Configurer l'affectation de stratégie de groupe pour SAML en utilisant Secure Firewall et Microsoft Entra ID

Table des matières

Introduction

Ce document décrit comment affecter des stratégies de groupe à l'aide de Microsoft Entra ID pour l'authentification SAML de Cisco Secure Client sur Cisco Secure Firewall.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- VPN AnyConnect Cisco Secure Client
- Configuration d'objet serveur Cisco Firepower Threat Defense (FTD) ou Cisco Secure Firewall ASA VPN d'accès à distance et SSO (Single Sign-on)
- Configuration de Microsoft Entra ID Identity Provider (IdP)

Composants utilisés

Les informations contenues dans ce guide sont basées sur les versions matérielles et logicielles

suivantes :

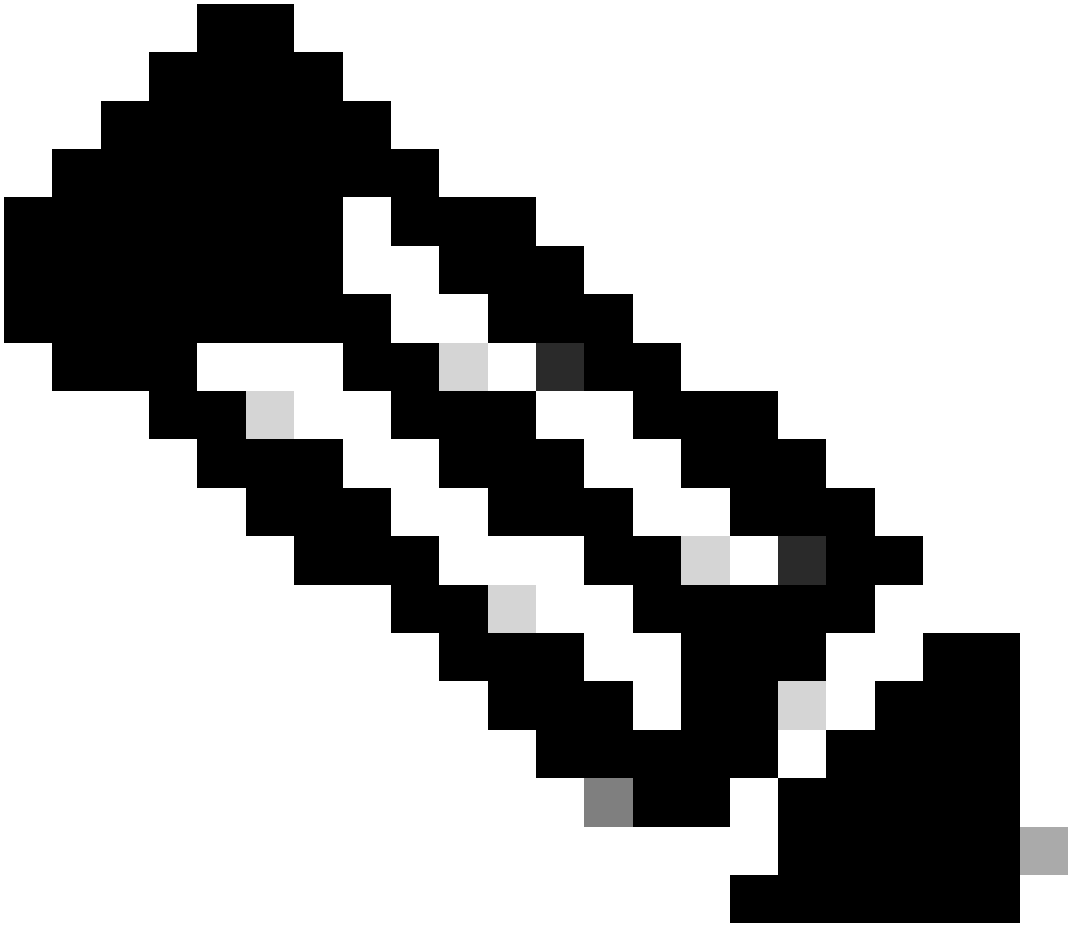
- FTD version 7.6
- FMC version 7.6
- ID MS Entra ID ID SAML IdP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

SAML (Security Assertion Markup Language) est un cadre XML d'échange de données d'authentification et d'autorisation entre domaines de sécurité. Il crée un cercle de confiance entre l'utilisateur, un fournisseur de services (SP) et un fournisseur d'identité (IdP) qui permet à l'utilisateur de se connecter en une seule fois pour plusieurs services. SAML peut être utilisé pour l'authentification VPN d'accès à distance pour les connexions du client sécurisé Cisco aux têtes de réseau VPN ASA et FTD, où ASA ou FTD est la partie SP du cercle de confiance.

Dans ce document, Microsoft Entra ID/Azure est utilisé comme fournisseur d'identité. Cependant, il est également possible d'attribuer des stratégies de groupe à l'aide d'autres IdP, car elles sont basées sur des attributs standard qui peuvent être envoyés dans l'assertion SAML.

