Configuración de la asignación de directivas de grupo para SAML mediante Secure Firewall y Microsoft Entry ID

Contenido

Introducción

Este documento describe cómo asignar políticas de grupo usando Microsoft Entra ID para la autenticación SAML de Cisco Secure Client en Cisco Secure Firewall.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- VPN AnyConnect de Cisco Secure Client
- Configuración de objetos de servidor de acceso remoto VPN y registro único (SSO) Cisco Firepower Threat Defense (FTD) o Cisco Secure Firewall ASA
- Configuración del proveedor de identidad (IdP) de Microsoft Entra ID

Componentes Utilizados

La información de esta guía se basa en las siguientes versiones de hardware y software:

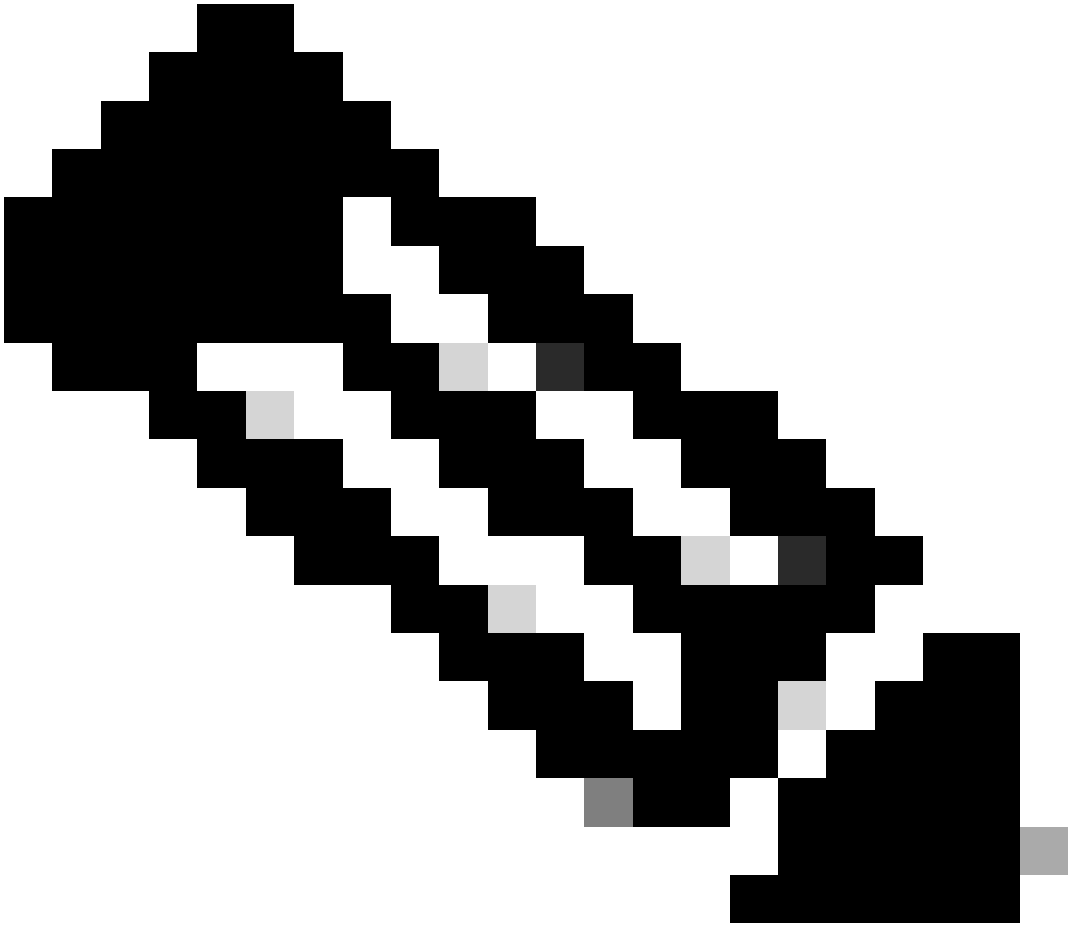
- FTD versión 7.6
- FMC versión 7.6
- ID de entrada de MS ID de SAML

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

SAML (lenguaje de marcado de aserción de seguridad) es un marco basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad. Crea un círculo de confianza entre el usuario, un proveedor de servicios (SP) y un proveedor de identidad (IdP) que permite al usuario iniciar sesión una sola vez para varios servicios. SAML se puede utilizar para la autenticación VPN de acceso remoto para conexiones de Cisco Secure Client a cabeceras ASA y FTD VPN, donde ASA o FTD es la parte SP del círculo de confianza.

En este documento, se utiliza Microsoft Entra ID/Azure como IdP. Sin embargo, también es posible asignar políticas de grupo mediante otros IdPs, ya que se basa en atributos estándar que se pueden enviar en la afirmación SAML.

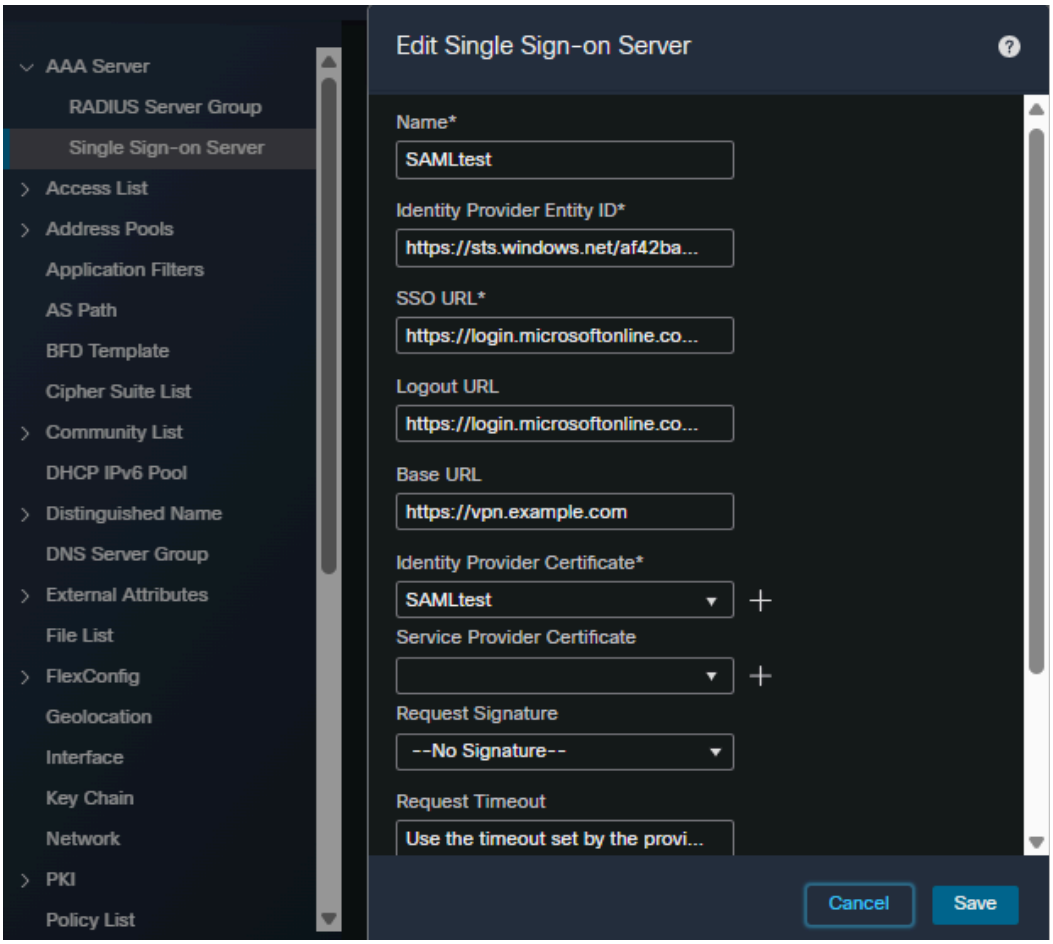


Nota: Tenga en cuenta que cada usuario solo debe pertenecer a un grupo de usuarios en MS Entra ID, ya que los múltiples atributos SAML que se envían al ASA o FTD pueden causar problemas con la asignación de políticas de grupo como se detalla en Cisco bug ID CSCwm33613

