

Configure a atribuição de endereço IP estático para usuários de VPN de cliente seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento descreve como atribuir endereços IP estáticos a usuários de VPN de acesso remoto usando um mapa de atributos LDAP.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Active Directory (AD)
- LDAP (Lightweight Directory Access Protocol)
- Defesa contra ameaças do Cisco Secure Firewall
- Cisco Secure Firewall Management Center

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Windows Server 2022
- FTD versão 7.4.2
- FMC versão 7.4.2

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

 Observação: a opção de usar um Realm para atribuição de endereço IP e configurar mapas de atributos LDAP é suportada no firepower versão 6.7 ou posterior. Verifique se a versão do firepower é 6.7 ou posterior antes de continuar.

Configurar

Etapa 1. Navegue até Devices > Remote Access e selecione a Remote Access VPN Policy desejada. Selecione o Perfil de Conexão desejado. Na guia AAA, selecione um território para Authentication Server e Authorization Server.

Edit Connection Profile ?

Connection Profile:*

Group Policy:* +
[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method:

Authentication Server:
 Fallback to LOCAL Authentication

Use secondary authentication

Authorization

Authorization Server:

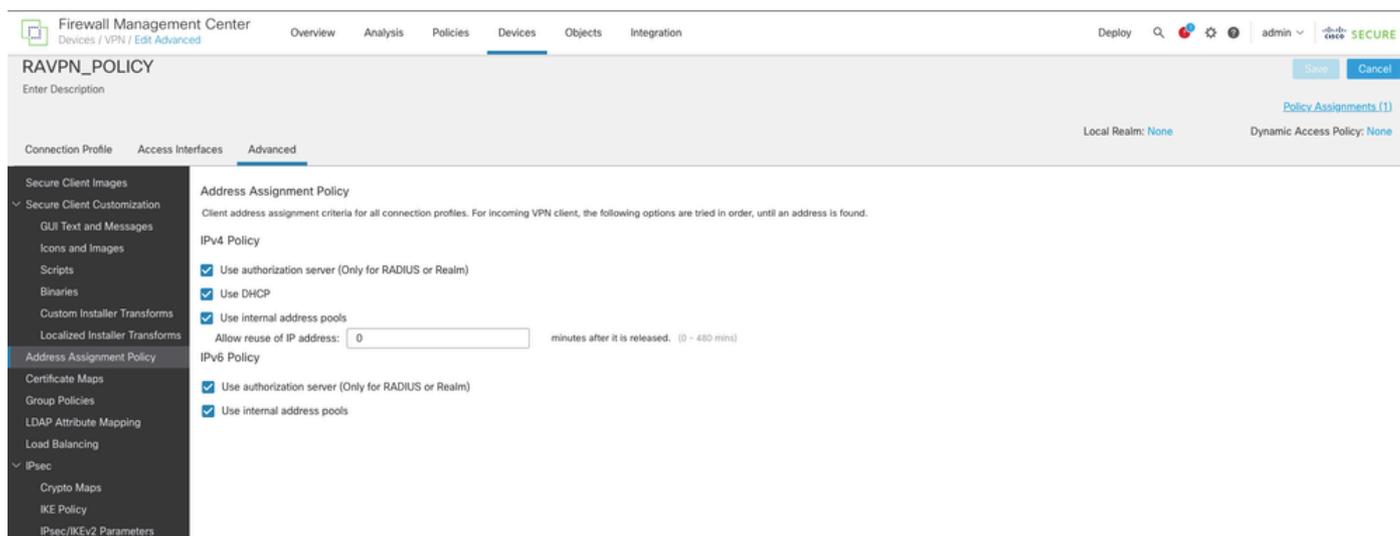
Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting

