보안 방화벽 및 Microsoft Entra ID를 사용하여 SAML에 대한 그룹 정책 할당 구성

목차

소개

이 문서에서는 Cisco Secure Firewall에서 Cisco Secure Client의 SAML 인증에 Microsoft Entra ID를 사용하여 그룹 정책을 할당하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- Cisco Secure Client AnyConnect VPN
- Cisco FTD(Firepower Threat Defense) 또는 Cisco Secure Firewall ASA 원격 액세스 VPN 및 SSO(Single Sign-on) 서버 개체 컨피그레이션
- Microsoft Entra ID IdP(Identity Provider) 컨피그레이션

사용되는 구성 요소

이 가이드의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- FTD 버전 7.6

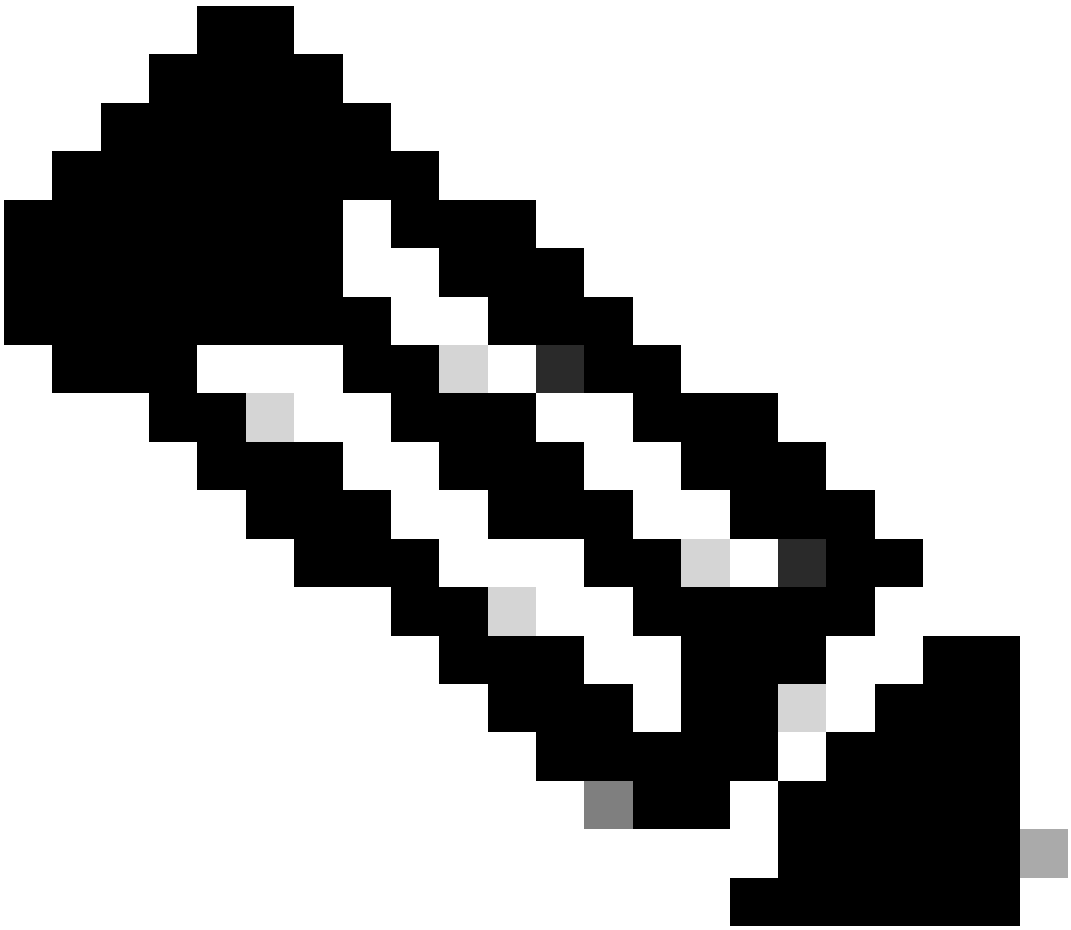
- FMC 버전 7.6
- MS Entra ID SAML IdP

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SAML(Security Assertion Markup Language)은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 프레임워크입니다. 사용자, 서비스 공급자(SP) 및 IDp(Identity Provider) 간에 신뢰 범위를 생성하여 여러 서비스에 대해 한 번에 로그인할 수 있습니다. SAML은 ASA 및 FTD VPN 헤드엔드에 대한 Cisco Secure Client 연결을 위한 원격 액세스 VPN 인증에 사용할 수 있습니다. 여기서 ASA 또는 FTD는 신뢰 서클의 SP 부분입니다.

이 문서에서는 Microsoft Entra ID/Azure가 IdP로 사용됩니다. 그러나 SAML 어설션에서 전송할 수 있는 표준 특성을 기반으로 하므로 다른 IdP를 사용하여 그룹 정책을 할당할 수도 있습니다.