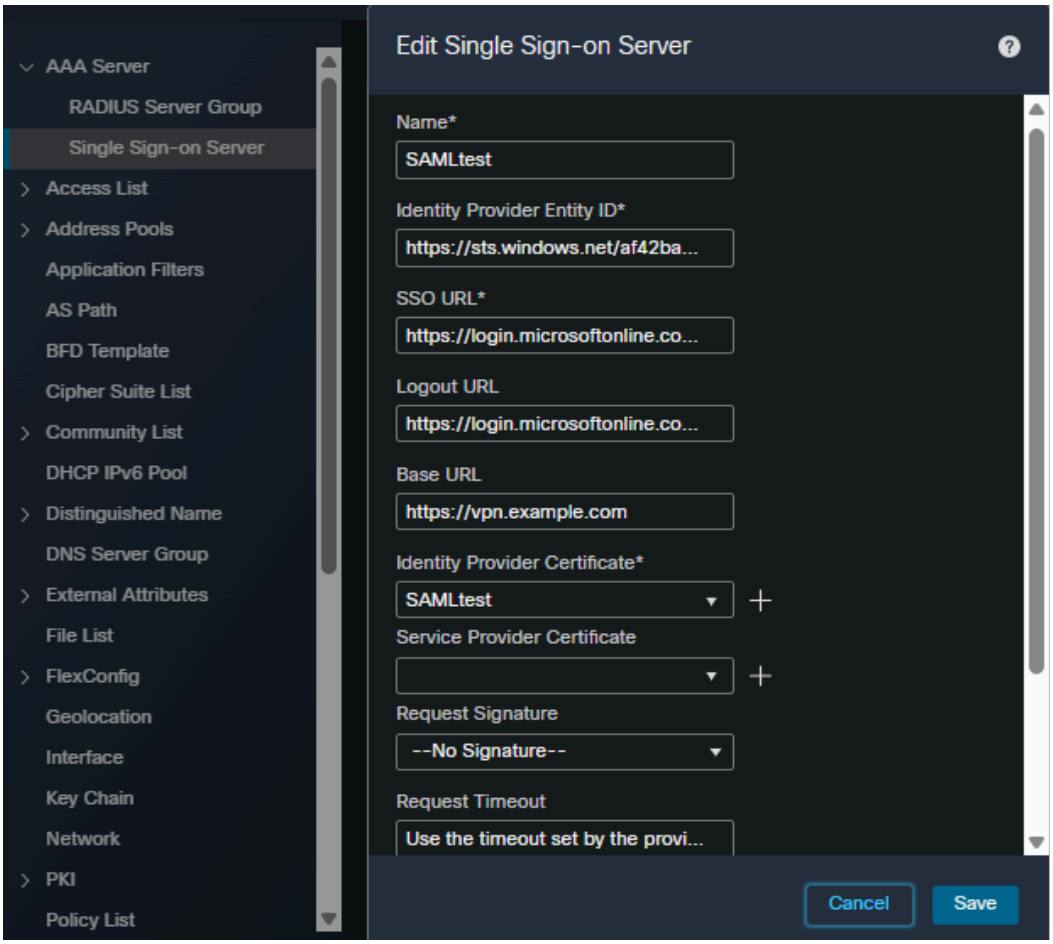


Remarque : N'oubliez pas que chaque utilisateur ne doit appartenir qu'à un seul groupe d'utilisateurs sur MS Entra ID, car plusieurs attributs SAML envoyés à l'ASA ou au FTD peuvent causer des problèmes avec l'affectation de stratégie de groupe comme détaillé dans l'ID de bogue Cisco CSCwm33613

Configurer

Configuration FMC SAML

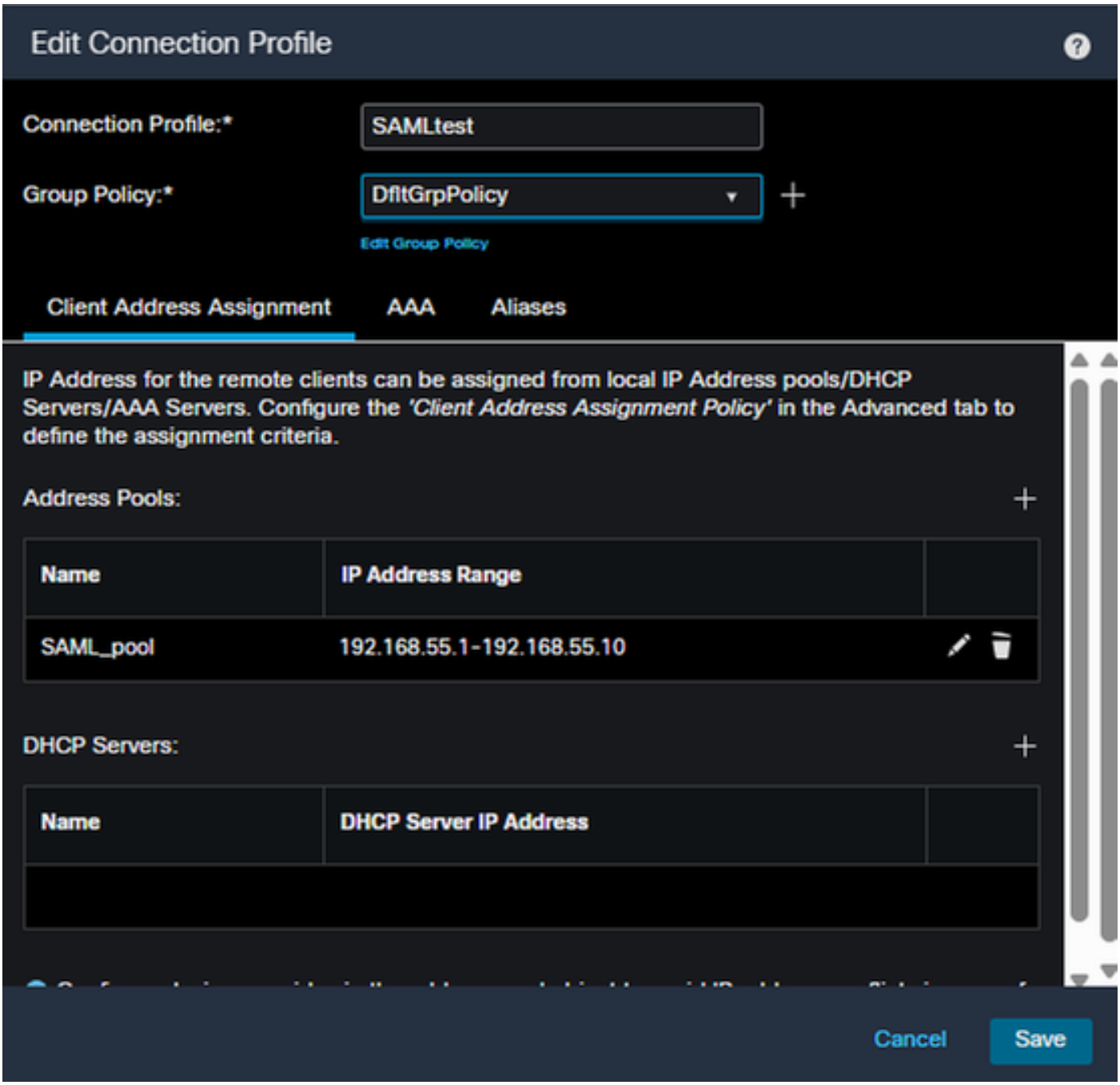
Sur le FMC, accédez à Objets > Gestion des objets > Serveur AAA > Serveur SSO. L'ID d'entité, l'URL SSO, l'URL de déconnexion et le certificat du fournisseur d'identité sont obtenus à partir du fournisseur d'identité, reportez-vous à l'étape 6 de la section Microsoft Entra ID. L'URL de base et le certificat du fournisseur de services sont spécifiques au FTD auquel la configuration est ajoutée.



