Configuración de Anyconnect con Autenticación SAML en FTD Administrado a través de FMC

Contenido

Introducción

En este documento, se describe **Security Assertion Markup Language (SAML)** autenticación en FTD gestionado a través de FMC.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- **AnyConnect** configuración en FMC
- Valores SAML y metatada.xml

Componentes Utilizados

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

- **Firepower Threat Defense (FTD)** versión 6.7.0
- **Firepower Management Center (FMC)** versión 6.7.0
- ADFS desde **AD Server** con SAML 2.0

> **Nota:** Si es posible, utilice un servidor NTP para sincronizar la hora entre el FTD y el IdP. De lo contrario, compruebe que la hora se sincroniza manualmente entre ellos.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La configuración permite a los usuarios de Anyconnect establecer una autenticación de sesión VPN con un proveedor de servicios de identidad SAML.

Algunas de las limitaciones actuales para SAML son:

- SAML en FTD es compatible con la autenticación (versión 6.7 en adelante) y la autorización (versión 7.0 en adelante).
- Atributos de autenticación SAML disponibles en la evaluación DAP (similar a **RADIUS** atributos enviados **RADIUS** respuesta de autorización del servidor AAA).
- ASA admite el grupo de túnel habilitado para SAML en la política DAP. Sin embargo, no puede verificar el atributo username con autenticación SAML, porque el atributo username está enmascarado por el proveedor de identidad SAML.

- Porque **AnyConnect** con el navegador integrado que utiliza una nueva sesión del navegador en cada intento de VPN, los usuarios deben volver a autenticarse cada vez si el IdP utiliza cookies de sesión HTTP para rastrear el estado de inicio de sesión.
- En este caso, el **Force Re-Authentication** configuración en **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** no tiene ningún efecto en **AnyConnect** autenticación SAML iniciada.

En el enlace que se proporciona aquí se describen más limitaciones para SAML.

https://www.cisco.com/c/en/us/td/docs/security/asa/asa915/configuration/vpn/asa-915-vpn-config/webvpn-configure-users.html#reference_55BA48B37D6443BEA5D2F42EC21075B5

Estas limitaciones se aplican a ASA y FTD: "**Guidelines and Limitations for SAML 2.0**"

> **Nota:** Toda la configuración SAML que se implementará en el FTD se puede encontrar en el archivo metadata.xml proporcionado por su IdP.

Configuración

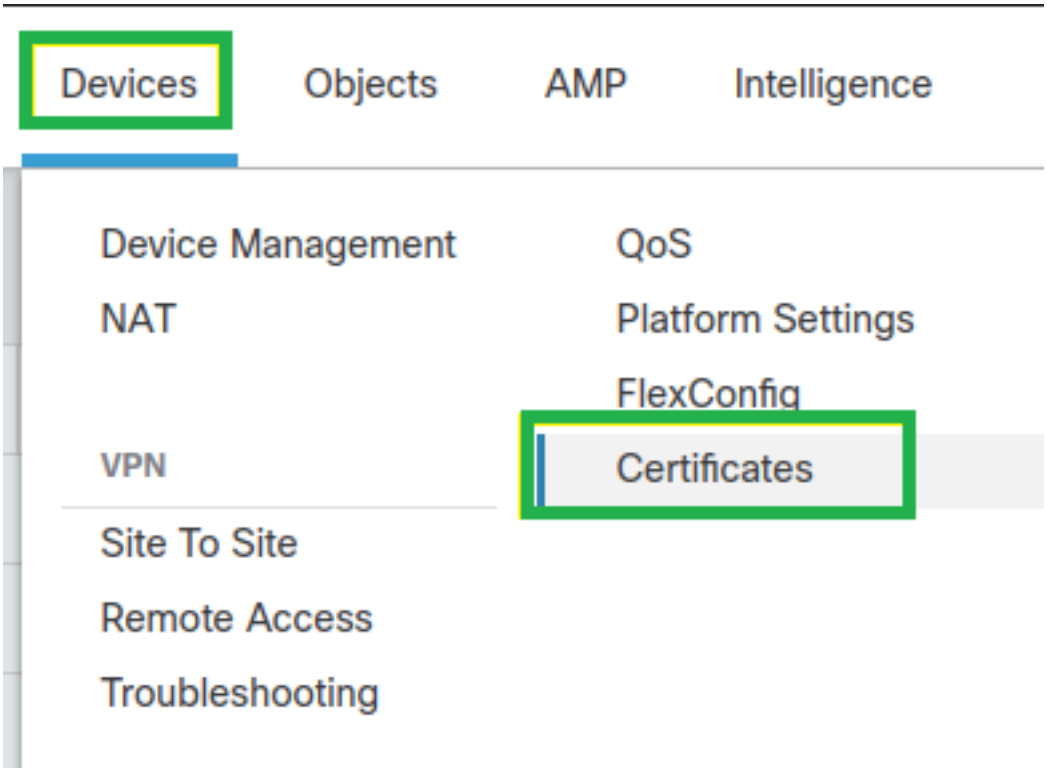
Esta sección describe cómo configurar **AnyConnect** con autenticación SAML en FTD