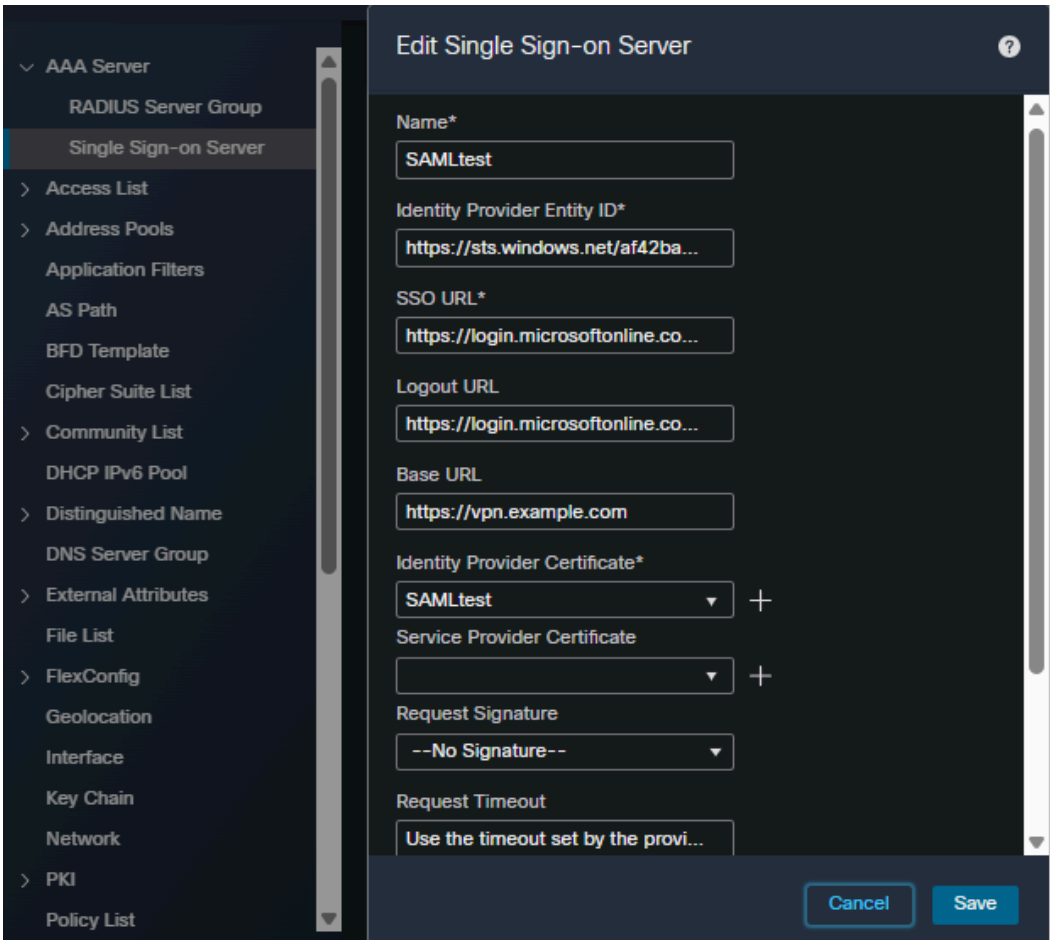


참고: ASA 또는 FTD로 전송되는 여러 SAML 특성은 Cisco 버그 ID CSCwm에 설명된 그룹 정책 할당에 문제를 일으킬 수 있으므로 각 사용자는 MS Entra ID에서 하나의 사용자 그룹에만 속해야 합니다33613

구성

FMC SAML 컨피그레이션

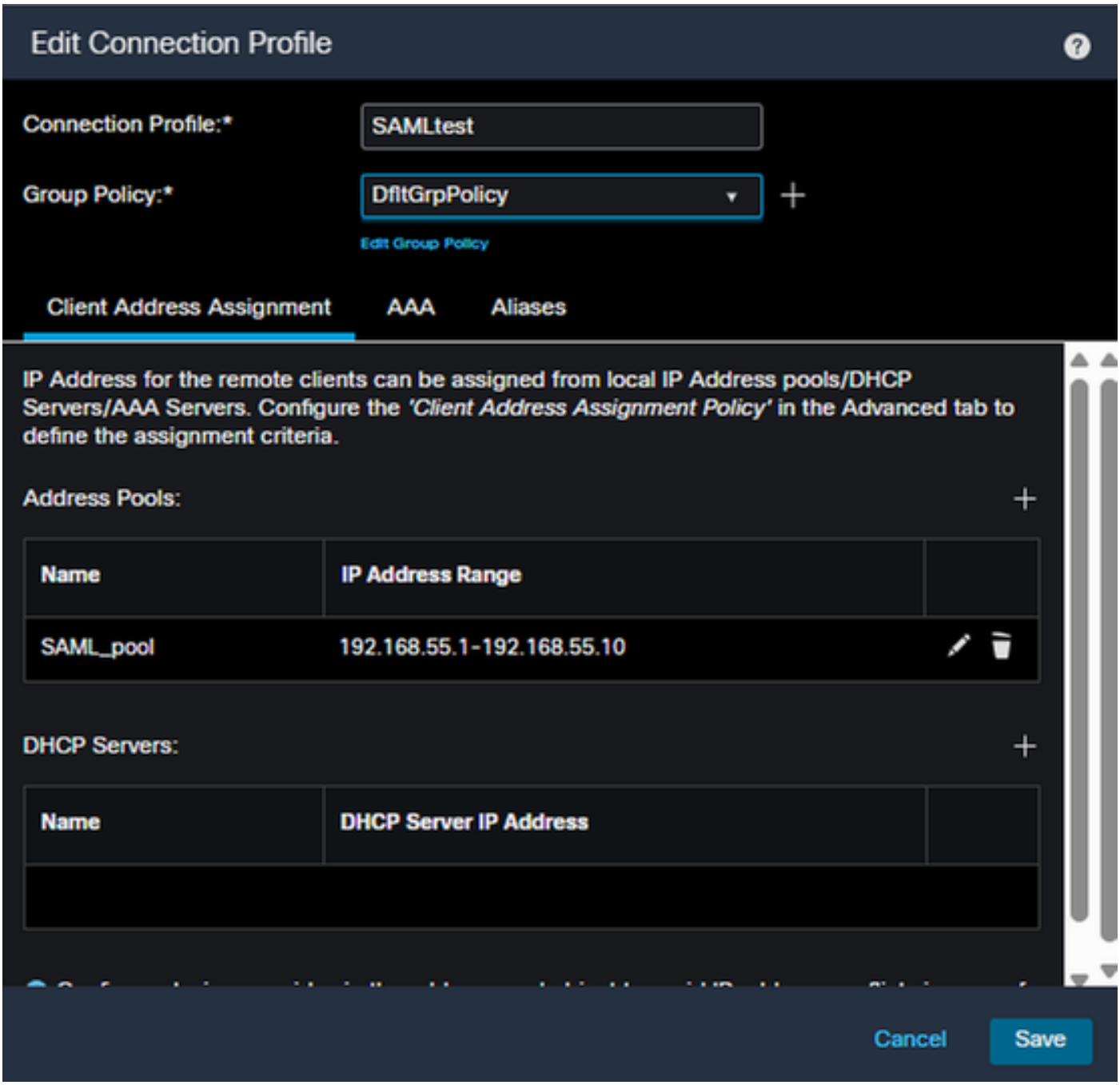
FMC에서 Objects(개체) > Object Management(개체 관리) > AAA Server(AAA 서버) > Single Sign-on Server(단일 로그인 서버)로 이동합니다. IdP에서 엔티티 ID, SSO URL, 로그아웃 URL 및 ID 공급자 인증서를 가져옵니다. Microsoft Entra ID 섹션의 6단계를 참조하십시오. 기본 URL 및 서비스 공급자 인증서는 컨피그레이션이 추가되는 FTD에 한정됩니다.



