Configurar o AnyConnect com autenticação SAML no FTD gerenciado via FMC

Contents

Introdução

Este documento descreve a autenticação SAML (Security Assertion Markup Language) no FTD gerenciado no FMC.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Configuração do AnyConnect no Firepower Management Center (FMC)
- Valores SAML e metatada.xml

Componentes Utilizados

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

- Firepower Threat Defense (FTD) versão 6.7.0
- FMC versão 6.7.0
- ADFS do Servidor AD com SAML 2.0

Observação: Se possível, use um servidor NTP para sincronizar o horário entre o FTD e o IdP. Caso contrário, verifique se a hora é sincronizada manualmente entre eles.

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

A configuração permite que os usuários do AnyConnect estabeleçam uma autenticação de sessão VPN com um provedor de serviço de identidade SAML.

Algumas das limitações atuais do SAML são:

- O SAML no FTD é suportado para autenticação (versão 6.7 e superior) e autorização (versão 7.0 e superior).
- Os atributos de autenticação SAML disponíveis na avaliação DAP (semelhante aos atributos RADIUS enviados na resposta de autorização RADIUS do servidor AAA) não são suportados.
- O ASA oferece suporte ao grupo de túneis habilitado para SAML na política DAP. No entanto, você não pode verificar o atributo de nome de usuário com a autenticação SAML, pois o atributo de nome de usuário é mascarado pelo provedor de identidade SAML.
- Como o AnyConnect com o navegador incorporado usa uma nova sessão do navegador em cada tentativa de VPN, os usuários devem reautenticar sempre que o IdP usar cookies de sessão HTTP para rastrear o estado de login.
- Neste caso, o **Force Re-Authentication** definição em **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** não tem efeito na autenticação SAML iniciada pelo AnyConnect.

Mais limitações para SAML são descritas no link fornecido aqui.

Diretrizes e Limitações do SAML 2.0

Essas limitações se aplicam ao ASA e ao FTD: Diretrizes e Limitações para SAML 2.0.

Observação: todas as configurações SAML a serem implementadas no FTD podem ser encontradas no arquivo metadata.xml fornecido pelo seu IdP.