Configurar

Configuración SAML de FMC

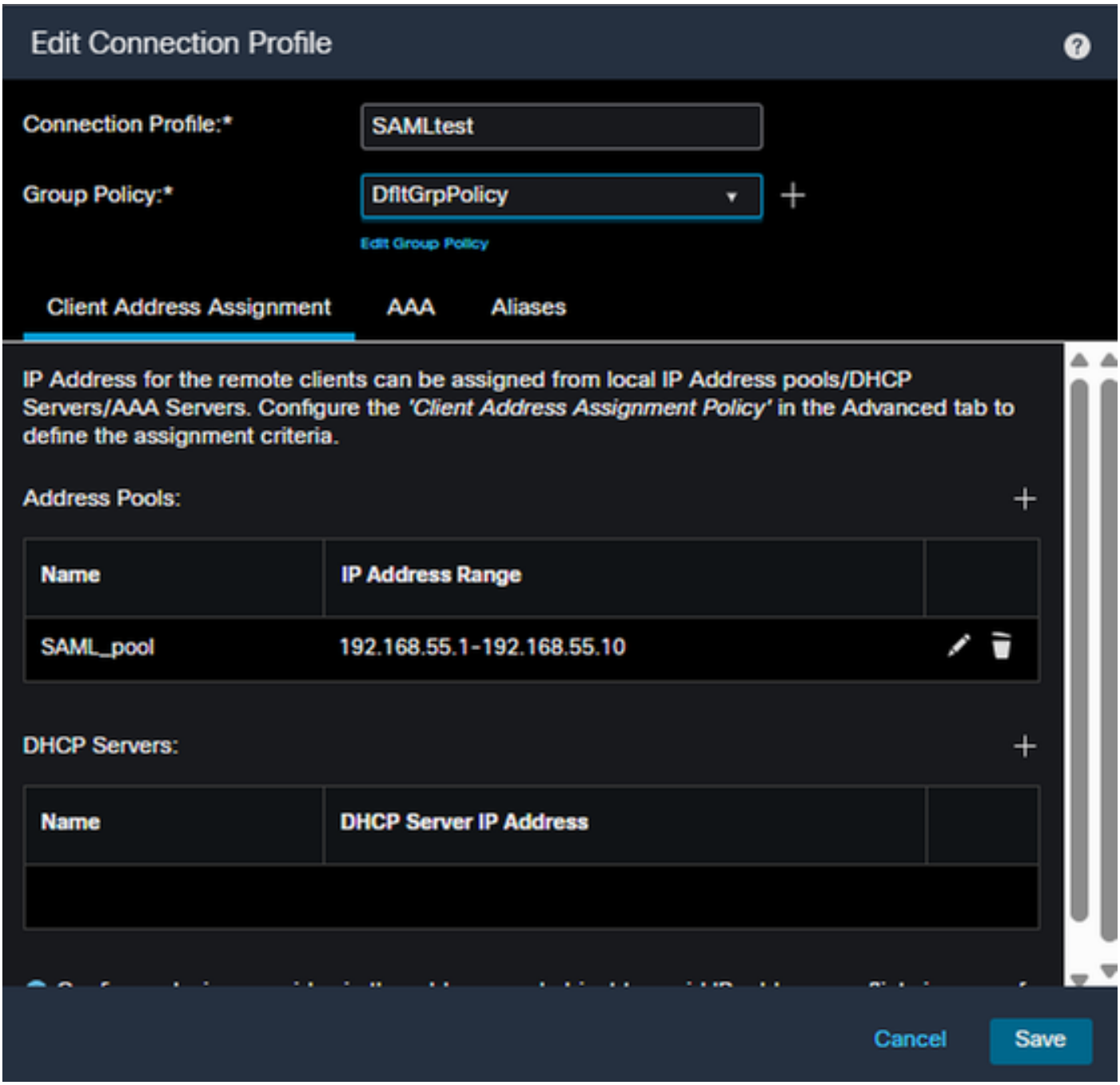
En el FMC, navegue hasta Objetos > Gestión de Objetos > Servidor AAA > Servidor de Single Sign-on. El ID de entidad, la URL SSO, la URL de cierre de sesión y el certificado del proveedor de identidad se obtienen del IdP, consulte el Paso 6 en la sección Microsoft Entra ID. La URL base y el certificado del proveedor de servicios son específicos del FTD al que se agrega la configuración.