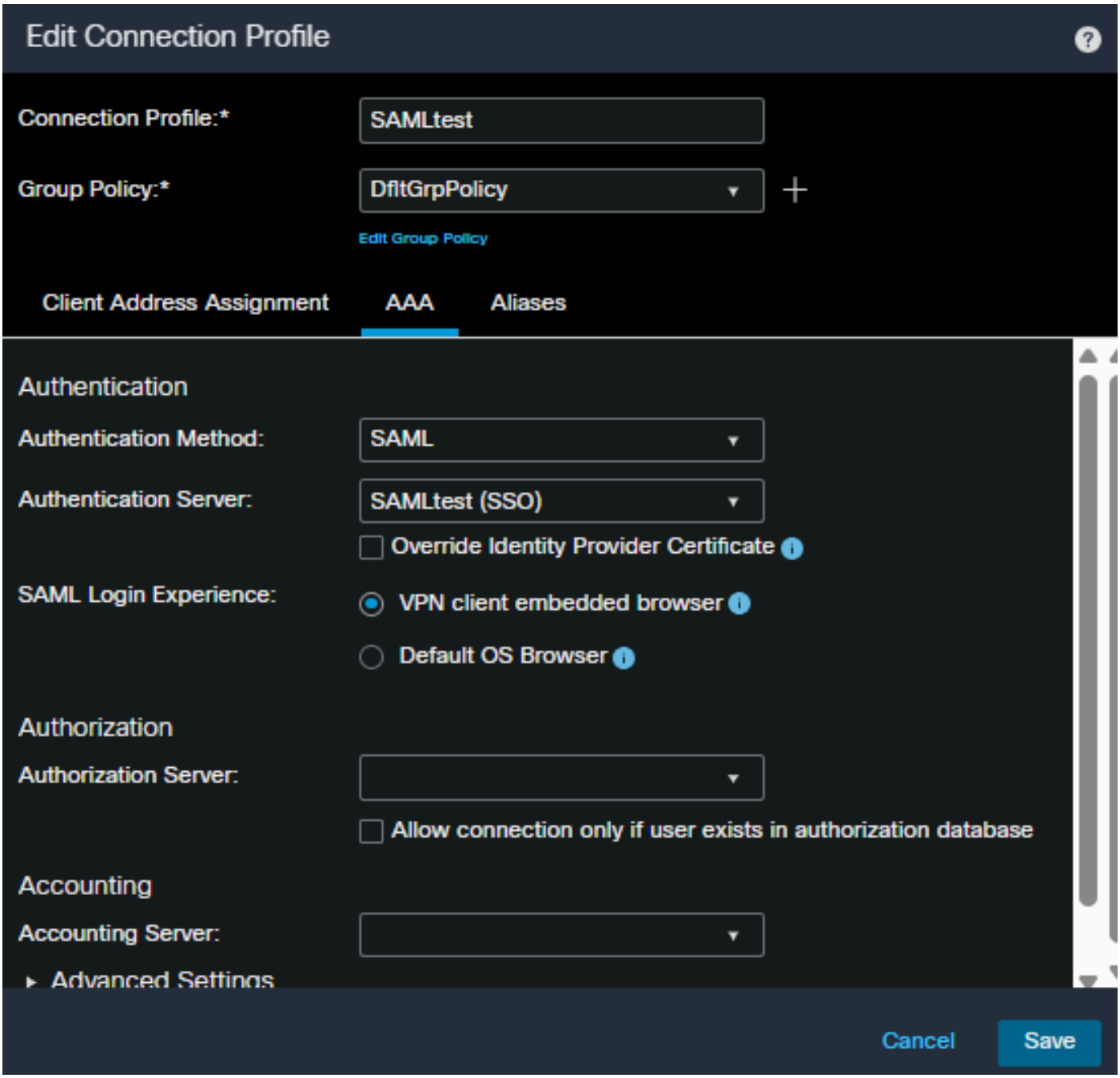
FMC SSO 개체 컨피그레이션

FMC RAVPN 터널 그룹 컨피그레이션

FMC에서 Devices(디바이스) > VPN > Remote Access(원격 액세스) > Connection Profile(연결 프로파일)로 이동하여 구성하는 FTD에 대한 VPN 정책을 선택하거나 생성합니다. 이 옵션을 선택하면 다음과 유사한 연결 프로파일을 생성합니다.