Configuração

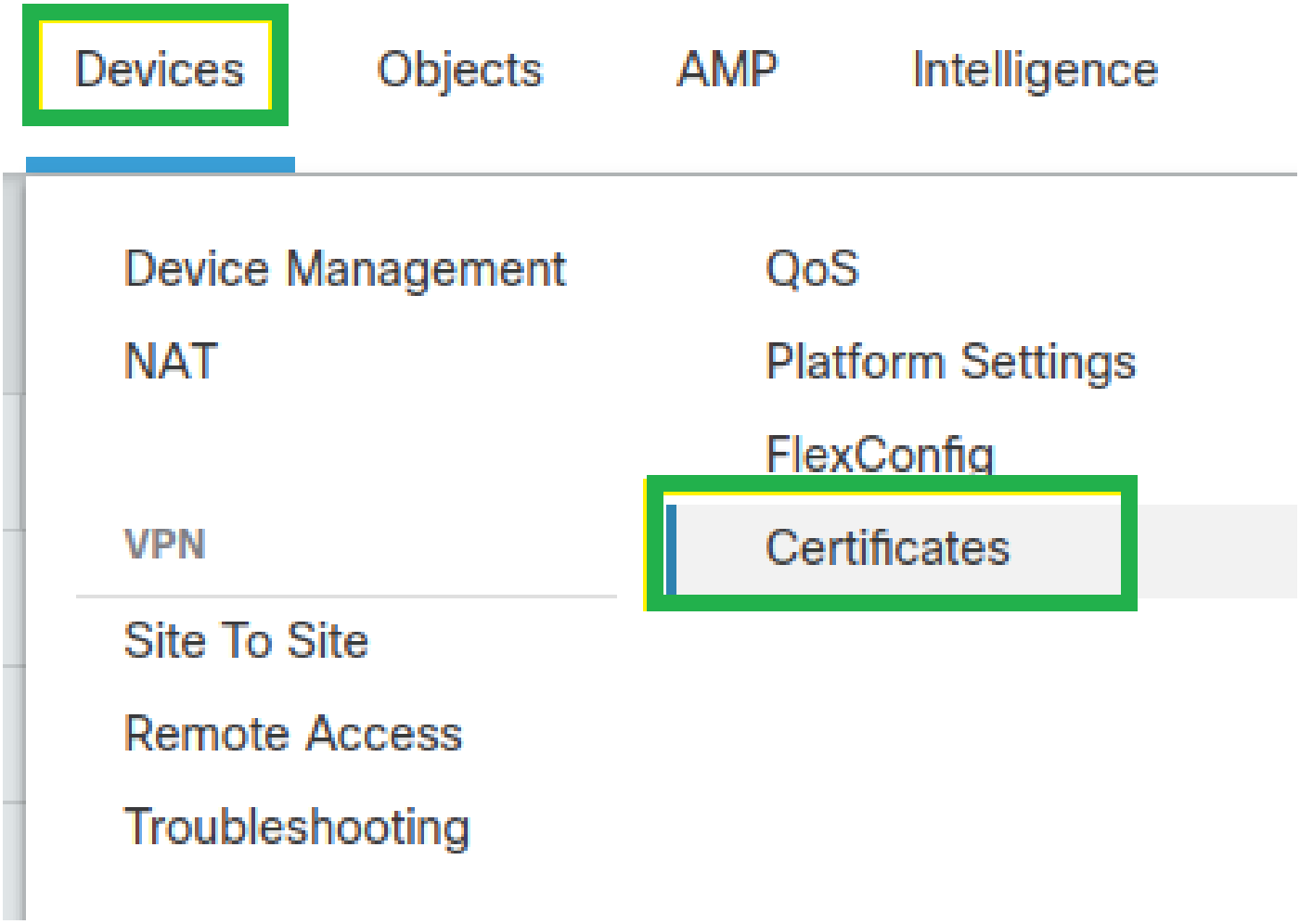
Esta seção descreve como configurar o AnyConnect com autenticação SAML no FTD

Obter os Parâmetros IdP SAML

Esta imagem mostra um arquivo metadata.xml do IdP SAML. Na saída, você pode obter todos os valores necessários para configurar o perfil do AnyConnect com SAML:

Configuração no FTD via FMC

Etapa 1. Instalar e registrar o certificado IdP no FMC. Navegue até **Devices** > **Certificates**.