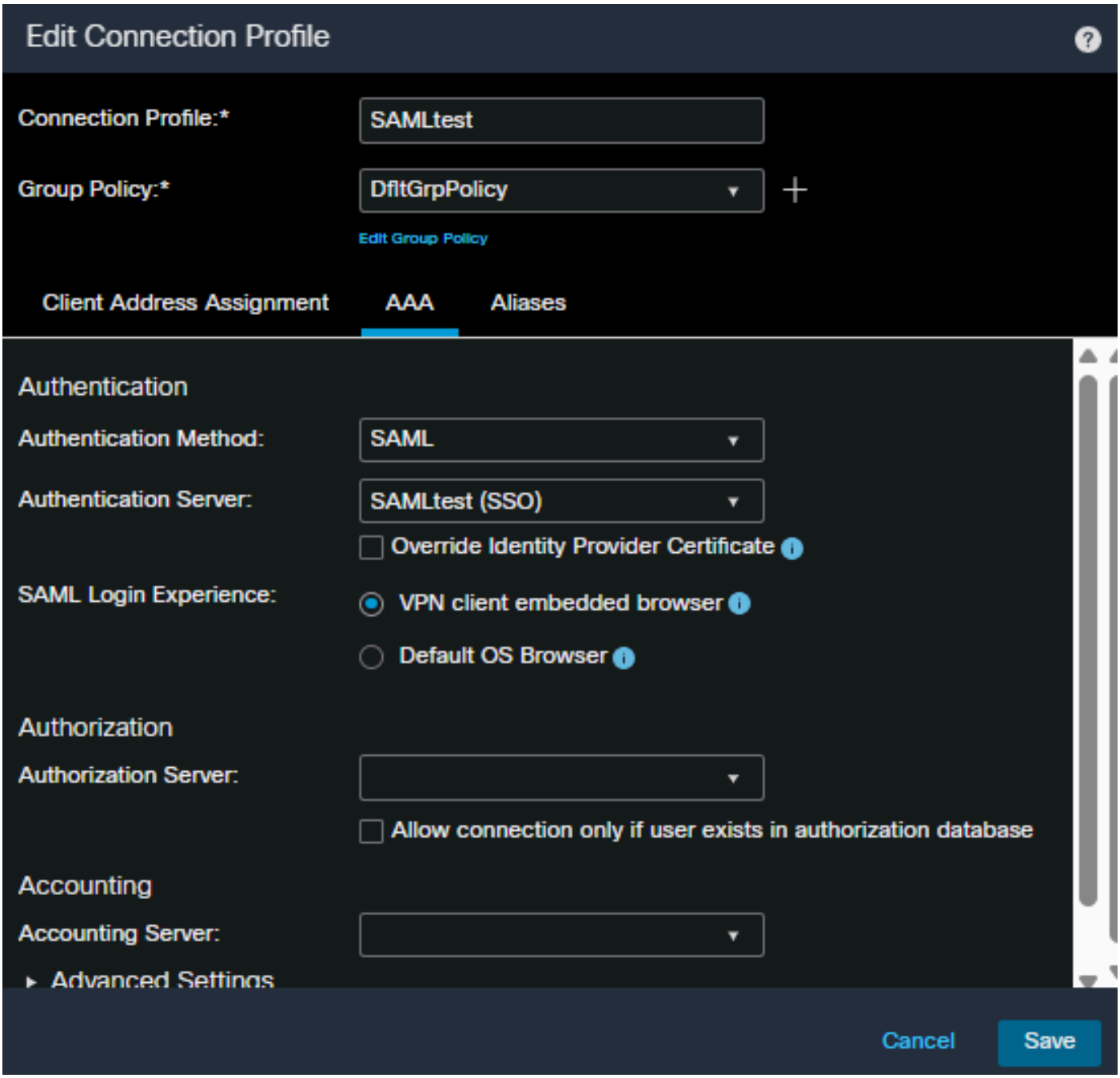
Configuración de objetos SSO de FMC

Configuración del Grupo de Túneles RAVPN FMC

En el FMC, navegue hasta Devices > VPN > Remote Access > Connection Profile y seleccione, o cree, la política VPN para el FTD que está configurando. Una vez seleccionado, cree un perfil de conexión similar al siguiente:



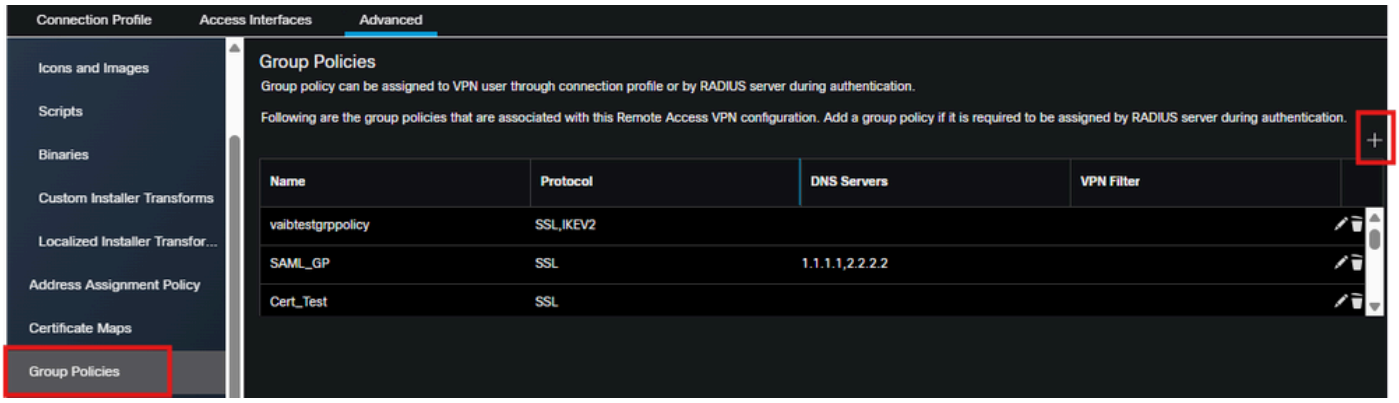
Asignación de dirección de perfil de conexión FMC



Configuración AAA del perfil de conexión FMC

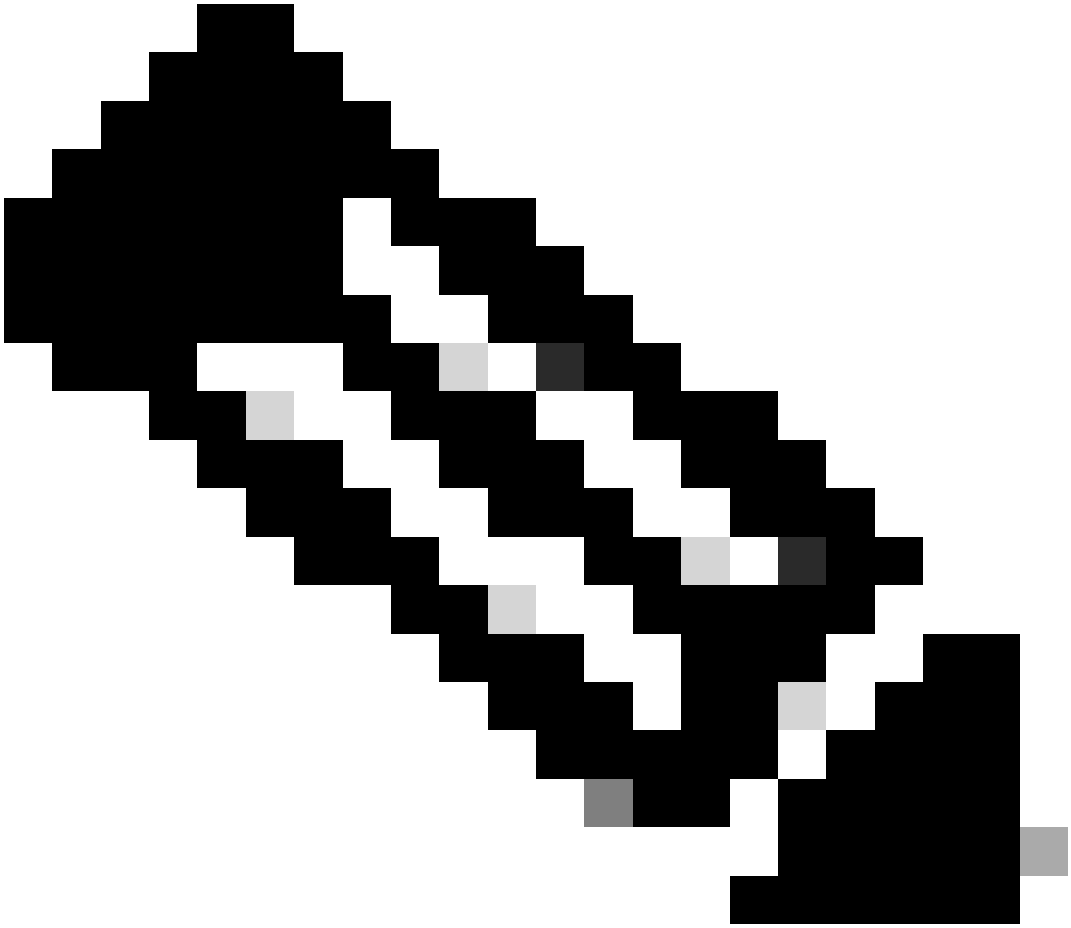
Configuración de la Política de Grupo FMC RAVPN

1. Debe crear una política de grupo con las opciones necesarias para cada grupo de usuarios en el ID de entrada y agregarla a la política RAVPN para el FTD que se está configurando. Esto se logra navegando hasta Devices > VPN > Remote Access > Advanced y seleccionando Group Policies desde el lado izquierdo, luego haciendo clic en + en la parte superior derecha para agregar una política de grupo.