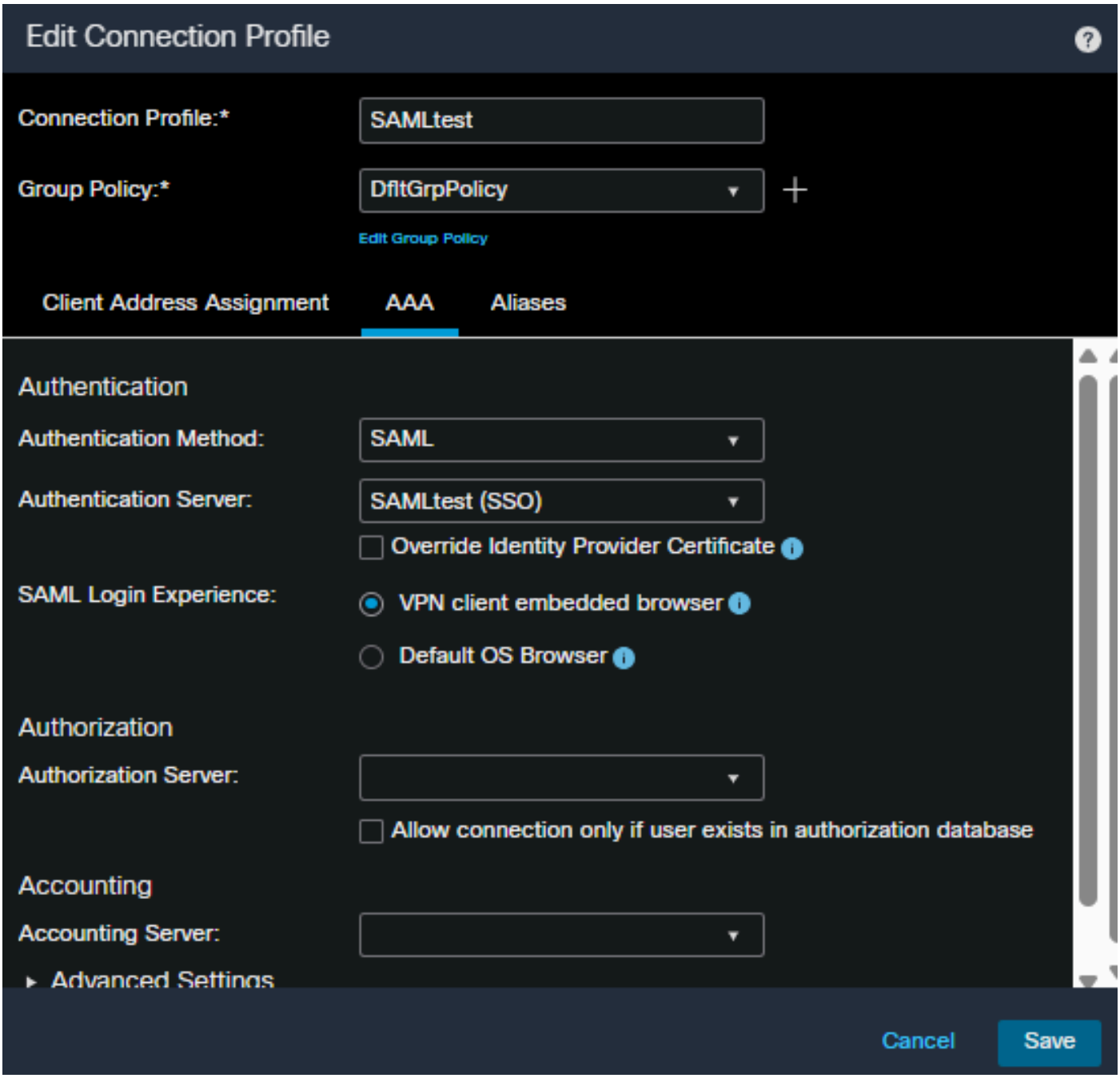
Configuration d'objet SSO FMC

Configuration du groupe de tunnels FMC RAVPN

Sur le FMC, accédez à Devices > VPN > Remote Access > Connection Profile et sélectionnez, ou créez, la stratégie VPN pour le FTD que vous configurez. Une fois sélectionné, créez un profil de connexion similaire à celui-ci :



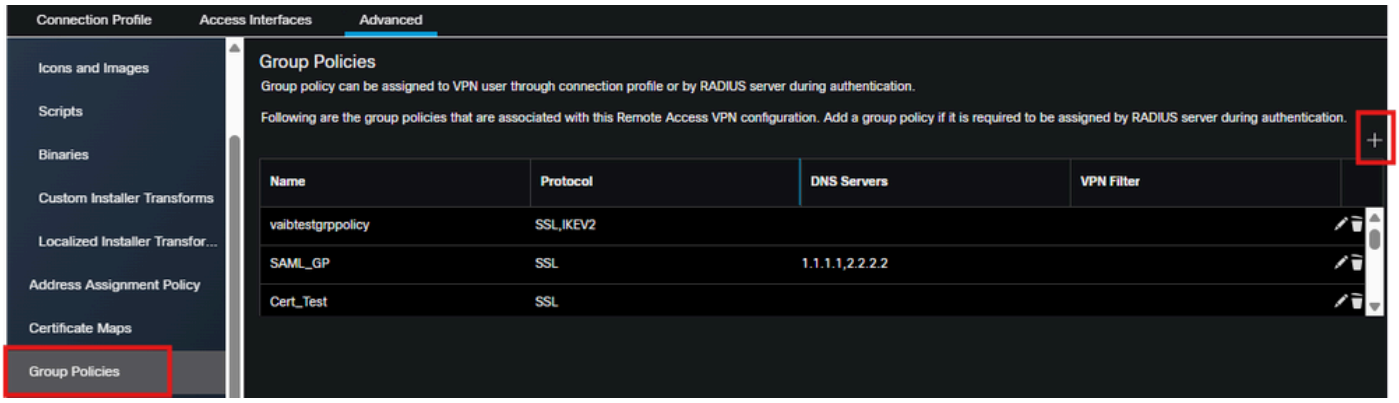
Attribution d'adresse de profil de connexion FMC



Configuration AAA du profil de connexion FMC

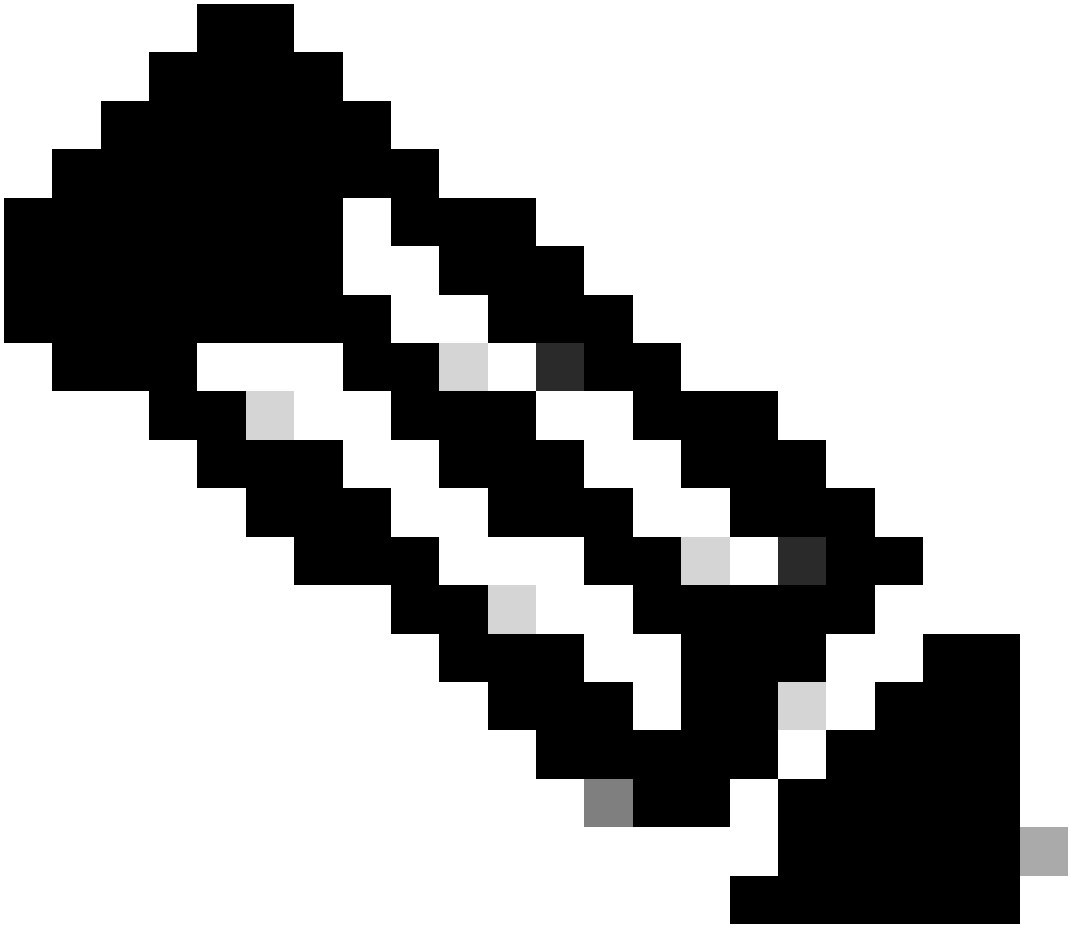
Configuration de la stratégie de groupe FMC RAVPN