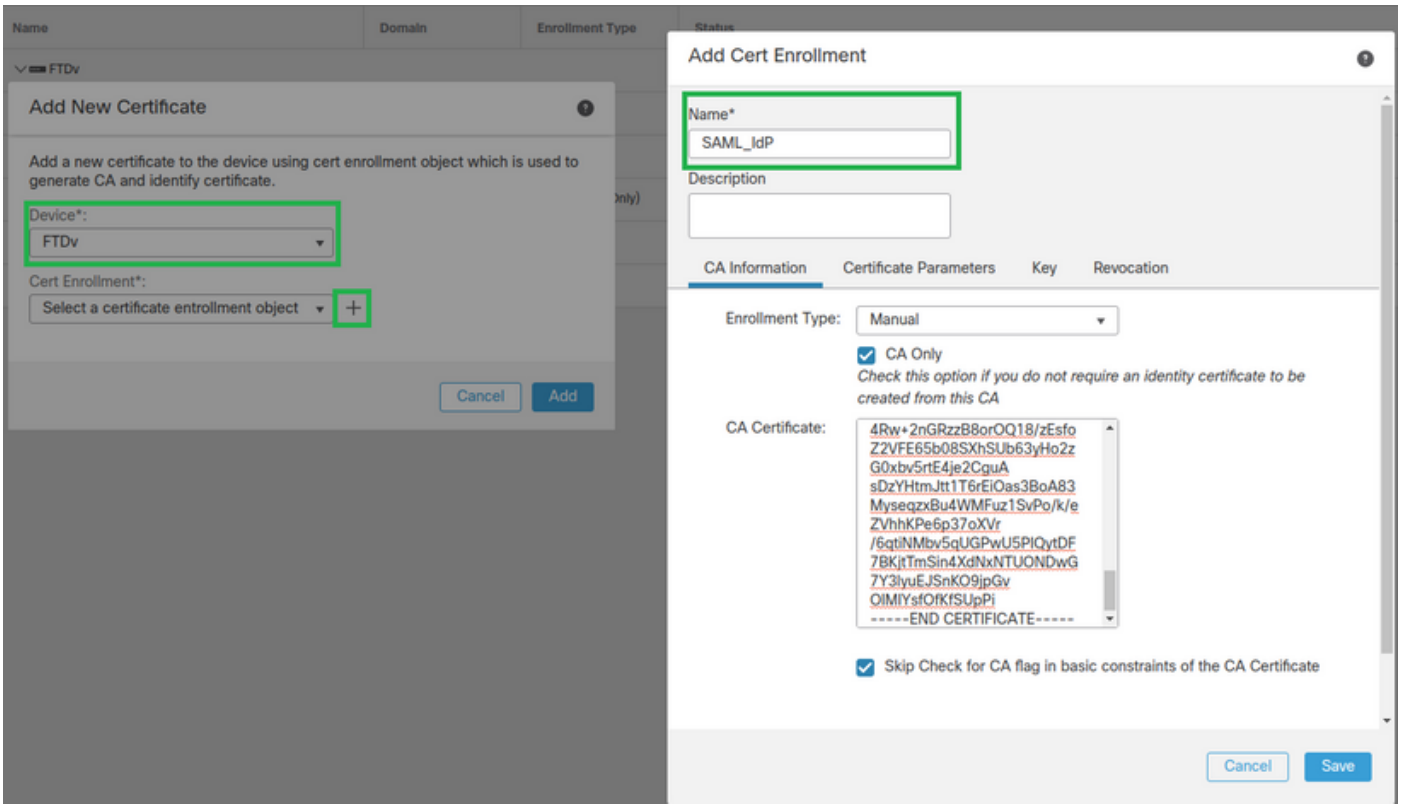
Etapa 2. Clique em **Add**. Selecione o FTD para se inscrever neste certificado. Em Cert Enrollment, clique no sinal de mais +.

No **Add Cert Enrollment** use qualquer nome como rótulo para o certificado IdP. Clique em **Manual**.

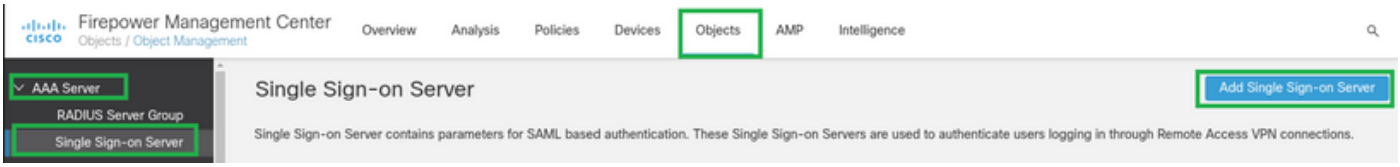
Marque a caixa **CA Only** e **Skip Check** para campos de flag CA.

Cole o **base64** formatar certificado IdP CA.

Clique em **Save** e clique em **Add**.



Etapa 3. Defina as configurações do servidor SAML. Navegue até **Objects** > **Object Management** > **AAA Servers** > **Single Sign-on** Server.Em seguida, selecione **Add Single Sign-on** Server.