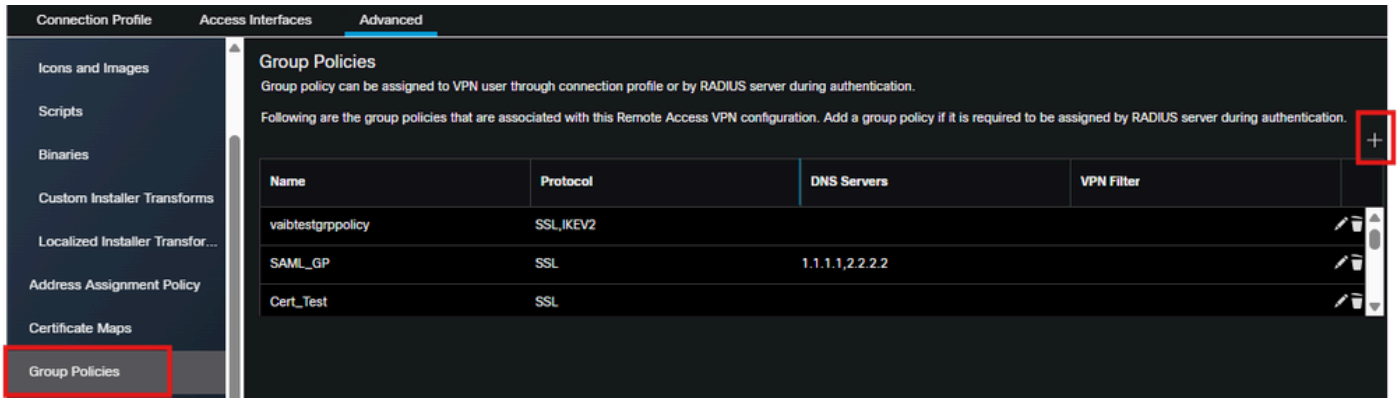
FMC 연결 프로파일 주소 할당



FMC 연결 프로파일 AAA 컨피그레이션

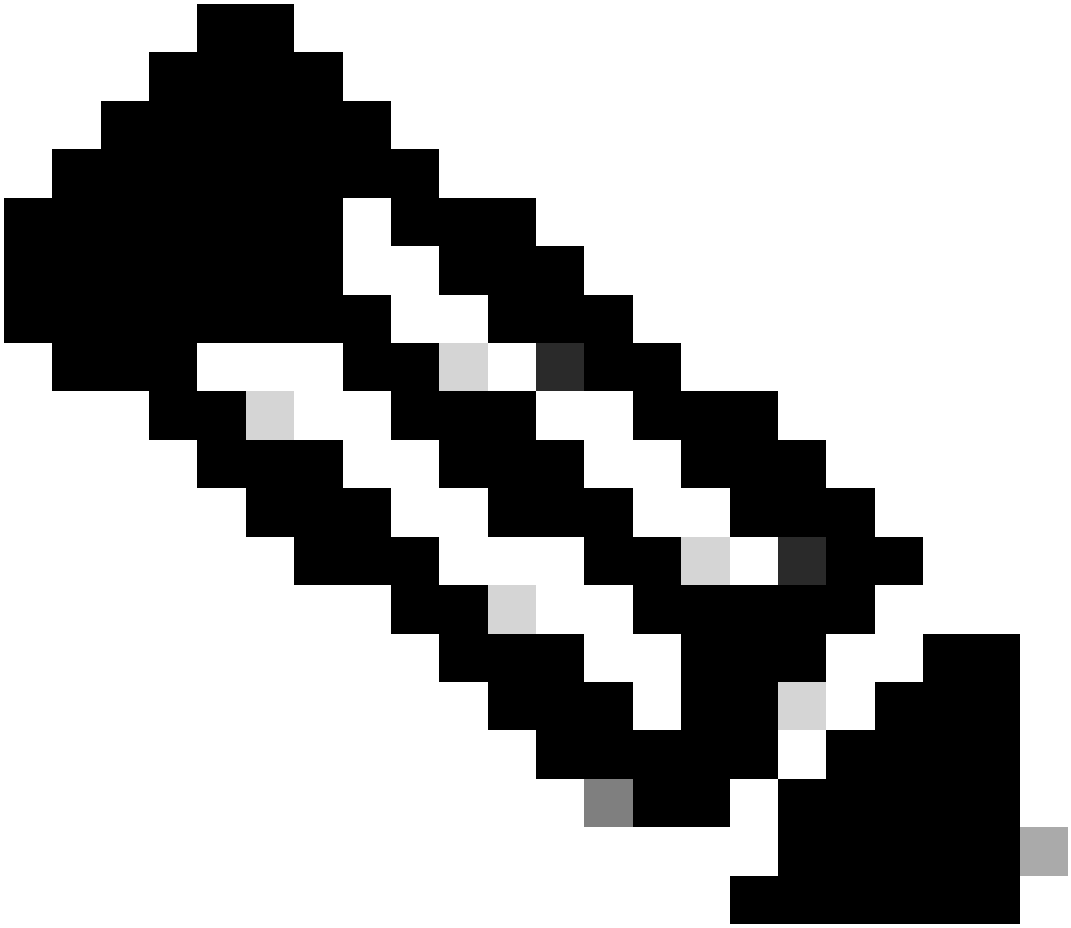
FMC RAVPN 그룹 정책 컨피그레이션

1. Entra ID의 각 사용자 그룹에 대해 필요한 옵션을 사용하여 그룹 정책을 생성하고 구성 중인 FTD에 대한 RAVPN 정책에 추가해야 합니다. 이렇게 하려면 Devices(디바이스) > VPN > Remote Access(원격 액세스) > Advanced(고급)로 이동하고 왼쪽에서 Group Policies(그룹 정책)를 선택한 다음 오른쪽 위의 +를 클릭하여 그룹 정책을 추가합니다.