1. Vous devez créer une stratégie de groupe avec les options requises pour chaque groupe d'utilisateurs sur Entra ID et l'ajouter à la stratégie RAVPN pour le FTD en cours de configuration. Pour ce faire, accédez à Devices > VPN > Remote Access > Advanced et sélectionnez Group Policies à gauche, puis cliquez sur le signe + dans le coin supérieur droit pour ajouter une stratégie de groupe.

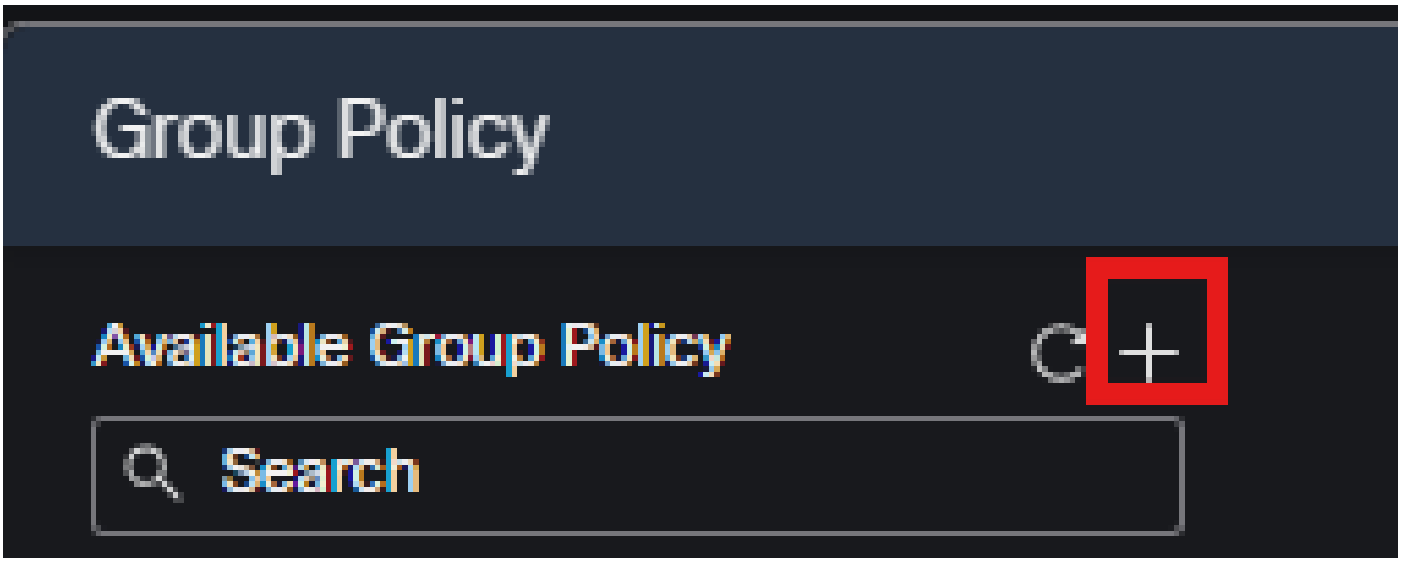


Ajouter une stratégie de groupe FMC

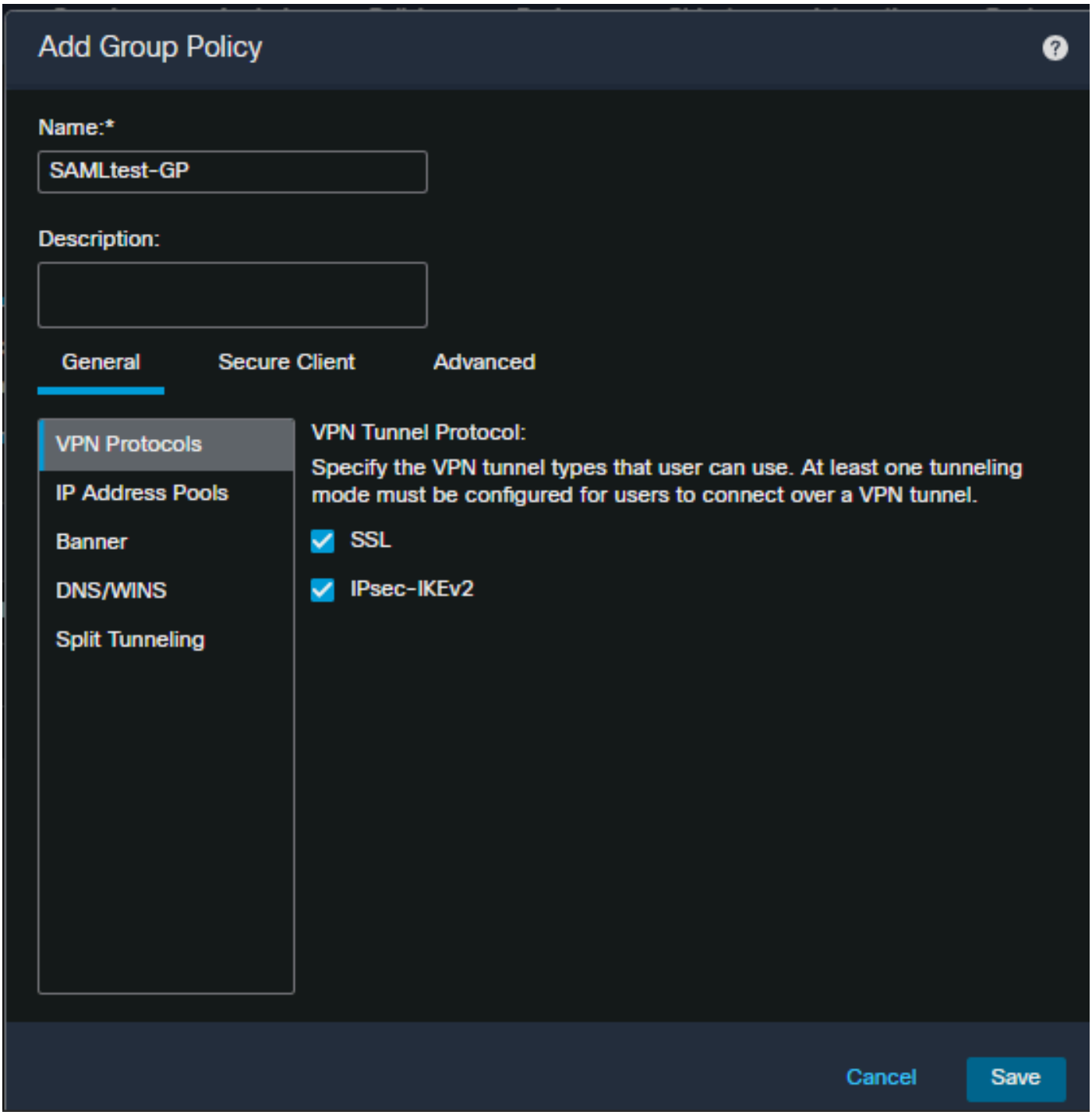
2. Cliquez sur le signe + dans la fenêtre contextuelle pour ouvrir la boîte de dialogue permettant de créer une nouvelle stratégie de groupe. Complétez les options requises et enregistrez.