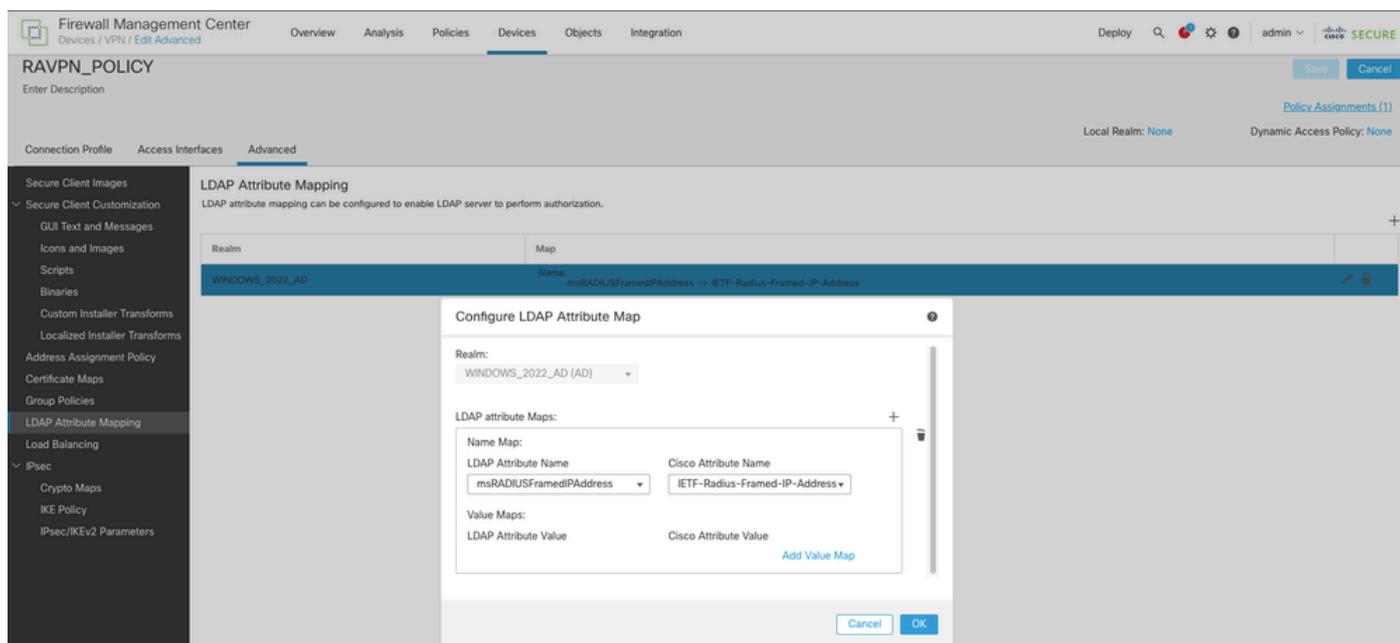
Accounting Server:

▶ Advanced Settings

Etapa 2. Navegue até Devices > Remote Access e selecione a política de VPN de acesso remoto desejada. Navegue até Advanced > Address Assignment Policy e verifique se a opção Use authorization server (Only for RADIUS or Realm) está habilitada.



Etapa 3. Navegue até Avançado > Mapeamento de atributos LDAP e adicione um Mapa de nomes com o Nome do atributo LDAP definido como msRADIUSFramedIPAddress e Nome do atributo Cisco definido como IETF-Radius-Framed-IP-Address.



Etapa 4. No servidor Windows AD, abra o Gerenciador do Servidor e navegue para Ferramentas > Usuários e Computadores do Active Directory. Clique com o botão direito do mouse em um usuário, selecione Properties > Dial-in e marque a caixa chamada Assign Static IP Addresses.

John Doe Properties



Remote control		Remote Desktop Services Profile			COM+
General	Address	Account	Profile	Telephones	Organization
Member Of		Dial-in	Environment		Sessions

Network Access Permission

Allow access

Deny access

Control access through NPS Network Policy

Verify Caller-ID:

Callback Options

No Callback

Set by Caller (Routing and Remote Access Service only)

Always Callback to:

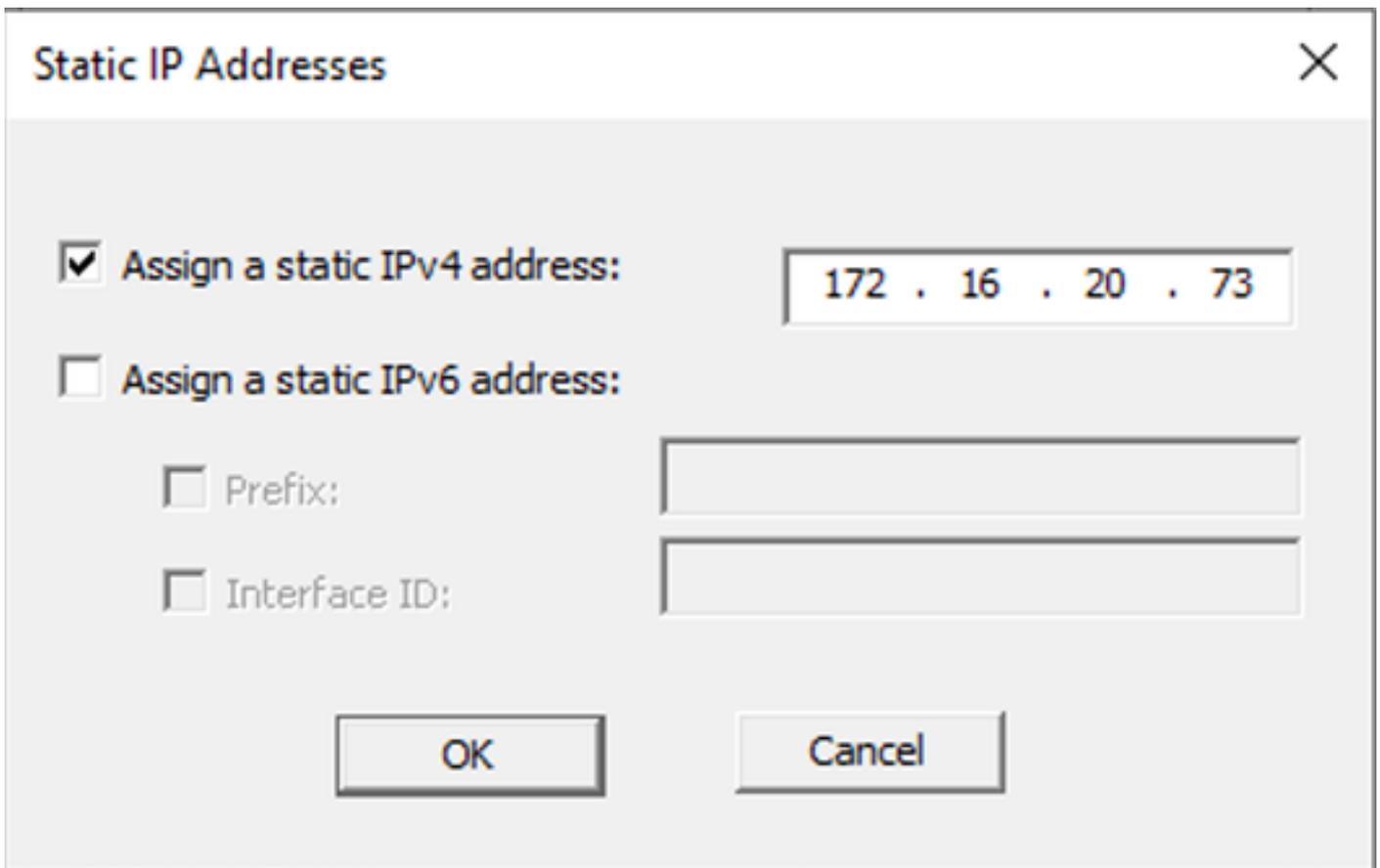
Assign Static IP Addresses

Define IP addresses to enable for this Dial-in connection.