Etapa 4. Com base na **metadata.xml** arquivo já fornecido pelo IdP, configure os valores SAML no **New Single Sign-on Server**.

```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.
```

New Single Sign-on Server

Name*

SAML_IdP

Identity Provider Entity ID*

http://saml.lab.local/adfs/services,

SSO URL*

https://saml.lab.local:444/adfs/ls/

Logout URL

https://saml.lab.local:444/adfs/ls/

Base URL

https://ftd.lab.local

Identity Provider Certificate*

SAML_IdP

Service Provider Certificate

SSL_Wildcard.lab.local

Request Signature

--No Signature--

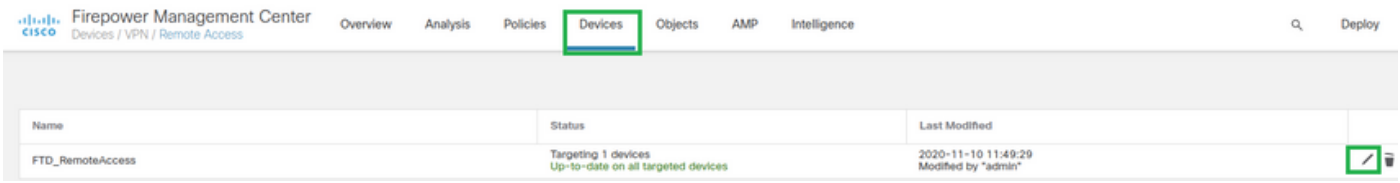
Request Timeout

Use the timeout set by the provide

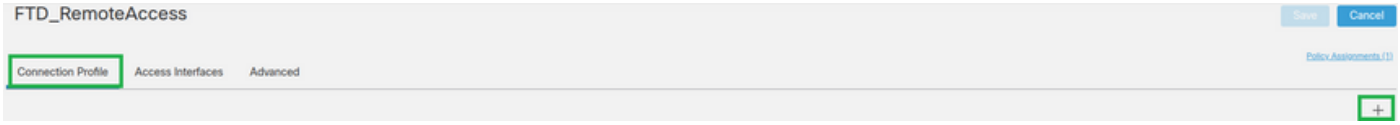
seconds (1-7200)