Remarque : Si vous avez déjà créé la stratégie de groupe requise, vous pouvez ignorer cette étape et passer à l'étape 3

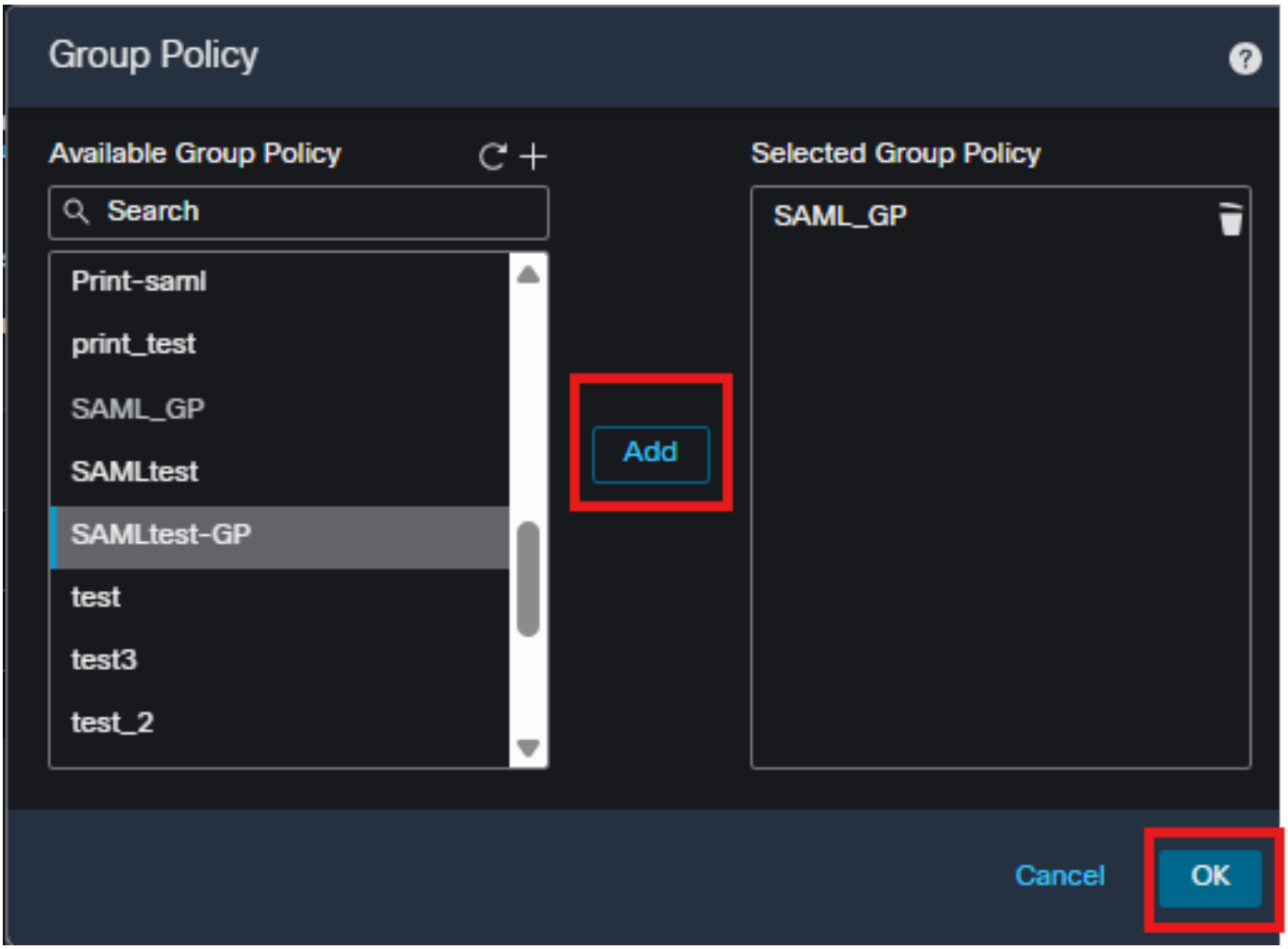


Créer une stratégie de groupe



Options de stratégie de groupe

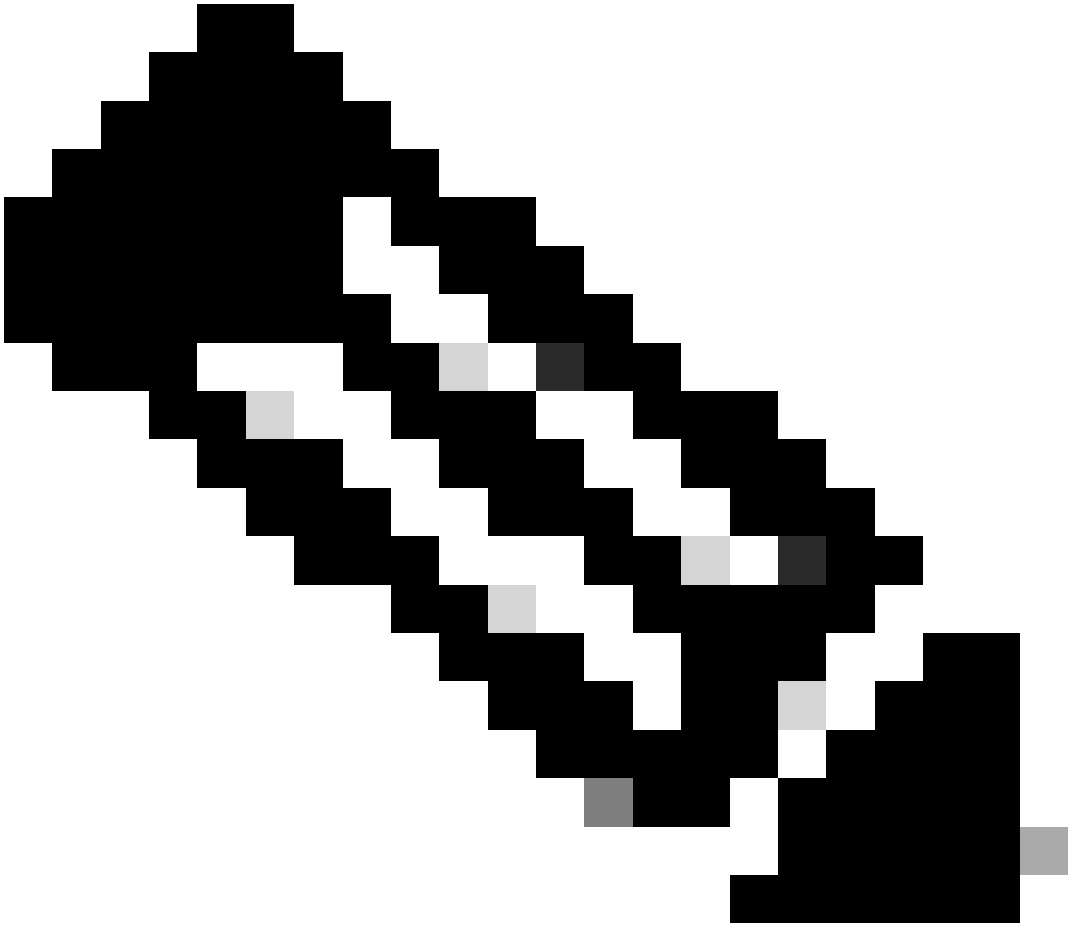
3. Sélectionnez la stratégie de groupe nouvellement créée dans la liste sur la gauche et cliquez sur le bouton Ajouter, puis cliquez sur Ok pour enregistrer la liste.