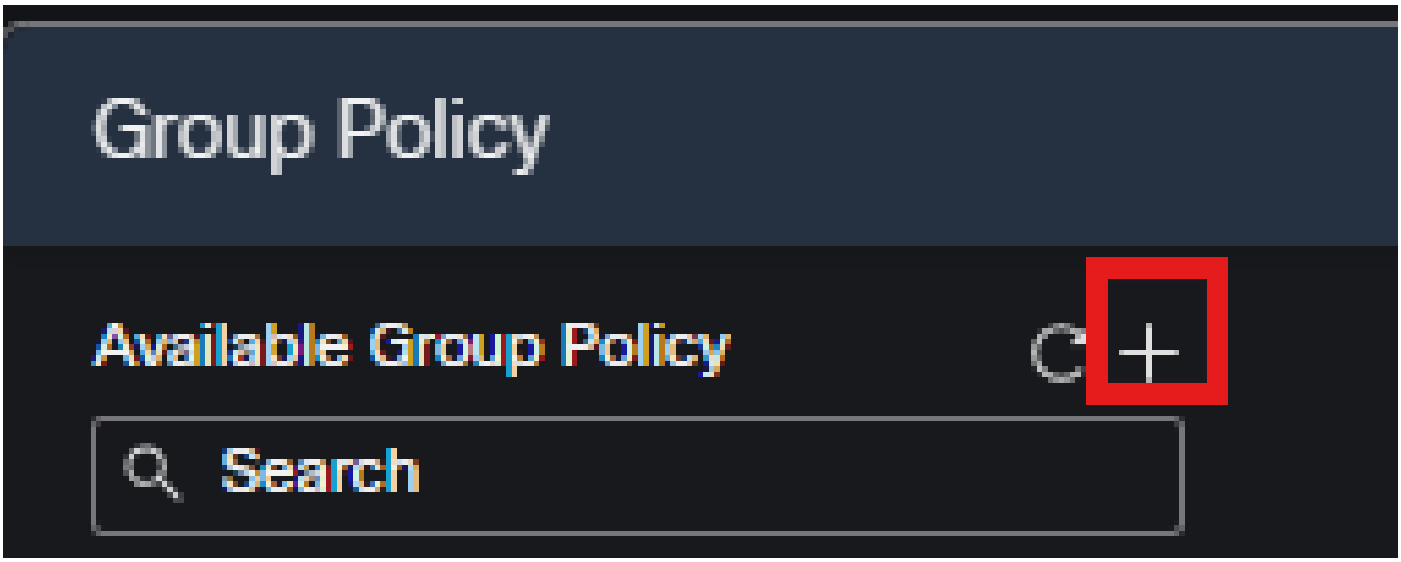


Política de agregar grupo de FMC

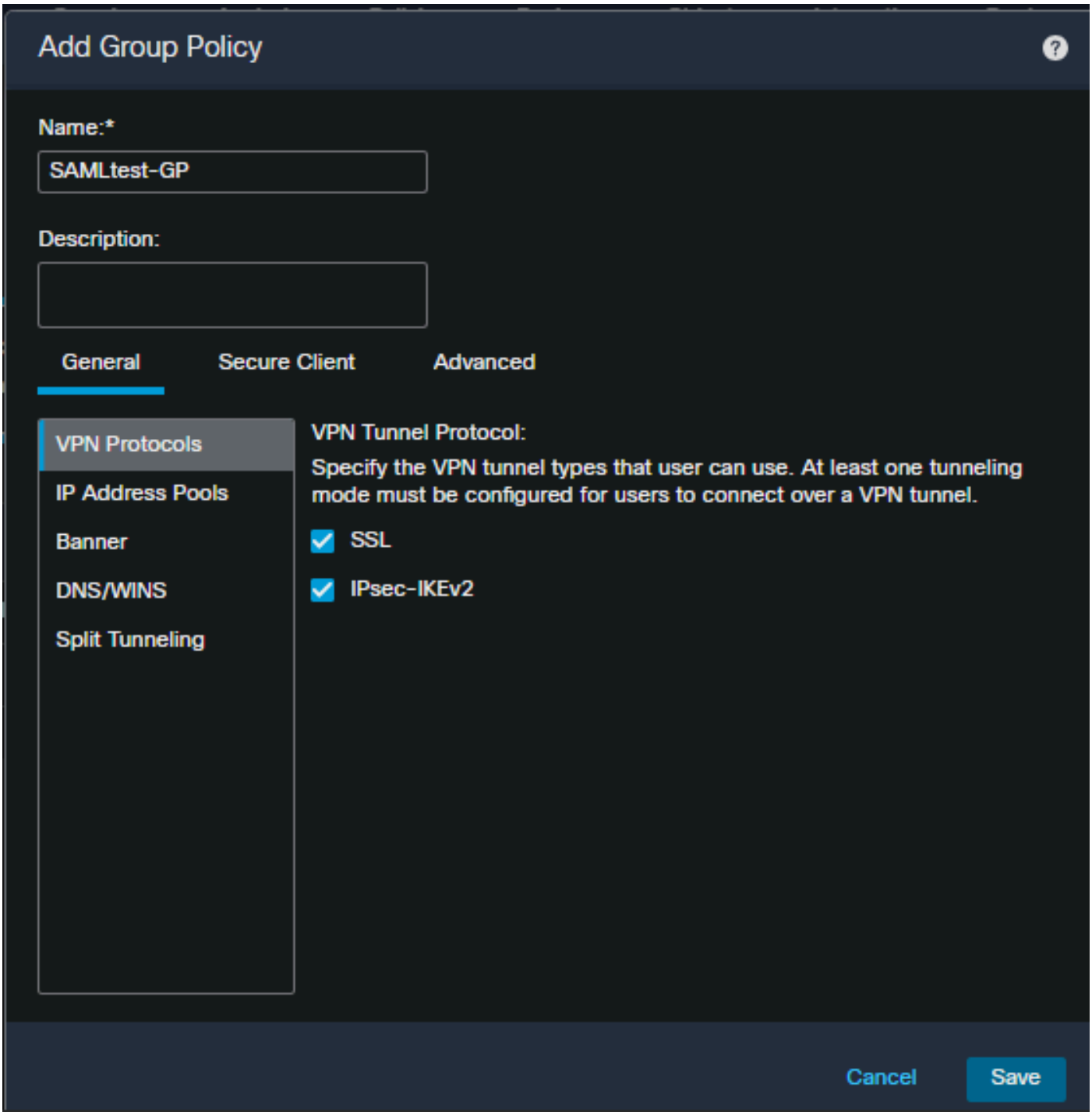
2. Haga clic en + en la ventana emergente para que aparezca el cuadro de diálogo para crear una nueva directiva de grupo. Rellene las opciones necesarias y guárdelas.