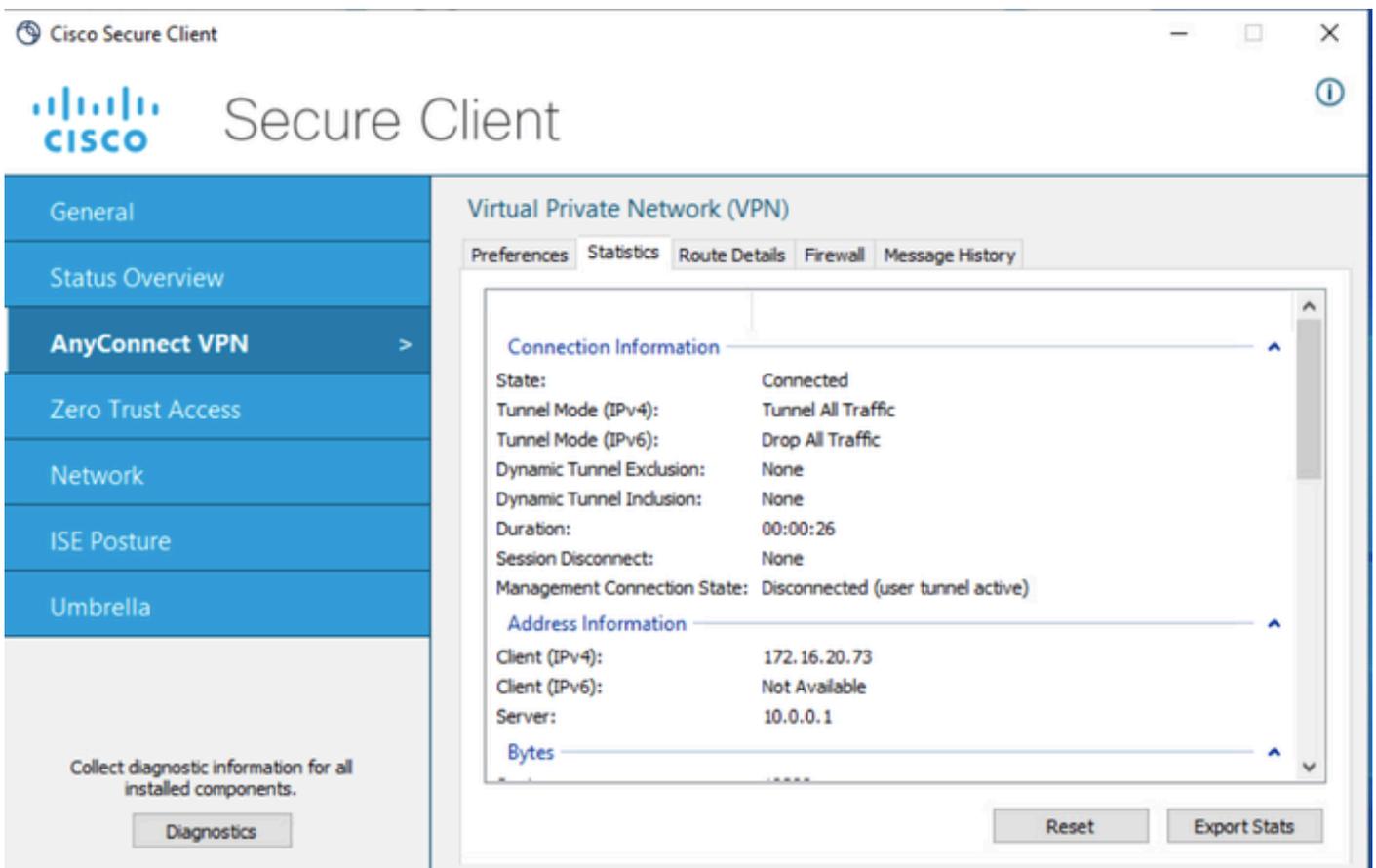
Apply Static Routes

Define routes to enable for this Dial-in connection.

Etapa 5. Selecione Static IP Addresses e atribua um endereço IP estático ao usuário.



Etapa 6. Conecte-se ao gateway VPN e faça login usando o Cisco Secure Client. O endereço IP estático configurado é atribuído ao usuário.



Verificar

Habilite debug ldap 255 e verifique se o atributo LDAP msRADIUSFramedIPAddress foi recuperado:

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe,CN=Users,DC=test,DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

```
[13] sAMAccountType: value = 805306368
[13] userPrincipalName: value = jdoe@test.example
[13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example
[13] msRADIUSFramedIPAddress: value = -1408232375
[13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375
[13] msRASSavedFramedIPAddress: value = -1408232375
[13] dScorePropagationData: value = 16010101000000.0Z
[13] lastLogonTimestamp: value = 133720093118057231
[13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1
[13] Session End
```

Troubleshooting

Comandos debug:

```
debug webvpn 255
```

```
debug ldap
```

Comando para validar o endereço IP estático atribuído ao usuário do RA VPN desejado:

```
show vpn-sessiondb anyconnect filter name <username>
```

```
<#root>
```

```
firepower#
```

```
show vpn-sessiondb anyconnect filter name jdoe
```

Session Type: AnyConnect

```
Username : jdoe Index : 7
Assigned IP : 172.16.20.73 Public IP : 10.0.0.10
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14664 Bytes Rx : 26949
Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE
Login Time : 11:45:48 UTC Sun Sep 29 2024
Duration : 0h:38m:59s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb0071820000700066f93dec
Security Grp : none Tunnel Zone : 0
```

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.