

Configurar a VPN RA com autenticação e autorização LDAP para FTD

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Requisitos de licença](#)

[Etapas de configuração no FMC](#)

[Configuração de servidor REALM / LDAP](#)

[Configuração de VPN RA](#)

[Verificar](#)

Introdução

Este documento descreve como configurar a VPN de acesso remoto com o LDAP AA em um Firepower Threat Defense (FTD) gerenciado por um Firepower Management Center.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico do funcionamento da VPN de acesso remoto (RA VPN).
- Compreenda a navegação pelo Firepower Management Center (FMC).
- Configuração de serviços LDAP no Microsoft Windows Server.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Cisco Firepower Management Center versão 7.3.0
- Cisco Firepower Threat Defense versão 7.3.0
- Microsoft Windows Server 2016, configurado como servidor LDAP

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.

Informações de Apoio

Este documento descreve a configuração da VPN de acesso remoto (RA VPN) com autenticação e autorização do protocolo LDAP em um Firepower Threat Defense (FTD) gerenciado por um Firepower Management Center (FMC).

O LDAP é um protocolo de aplicativo aberto, neutro em relação ao fornecedor e padrão do setor, para acessar e manter serviços de informações de diretório distribuídos.

Um mapa de atributos LDAP equipara atributos que existem no Ative Directory (AD) ou no servidor LDAP com nomes de atributos Cisco. Em seguida, quando o servidor AD ou LDAP retorna respostas de autenticação para o dispositivo FTD durante o estabelecimento de uma conexão VPN de acesso remoto, o dispositivo FTD pode usar as informações para ajustar como o cliente AnyConnect conclui a conexão.

A VPN RA com autenticação LDAP tem suporte no FMC desde a versão 6.2.1 e a autorização LDAP anterior à versão 6.7.0 do FMC foi aconselhada via FlexConfig para configurar o Mapa de Atributos LDAP e associá-lo ao Servidor do Realm. Esse recurso, com a versão 6.7.0, foi integrado ao assistente de configuração de VPN do RA no FMC e não exige mais o uso do FlexConfig.

Nota: Este recurso exige que o FMC esteja na versão 6.7.0; por outro lado, o FTD gerenciado pode estar em qualquer versão superior a 6.3.0.

Requisitos de licença

Exige licença AnyConnect Apex, AnyConnect Plus ou AnyConnect VPN Only com funcionalidade de exportação controlada habilitada.

Para verificar a licença, navegue até **System > Licenses > Smart Licenses**.

The screenshot displays the Cisco Smart License Status and Edit Licenses interface. The top section, titled "Smart License Status", shows the following information:

Usage Authorization:	Authorized (Last Synchronized On May 18 2023)
Product Registration:	Registered (Last Renewed On May 18 2023)
Assigned Virtual Account:	SEC TAC
Export-Controlled Features:	Enabled

The bottom section, titled "Edit Licenses", shows the "Secure Client Advantage" tab selected. It displays two lists of devices:

- Devices without license:** A search bar and a list containing "FTD73".
- Devices with license (1):** A list containing "FTD73".

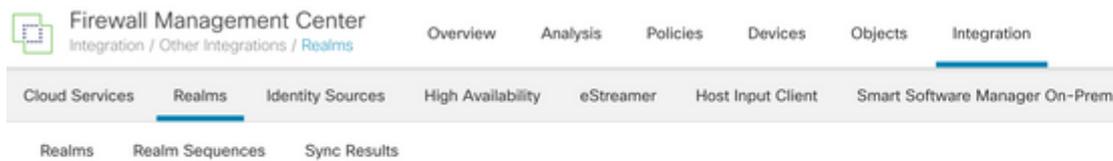
Buttons for "Add", "Cancel", and "Apply" are visible at the bottom of the interface.