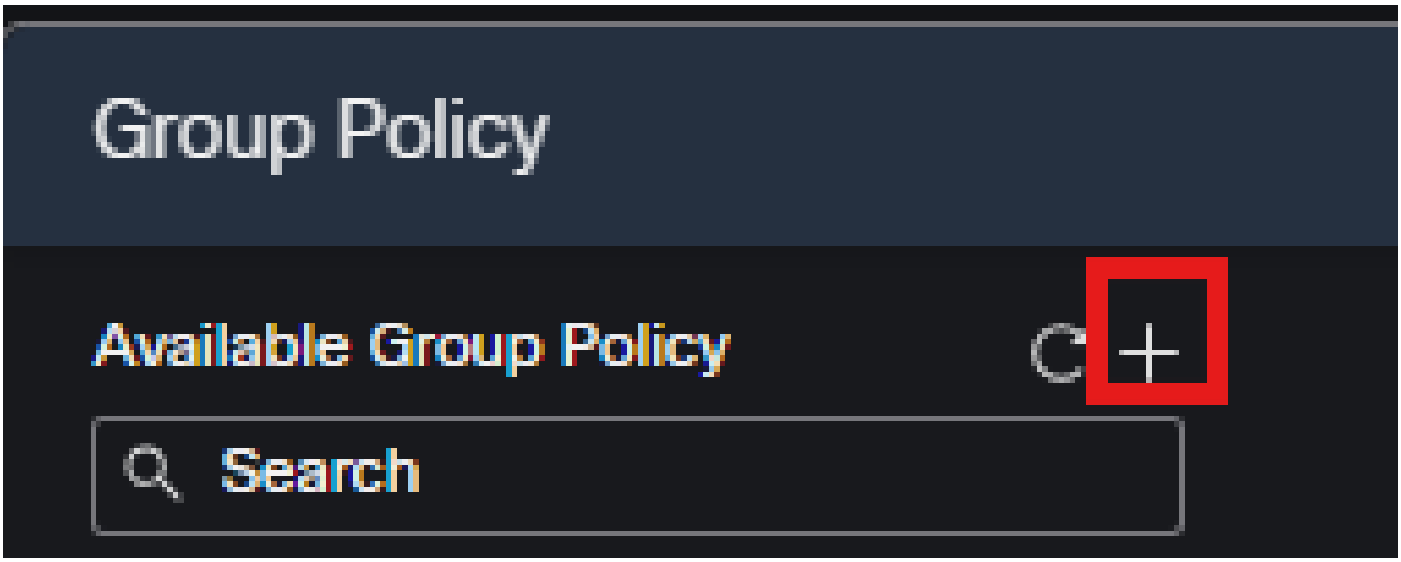


FMC 그룹 정책 추가

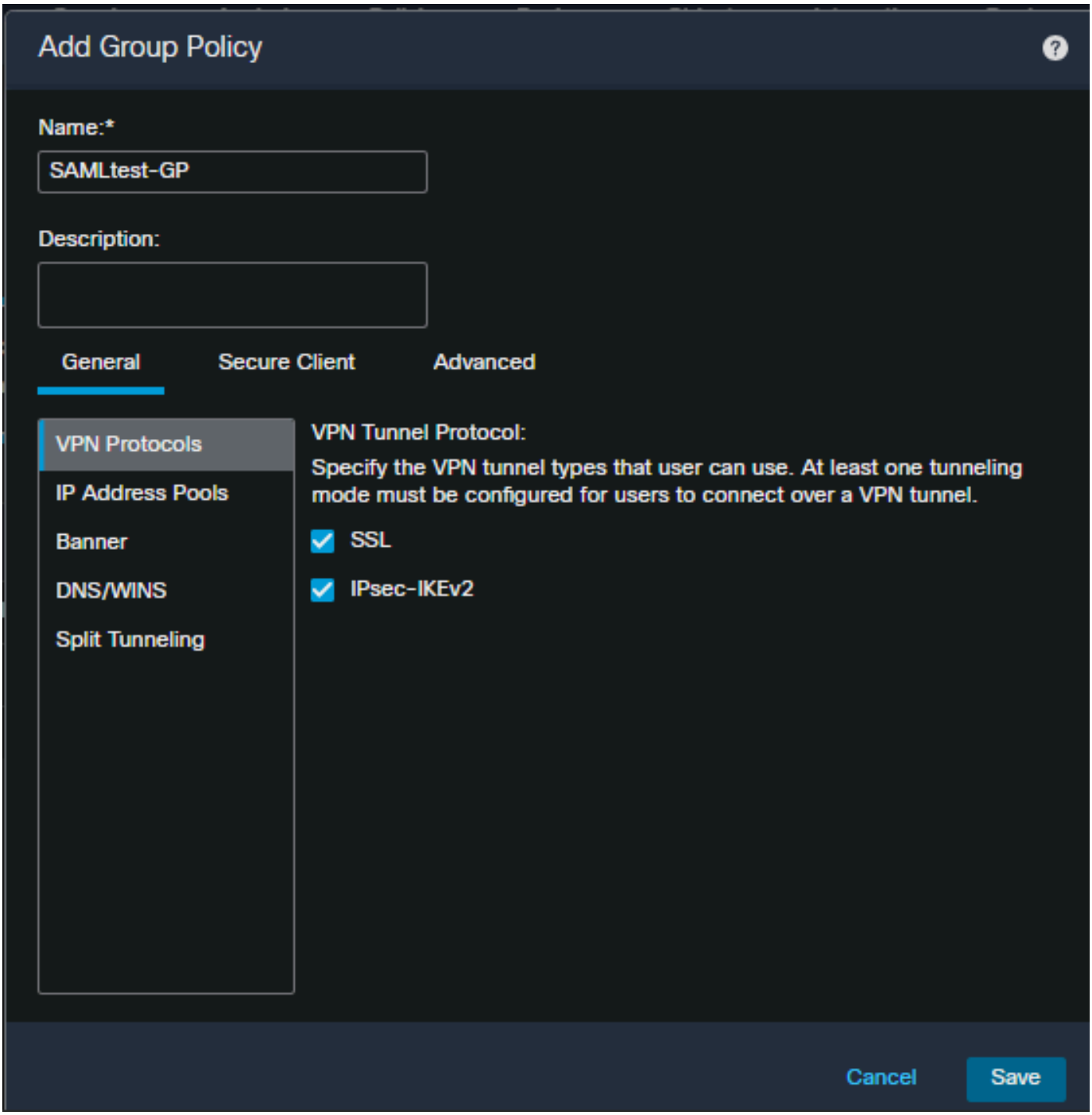
2. 팝업에서 +를 클릭하여 대화 상자를 열고 새 그룹 정책을 생성합니다. 필요한 옵션을 입력하고 저장합니다.