Cancel Save

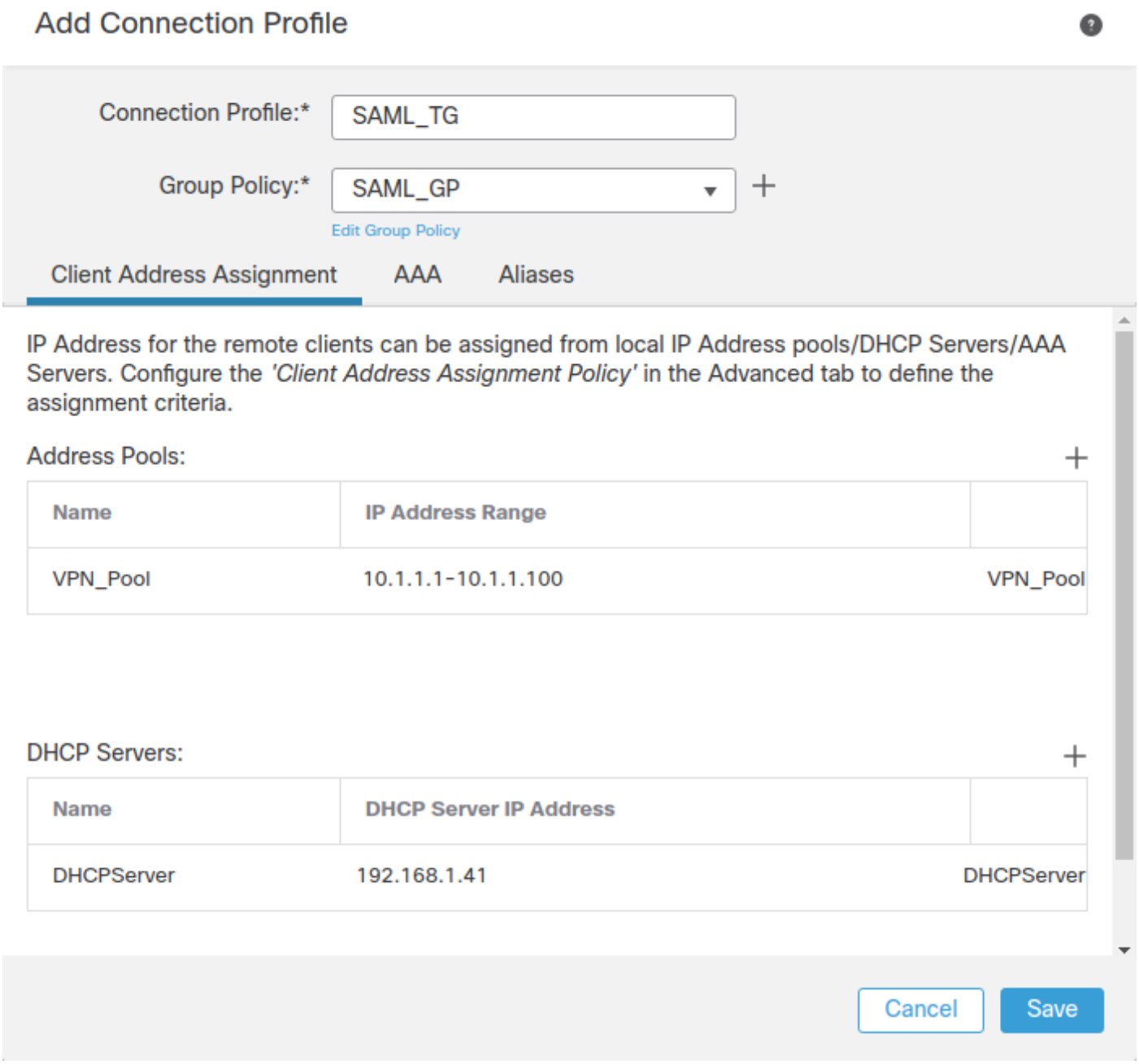
Etapa 5. Configurar o **Connection Profile** que usa esse método de autenticação. Navegue até **Devices** > **Remote Access** e, em seguida, edite seu VPN Remote Access configuração.



Etapa 6. Clique no sinal de mais + e adicione outro Perfil de conexão.