Etapas de configuração no FMC

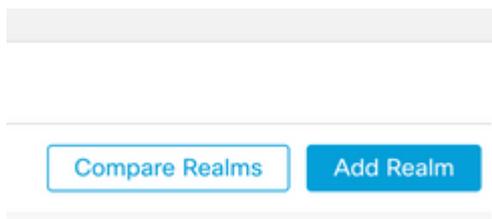
Configuração de servidor REALM / LDAP

Observação: as etapas listadas só serão necessárias se for para a configuração de um novo servidor REALM/LDAP. Se você tiver um servidor pré-configurado, que pode ser usado para autenticação em VPN RA, navegue para [Configuração de VPN RA](#).

Etapa 1. Navegue até System > Other Integrations > Realms, como mostrado nesta imagem.



Etapa 2. Como mostrado na imagem, clique em **Add a new realm**.



Etapa 3. Forneça os detalhes do servidor e do diretório do AD. Clique em OK.

Para efeitos desta demonstração:

Nome: LDAP

Tipo: AD

Domínio primário do AD: test.com

Nome de usuário do diretório: CN=Administrator,CN=Users,DC=test,DC=com

Senha do Diretório: <Hidden>

DN base: DC=teste,DC=com

DN do grupo: DC=teste,DC=com

Add New Realm



Name*	Description
<input type="text"/>	<input type="text"/>
Type	AD Primary Domain
AD	<input type="text"/>
	<small>E.g. domain.com</small>
Directory Username*	Directory Password*
<input type="text"/>	<input type="password"/>
<small>E.g. user@domain.com</small>	
Base DN	Group DN
<input type="text"/>	<input type="text"/>
<small>E.g. ou=group,dc=cisco,dc=com</small>	<small>E.g. ou=group,dc=cisco,dc=com</small>

Directory Server Configuration

^ New Configuration

Hostname/IP Address*	Port*
<input type="text"/>	636
Encryption	CA Certificate*
LDAPS	Select certificate

Interface used to connect to Directory server ⓘ

Resolve via route lookup

Choose an interface

Default: Management/Diagnostic Interface

Test

[Add another directory](#)

Cancel

Configure Groups and Users

Etapa 4. Clique em Save para salvar as alterações de realm/diretório, conforme mostrado nesta imagem.

Cancel Save

Etapa 5. Alterne a State para alterar o Estado do servidor para Ativado, conforme mostrado nesta imagem.

State



Enabled



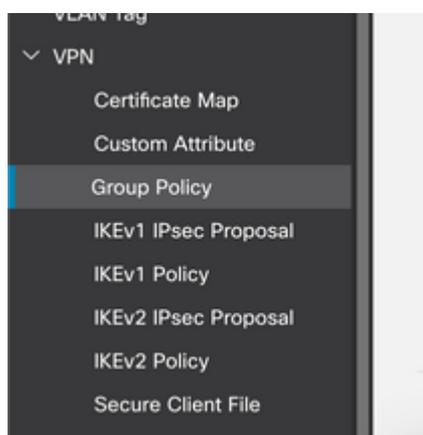
Configuração de VPN RA

Essas etapas são necessárias para configurar a Diretiva de Grupo, que é atribuída aos usuários VPN Autorizados. Se a Diretiva de grupo já estiver definida, vá para a [Etapa 5](#).

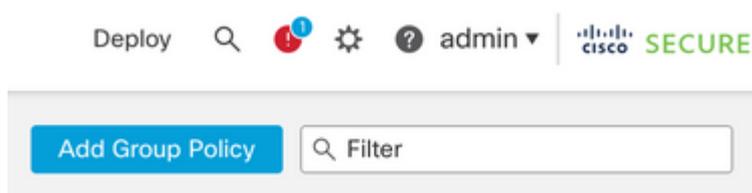
Etapa 1. Navegue até Objects > Object Management.



Etapa 2: no painel esquerdo, navegue até VPN > Group Policy.



Etapa 3: Clique em Add Group Policy.



Etapa 4: forneça os valores da Diretiva de Grupo.