ajouter une stratégie de groupe

Métadonnées FTD

Une fois la configuration déployée sur le FTD, accédez à l'interface de ligne de commande du FTD et exécutez la commande « show saml metadata <tunnel group name> » et collectez l'ID d'entité FTD et l'URL ACS.



Remarque : Le certificat dans les métadonnées a été tronqué pour des raisons de concision.

<#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
```

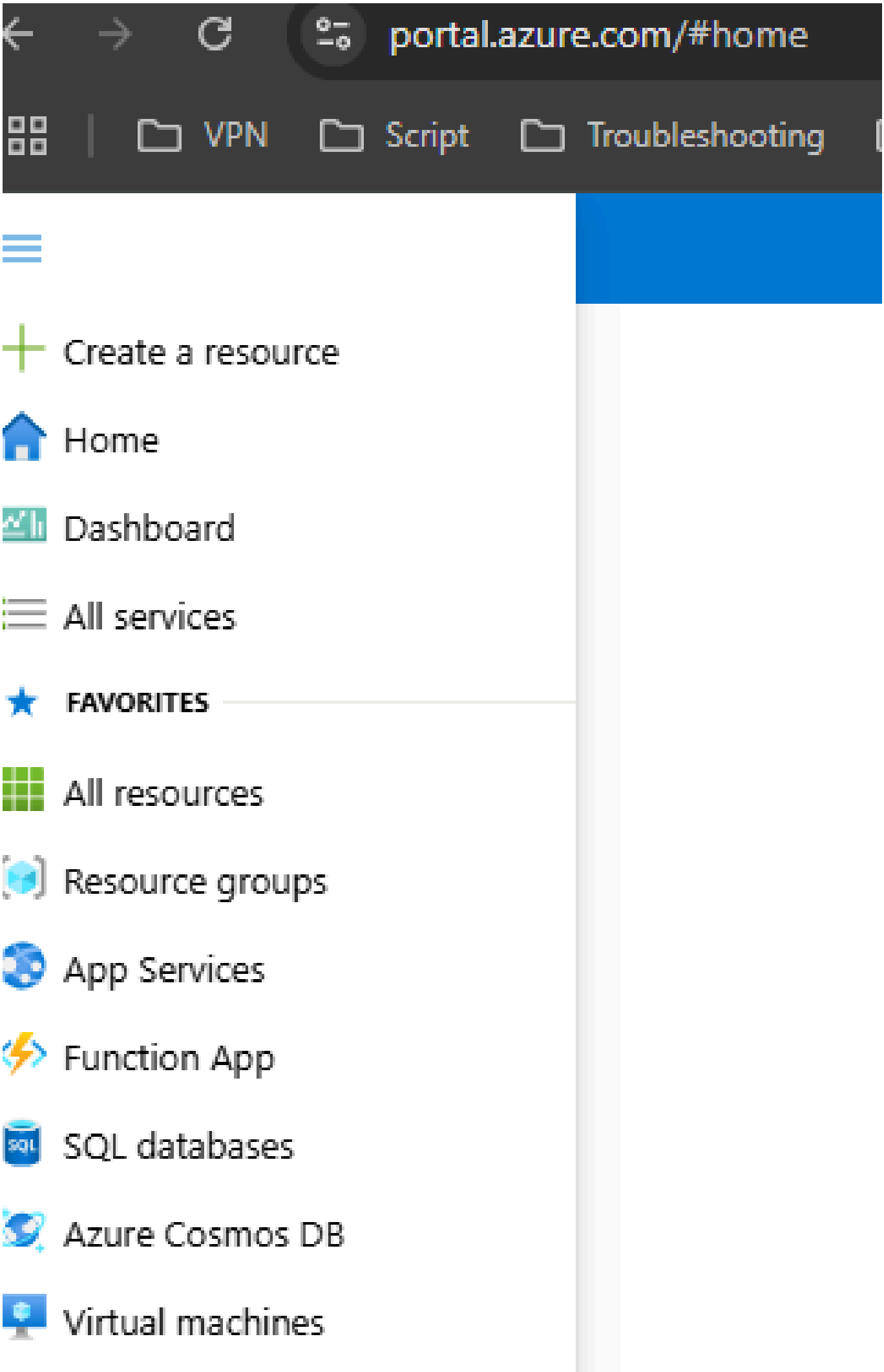
```
NzAzMjUxNzU5NDZaMDAxDzANBgNVBAoTBlJUUFZQTjEdMBsGA1UEAxMUcnRwdnBu
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+10DRPA06a6QNwkehB0Un7XzTNepJO2JQtxdNR2t