Obtener los parámetros IdP de SAML

Esta imagen muestra un archivo metadata.xml de SAML IdP. En el resultado, puede obtener todos los valores necesarios para configurar el **AnyConnect** perfil con SAML:

Configuración en el FTD mediante FMC

Paso 1. Instalar e inscribir el certificado IdP en el FMC. Vaya a **Devices > Certificates**



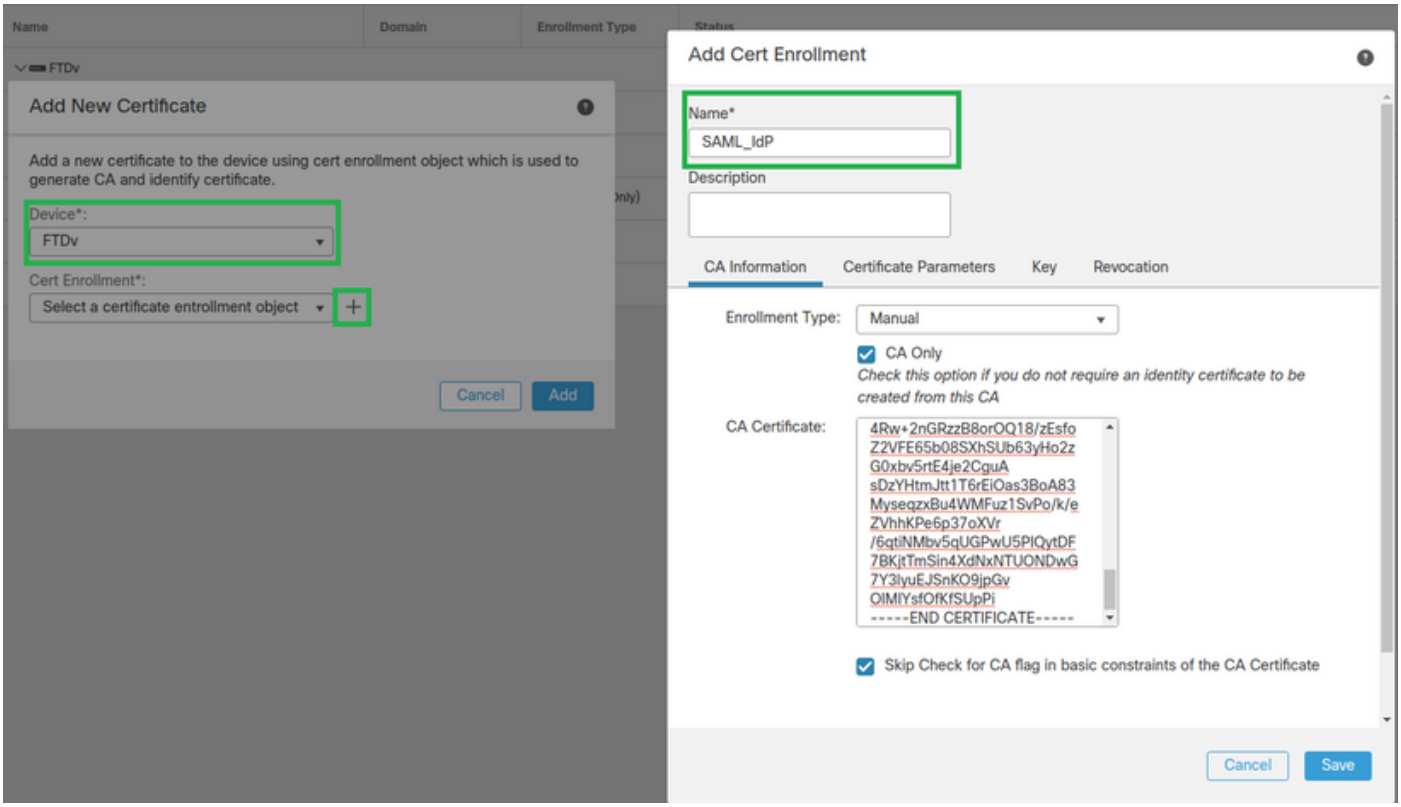
Paso 2. Haga clic en **Add**. Seleccione el FTD para inscribirse en este certificado. En Inscripción de certificados, haga clic en el signo **+** más

