKEV2/IPsec em um Cisco IOS® XE Router via CLI
- Configuração do Cisco Identity Services Engine (ISE)
- Cisco Secure Client (CSC)
- protocolo RADIUS

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
- Cisco Secure Client (CSC) - Versão 5.0.05040
- Windows 11

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

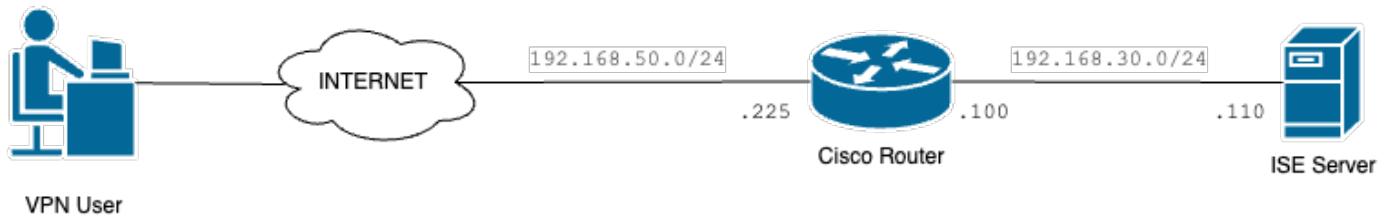


Diagrama básico de rede

Configurações

Configuração do roteador

Etapa 1. Configure um servidor RADIUS para autenticação e autorização local no dispositivo:

```
aaa new-model
aaa group server radius FlexVPN-Authentication-Server
server-private 192.168.30.110 key Cisco123
aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server
aaa authorization network FlexVPN-Authorization-List local
```

O comando `aaa authentication login <list_name>` refere-se ao grupo de autenticação, autorização e contabilização (AAA) (que define o servidor RADIUS).

O comando `aaa authorization network <list_name> local` informa que usuários/grupos definidos localmente devem ser usados.

Etapa 2. Configurar um ponto confiável para armazenar o certificado do roteador. Como a autenticação local do roteador é do tipo RSA, o dispositivo exige que o servidor se autentique usando um certificado:

```
crypto pki trustpoint FlexVPN-TP
enrollment url http://192.168.50.230:80
subject-name CN=192.168.50.225
revocation-check none
rsakeypair FlexVPN_KEY
```

Etapa 3. Defina um pool local de IP para cada grupo de usuários diferente:

```
ip local pool group1 172.16.10.1 172.16.10.50
ip local pool group2 172.16.20.1 172.16.20.50
```

Etapa 4. Configure a diretiva de autorização local:

```
crypto ikev2 authorization policy FlexVPN-Local-Policy
```

Nenhuma configuração é necessária na política de autorização, pois o servidor de autenticação é responsável por enviar os valores relevantes (DNS, pool, rotas protegidas e assim por diante) com base no grupo ao qual o usuário pertence. No entanto, ele deve ser configurado para definir o nome de usuário em nosso banco de dados de autorização local.

Etapa 5 (opcional). Crie uma proposta e uma política IKEv2 (se não estiverem configuradas, serão usados padrões inteligentes):

```
crypto ikev2 proposal IKEv2-prop
  encryption aes-cbc-256
  integrity sha256
  group 14
```

```
crypto ikev2 policy IKEv2-pol
  proposal IKEv2-prop
```

Etapa 6 (opcional). Configure o conjunto de transformação (se não estiver configurado, os padrões inteligentes serão usados):

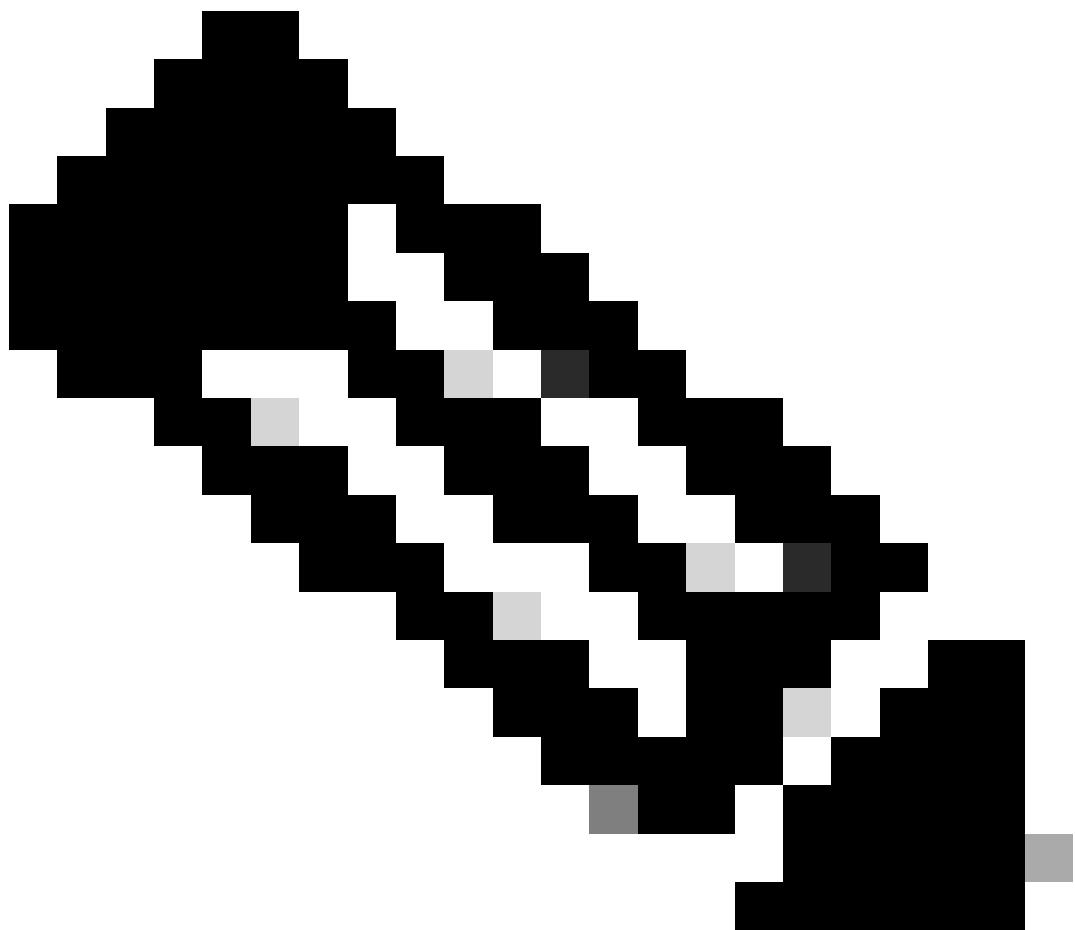
```
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
  mode tunnel
```

Passo 7. Configure um perfil IKEv2 com as identidades locais e remotas apropriadas, métodos de

autenticação (locais e remotos), ponto confiável, AAA e a interface de modelo virtual usada para as conexões:

```
crypto ikev2 profile FlexVPN-IKEv2-Profile
match identity remote key-id cisco.example
identity local dn
authentication local rsa-sig
authentication remote eap query-identity
pki trustpoint FlexVPN-TP
aaa authentication eap FlexVPN-Authentication-List
aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy
aaa authorization user eap cached
virtual-template 100
```

O comando aaa authorization user eap cached especifica que os atributos recebidos durante a autenticação EAP devem ser armazenados em cache. Esse comando é essencial para a configuração porque, sem ele, os dados enviados pelo servidor de autenticação não são usados, levando a uma falha na conexão.



Observação: o key-id remoto deve corresponder ao valor key-id no arquivo XML. Se não for modificado no arquivo XML, o valor padrão ("\$AnyConnectClient\$") será usado e deverá ser configurado no perfil IKEv2.

Etapa 8. Configure um perfil IPsec e atribua o conjunto de transformação e o perfil IKEv2:

```
crypto ipsec profile FlexVPN-IPsec-Profile  
set transform-set TS  
set ikev2-profile FlexVPN-IKEv2-Profile
```

Etapa 9. Configure uma interface de loopback. As interfaces de acesso virtual pegam emprestado o endereço IP:

```
interface Loopback100
```

```
ip address 10.0.0.1 255.255.255.255
```

Etapa 10. Crie o modelo virtual que será usado para criar as diferentes interfaces de acesso virtual e vincule o perfil IPSec criado na Etapa 8:

```
interface Virtual-Template100 type tunnel  
ip unnumbered Loopback100  
tunnel mode ipsec ipv4  
tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```

Etapa 11. Desabilite a pesquisa de certificado baseada em URL HTTP e o servidor HTTP no roteador:

```
no crypto ikev2 http-url cert  
no ip http server  
no ip http secure-server
```

Configuração do Identity Services Engine (ISE)

Etapa 1. Faça login no servidor ISE e navegue até Administração > Recursos de rede > Dispositivos de rede:

The screenshot shows the Cisco ISE web interface. The top navigation bar has tabs: Dashboard, Context Visibility, Operations, Policy, Administration (which is highlighted with a red box), and Work Centers. Below the navigation is a search bar. On the left, there's a sidebar with Recent Pages (Identities, Groups, Authorization Profiles, Results, Network Devices, Policy Sets) and Shortcuts (+ / - 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), and Threat Centric NAC (Third Party Vendors). A 'Make a wish' button is at the bottom left.

Menu geral do ISE

Etapa 2. Clique em Add para configurar o roteador como um cliente AAA:

The screenshot shows the 'Network Devices' section of the Cisco ISE interface. At the top, there are tabs for 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'More'. The 'Network Devices' tab is selected. On the left, there are links for 'Default Device' and 'Device Security Settings'. The main area is titled 'Network Devices' and contains a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. A single row is visible, showing 'CISCO_ROU...' as the name, 'Cisco' as the profile, 'All Locations' as the location, and 'All Device Types' as the type. Below the table are buttons for 'Edit', '+ Add' (which is highlighted with a red box), 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete'. At the bottom right, there are filters for 'All' and 'Selected 0 Total 1'.

Adicionando um novo dispositivo de rede

Insira os campos Nome do dispositivo de rede e Endereço IP e marque a caixa Configurações de autenticação RADIUS e adicione o Segredo compartilhado. Esse valor deve ser o mesmo que foi usado quando o objeto Servidor RADIUS no roteador foi criado.

Network Devices

The screenshot shows the 'Add Network Device' form. It has fields for 'Name' (containing 'CISCO_ROUTER'), 'Description' (empty), 'IP Address' (containing '192.168.30.110'), and a subnet mask ('/32'). There is also a gear icon for settings. The 'IP Address' field is highlighted with a red box.

Nome e endereço IP



✓ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret [Show](#)

Use Second Shared Secret [i](#)

networkDevices.secondSharedSecret

[Show](#)

Senha Radius

Click Save.

Etapa 3. Navegue até Administração > Gerenciamento de identidades > Grupos:

The screenshot shows the Cisco ISE Administration interface. The top navigation bar has tabs: Dashboard, Context Visibility, Operations, Policy, Administration (which is highlighted with a red box), and Work Centers. On the left, there's a sidebar with 'Recent Pages' (Identities, Groups, Authorization Profiles, Results, Policy Sets) and 'Shortcuts' (Expand menu, 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); and 'Threat Centric NAC' (Third Party Vendors). A red box highlights the 'Groups' link under the 'Identity Management' heading in the 'System' section. A watermark of a fingerprint is visible in the bottom right corner.

Menu geral do ISE

Etapa 4. Clique em User Identity Groups e, em seguida, clique em Add:

Identity Groups

<

> Endpoint Identity Groups

> User Identity Groups

User Identity Groups

Selected 0 Total 10

All

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group