Nota: Si ya ha creado la directiva de grupo necesaria, puede omitir este paso y continuar con el paso 3

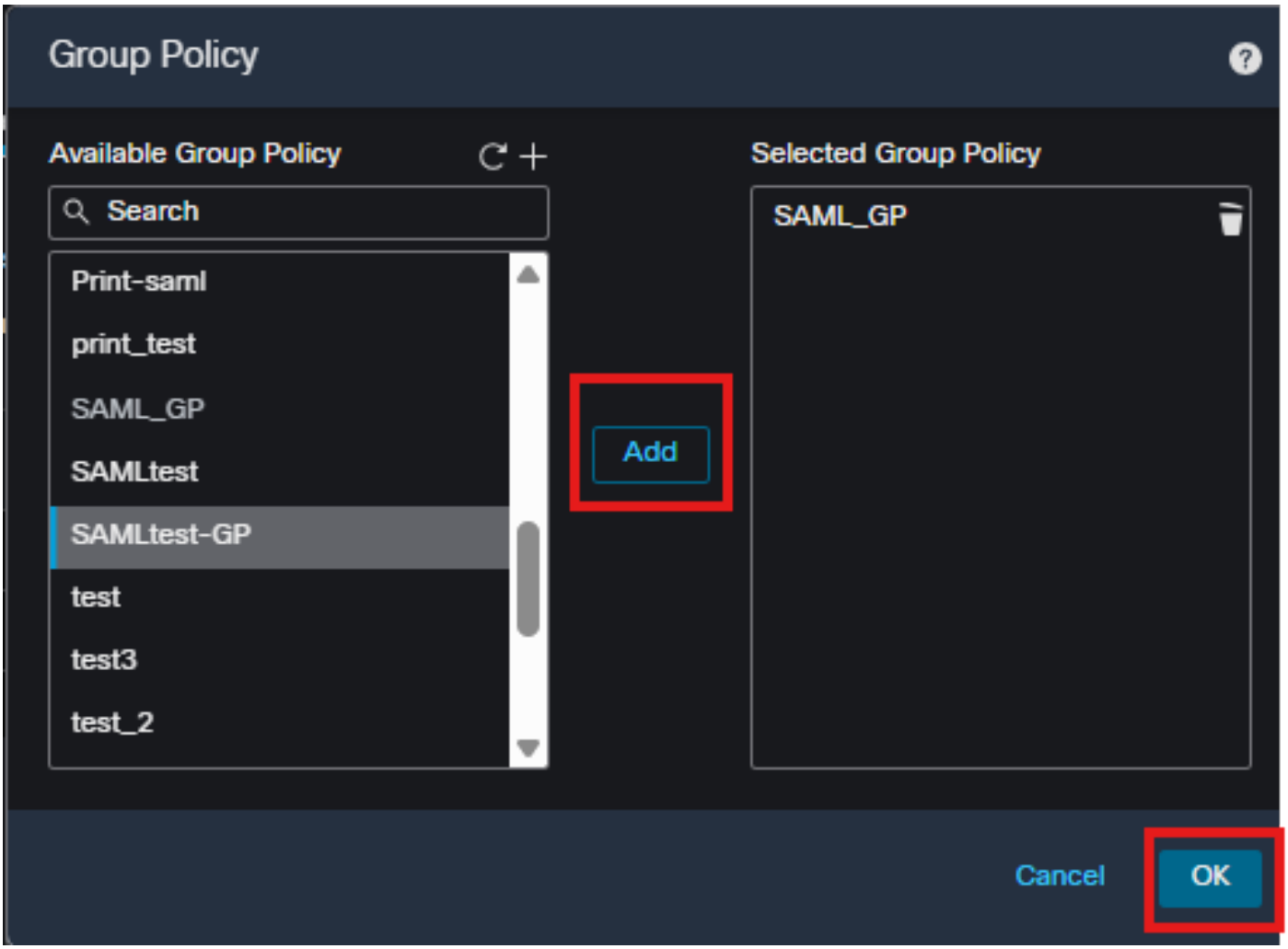


Crear nueva directiva de grupo



Opciones de Directiva de grupo

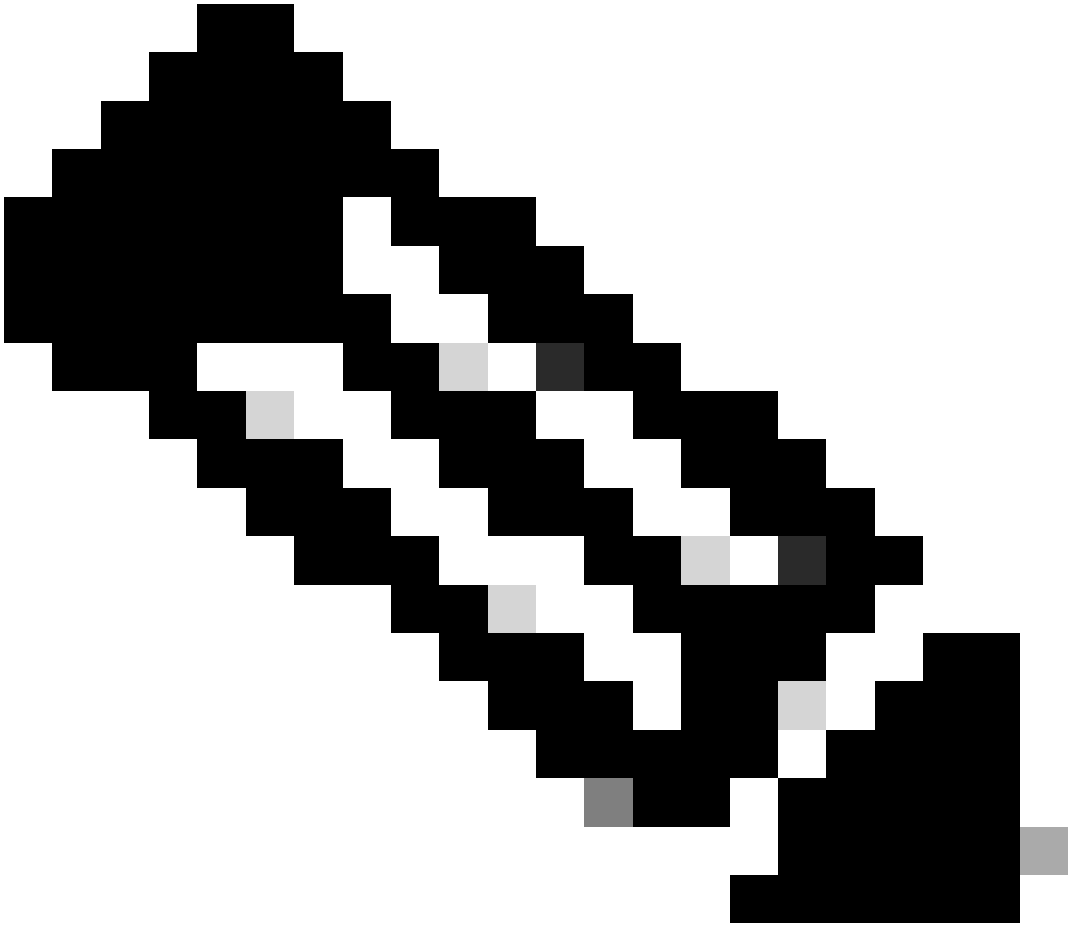
3. Seleccione la política de grupo recién creada en la lista de la izquierda y haga clic en el botón Agregar, luego haga clic en Aceptar para guardar la lista.



agregar directiva de grupo

Metadatos de FTD

Una vez que la configuración se haya implementado en el FTD, navegue hasta la CLI del FTD y ejecute el comando "show saml metadata <tunnel group name>" y recopile el ID de entidad del FTD y la URL del ACS.