En el **Add Cert Enrollment** utilice cualquier nombre como etiqueta para el certificado de IdP. Haga clic **Manual**.

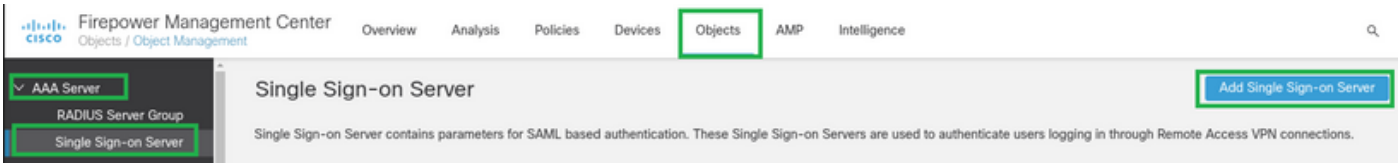
Compruebe el **CA Only** y **Skip Check** para campos de indicador de CA.

Pegue el **base64** format IdP CA cert.

Haga clic **Save** y, a continuación, haga clic en **Add**.

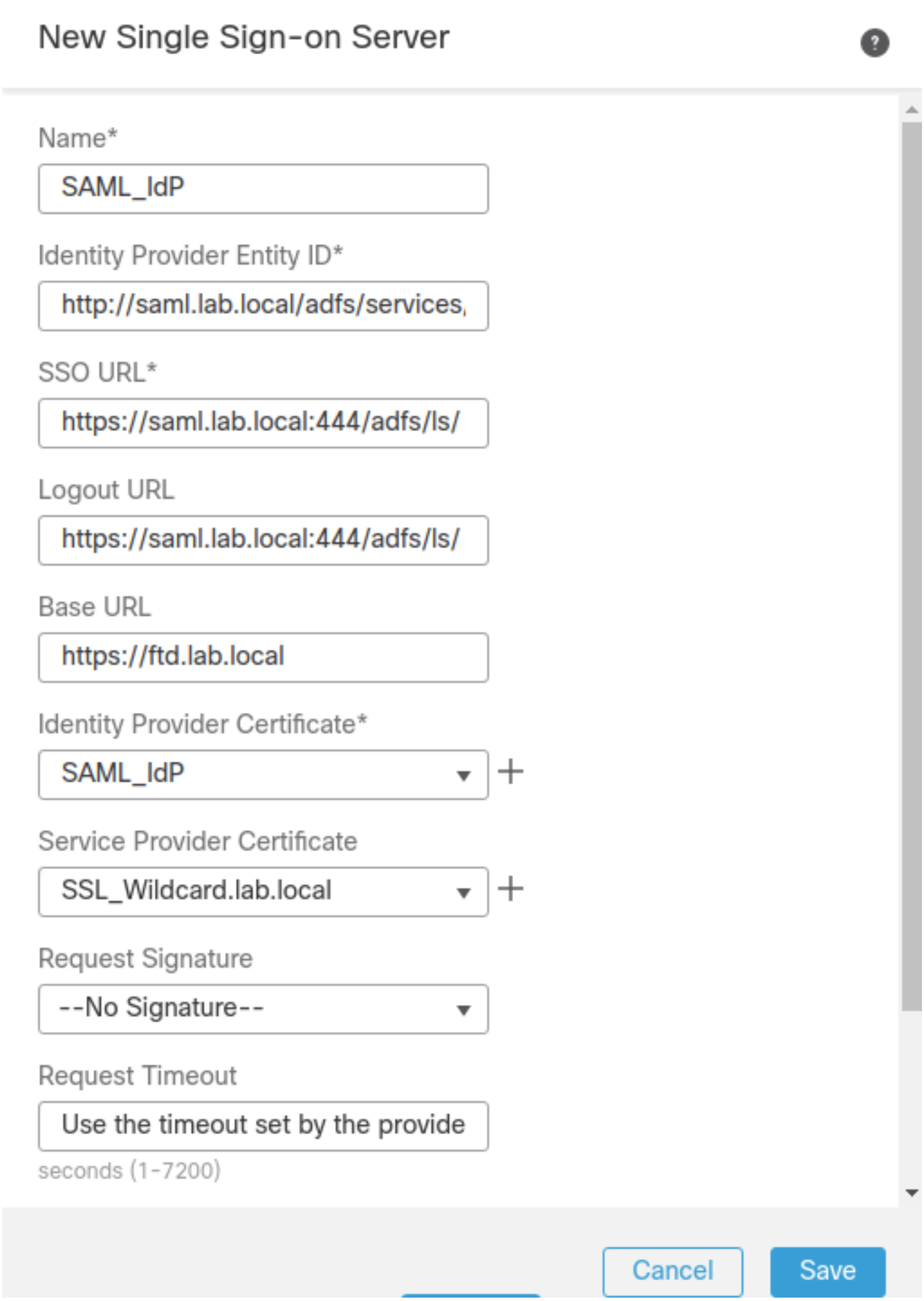