참고: 필요한 그룹 정책을 이미 생성한 경우 이 단계를 건너뛰고 3단계로 계속할 수 있습니다

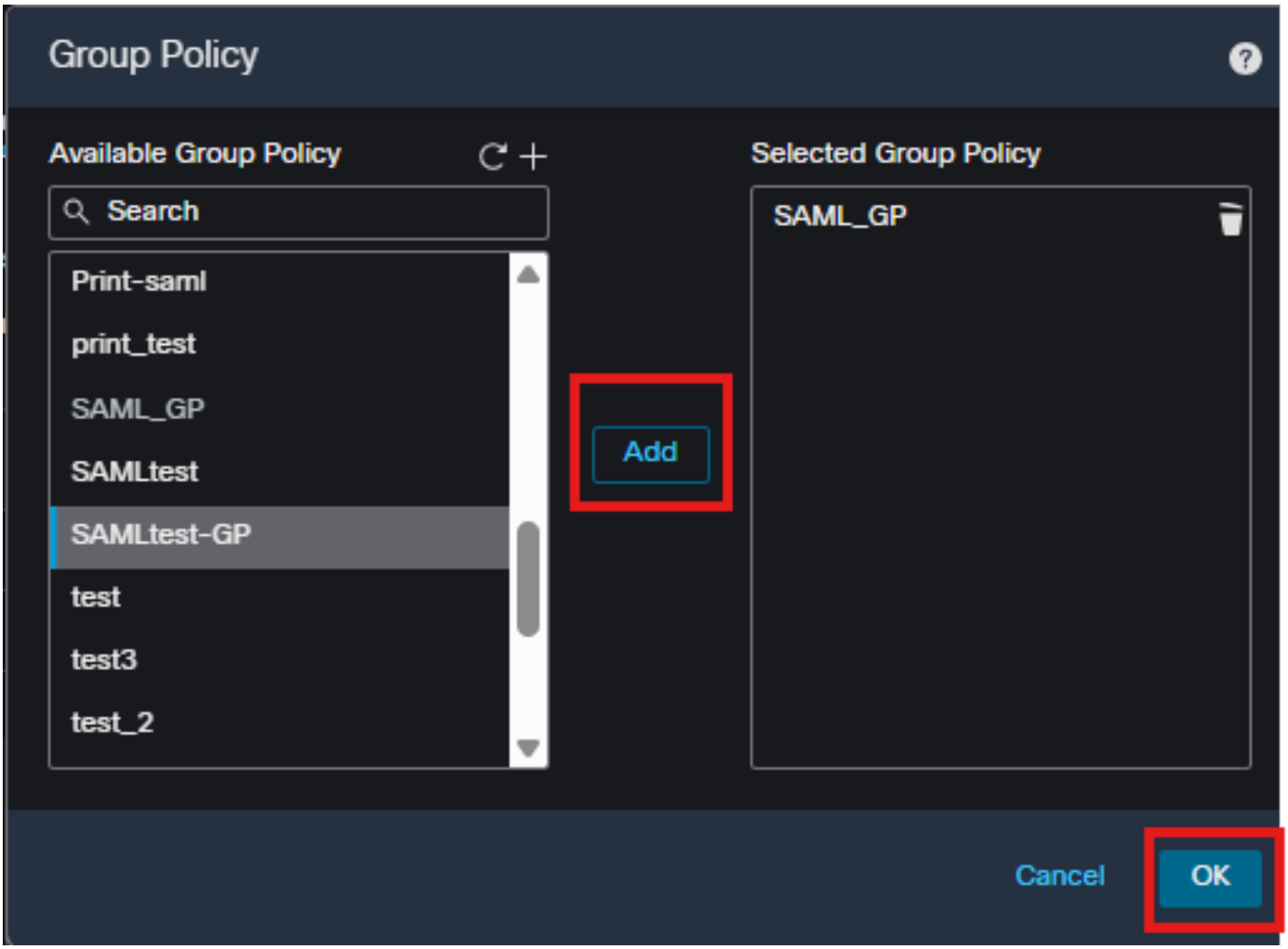


새 그룹 정책 만들기



그룹 정책 옵션

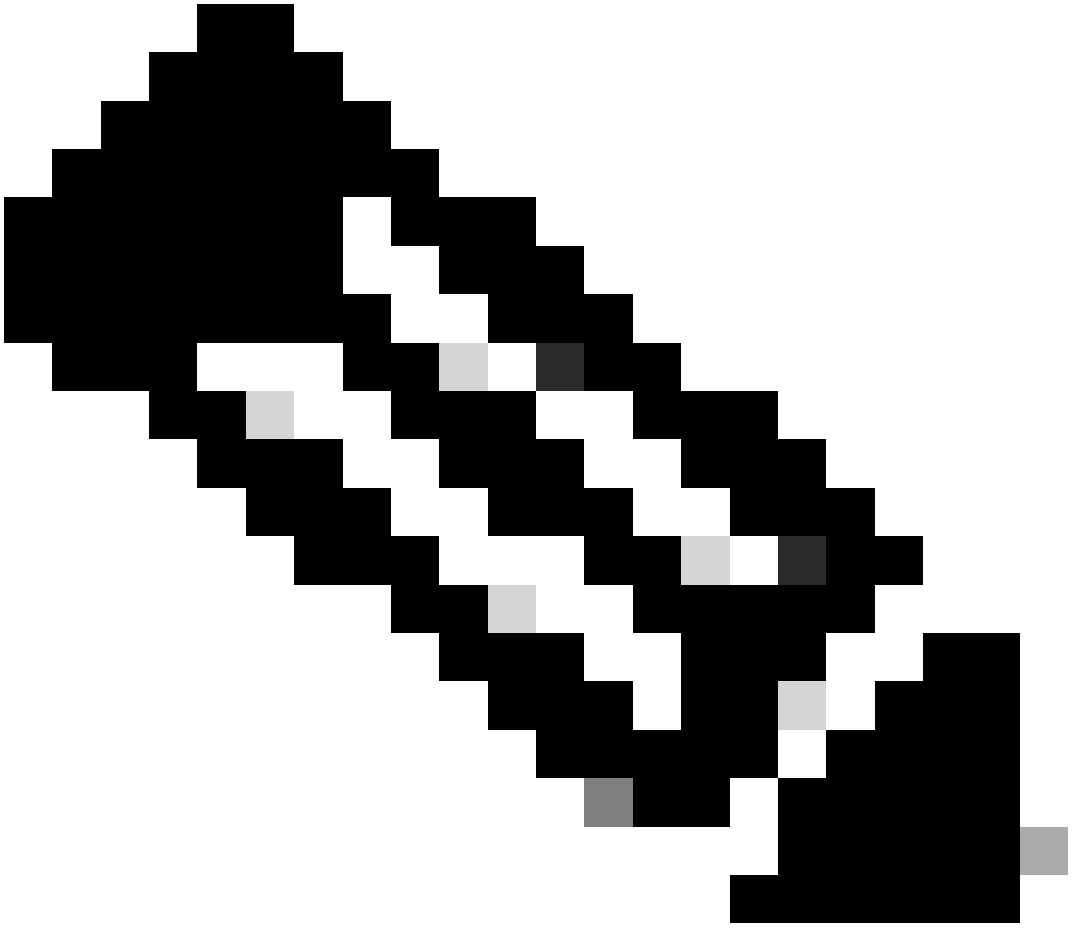
3. 왼쪽 목록에서 새로 생성된 그룹 정책을 선택하고 Add(추가) 버튼을 클릭한 다음 Ok(확인)를 클릭하여 목록을 저장합니다.