Nota: El certificado de los metadatos se truncó por motivos de brevedad.

<#root>

```
FTD# show saml metadata SAMLtest
SP Metadata
-----------
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="
```

https://vpn.example.net/saml/sp/metadata/SAMLtest

```
" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="ur
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
MIIFWzCCBEOgAwIBAgITRwAAAAgZ9Nmfv5mpJQAAAAAACDANBgkqhkiG9w0BAQsF
ADBJMRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGcnRwdnBu
MRowGAYDVQQDExFydHB2cG4tV0lOQVVUSC1DQTAeFw0yNTAzMjUxNzU5NDZaFw0y
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTBlJUUFZQTjEdMBsGA1UEAxMUcnRwdnBu
```

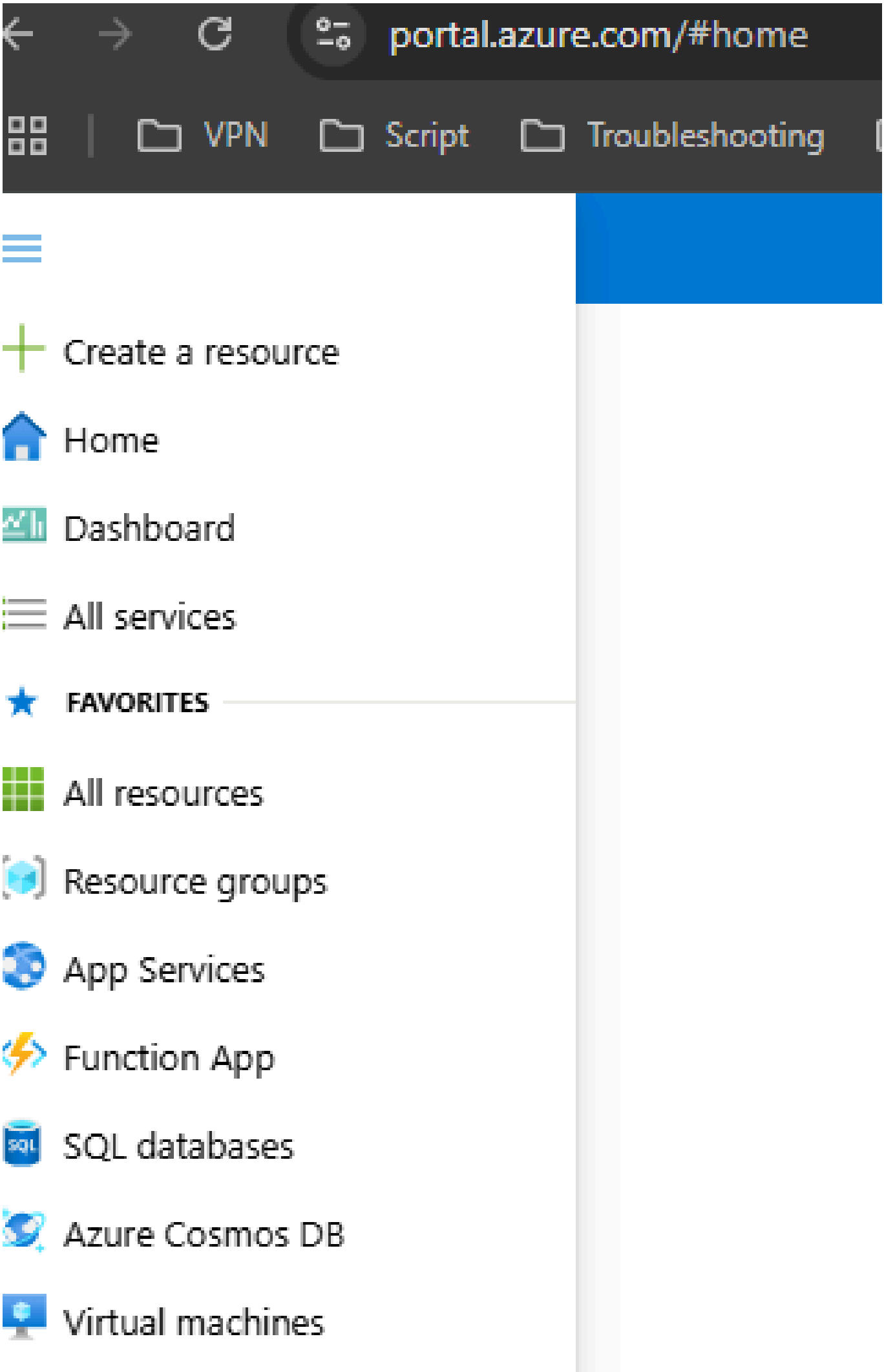
```
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP
```

