

Configuración de la Asignación de Dirección IP Estática para Usuarios VPN de Secure Client

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo asignar direcciones IP estáticas a usuarios de VPN de acceso remoto mediante un mapa de atributos LDAP.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Active Directory (AD)
- Protocolo ligero de acceso a directorios (LDAP)
- Cisco Secure Firewall Threat Defence
- Cisco Secure Firewall Management Center


Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Windows Server 2022
- FTD versión 7.4.2
- FMC versión 7.4.2

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

 Nota: La opción de utilizar un rango para la asignación de direcciones IP y configurar los mapas de atributos LDAP es compatible con firepower versión 6.7 o posterior. Asegúrese de que la versión de firepower es 6.7 o posterior antes de continuar.

Configurar

Paso 1. Navegue hasta Devices > Remote Access y seleccione la Política VPN de acceso remoto que desee. Seleccione el perfil de conexión que desee. En la pestaña AAA, seleccione un rango para Authentication Server y 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:

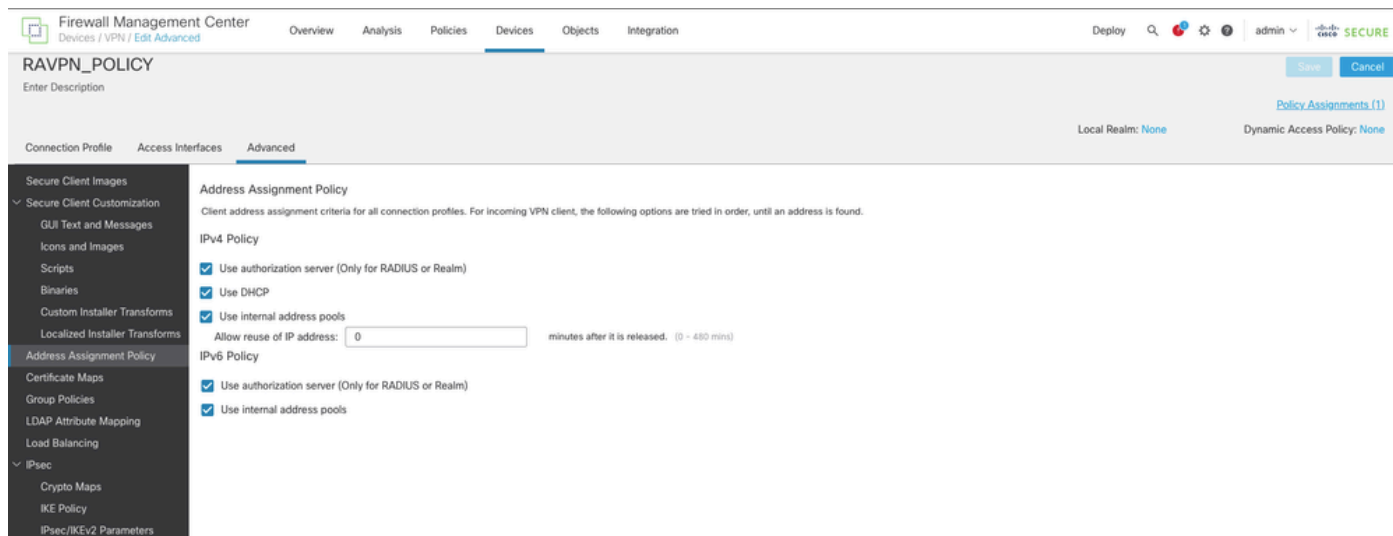
Allow connection only if user exists in authorization database
[Configure LDAP Attribute Map](#)