Adicionar um novo grupo

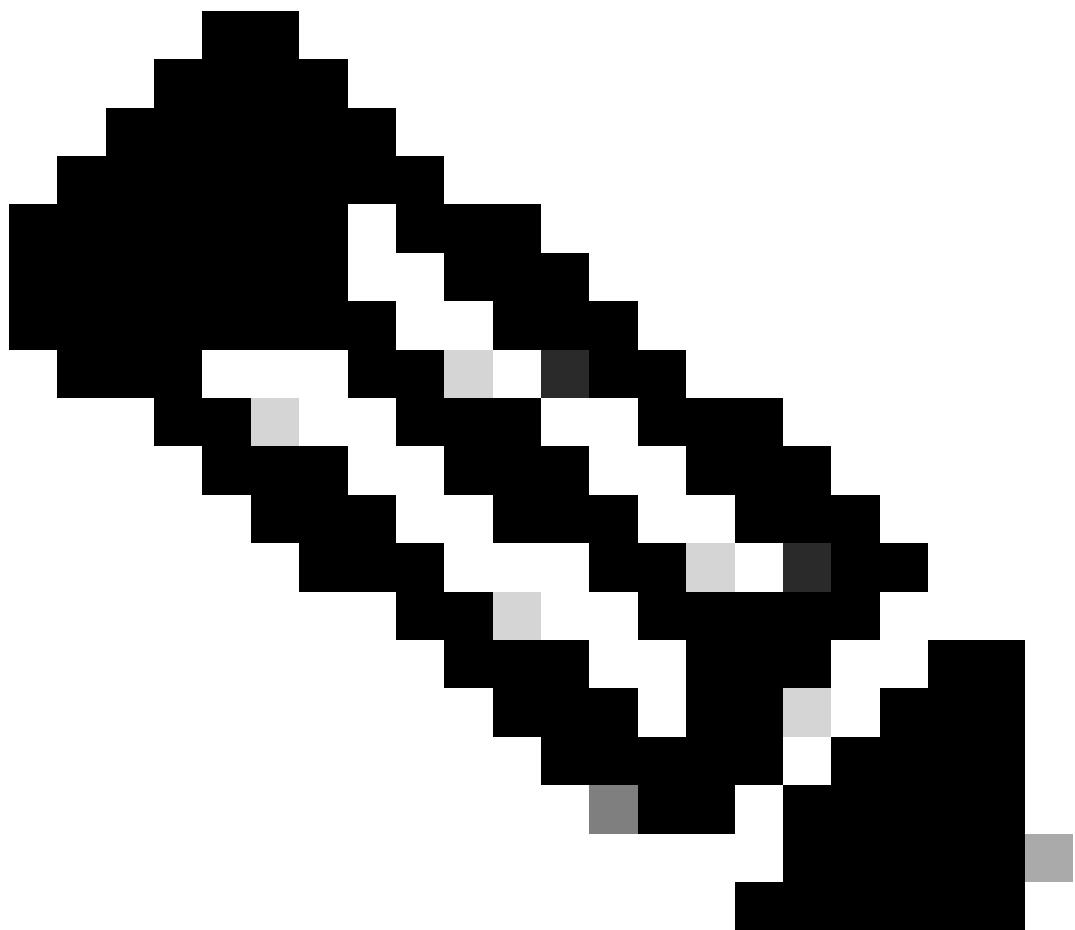
Insira o Nome do grupo e clique em Enviar.

Identity Group

* Name

Description

Informações do grupo



Observação: repita as etapas 3 e 4 para criar quantos grupos forem necessários.

Etapa 5. Navegue até Administração > Gerenciamento de identidades > Identidades:

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes links for Dashboard, Context Visibility, Operations, Policy, Administration (which is highlighted with a red box), and Work Centers. On the left, there's a sidebar with 'Recent Pages' (Groups, Network Devices, Authorization Profiles, Results, Policy Sets) and 'Shortcuts' (Expand menu, 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 Manageme...); 'Threat Centric NAC' (Third Party Vendors); and 'Identity Management' (Identities, Groups, External Identity Sources, Identity Source Sequences, Settings). A large blue button labeled 'Make a wish' is at the bottom left. A watermark of a fingerprint is on the right.

Menu geral do ISE

Etapa 6. Clique em Add para criar um novo usuário no banco de dados local do servidor:

The screenshot shows the 'Network Access Users' page under the 'Identities' tab. The top navigation bar includes 'Identities' (highlighted with a red box), 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. On the left, there's a sidebar with 'Users' (Latest Manual Network Scan Res...). The main content area has a title 'Network Access Users' and a toolbar with 'Edit', 'Add' (highlighted with a red box), 'Change Status', 'Import', 'Export', 'Delete', 'Duplicate', 'Selected 0 Total 0', and filters. Below is a table header with columns: Status, Username, Description, First Name, Last Name, Email Address, User Identity Grou..., and Admin. The message 'No data available' is displayed below the table.

Adicionar um usuário

Insira o nome de usuário e a senha de login. Em seguida, navegue até o final desta página e selecione o Grupo de usuários:

✓ Network Access User

* Username user1

Status Enabled

Email

✓ Passwords

Password Type: Internal Users

Password

Re-Enter Password

* Login Password

.....

Generate Password

(i)

Enable Password

Generate Password

(i)

Nome de usuário e senha

✓ Account Options

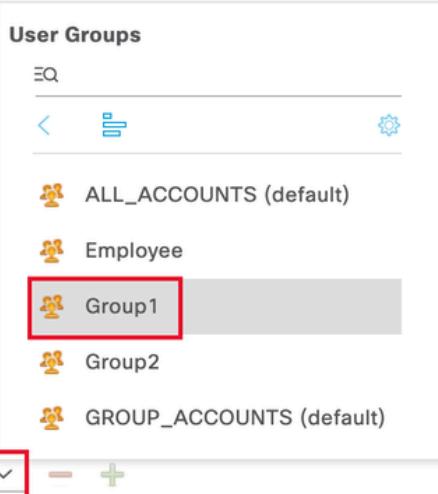
Description

Change password on next login

✓ Account Disable Policy

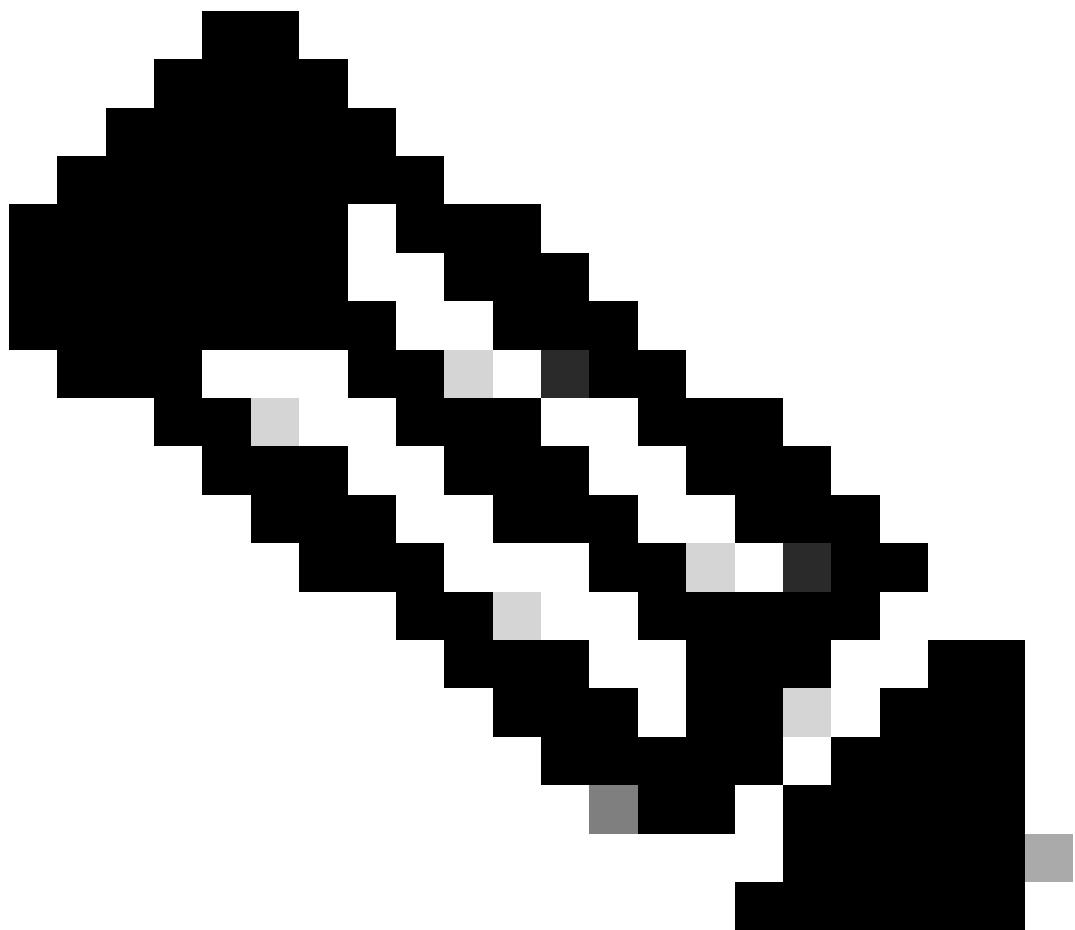
Disable account if date exceeds 20

✓ User Groups



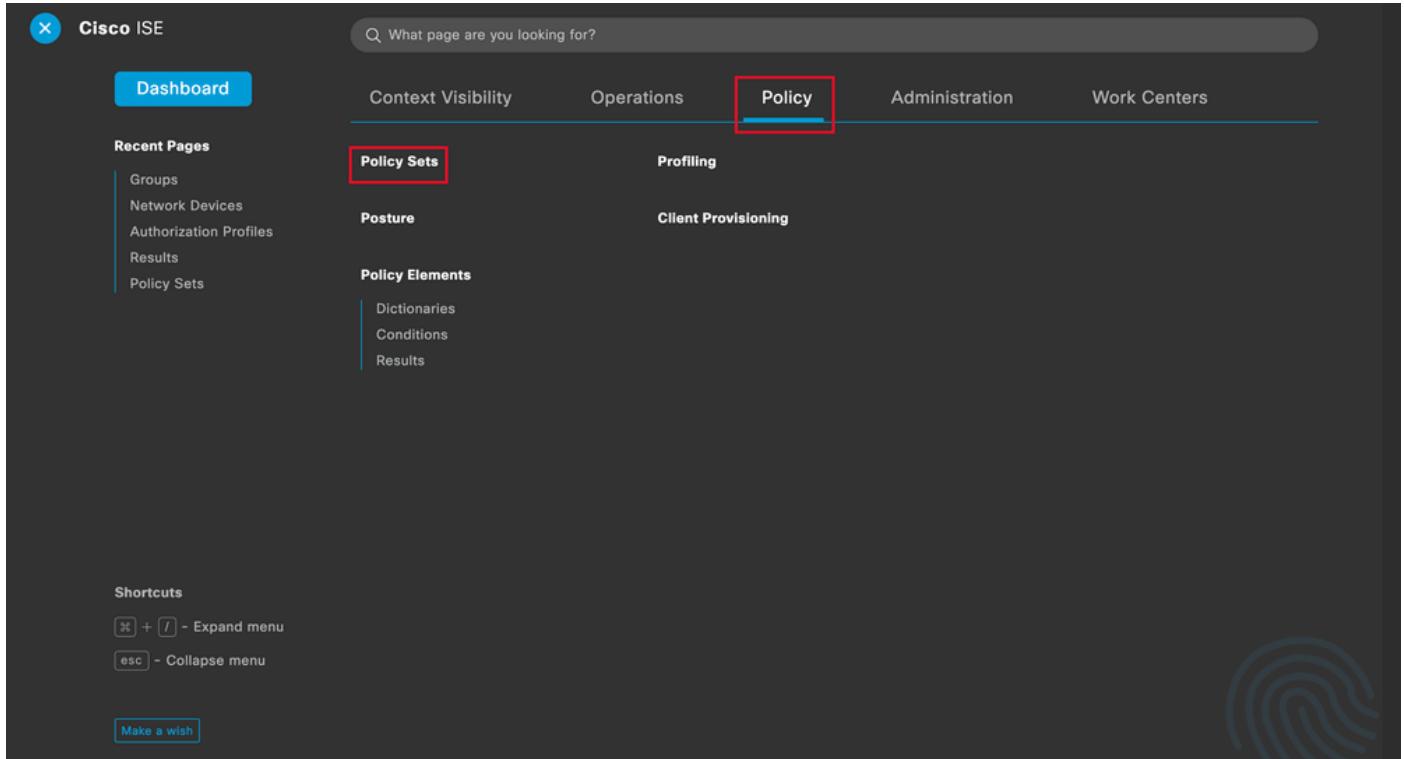
Atribuir o grupo correto ao usuário

Click Save.



Observação: Repita as etapas 5 e 6 para criar os usuários necessários e atribuí-los ao grupo correspondente.

Etapa 7. Navegue até Política > Conjuntos de Políticas:



Menu geral do ISE

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

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input checked="" type="checkbox"/>	Default	Default policy set		Default Network Access	35		

Seleciona a Política de Autorização

Etapa 8. Clique na seta do menu suspenso ao lado de Diretiva de autorização para expandi-la. Em seguida, clique no ícone add (+) para adicionar uma nova regra:

Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
<input checked="" type="checkbox"/>						

Adicionar uma nova regra de autorização

Digite o nome da regra e selecione o ícone adicionar (+) na coluna Condições:

The screenshot shows the 'Conditions' tab selected in the Rule Editor. The 'Rule Name' field contains 'Group1_AuthZ_Rule'. There is a red box around both the 'Rule Name' field and the 'Conditions' tab.