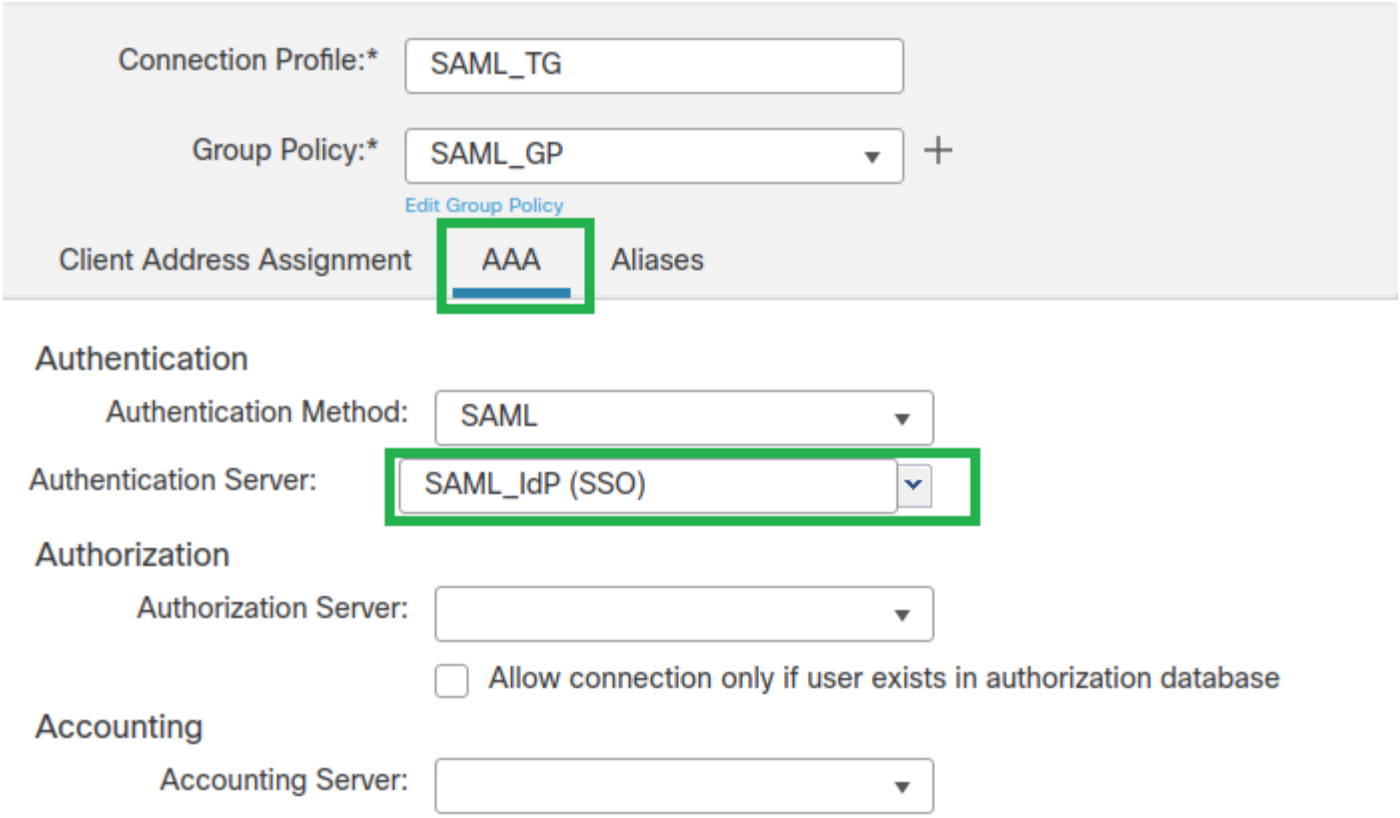


Passo 7. Crie o novo Perfil de Conexão e adicione a VPN, o Pool ou o Servidor DHCP apropriados.