https://vpn.example.net/+CSCOE+/saml/sp/acs?tgname=SAMLtest

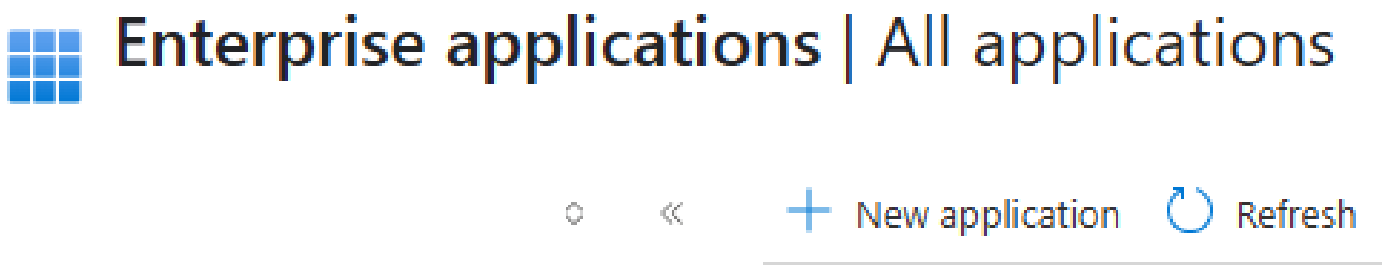
```
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

ID de Microsoft Entra

1. En el portal de Microsoft Azure, seleccione Microsoft Entra ID en el menú de la izquierda.

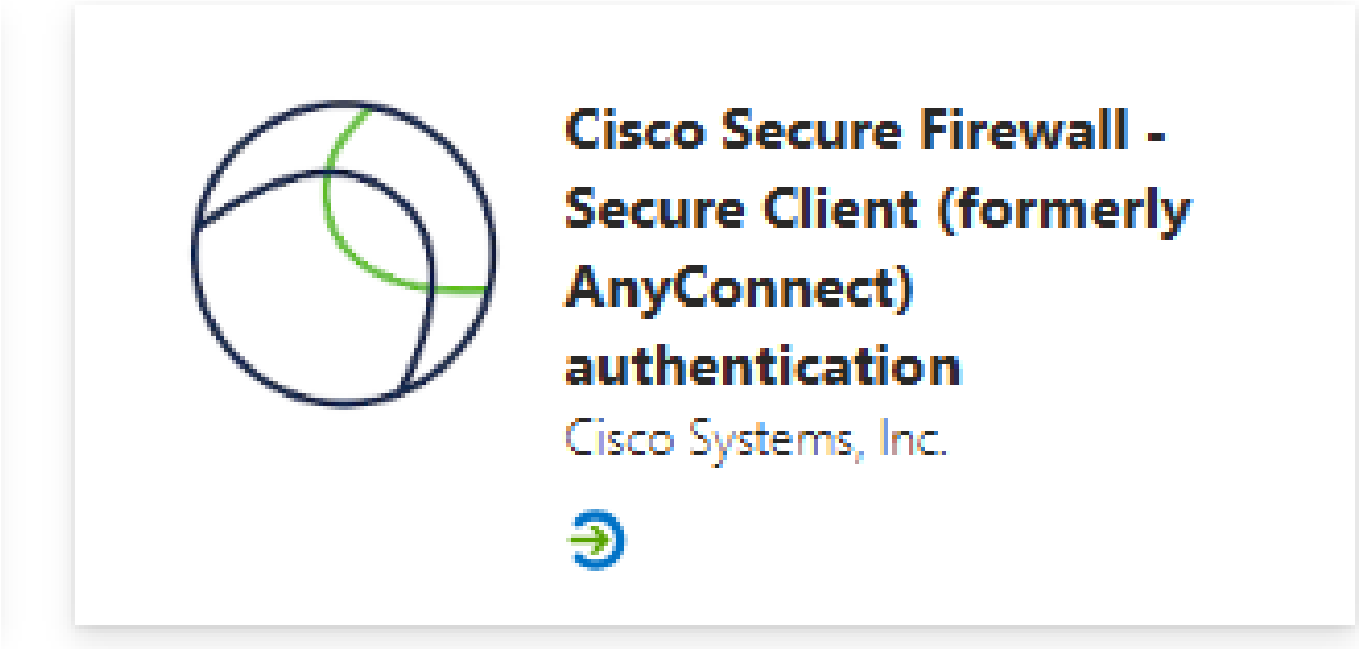

portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

Si ya existe una aplicación empresarial configurada para la configuración de RAVPN de FTD, omita los siguientes pasos y continúe en el paso 7.



Aplicación MS Entra ID Enterprise

4. Seleccione Cisco Secure Firewall - Secure Client (anteriormente AnyConnect) authentication en Featured Applications. Asigne un nombre a la aplicación y seleccione Create.



Aplicación de autenticación MS Entra ID Cisco Secure Firewall Secure Client (anteriormente AnyConnect)

5. Una vez en la aplicación, seleccione Usuarios y grupos y asigne los nombres de usuario o grupo necesarios a la aplicación.

Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators

y recupere la URL de inicio de sesión, el Identificador de entrada de Microsoft y la URL de cierre de sesión para la sección Configuración SAML de FMC de esta guía.

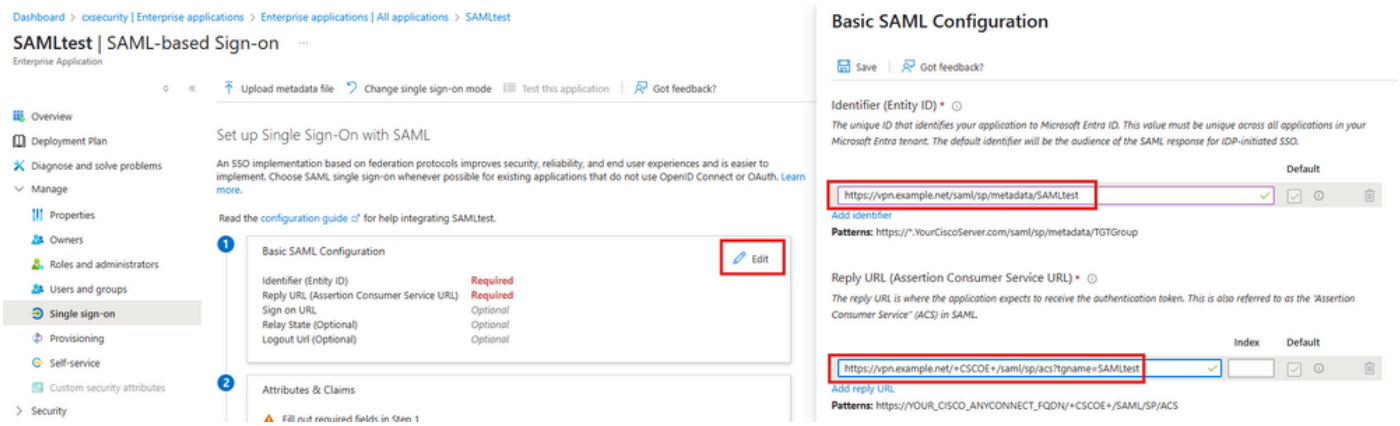
Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

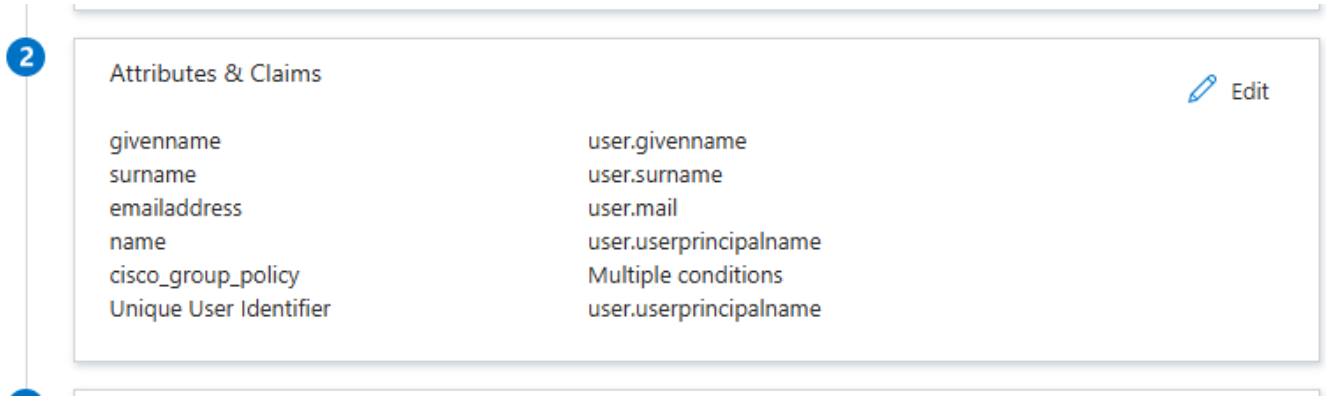
- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators

con el identificador (ID de entidad) y la URL de respuesta (ACS) recuperados de los metadatos de FTD y guárdelos.



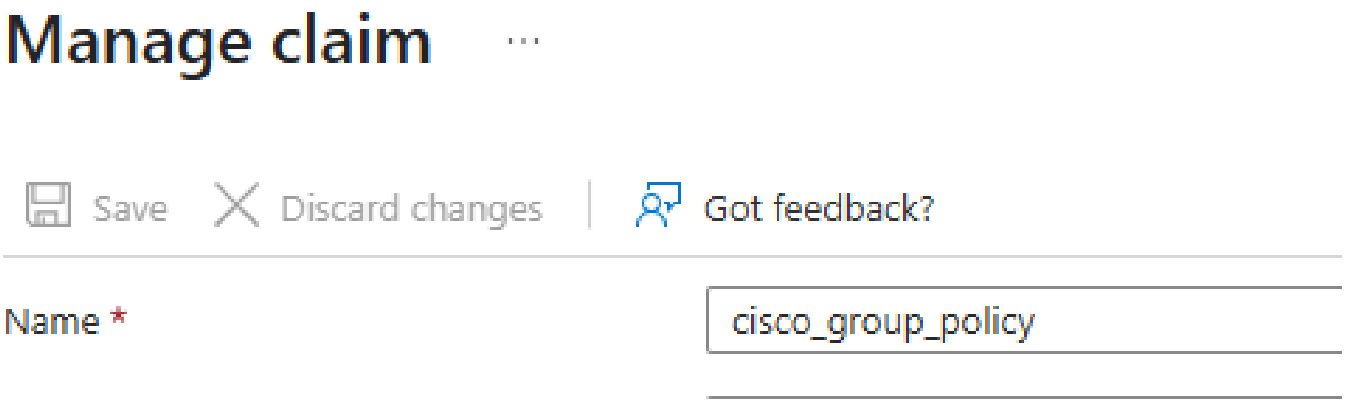
Configuración básica de SAML

8. Seleccione Editar para Atributo y Reclamaciones y haga clic en Agregar nueva reclamación



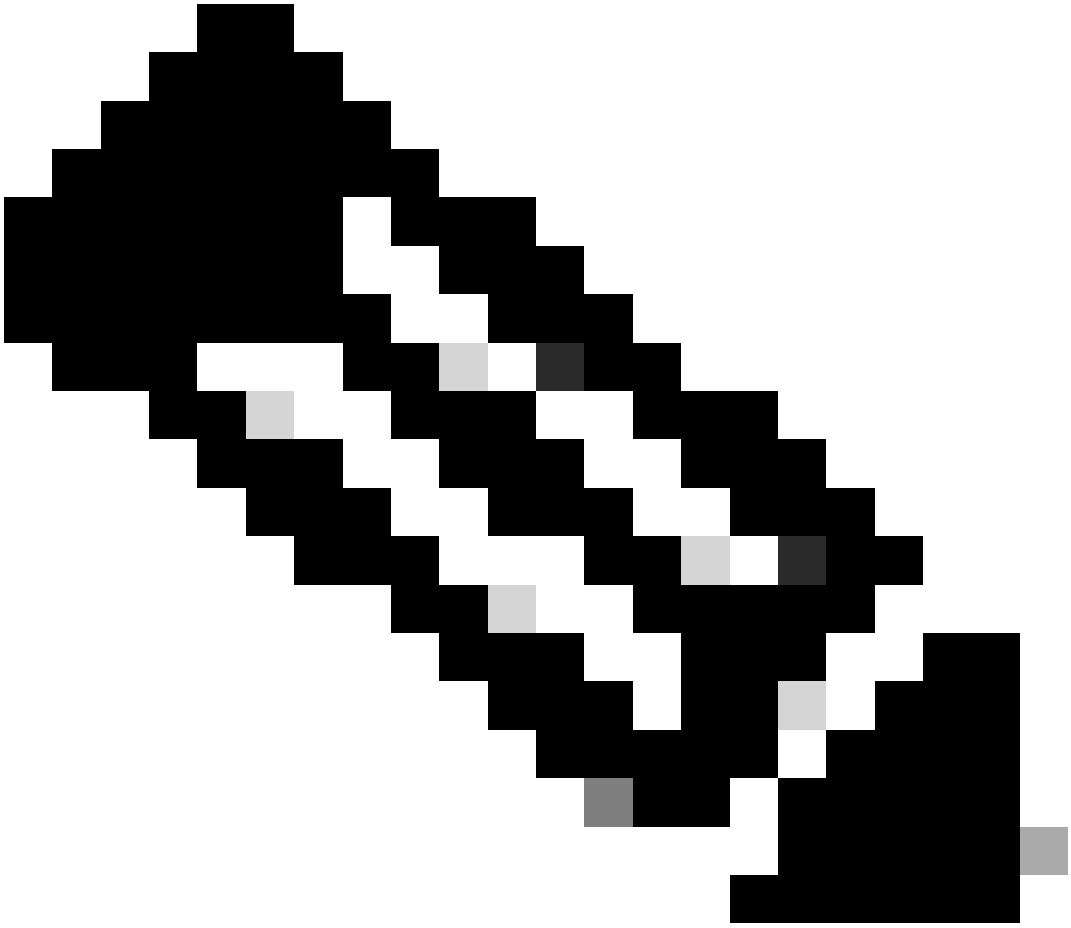
Atributos y reclamaciones

9. La nueva reclamación debe tener el nombre cisco_group_policy.

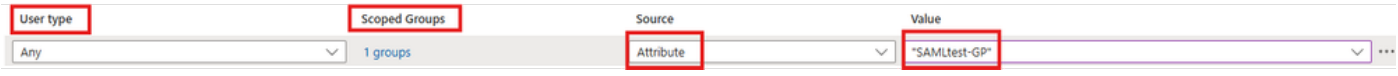


Gestionar reclamación

10. Expanda la sección de Condiciones de reclamación. Seleccione el tipo de usuario y los grupos de ámbito, elija Atributo para el Origen y agregue el nombre de directiva de grupo correcto de la configuración de FTD en el campo Valor y haga clic en Guardar.



Nota: El nombre de política de grupo personalizado del FTD utilizado en este ejemplo es la política de grupo denominada SAMLtest-GP que se creó en la sección Configuración de Política de Grupo de RAVPN de FMC de esta guía. Este valor se debe reemplazar por el nombre de política de grupo del FTD que corresponda a cada grupo de usuarios en el IdP.



condición de reclamación de MS Entra ID

Verificación

FTD

Para verificar la política de grupo deseada, valide el resultado de "show vpn-sessiondb anyconnect".

<#root>