</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

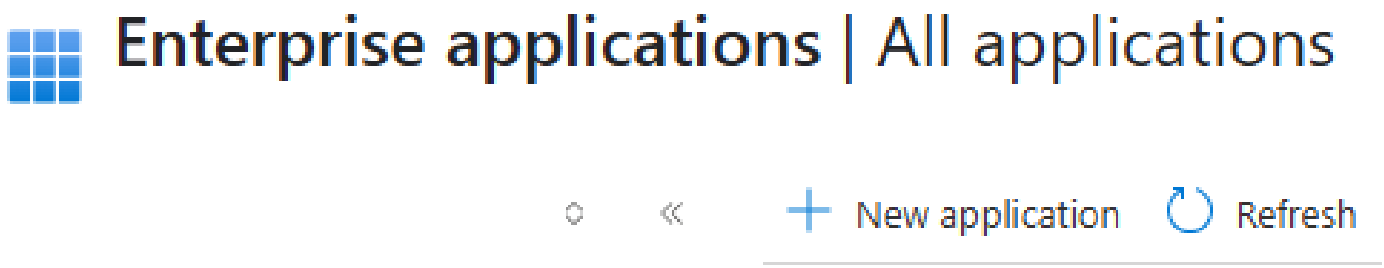
```
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

ID d'entrée Microsoft

1. Sur le portail Microsoft Azure, sélectionnez Microsoft Entra ID dans le menu de gauche.

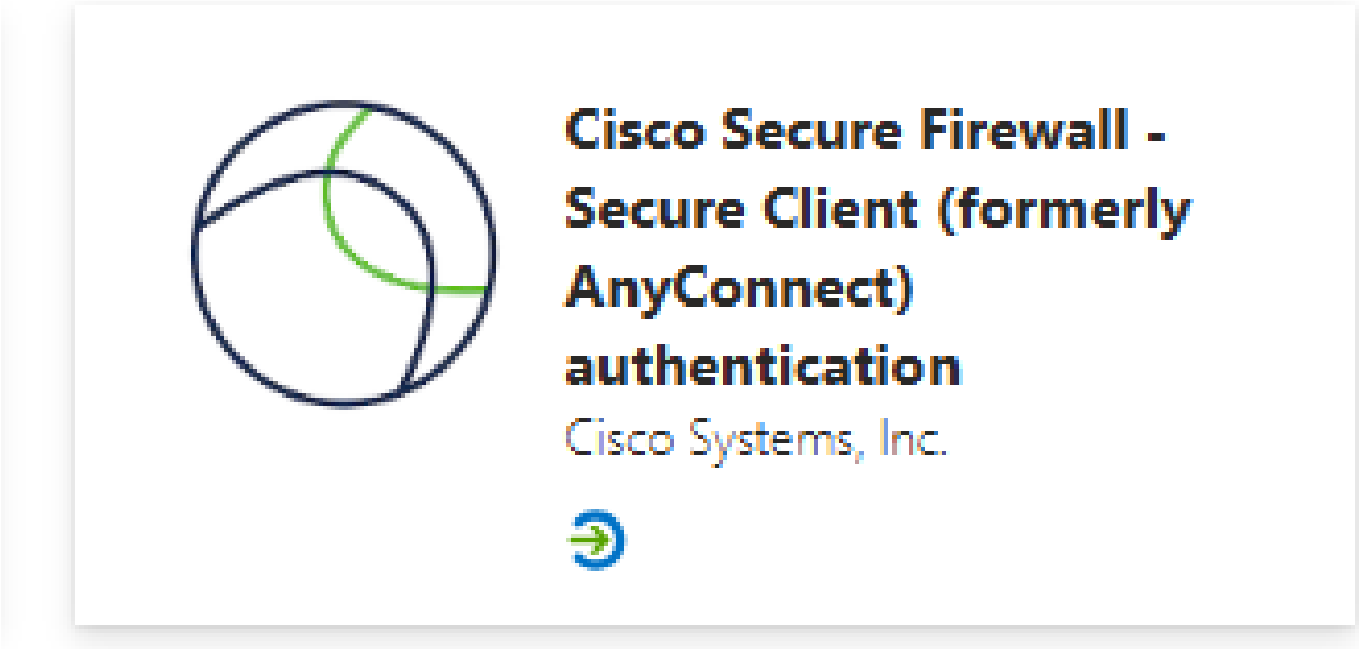

portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

Si une application d'entreprise est déjà configurée pour la configuration FTD RAVPN, ignorez les étapes suivantes et passez à l'étape 7.



Application MS Entra ID Enterprise

4. Sélectionnez Cisco Secure Firewall - Secure Client (anciennement AnyConnect) authentication sous Featured Applications. Donnez un nom à l'application et sélectionnez Créer.



Application d'authentification MS Entra ID Cisco Secure Firewall Secure Client (anciennement AnyConnect)

5. Une fois dans l'application, sélectionnez Utilisateurs et groupes et attribuez les noms d'utilisateur ou de groupe nécessaires à l'application.

Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

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

et récupérez l'URL de connexion, l'identificateur Microsoft Entra et l'URL de déconnexion pour la section Configuration SAML FMC de ce guide.

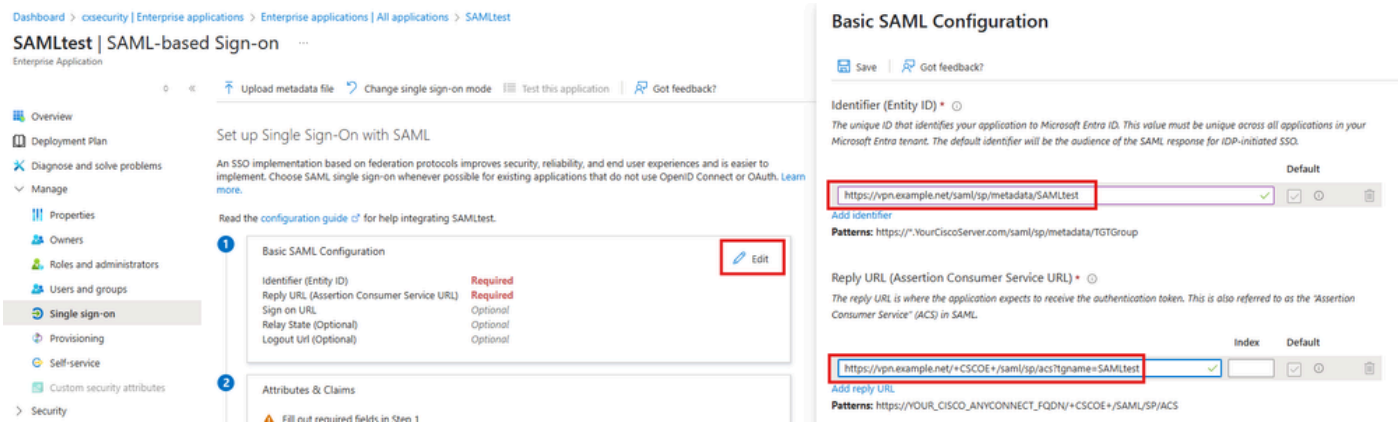
Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

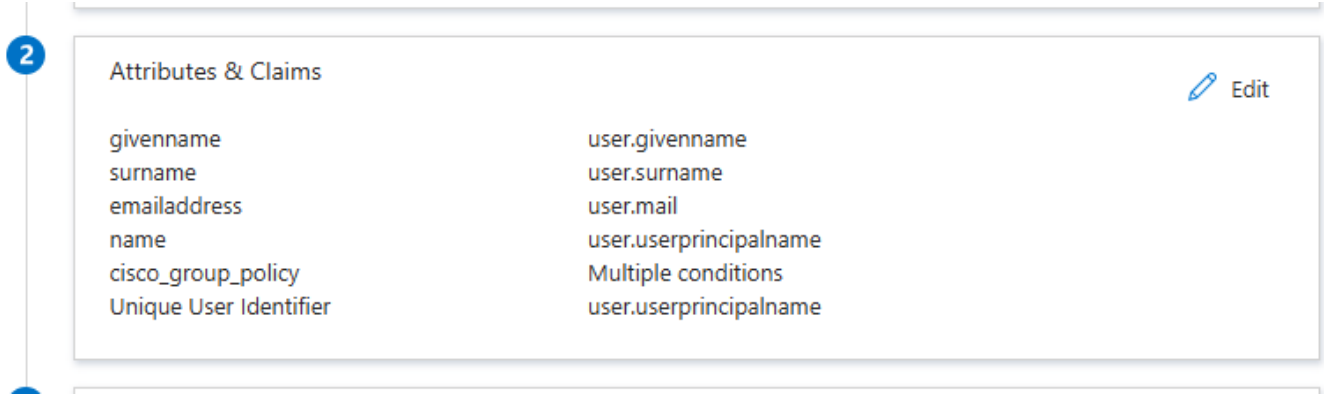
- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
  - Properties
  - Owners
  - Roles and administrators

avec l'identificateur (ID d'entité) et l'URL de réponse (ACS) récupérés à partir des métadonnées FTD et enregistrez.



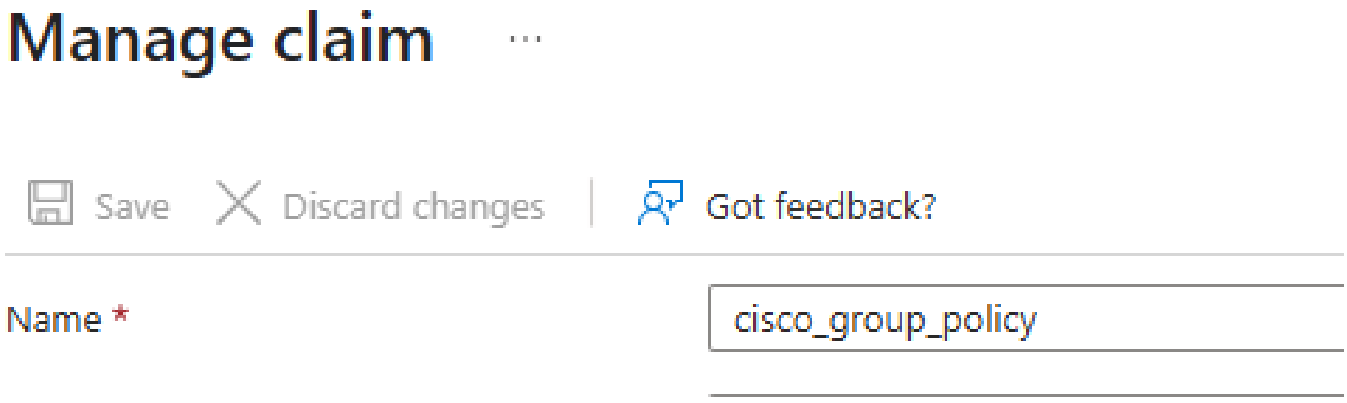
Configuration SAML de base

8. Sélectionnez Modifier pour Attribut et revendications et cliquez sur Ajouter une nouvelle revendication