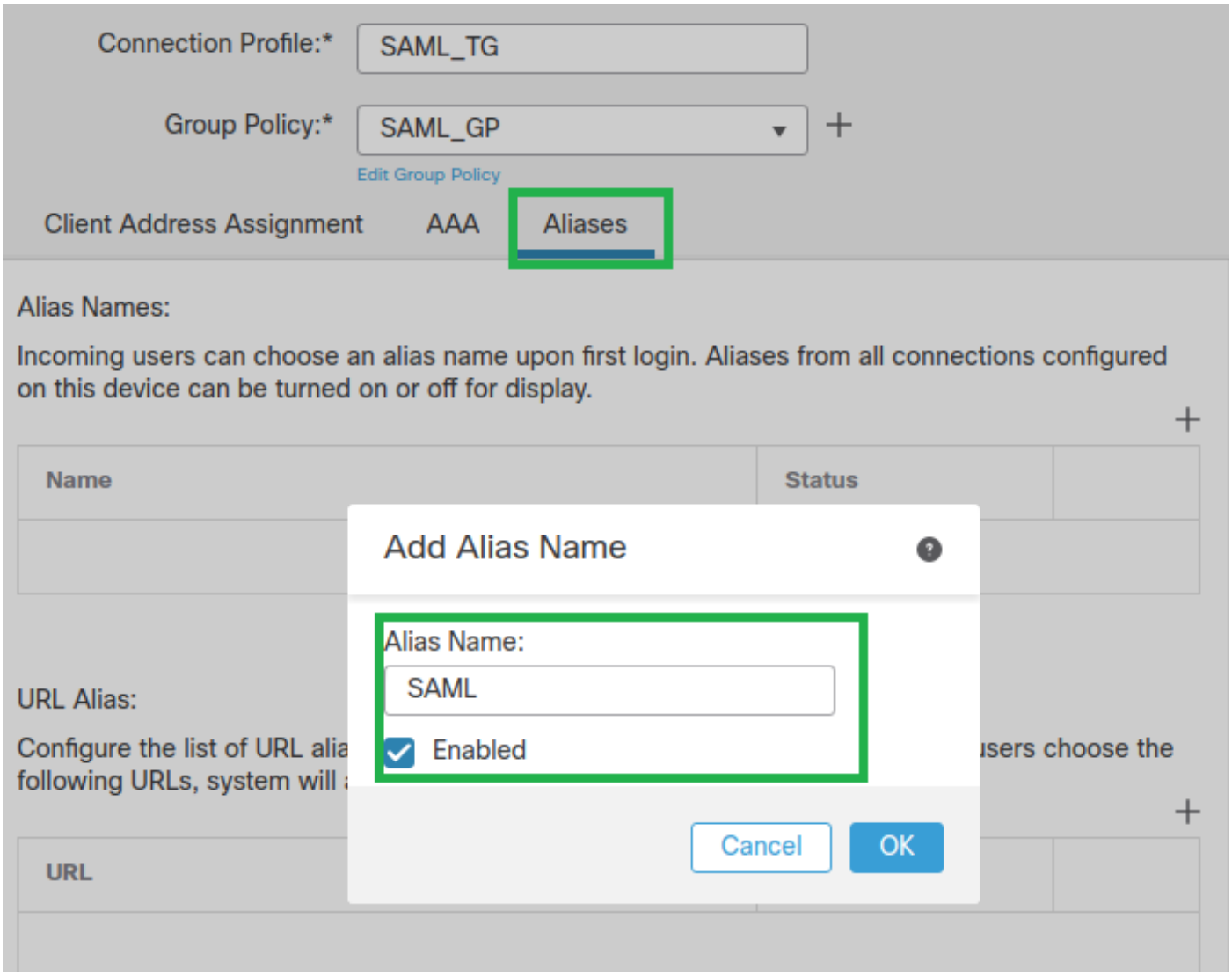
Etapa 8. Selecione a guia AAA. Sob o comando **Authentication Method** selecione SAML.

Sob o comando **Authentication Server** selecione o objeto SAML criado na Etapa 4.



Etapa 9. Crie um alias de grupo para mapear as conexões para este Perfil de Conexão. Essa é a marca que os usuários podem ver no menu suspenso Software AnyConnect.

Quando isso estiver configurado, clique em OK e salve a configuração completa da VPN de Autenticação SAML.



Etapa 10. Navegue até **Deploy** > **Deployment** e selecione o FTD apropriado para aplicar as alterações de VPN de autenticação SAML.

Etapa 11. Forneça o arquivo metadata.xml do FTD ao IDP para que ele adicione o FTD como um dispositivo confiável.

Na CLI do FTD, execute o comando **show saml metadata SAML_TG** onde SAML_TG é o nome do Perfil de Conexão criado na Etapa 7.