```
FTD# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username : RTPVPNtest
Index : 7110
Assigned IP : 192.168.55.3 Public IP : 10.26.162.189
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA256
Bytes Tx : 105817 Bytes Rx : 63694
Group Policy :
```

SAMLtest-GP

```
 Tunnel Group : SAMLtest
Login Time : 16:54:17 UTC Fri May 9 2025
Duration : 0h:11m:19s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : ac127ca101bc6000681e3339
Security Grp : none Tunnel Zone : 0
```

Para verificar que el IdP está enviando la reclamación deseada, recopile el resultado de "debug webvpn saml 255" mientras se conecta a la VPN. Analice la salida de aserción en los debugs y compare la sección de atributos con lo que está configurado en el IdP.

<#root>

```
<Attribute Name="cisco_group_policy">
<AttributeValue>
```

SAMLtest-GP

```
</AttributeValue>
</Attribute>
```

Troubleshoot

<#root>

```
firepower#
```

show run webvpn

```
firepower#
```

show run tunnel-group

```
firepower#
show crypto ca certificate
firepower#
 debug webvpn saml 255
firepower#
debug webvpn 255
firepower#
debug aaa authorization
```

Información Relacionada

Soporte técnico y descargas de Cisco

Guías de configuración de ASA

Guías de configuración de FMC/FDM

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).