Para efeitos desta demonstração:

Nome: RA-VPN

Banner: ! Bem-vindo à VPN!

Login Simultâneo Por Usuário: 3 (Padrão)

Add Group Policy

Name:*

Description:

General Secure Client Advanced

VPN Protocols
 IP Address Pools
Banner
 DNS/WINS
 Split Tunneling

Banner:
 Maximum total size: 3999, Maximum characters in a line : 497.
 In case of a line spanning more than 497 characters, split the line into multiple lines.
 ** Only plain text is supported (symbols "<" and ">" are not allowed)

Add Group Policy

Name:*

Description:

General Secure Client **Advanced**

Traffic Filter
Session Settings

Access Hours:
 +

Simultaneous Login Per User:
 (Range 0-2147483647)

Etapa 5. Navegue até Devices > VPN > Remote Access.

Devices	Objects	Integration
Device Management	VPN	Troubleshoot
Device Upgrade	Site To Site	File Download
NAT	Remote Access	Threat Defense CLI
QoS	Dynamic Access Policy	Packet Tracer
Platform Settings	Troubleshooting	Packet Capture
FlexConfig		
Certificates		

Etapa 6. Clique em Add a new configuration.

Status	Last Modified
No configuration available Add a new configuration	

Passo 7. Fornecer uma Name para a política de VPN do RA. Escolher VPN Protocols e escolher Targeted Devices. Clique em Next.

Para efeitos desta demonstração:

Nome: RA-VPN

Protocolos VPN: SSL

Dispositivos direcionados: FTD

Remote Access VPN Policy Wizard

1 Policy Assignment 2 Connection Profile 3 Secure Client 4 Access & Certificate 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:*
RA-VPN

Description:

VPN Protocols:

SSL
 IPsec-IKEv2

Targeted Devices:

Available Devices
Q Search
FTD73

Selected Devices
FTD73

Add

Etapa 8. Para a Authentication Method, escolha **AAA Only**. Escolha o servidor **REALM / LDAP** para o Authentication Server. Clique em **Configure LDAP Attribute Map** (para configurar a Autorização LDAP).

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name:* RA-VPN

This name is configured as a connection alias, it can be used to connect to the VPN gateway

Authentication, Authorization & Accounting (AAA):

Specify the method of authentication (AAA, certificates or both), and the AAA servers that will be used for VPN connections.

Authentication Method: AAA Only

Authentication Server:* AD (LOCAL or Realm or RADIUS)
 Fallback to LOCAL Authentication

Authorization Server: Use same authentication server (Realm or RADIUS)

Configure LDAP Attribute Map

Etapa 9. Forneça o LDAP Attribute Name e o Cisco Attribute Name. Clique em **Add Value Map**.

Para efeitos desta demonstração:

Nome do Atributo LDAP: memberOf

Nome do atributo da Cisco: política de grupo

Configure LDAP Attribute Map ?

Realm:
AD (AD) ▼

LDAP attribute Maps: + 🗑️

Name Map:

LDAP Attribute Name: memberOf ▼ Cisco Attribute Name: Group-Policy ▼

Value Maps:

LDAP Attribute Value: Cisco Attribute Value: [Add Value Map](#)

Cancel OK

Etapa 10. Forneça o LDAP Attribute Value e o Cisco Attribute Value. Clique em **OK**.

Para efeitos desta demonstração:

Valor do atributo LDAP: DC=tlalocan,DC=sec

Valor do atributo da Cisco: RA-VPN

LDAP attribute Maps: + 🗑️

Name Map:

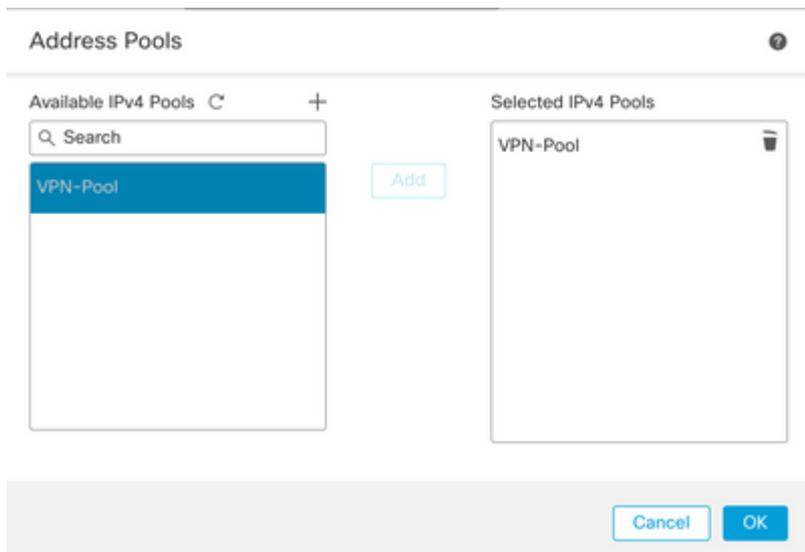
LDAP Attribute Name: memberOf ▼ Cisco Attribute Name: Group-Policy ▼

Value Maps:

LDAP Attribute Value: dc=tlalocan,dc=sec Cisco Attribute Value: RA-VPN ▼ + 🗑️

Observação: você pode adicionar mais Mapas de Valores de acordo com o requisito.

Etapa 11. Adicione o comando Address Pool para a atribuição de endereço local. Clique em **OK**.



Etapa 12. Forneça o **Connection Profile Name** e o Group-Policy. Clique em Next.

Para efeitos desta demonstração:

Nome do perfil de conexão: RA-VPN

Método de autenticação: somente AAA

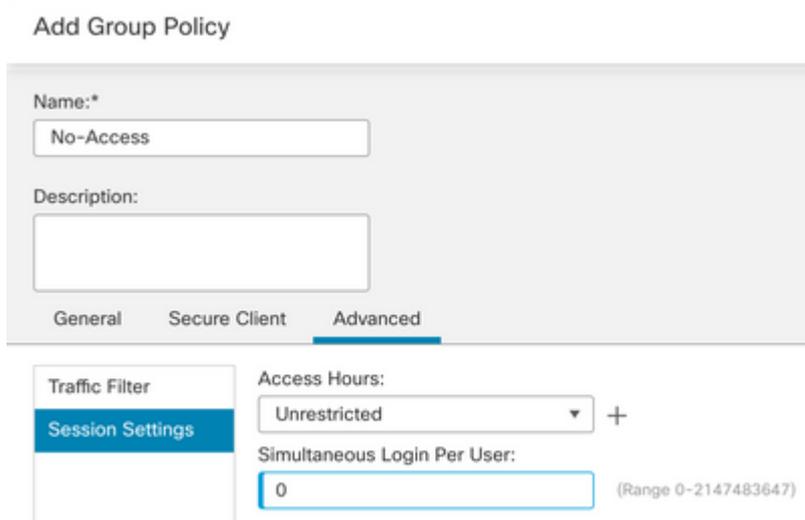
Servidor de autenticação: LDAP

Pool de Endereços IPv4: Pool de VPN

Política de Grupo: Sem Acesso

Observação: o **Método de autenticação**, o **Servidor de autenticação** e o Pool de endereços IPV4 foram configurados nas etapas anteriores.

A política de grupo Sem Acesso tem o Simultaneous Login Per User parâmetro definido como 0 (Para não permitir que os usuários possam fazer logon se receberem a política de grupo Sem acesso padrão).



Etapa 13. Clique em Add new AnyConnect Image para adicionar um AnyConnect Client Image ao DTF.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

- Select at least one Secure Client image

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/> Secure Client File Object Name	Secure Client Package Name	Operating System
No Secure Client Images configured Add new Secure Client Image		

Etapa 14. Fornecer uma Name para a imagem carregada e navegue do armazenamento local para carregá-la. Clique em Save.