그룹 정책 추가

FTD 메타데이터

컨피그레이션이 FTD에 구축되면 FTD CLI로 이동하여 "show saml metadata <tunnel group name>" 명령을 실행하고 FTD 엔티티 ID 및 ACS URL을 수집합니다.



참고: 메타데이터의 인증서가 간결성을 위해 잘렸습니다.

<#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
```

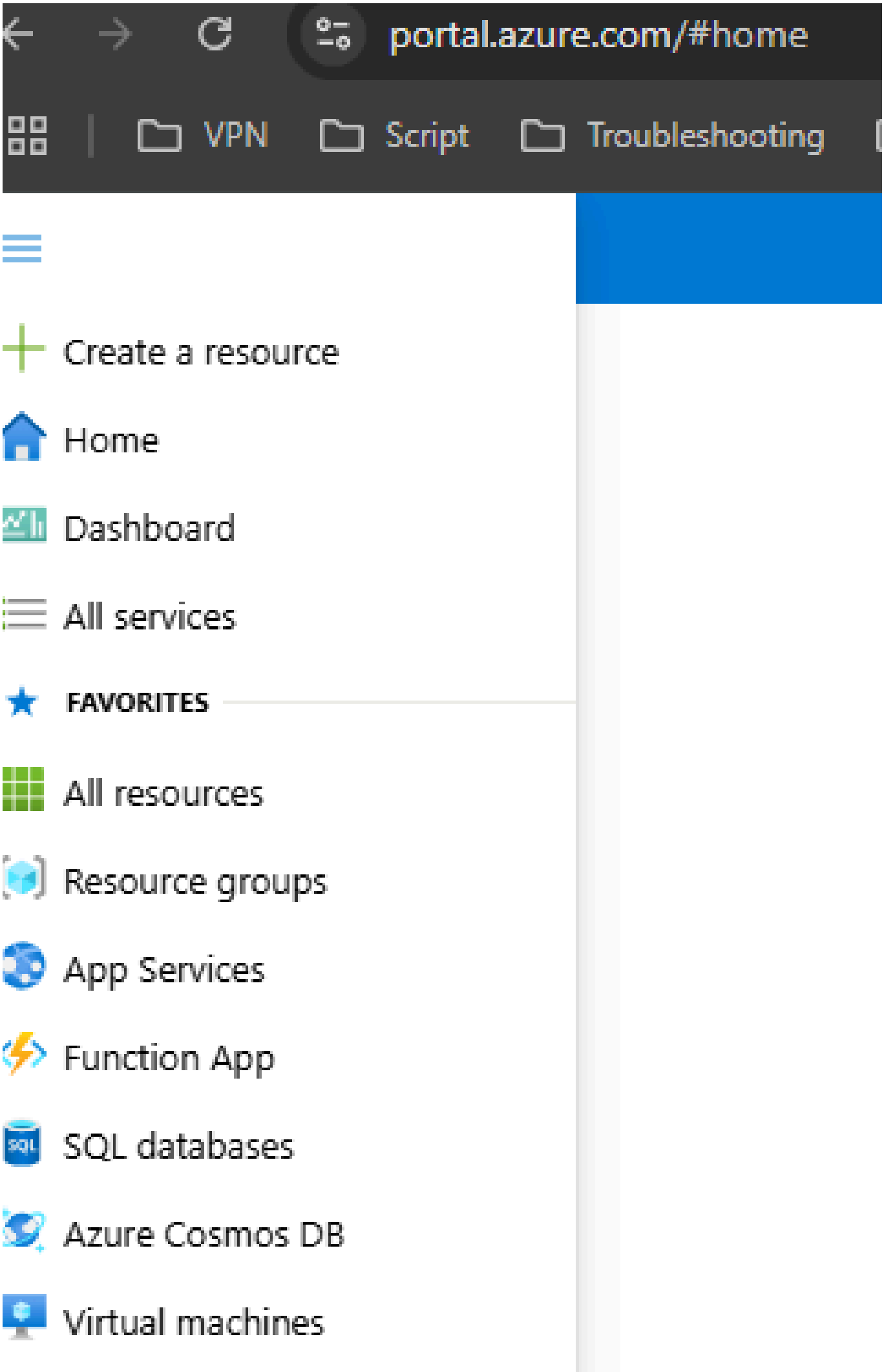
```
LWZ0ZC5jaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC5
5B0tH9RIjvG0MxhpDT3/BpDEFfTcVE2w2fxu5m8gZFTeeezyF5B93rWx+N26V8JE
sB5I1KLTGRj8b9TK6L357cdbgr692Wl952TLFB3XC43gpe0fnN3+Uas/HJ3IudsF
N+QPC9FO4LE88attuGuVMquV+1ODRPA06a6QNwkehB0Un7XzTNepJ02JQtxdNR2t