Adicionar uma Condição

Etapa 9. Clique na caixa de texto Editor de atributos e clique no ícone de grupo Identidade. Selecione o atributo Grupo de identidade - Nome:

Conditions Studio

The screenshot shows the 'Select attribute for condition' dialog in the Conditions Studio. The 'Dictionary' dropdown menu icon is highlighted with a red box. The 'IdentityGroup' row, specifically the 'Name' column, is also highlighted with a red box.

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
CWA	CWA_ExternalGroups		
IdentityGroup	Description		
IdentityGroup	Name		
InternalUser	IdentityGroup		
PassiveID	PassiveID_Groups		

Selecione a Condição

Selecionelqual como o operador e, em seguida, clique na seta do menu suspenso para mostrar as opções disponíveis e selecione User Identity Groups:<GROUP_NAME>.

Editor

IdentityGroup·Name

Equals Choose from list or type

User Identity Groups:GROUP_ACCOUNTS (default)

User Identity Groups:Group1 **Save**

User Identity Groups:Group2

User Identity Groups:GuestType_Contractor (default)

User Identity Groups:GuestType_Daily (default)

Selecione o grupo

Click Save.

Etapa 10. Na coluna Profiles, clique no ícone add (+) e escolha Create a New Authorization Profile:

Results					
Status	Rule Name	Conditions	Profiles	Security Groups	Hits Actions
+	Group1_AuthZ_Rule	IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list + Create a New Authorization Profile	Select from list	10
+	Wireless Black List Default	AND	Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	Select from list	0

Criar o Perfil de Autorização

Insira o nome do perfil

Add New Standard Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile   

Service Template

Track Movement 

Agentless Posture 

Passive Identity Tracking 

Informações de perfil

Navegue até o final desta página em Advanced Attribute Settings e clique na seta do menu suspenso. Em seguida, clique em Cisco e selecione cisco-av-pair—[1]:

Advanced Attributes Settings

Select an item  =  

Cisco

cisco-abort-cause--[21]
cisco-account-info--[250]
cisco-assign-ip-pool--[218]
cisco-av-pair--[1]
cisco-call-filter--[243]
cisco-call-id--[141]

Attributes Details
Access Type = ACCESS_ACCEPT

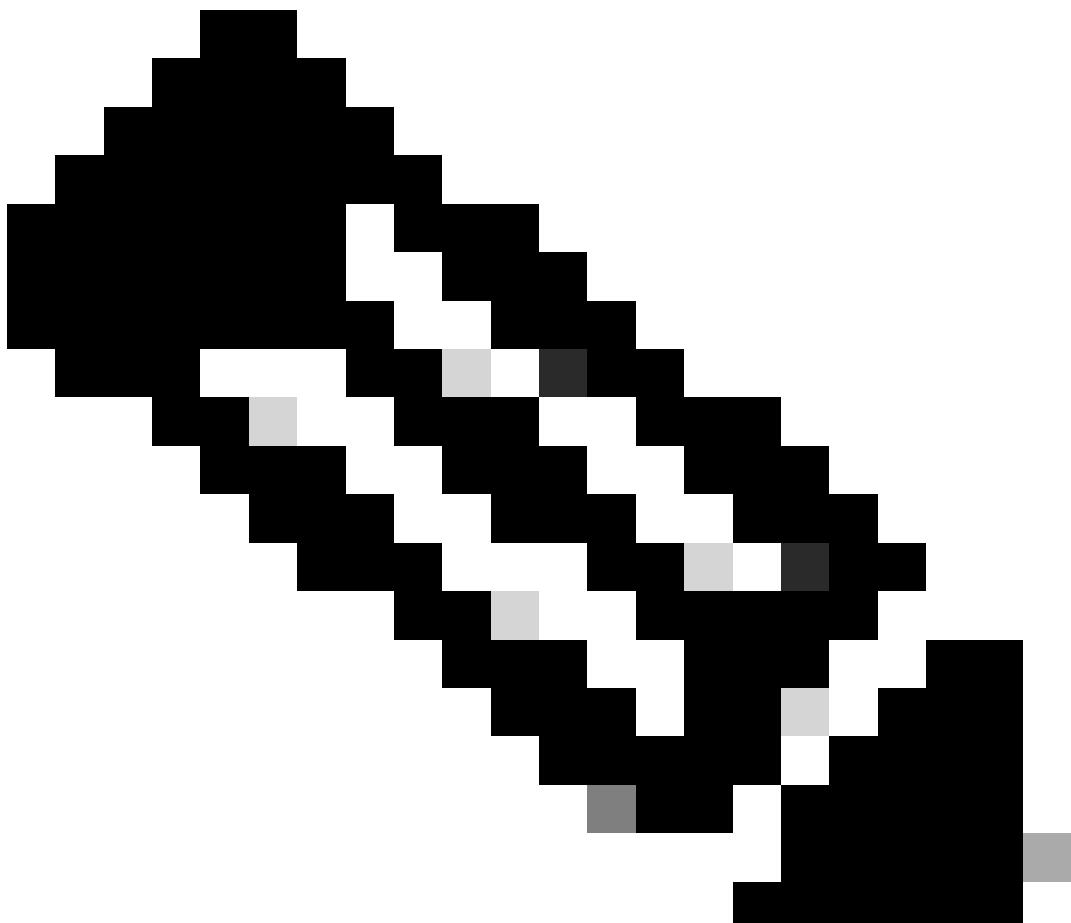
Selecione o Tipo de Atributo

Adicione o atributo cisco-av-pair que deseja configurar e clique no ícone add (+) para adicionar outro atributo:

Advanced Attributes Settings

Cisco:cisco-av-pair = ipsec:dns-servers=10.0.50.10

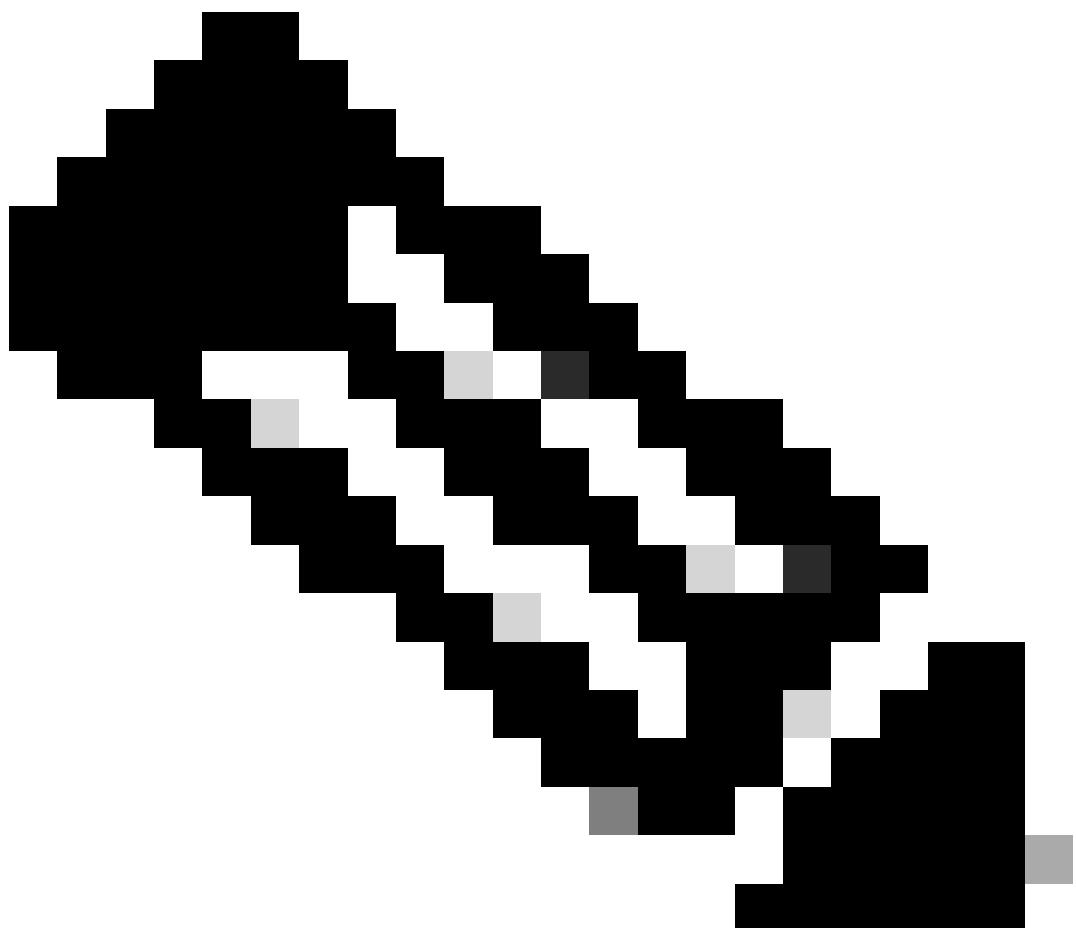
Configurar o Atributo



Observação: para obter as especificações de atributo (nome, sintaxe, descrição, exemplo, etc.), consulte o guia de configuração de atributos RADIUS FlexVPN:

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

[Fuji 16.9.x - Atributos RADIUS suportados](#)



Observação: Repita a etapa anterior para criar os atributos necessários.

Click Save.

Os atributos que vêm em seguida foram atribuídos a cada grupo:

- Atributos do grupo 1:

✓ Advanced Attributes Settings

⋮ Cisco:cisco-av-pair	▼	=	ipsec:dns-servers=10.0.50.10	▼	—
⋮ Cisco:cisco-av-pair	▼	=	ipsec:route-set=prefix 192.168.100.0/24	▼	—
⋮ Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=group1	▼	— +

✓ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ipsec:dns-servers=10.0.50.101
cisco-av-pair = ipsec:route-set=prefix 192.168.100.0/24
cisco-av-pair = ipsec:addr-pool=group1
```