Add Secure Client File ?

Name:*

File Name:*

File Type:*

Description:

Etapa 15. Clique na caixa de seleção ao lado da imagem para habilitá-la para uso. Clique em Next.

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

[Show Re-order buttons](#) +

<input checked="" type="checkbox"/> Secure Client File Object Name	Secure Client Package Name	Operating System
<input checked="" type="checkbox"/> Mac	anyconnect-macos-4.10.07061-webdeploy...	Mac OS <input type="text" value="v"/>

Etapa 16. Escolha o Interface group/Security Zone e o Device Certificate. Clique em Next.

Para efeitos desta demonstração:

Grupo de interface/Zona de segurança: Out-Zone

Certificado do dispositivo: autoassinado

Observação: você pode optar por ativar a opção de política Ignorar Controle de Acesso para ignorar qualquer verificação de controle de acesso para tráfego criptografado (VPN) (Desativado por padrão).



Network Interface for Incoming VPN Access

Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:* +

Enable DTLS on member interfaces

▲ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates

Device certificate (also called Identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:* +

Enroll the selected certificate object on the target devices

Access Control for VPN Traffic

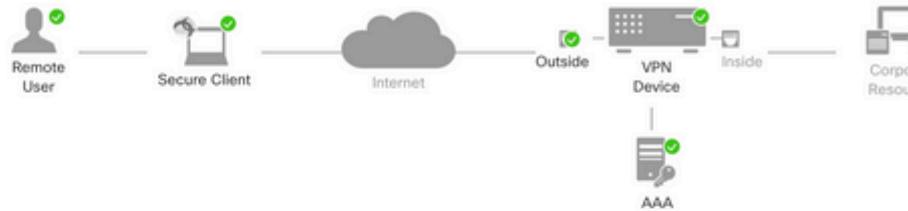
All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)
This option bypasses the Access Control Policy inspection, but VPN filter ACL and authorization ACL downloaded from AAA server are still applied to VPN traffic.

Etapa 17. Exiba o resumo da configuração da VPN do RA. Clique em Finish para salvar, como mostrado na imagem.

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary



Remote Access VPN Policy Configuration

Firewall Management Center will configure an RA VPN Policy with the following settings

Name:	RA-VPN
Device Targets:	FTD73
Connection Profile:	RA-VPN
Connection Alias:	RA-VPN
AAA:	
Authentication Method:	AAA Only
Authentication Server:	AD (AD)
Authorization Server:	-
Accounting Server:	-
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	VPN-Pool
Address Pools (IPv6):	-
Group Policy:	No-Access
Secure Client Images:	Mac
Interface Objects:	InZone

Additional Configuration Required

After the wizard completes, the following configuration needs to be completed on all device targets.

- 1 Access Control Policy Update
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- 1 NAT Exemption
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- 1 DNS Configuration
To resolve hostname specified in the Connection Profile or CA Servers, configure DNS using the DNS Policy on the targeted devices.
- 1 Port Configuration
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and 4500. NAT-Traversal will be enabled on port 443 for image download.

Etapa 18. Navegue até Deploy > Deployment. Escolha o FTD no qual a configuração precisa ser implantada. Clique em Deploy.

A configuração é enviada para a CLI do FTD após a implantação bem-sucedida:

```
<#root>
```

```
!--- LDAP Server Configuration ---!
```

```
ldap attribute-map LDAP
```

```
map-name memberOf Group-Policy  
map-value memberOf DC=tlalocan,DC=sec RA-VPN
```

```
aaa-server LDAP protocol ldap  
max-failed-attempts 4  
realm-id 2  
aaa-server LDAP host 10.106.56.137  
server-port 389  
ldap-base-dn DC=tlalocan,DC=sec  
ldap-group-base-dn DC=tlalocan,DC=sec  
ldap-scope subtree  
ldap-naming-attribute sAMAccountName  
ldap-login-password *****  
ldap-login-dn CN=Administrator,CN=Users,DC=test,DC=com  
server-type microsoft
```