</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

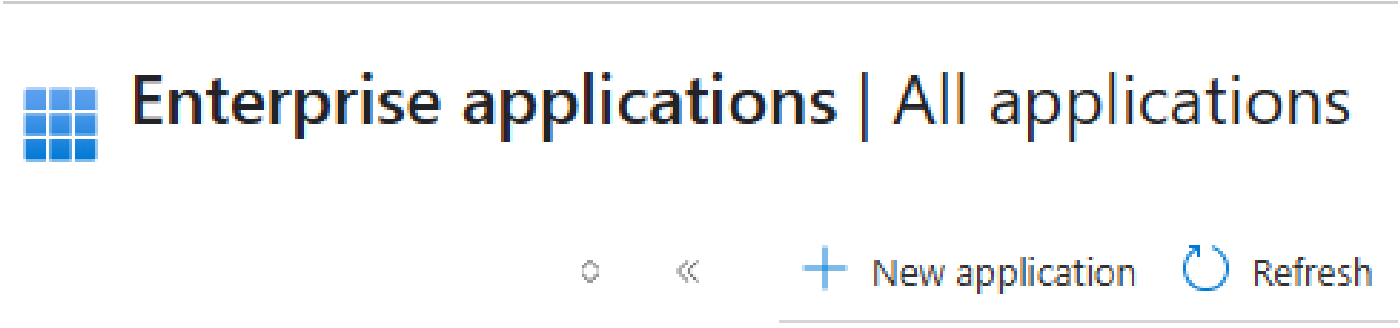
```
" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://vpn
</EntityDescriptor>
```

Microsoft Entra ID

1. Microsoft Azure 포털의 왼쪽 메뉴에서 Microsoft Entra ID를 선택합니다.

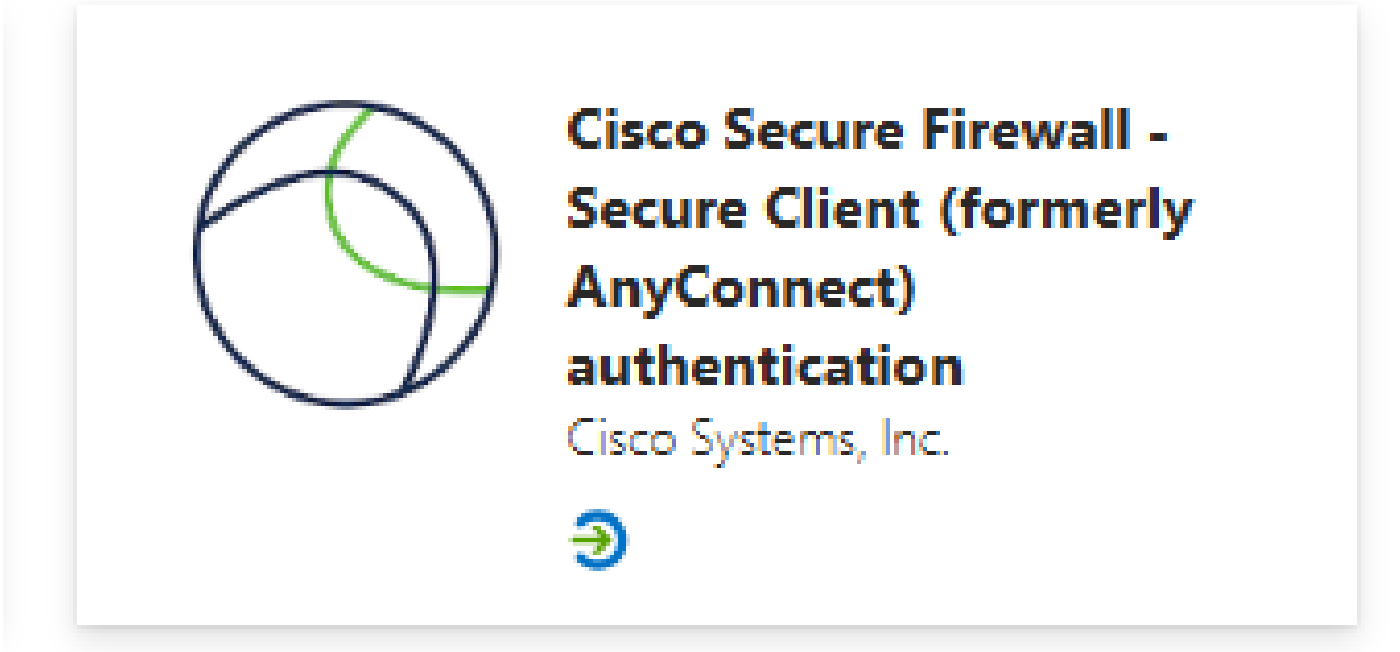

portal.azure.com/#home
VPN
Script
Troubleshooting
Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines

컨피그레이션에 대해 구성된 엔터프라이즈 애플리케이션이 이미 있는 경우, 다음 단계를 건너뛰고 7단계에서 계속합니다.



MS Entra ID 엔터프라이즈 애플리케이션

4. Featured Applications(주요 애플리케이션) 아래에서 Cisco Secure Firewall - Secure Client(이전의 AnyConnect) 인증을 선택합니다. 응용 프로그램에 이름을 지정하고 생성을 선택합니다.



MS Entra ID Cisco Secure Firewall Secure Client(이전의 AnyConnect) 인증 애플리케이션

5. 애플리케이션에서 사용자 및 그룹을 선택하고 필요한 사용자 또는 그룹 이름을 애플리케이션에 지정합니다.

Home > Enterprise applications | All

SAMLtest | Overvi

Enterprise Application

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

```
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
```

IdP에서 원하는 클레임을 보내고 있는지 확인하려면 VPN에 연결하는 동안 "debug webvpn saml 255"의 출력을 수집합니다. 디버그의 어설션 출력을 분석하고 특성 섹션을 IdP에 구성된 것과 비교합니다.

<#root>

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

SAMLtest-GP

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

문제 해결

<#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
```

관련 정보

Cisco 기술 지원 및 다운로드

ASA 컨피그레이션 가이드

FMC/FDM 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.