Atributo Group1

- Atributos do grupo 2:

✓ Advanced Attributes Settings

⋮ Cisco:cisco-av-pair	▼	=	ipsec:dns-servers=10.0.50.20	▼	—
⋮ Cisco:cisco-av-pair	▼	=	ipsec:route-set=prefix 192.168.200.0/24	▼	—
⋮ Cisco:cisco-av-pair	▼	=	ipsec:addr-pool=group2	▼	— +

✓ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ipsec:dns-servers=10.0.50.202
cisco-av-pair = ipsec:route-set=prefix 192.168.200.0/24
cisco-av-pair = ipsec:addr-pool=group2
```

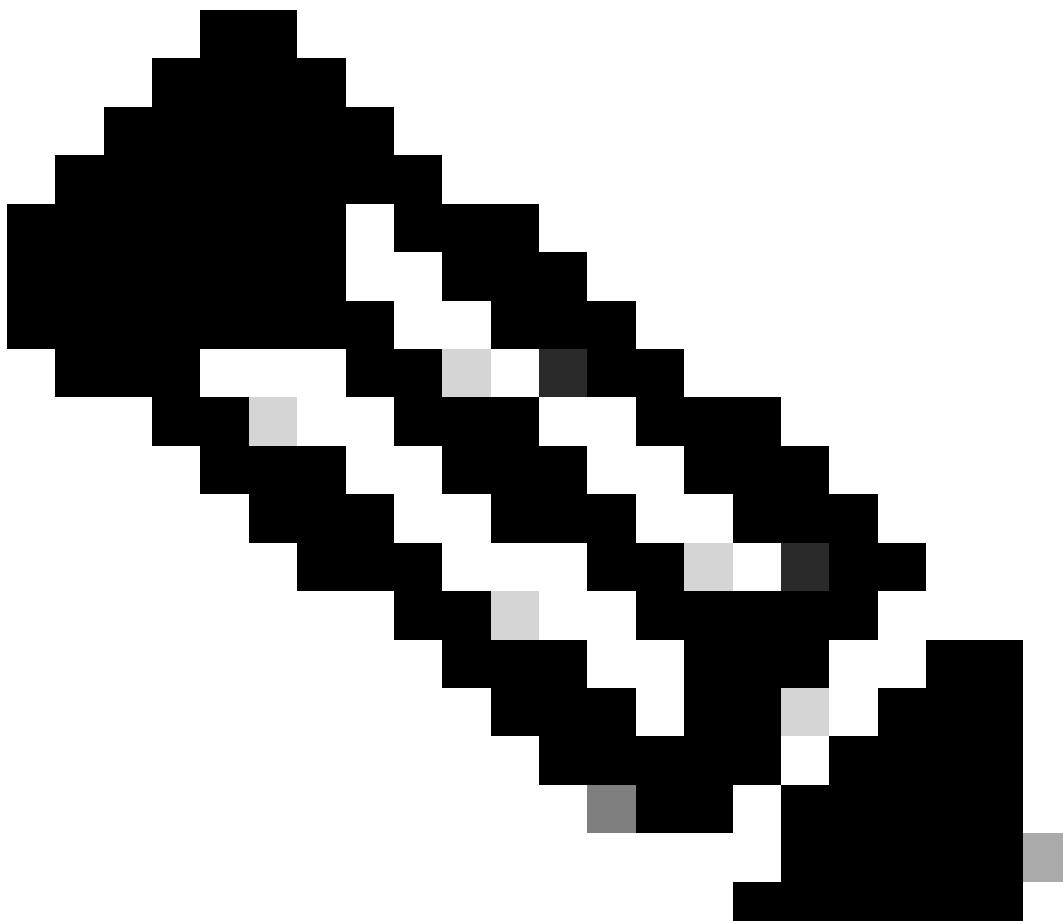
Atributos do Grupo2

Etapa 11. Clique na seta do menu suspenso e selecione o perfil de autorização criado na Etapa 10:

Status Rule Name		Conditions	Profiles	Security Groups	Hits	Actions
<input type="text"/> Search						
<input checked="" type="checkbox"/>	Group1_AuthZ_Rule	<input type="text"/> IdentityGroup-Name EQUALS User Identity Groups:Group1	Select from list <input type="button" value="^"/> <input type="button" value="+"/>	Select from list <input type="button" value="^"/> <input type="button" value="+"/> 10 <input type="button" value="gear"/>		
<input checked="" type="checkbox"/>	Wireless Black List Default	AND <input type="text"/> Wireless_Access <input type="text"/> IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DenyAccess NSP_Onboard Non_Cisco_IP_Phones PermitAccess <input type="text"/> Profile_group1	Select from list <input type="button" value="^"/> <input type="button" value="+"/> 0 <input type="button" value="gear"/>		
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	<input type="text"/> IdentityGroup-Name EQUALS Endpoint Identity Groups:Profiled:Cisco-IP-Phone		Select from list <input type="button" value="^"/> <input type="button" value="+"/> 0 <input type="button" value="gear"/>		
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	<input type="text"/> Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phones <input type="button" value="x"/> <input type="button" value="+"/>	Select from list <input type="button" value="^"/> <input type="button" value="+"/> 0 <input type="button" value="gear"/>		

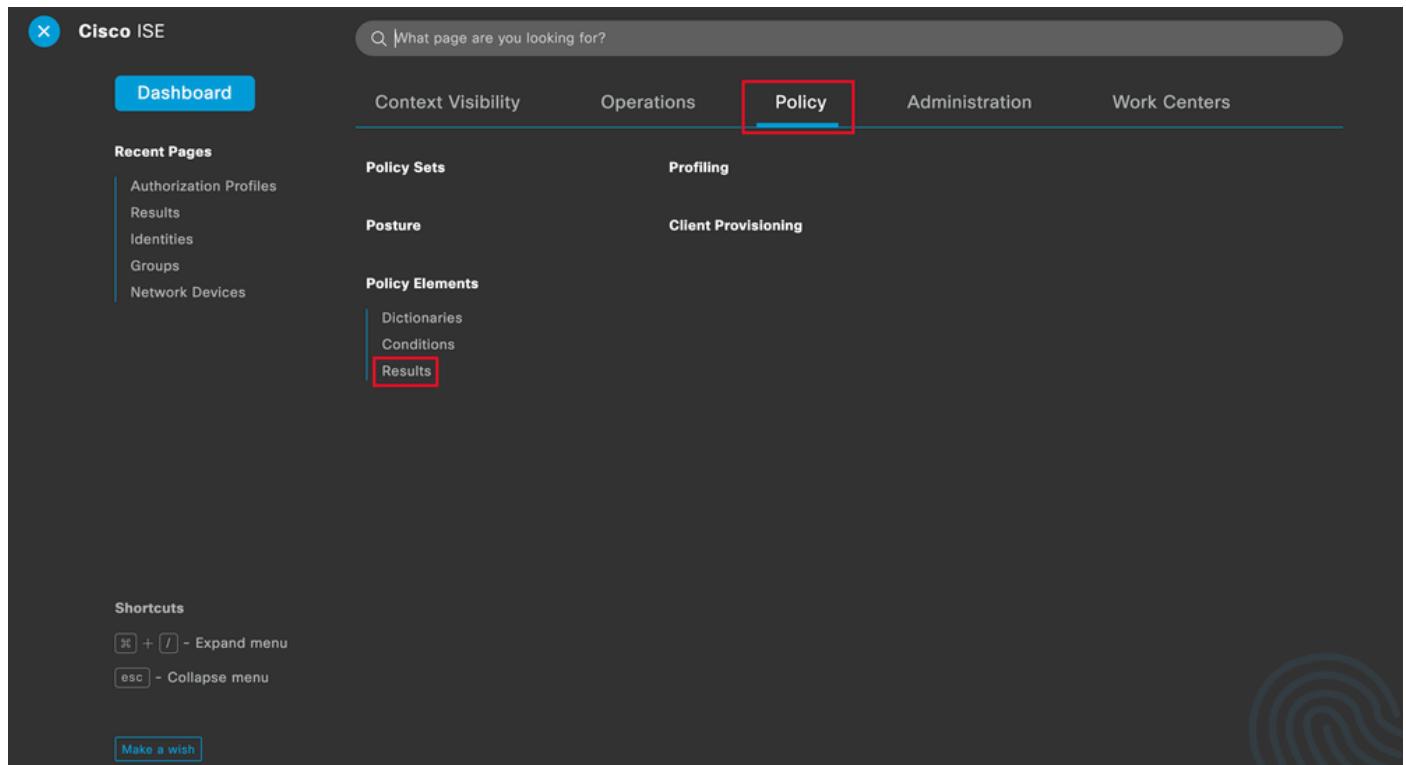
Atribuir perfil de autorização

Click Save.



Observação: repita as etapas de 8 a 11 para criar as regras de autorização necessárias para cada grupo.

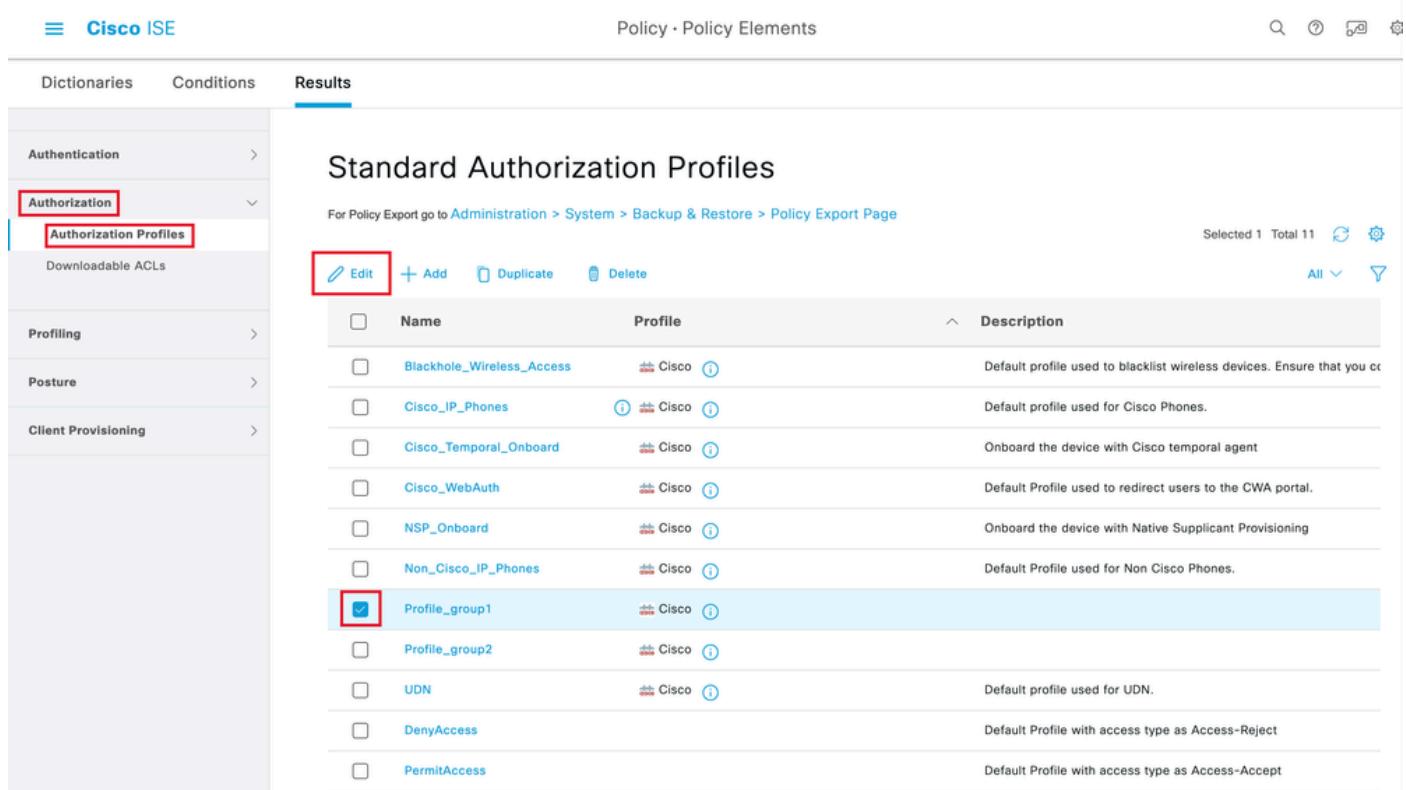
Etapa 12 (opcional). Se você precisar editar o perfil de autorização, navegue para Política > Resultados:



The screenshot shows the Cisco ISE dashboard with the 'Policy' tab selected. In the 'Policy Elements' section, the 'Results' link is highlighted with a red box.

Menu geral do ISE

Navegue até Autorização > Perfis de autorização. Clique na caixa de seleção do perfil que deseja modificar e, em seguida, clique em Edit:



The screenshot shows the 'Standard Authorization Profiles' page in Cisco ISE. The 'Edit' button is highlighted with a red box. The 'Profile_group1' row has a checked checkbox next to it, also highlighted with a red box.

<input type="checkbox"/>	Name	Profile	Description
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco	Default profile used to blacklist wireless devices. Ensure that you correctly define the blacklisted devices.
<input type="checkbox"/>	Cisco_IP_Phones	Cisco	Default profile used for Cisco Phones.
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco	Onboard the device with Cisco temporal agent
<input type="checkbox"/>	Cisco_WebAuth	Cisco	Default Profile used to redirect users to the CWA portal.
<input type="checkbox"/>	NSP_Onboard	Cisco	Onboard the device with Native Suplicant Provisioning
<input type="checkbox"/>	Non_Cisco_IP_Phones	Cisco	Default Profile used for Non Cisco Phones.
<input checked="" type="checkbox"/>	Profile_group1	Cisco	
<input type="checkbox"/>	Profile_group2	Cisco	
<input type="checkbox"/>	UDN	Cisco	Default profile used for UDN.
<input type="checkbox"/>	DenyAccess		Default Profile with access type as Access-Reject
<input type="checkbox"/>	PermitAccess		Default Profile with access type as Access-Accept

Editar o perfil de autorização

Configuração do Cliente

Etapa 1. Crie um perfil XML usando o editor de perfil XML. Este exemplo é aquele usado para a criação deste documento:

```
<#root>
```

```
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreMac>All</CertificateStoreMac>
<CertificateStoreLinux>All</CertificateStoreLinux>
<CertificateStoreOverride>true</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true</AllowLocalProxyConnections>
<AuthenticationTimeout>30</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection>
<ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin>
<IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
<AutoReconnect UserControllable="false">
    true
    <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
<SuspendOnConnectedStandby>false</SuspendOnConnectedStandby>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">
    Disable
    <PPPExclusionServerIP UserControllable="false"/>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">
    false
    <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
    <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>
    FlexVPN HUB
</HostName>
<HostAddress>

```

192.168.50.225

```
</HostAddress>
<PrimaryProtocol>

IPsec

<StandardAuthenticationOnly>
true
<AuthMethodDuringIKENegotiation>

EAP-MD5

</AuthMethodDuringIKENegotiation>
<IKEIdentity>

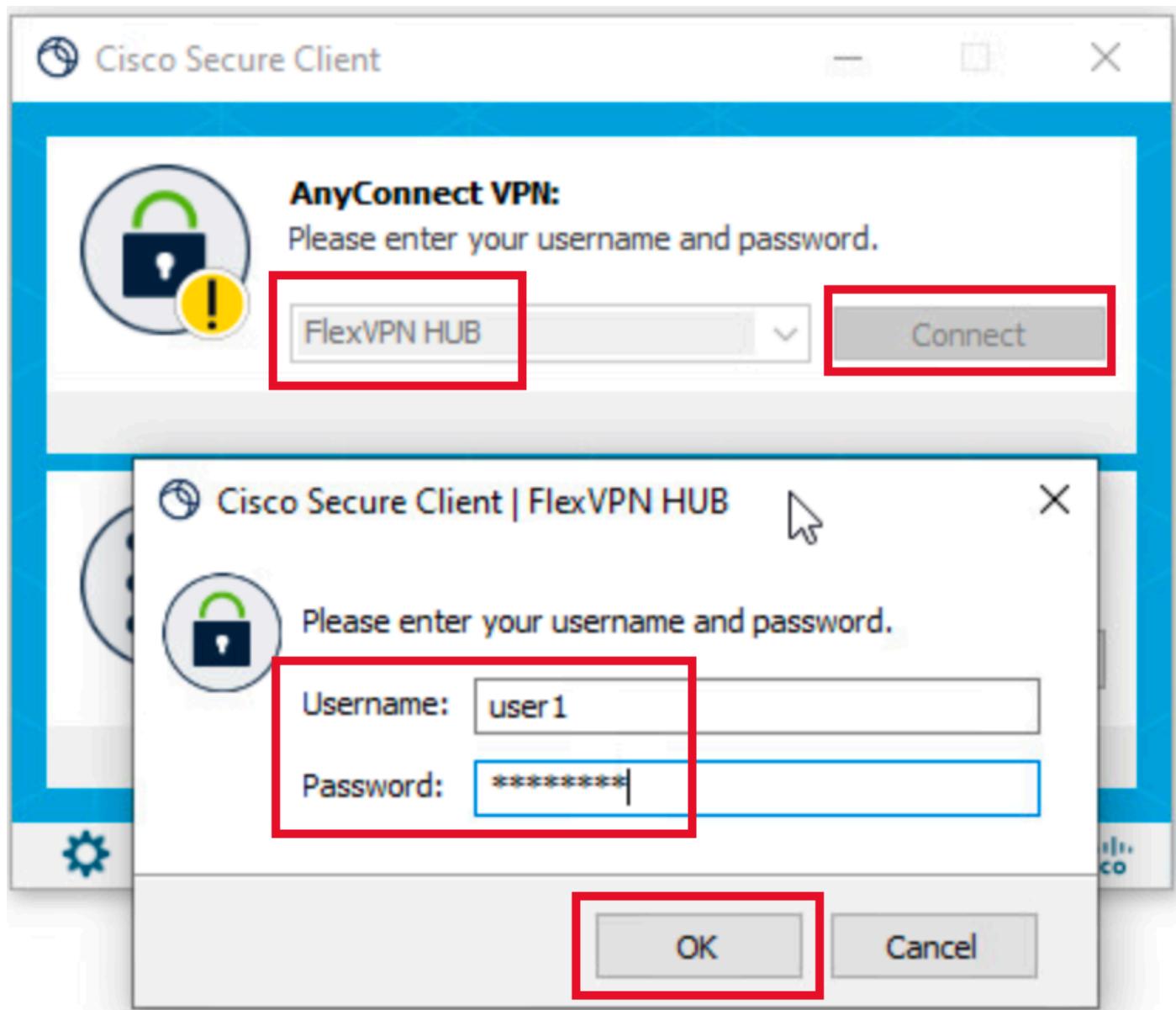
cisco.example

</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

- <HostName> - O alias usado para se referir ao host, endereço IP ou FQDN (Nome de domínio totalmente qualificado). Isso é exibido na caixa CSC.
- <HostAddress> - Endereço IP ou FQDN do hub FlexVPN.
- <PrimaryProtocol> - Deve ser definido como IPsec para forçar o cliente a usar IKEv2/IPsec em vez de SSL.
- <AuthMethodDuringIKENegotiation> - Deve ser definido para usar EAP-MD5 em EAP. Isso é necessário para autenticação no servidor ISE.
- <IKEIdentity> - Esta cadeia de caracteres é enviada pelo cliente como o payload de ID do tipo ID_GROUP. Isso pode ser usado para corresponder o cliente a um perfil IKEv2 específico no hub.

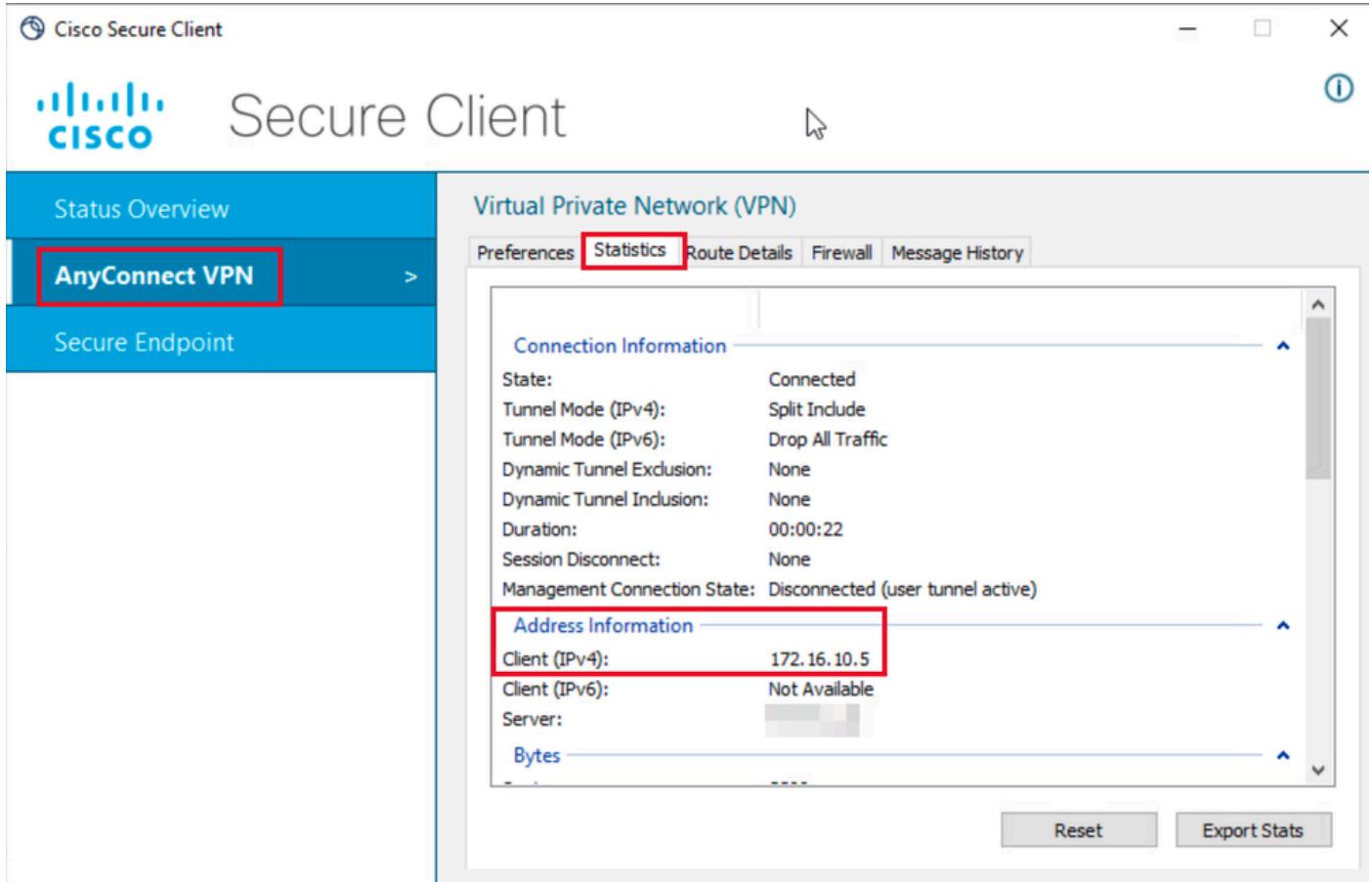
Verificar

Etapa 1. Navegue até a máquina do cliente na qual o CSC está instalado. Conecte-se ao hub FlexVPN e insira as credenciais do usuário1:



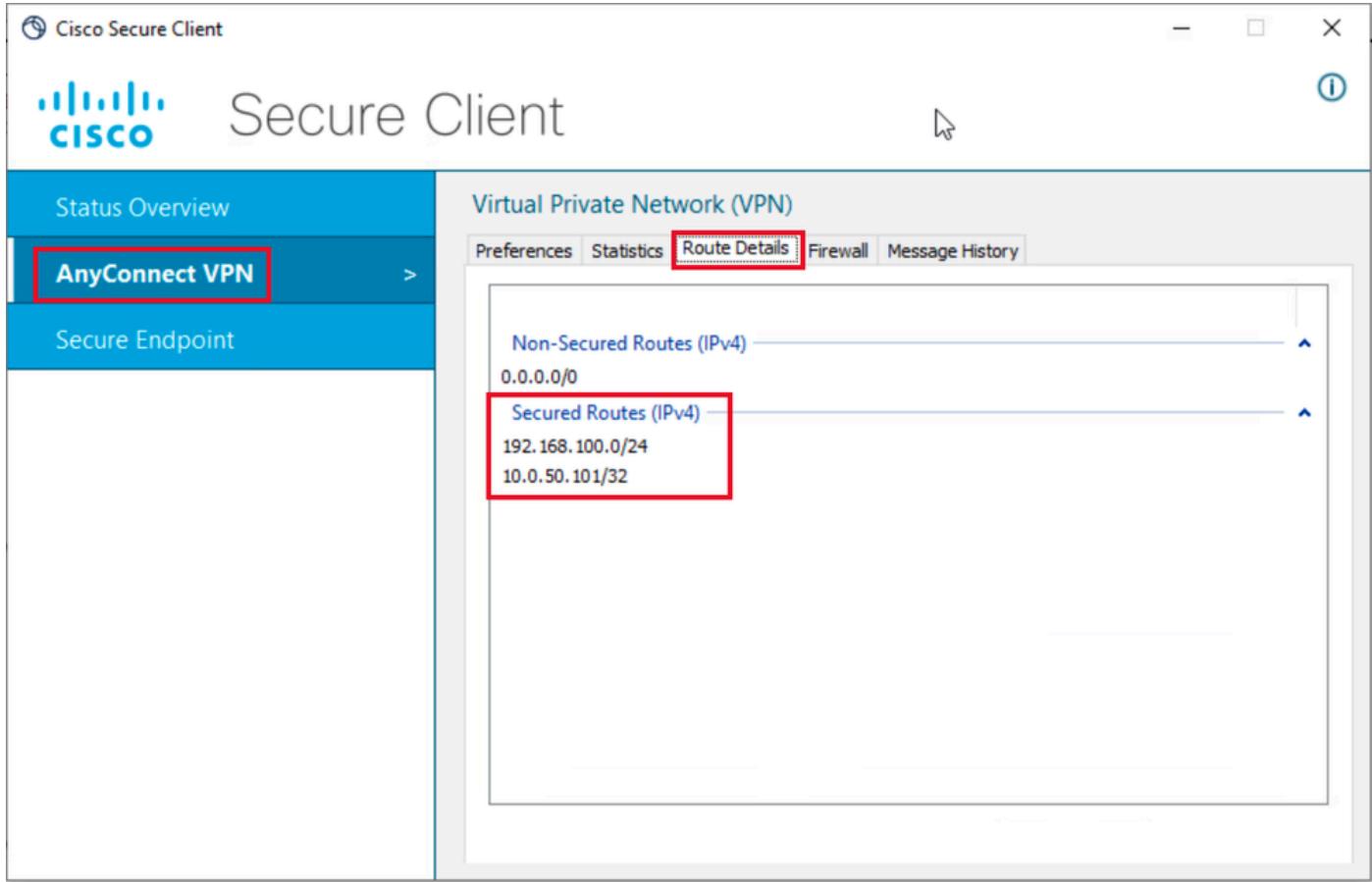
Credenciais do Usuário1

Etapa 2. Quando a conexão estiver estabelecida, clique no ícone de engrenagem (canto inferior esquerdo) e navegue para AnyConnectVPN > Statistics. Confirme na seção Informações de endereço que o endereço IP atribuído pertence ao pool configurado para group1:



Estatísticas do Usuário1

Navegue para AnyConnectVPN > Route details e confirme se as informações exibidas correspondem às rotas seguras e ao DNS configurado para group1:



Detalhes da Rota do Usuário1

Etapa 3. Repita as etapas 1 e 2 com as credenciais do usuário2 para verificar se as informações correspondem aos valores configurados na política de autorização do ISE para este grupo:



Cisco Secure Client



AnyConnect VPN:

Please enter your username and password.

FlexVPN HUB

Connect



Cisco Secure Client | FlexVPN HUB



Please enter your username and password.

Username: user2

Password: *****

OK

Cancel

Credenciais do Usuário2

Cisco Secure Client

Secure Client

Status Overview

AnyConnect VPN >

Secure Endpoint

Virtual Private Network (VPN)

Preferences Statistics Route Details Firewall Message History

Connection Information

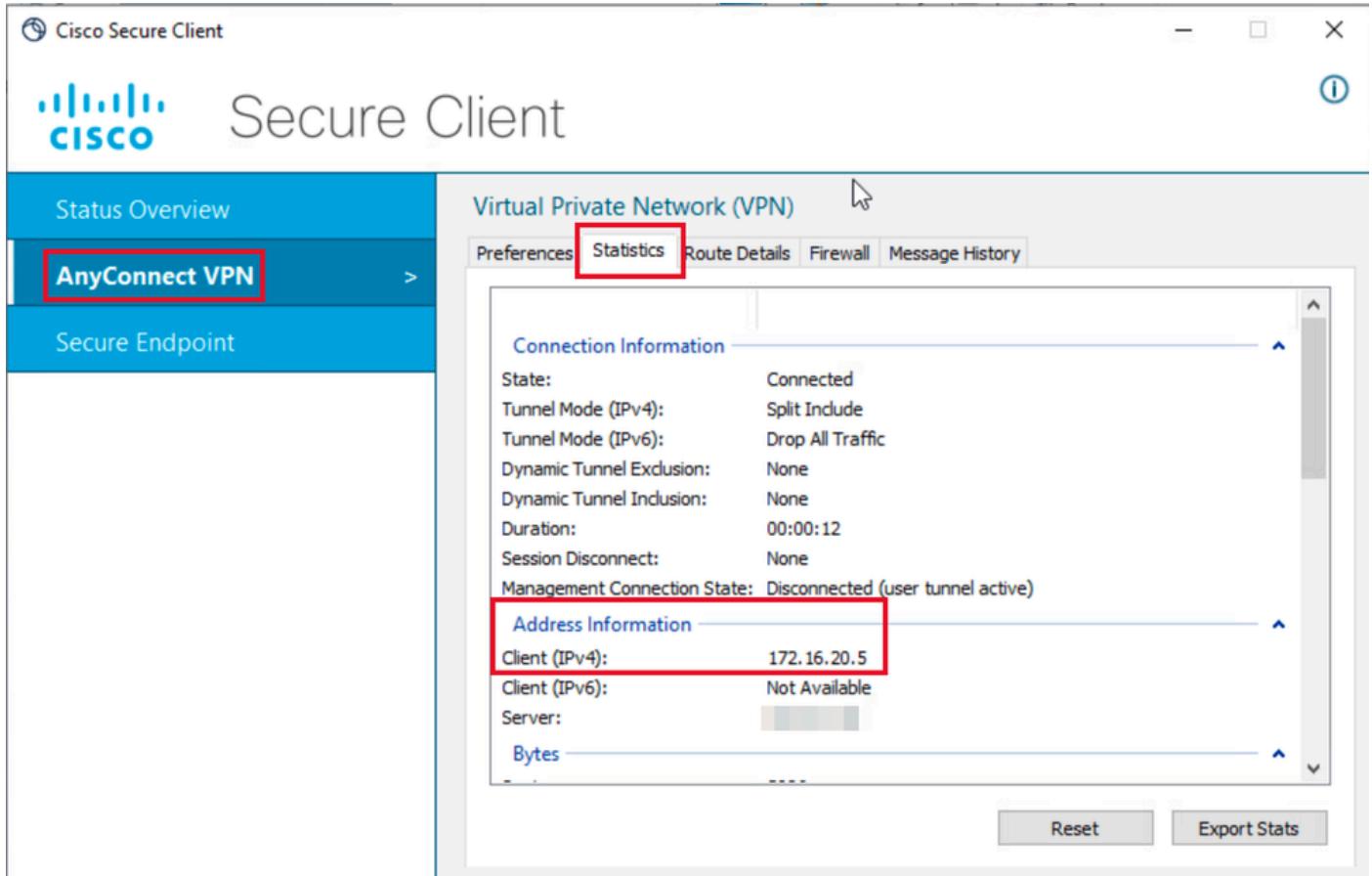
State:	Connected
Tunnel Mode (IPv4):	Split Include
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	None
Dynamic Tunnel Inclusion:	None
Duration:	00:00:12
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)

Address Information

Client (IPv4):	172.16.20.5
Client (IPv6):	Not Available
Server:	[REDACTED]

Bytes

Reset Export Stats



Estatísticas do Usuário2

Cisco Secure Client

Secure Client

Status Overview

AnyConnect VPN >

Secure Endpoint

Virtual Private Network (VPN)