ldap-attribute-map LDAP

!--- RA VPN Configuration ---!

```
webvpn
  enable Outside
  anyconnect image disk0:/csm/anyconnect-win-4.10.07061-webdeploy-k9.pkg 1 regex "Mac"
  anyconnect enable
  tunnel-group-list enable
  error-recovery disable
```

```
ssl trust-point Self-Signed
```

```
group-policy No-Access internal
```

```
group-policy No-Access attributes
```

```
vpn-simultaneous-logins 0
```

```
vpn-idle-timeout 30
```

!--- Output Omitted ---!

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list none
```

```
group-policy RA-VPN internal
```

```
group-policy RA-VPN attributes
```

```
banner value ! Welcome to VPN !
```

```
vpn-simultaneous-logins 3
```

```
vpn-idle-timeout 30
```

!--- Output Omitted ---!

```
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-tunnel-network-list non
```

```
ip local pool VPN-Pool 10.72.1.1-10.72.1.150 mask 255.255.255.0
```

```
tunnel-group RA-VPN type remote-access
```

```
tunnel-group RA-VPN general-attributes
```

```
address-pool VPN-Pool
```

```
authentication-server-group LDAP
```

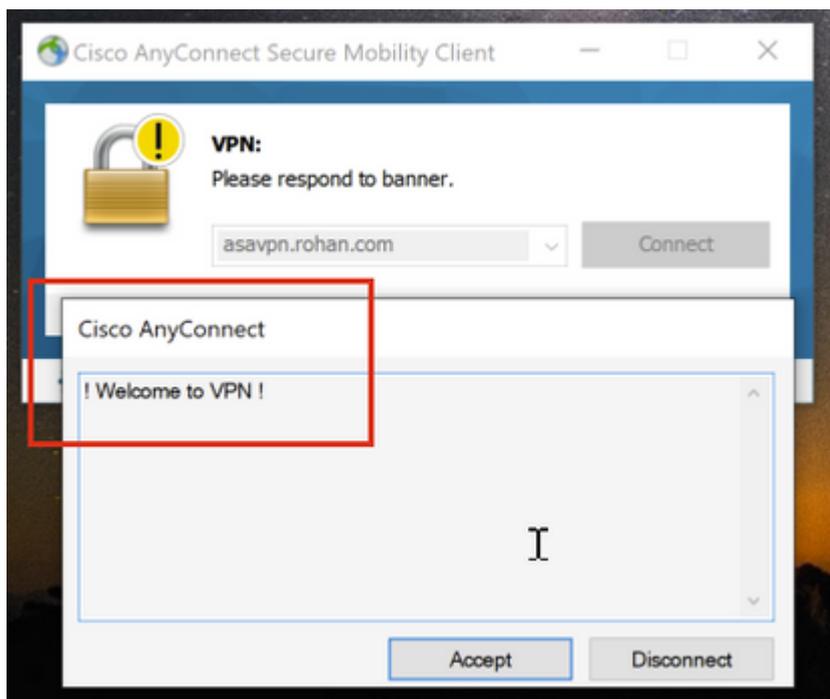
```
default-group-policy No-Access
```

```
tunnel-group RA-VPN webvpn-attributes
```

```
group-alias RA-VPN enable
```

Verificar

No cliente AnyConnect, faça login com Credenciais de grupo de usuários VPN válidas e você obterá a política de grupo correta atribuída pelo Mapa de atributos LDAP:



No trecho de depuração LDAP (debug ldap 255), você pode ver que há uma correspondência no mapa de atributos LDAP:

```
<#root>
```

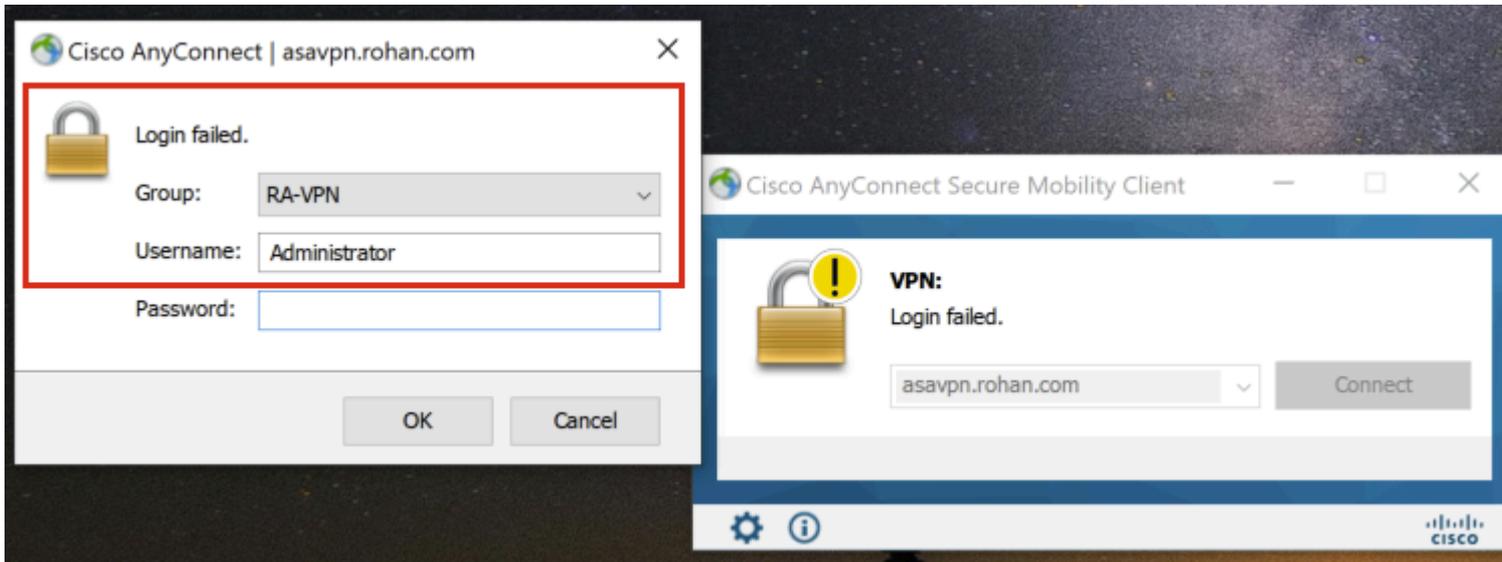
```
Authentication successful for test to 10.106.56.137
```

```
memberOf: value = DC=tlalocan,DC=sec
```

```
mapped to Group-Policy: value = RA-VPN
```

```
mapped to LDAP-Class: value = RA-VPN
```

No cliente AnyConnect, faça login com uma credencial de grupo de usuários de VPN inválida e você obterá a política de grupo Sem acesso.



<#root>

```
%FTD-6-113004: AAA user authentication Successful : server = 10.106.56.137 : user = Administrator
%FTD-6-113009: AAA retrieved default group policy (No-Access) for user = Administrator

%FTD-6-113013: AAA unable to complete the request Error : reason =
Simultaneous logins exceeded for user : user = Administrator
```

A partir do trecho de depuração LDAP (debug ldap 255), você pode ver que não há correspondência no mapa de atributos LDAP:

<#root>

```
Authentication successful for Administrator to 10.106.56.137
```

```
memberOf: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Group Policy Creator Owners,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Domain Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Enterprise Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Schema Admins,CN=Users,DC=tlalocan,DC=sec
memberOf: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=IIS_IUSRS,CN=Builtin,DC=tlalocan,DC=sec
memberOf: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
mapped to Group-Policy: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
mapped to LDAP-Class: value = CN=Administrators,CN=Builtin,DC=tlalocan,DC=sec
```

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.