Accounting

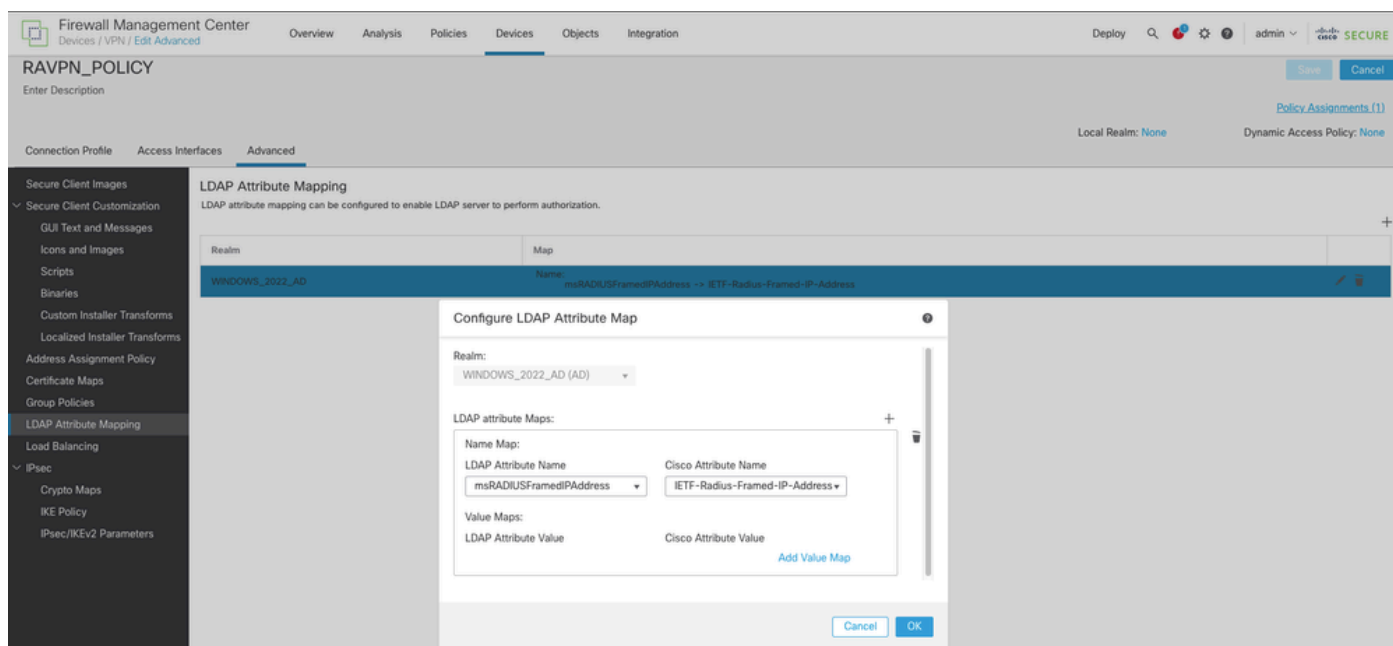
Accounting Server:

▶ Advanced Settings

Paso 2. Navegue hasta Devices > Remote Access y seleccione la política de acceso remoto VPN deseada. Navegue hasta Avanzado > Política de asignación de direcciones y asegúrese de que la opción Usar servidor de autorización (sólo para RADIUS o rango) esté habilitada.



Paso 3. Navegue hasta Avanzado > Asignación de atributos LDAP y agregue un mapa de nombres con el nombre de atributo LDAP establecido en msRADIUSFramedIPAddress y el nombre de atributo Cisco establecido en IETF-Radius-Framed-IP-Address.



Paso 4. En el servidor de Windows AD, abra el Administrador del servidor y vaya a Herramientas > Usuarios y equipos de Active Directory. Haga clic con el botón derecho del ratón en un usuario, seleccione Properties > Dial-in y marque la casilla denominada 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:

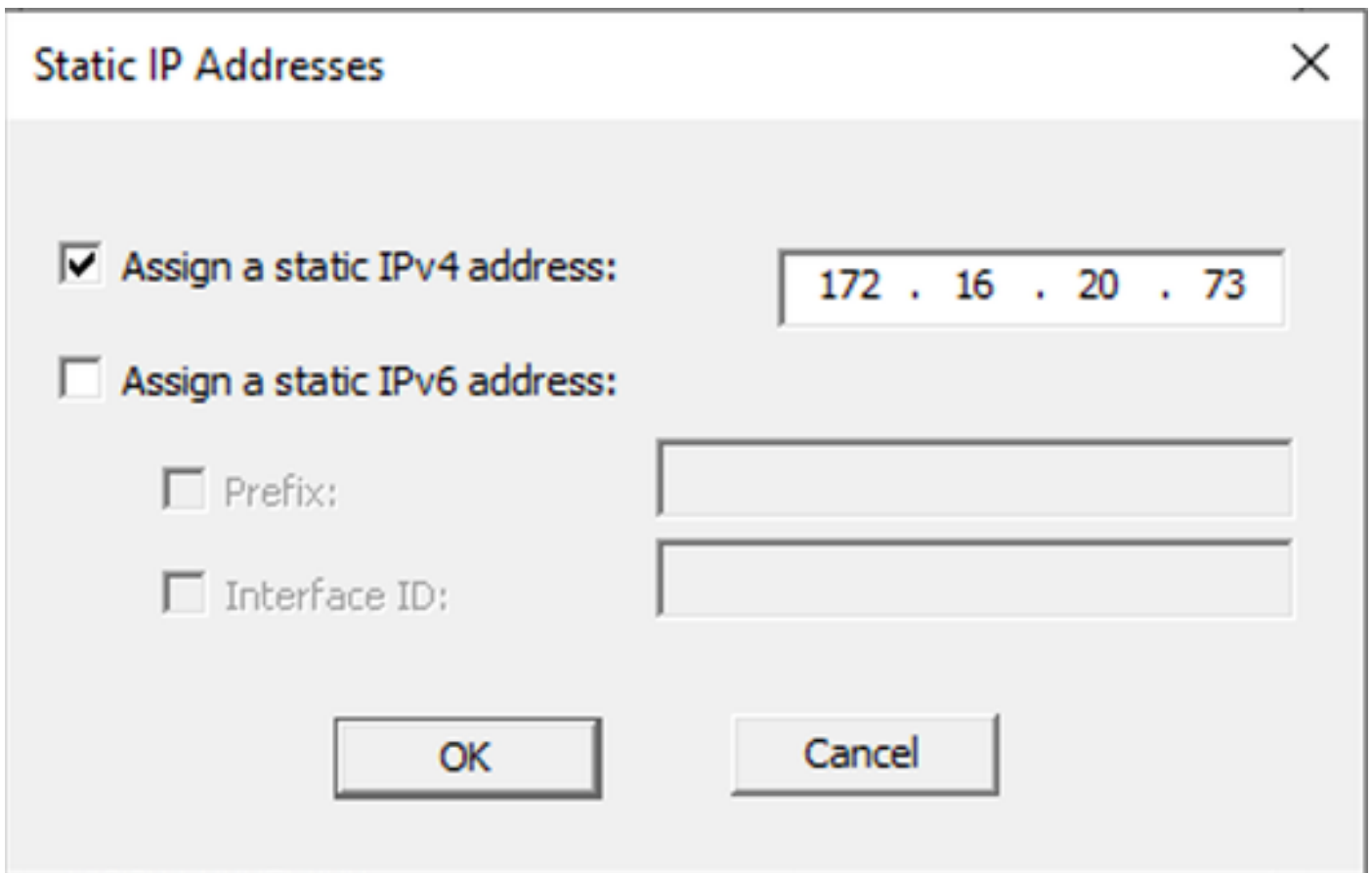
Assign Static IP Addresses

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

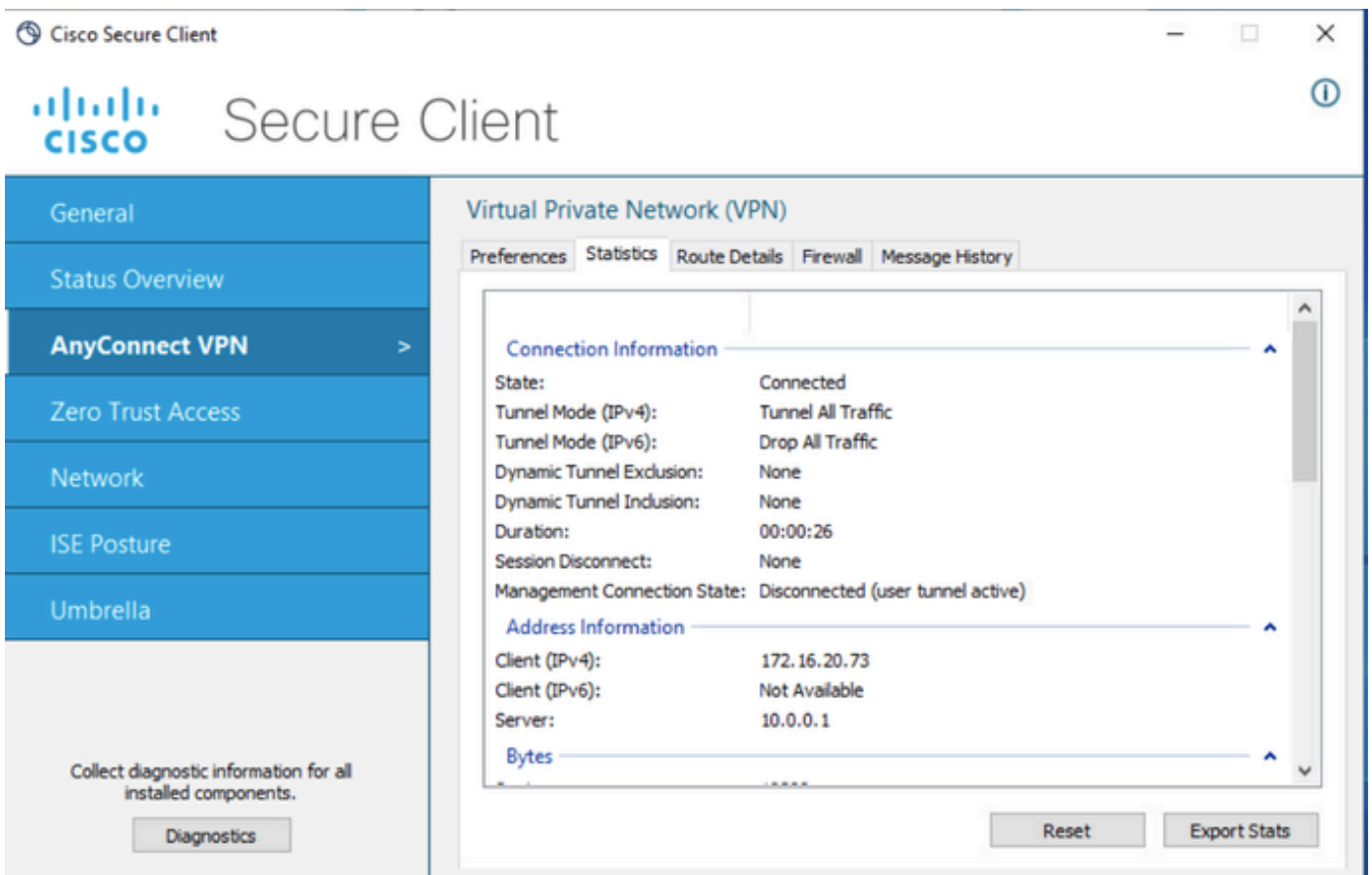
Apply Static Routes

Define routes to enable for this Dial-in connection.

Paso 5. Seleccione Static IP Addresses y asigne una dirección IP estática al usuario.



Paso 6. Conéctese al gateway VPN e inicie sesión con Cisco Secure Client. Se asigna al usuario la dirección IP estática que ha configurado.



Verificación

Habilite debug ldap 255 y asegúrese de que se recupera el atributo msRADIUSFramedIPAddress LDAP:

```
[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
```

Troubleshoot

Comandos debug:

```
debug webvpn 255
```

```
debug ldap
```

Comando para validar la dirección IP estática asignada al usuario VPN de RA deseado:

```
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
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).