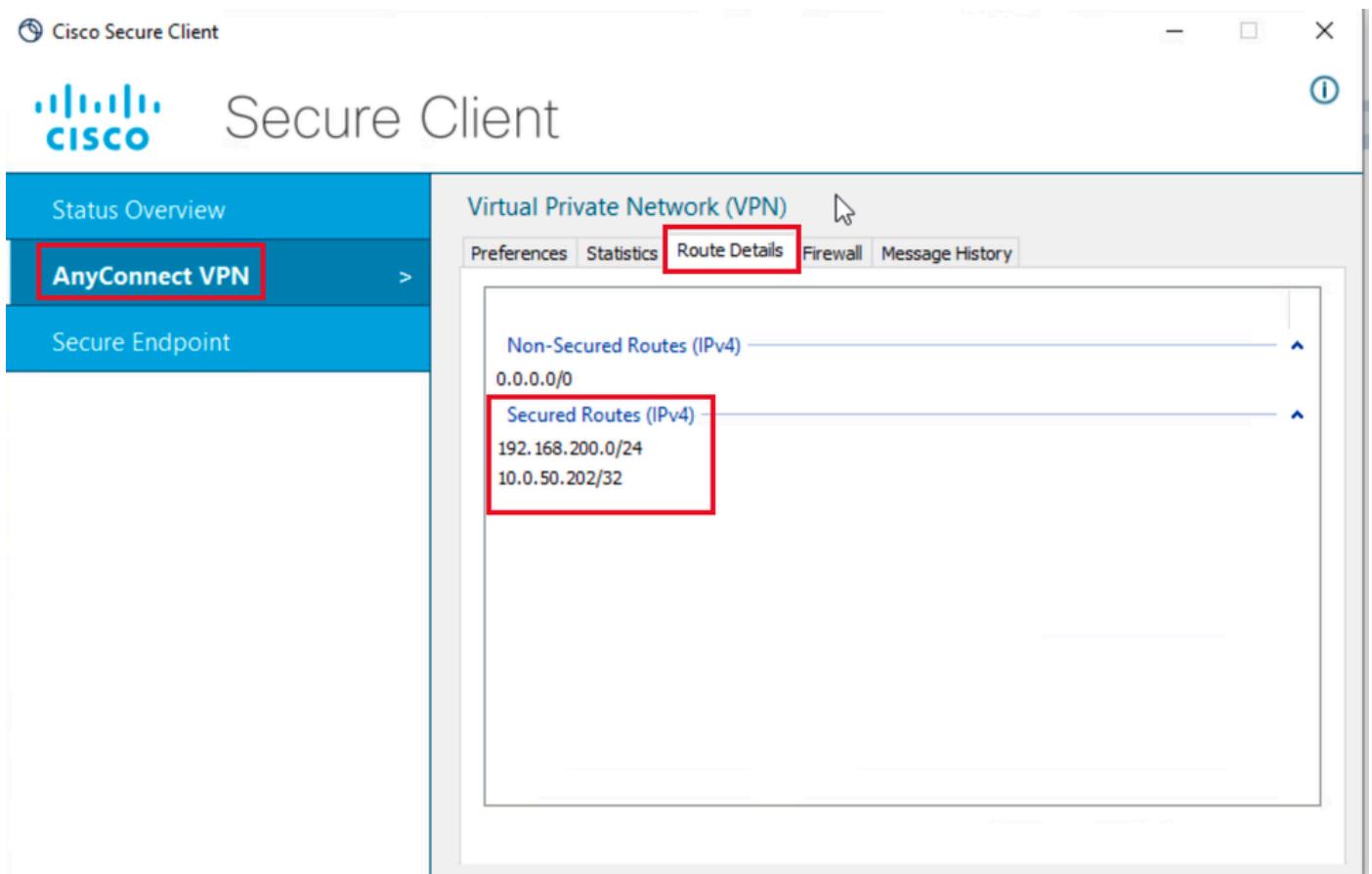
Preferences Statistics Route Details Firewall Message History

Non-Secured Routes (IPv4)

0.0.0.0/0

Secured Routes (IPv4)

192.168.200.0/24
10.0.50.202/32



Detalhes da Rota do Usuário2

Troubleshooting

Depurações e logs

No roteador Cisco:

1. Use as depurações de IKEv2 e IPSec para verificar a negociação entre o headend e o cliente:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 error
debug crypto ikev2 internal
debug crypto ipsec
debug crypto ipsec error
```

2. Use depurações AAA para verificar a atribuição de atributos locais e/ou remotos:

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

No ISE:

- Logs ao vivo RADIUS

Cenário de trabalho

As próximas saídas são exemplos de conexões bem-sucedidas:

- Saída de depuração do usuário1:

```
<#root>
```

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.088: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.088: idb is NULL
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IPv6: ::
```

```
Jan 30 02:57:21.089: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.089: RADIUS(000000FF): sending
Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.089: RADIUS(000000FF):
```

```
Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229
```

```
RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34
Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30
```

```
"isakmp-phase1-id=cisco.example"
```

```
Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z"
Jan 30 02:57:21.089: RADIUS: User-Name [1] 7
```

```
"user1"
```

```
Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1]
Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18
RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II*?0"]
Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.089: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.090: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.094: RADIUS:
```

```
Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137
```

```
RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5
Jan 30 02:57:21.094: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8
RADIUS: 01 52 00 06 0D 20 [ R ]
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@0XH6]
Jan 30 02:57:21.094: RADIUS(000000FF): Received from id 1645/85
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (000000FF):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.097: idb is NULL
```

```

Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::  

Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): acct_session_id: 4245  

Jan 30 02:57:21.097: RADIUS(000000FF): sending  

Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.100  

Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded  

Jan 30 02:57:21.097: RADIUS(000000FF):  

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC  

Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1]  

Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26  

Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login"  

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36  

Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"  

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64  

Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z"  

Jan 30 02:57:21.098: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21  

Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true"  

Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8  

RADIUS: 02 52 00 06 03 04 [ R ]  

Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18  

RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g$D&d ]  

Jan 30 02:57:21.098: RADIUS: State [24] 91  

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  

RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  

RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29; ]  

Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100  

Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet  

Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout  

Jan 30 02:57:21.101: RADIUS:  

Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161

RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1  

Jan 30 02:57:21.101: RADIUS: State [24] 91  

RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]  

RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]  

RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]  

RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]  

RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]  

RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29; ]  

Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32  

RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC OF B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai  

Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18  

RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL! ]  

Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86  

RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes  

Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.103: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.104: idb is NULL
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::

Jan 30 02:57:21.104: RADIUS/ENCODE(000000FF): acct_session_id: 4245
Jan 30 02:57:21.104: RADIUS(000000FF): sending
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.104: RADIUS(000000FF):
```

```
Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332
```

```
RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46
Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30
```

```
"isakmp-phase1-id=cisco.example"
```

```
Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z"
Jan 30 02:57:21.104: RADIUS: User-Name [1] 7
```

```
"user1"
```

```
Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24
RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/]
Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>;Tv]
Jan 30 02:57:21.104: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet
Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout
Jan 30 02:57:21.170: RADIUS:
```

```
Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233
```

```
RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6
Jan 30 02:57:21.170: RADIUS: User-Name [1] 7
```

```
"user1"
```

```
Jan 30 02:57:21.170: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
```

```

RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]
RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams()]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.101"

Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.100.0/24"

Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group1"

Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f
Jan 30 02:57:21.175: AAA/AUTHOR (0x100):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
Jan 30 02:57:21.192: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access1, changed state to up

```

- Saída de depuração do usuário2:

```

<#root>

Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f
Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: :::
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.103: RADIUS(00000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(00000103):

```

```
Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229
```

```
RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64
Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30
```

```
"isakmp-phase1-id=cisco.example"
```

```
Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"
Jan 30 03:28:58.104: RADIUS: User-Name [1] 7
```

```
"user2"
```

```
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]
Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]
Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.109: RADIUS:
```

```
Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137
```

```
RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43
Jan 30 03:28:58.109: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8
RADIUS: 01 35 00 06 0D 20 [ 5 ]
Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18
RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]
Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.113: idb is NULL
Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: :::
Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.113: RADIUS(00000103): sending
Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.113: RADIUS(00000103):
```

```
Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316
```

```
RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C
Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30
```

```
"isakmp-phase1-id=cisco.example"
```

```
Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"
Jan 30 03:28:58.113: RADIUS: User-Name [1] 7
```

```
"user2"
```

```
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8
RADIUS: 02 35 00 06 03 04 [ 5]
Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18
RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]
Jan 30 03:28:58.113: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.116: RADIUS:
```

```
Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161
```

```
RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02
Jan 30 03:28:58.116: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32
RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM]
Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18
RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]
Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):
```

```
Pick method list 'FlexVPN-Authentication-List'
```

```
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0]
```

```
Jan 30 03:28:58.118: idb is NULL
Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: :: 
Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.118: RADIUS(00000103): sending
Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.119: RADIUS(00000103):
```

```
Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332
```

```
RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE
Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30
```

```
"isakmp-phase1-id=cisco.example"
```

```
Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z"
Jan 30 03:28:58.119: RADIUS: User-Name [1] 7
```

```
"user2"
```

```
Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24
RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w]
Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18
RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo]
Jan 30 03:28:58.119: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233
RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD
Jan 30 03:28:58.186: RADIUS: User-Name [1] 7
```

```
"user2"
```

```
Jan 30 03:28:58.186: RADIUS: Class [25] 68
RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011]
RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH]
RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE]
RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 33 30 [ 30]
Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6
RADIUS: 03 36 00 04 [ 6]
Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18
RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S]
Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31
```

```
"ipsec:dns-servers=10.0.50.202"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.200.0/24"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30
Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group2"

Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f
Jan 30 03:28:58.190: AAA/AUTHOR (0x104):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to up
Jan 30 03:28:58.209: %SYS-5-CONFIG_P: Configured programmatically by process Crypto INT from console as
Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access2, changed state to up
```

Informações Relacionadas

- [Supporte técnico e downloads da Cisco](#)

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.