Esta é a saída esperada:

<#root>

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

show saml metadata SAML_TG

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<EntityDescriptor entityID="https://ftd.lab.local/saml/sp/metadata/SAML_TG" xmlns="urn:oasis:names:tc:S
<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>MIIF1zCCBL+gAwIBAgITYAAAABN6dX+H0cOFYwAAAAAAEzANBgkqhkiG9w0BAQsF
ADBAMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IsZAEZFgNsYWIx
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQy
MTlaMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQQDDAsqLmxhYi5sb2NhbDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfWk+V1f+YlsIE4hyY6+Qr1yKf
g1wEqLOFHtGVM3re/WmFuD+4sCyU1VkoiJhf2+X8tG7x2WTpKKtZM3N7bHpb7oPc
uz8N4GabfAIw287soLM521h6ZMO1bWGQOvxXR+xtCAyqz6JJdKOCNjNEdEkYcaG8
PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdic7btlQQPKG9JIaWny9RvHBmLgjOpx2i5Rp5k1JIECD9kHGj44O5lBEcv
OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWBBROkmTIhXT/
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWHlHqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V0lOLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNl
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXNOP2Jhc2U/b2JqZWNOQ2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMIGmBggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWNOQ2xhc3M9Y2VydGlmaWNhdGlv
bkF1dGhvcml0eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB
BAGCNxUIgYKsboLeOU6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR0l
BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG
AQUFBwMFBggrBgEFBQcDAgYEVR0lADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYFtSttz/9XlTAe1KbZOGlRVg9LblPiF17kZAxALjLJHlCTG
5EQSC1YqS31sTuarm4WPDJyMShc6hlUpswnCokGRMMgpx2GmDgv4Zf8SzJJ0NI4y
DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidpl+V9kp1RYamyjFUo+agx0E+L1zp8C
i0YEwYKXgKk3CZdwJfnYQuCWjmapYwlLGt5S59Uwegwro6AsUXY335+ZOrY/kuLF
tzR3/S90jDq6dqk=
</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ftd
</EntityDescriptor>

Depois que o metadata.xml do FTD é fornecido ao IdP e é como um dispositivo confiável, um teste na conexão VPN pode ser executado.

Verificar

Verifique se a conexão VPN AnyConnect foi estabelecida com SAML como um método de autenticação com os comandos vistos aqui:

<#root>

```
firepower#
```

show vpn-sessiondb detail AnyConnect

```
Session Type: AnyConnect Detailed
Username : xxxx  Index : 4
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384
Bytes Tx : 12772 Bytes Rx : 0
Pkts Tx : 10 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : SAML_GP Tunnel Group : SAML_TG
Login Time : 18:19:13 UTC Tue Nov 10 2020
Duration : 0h:03m:12s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : c0a801090000040005faad9a1
Security Grp : none Tunnel Zone : 0
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
AnyConnect-Parent:
Tunnel ID : 4.1
Public IP : 192.168.1.104
Encryption : none Hashing : none
TCP Src Port : 55130 TCP Dst Port : 443
```

Auth Mode : SAML

```
Idle Time Out: 30 Minutes Idle TO Left : 26 Minutes
Client OS : linux-64
Client OS Ver: Ubuntu 20.04.1 LTS (Focal Fossa)
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047
Bytes Tx : 6386 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
SSL-Tunnel:
Tunnel ID : 4.2
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2 TCP Src Port : 55156
TCP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Linux_64
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047
Bytes Tx : 6386 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
DTLS-Tunnel:
Tunnel ID : 4.3
Assigned IP : 10.1.1.1 Public IP : 192.168.1.104
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 40868
```

```
UDP Dst Port : 443 Auth Mode : SAML
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Linux_64
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 4.9.03047
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Troubleshooting

Alguns comandos de verificação na CLI de FTD podem ser usados para solucionar problemas de SAML e conexão de VPN de acesso remoto, conforme visto no parêntese:

<#root>

```
firepower#
show run webvpn

firepower#
show run tunnel-group

firepower#
show crypto ca certificate
firepower#
 debug webvpn saml 25
```

Observação: você também pode solucionar problemas do DART no PC do usuário do AnyConnect.

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.