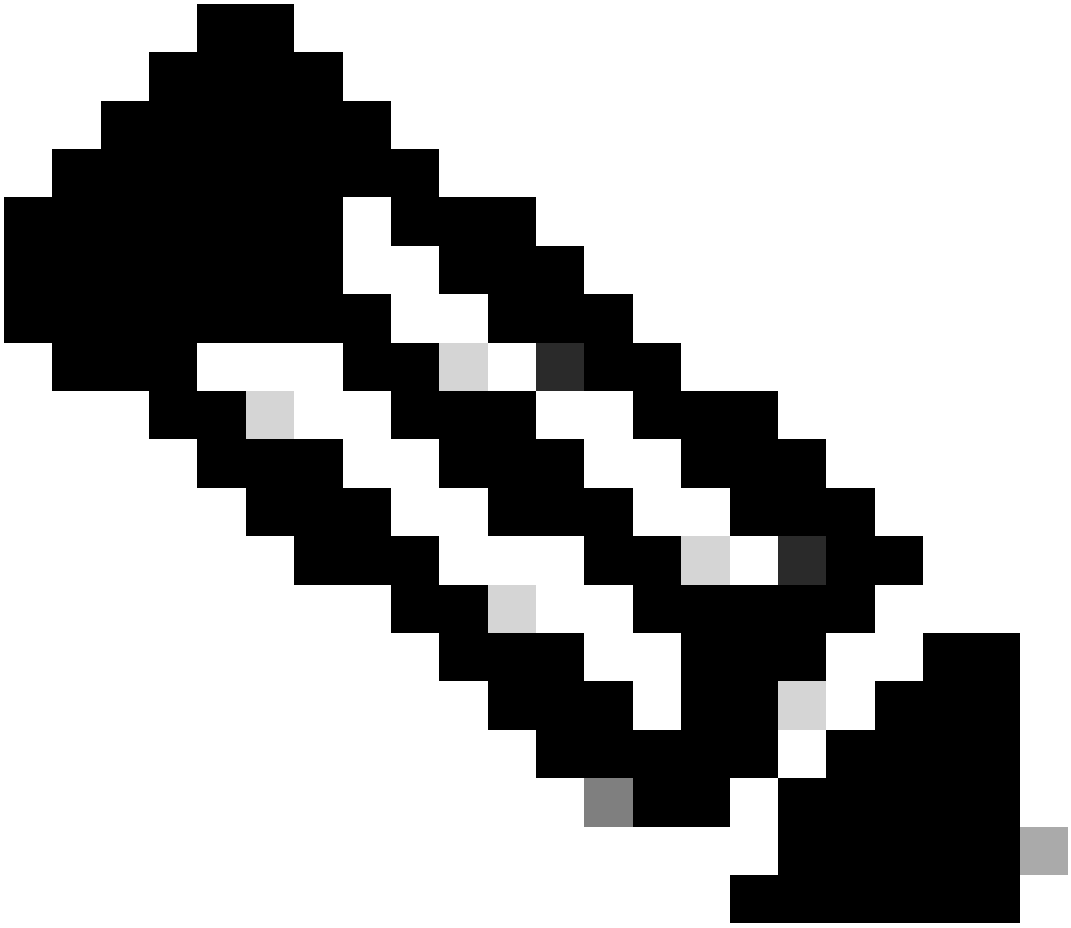
Attributs et revendications

9. La nouvelle demande doit porter le nom cisco_group_policy.

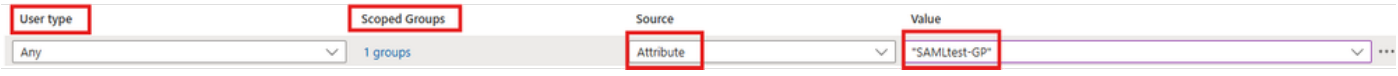


Gérer la demande

10. Élargissez la section pour les conditions de demande. Sélectionnez le type d'utilisateur et les groupes avec portée, puis choisissez Attribut pour la source et ajoutez le nom de stratégie de groupe correct à partir de la configuration FTD dans le champ Valeur et cliquez sur Enregistrer.



> Remarque : Le nom de stratégie de groupe personnalisé du FTD utilisé dans cet exemple est la stratégie de groupe nommée SAMLtest-GP qui a été créée dans la section Configuration de stratégie de groupe RAVPN FMC de ce guide. Cette valeur doit être remplacée par le nom de stratégie de groupe du FTD qui correspond à chaque groupe d'utilisateurs sur le fournisseur d'identité.



Condition de demande MS Entra ID

Vérifier

FTD

Pour vérifier la stratégie de groupe souhaitée, validez le résultat 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
```

Pour vérifier que l'IdP envoie la revendication souhaitée, collectez la sortie de « debug webvpn saml 255 » lors de la connexion au VPN. Analysez la sortie d'assertion dans les débogages et comparez la section d'attribut à ce qui est configuré sur le fournisseur d'identité.

<#root>

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

SAMLtest-GP

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

Dépannage

<#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
```

Informations connexes

Assistance technique de Cisco et téléchargements

Guides de configuration ASA

Guides de configuration FMC/FDM

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.