Paso 3. Configure los parámetros del servidor SAML. Vaya a **Objects > Object Management > AAA Servers > Single Sign-on Server**. A continuación, seleccione **Add Single Sign-on Server**.

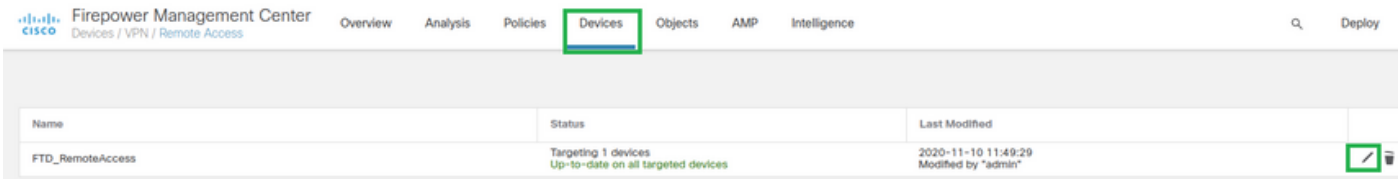


Paso 4. Basado en la **metadata.xml** proporcionado por su IdP, configure los valores SAML en el **New Single Sign-on Server**.

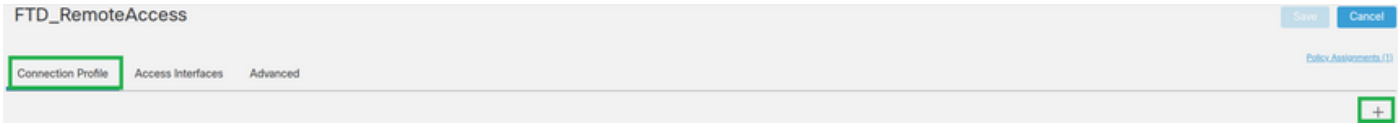
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



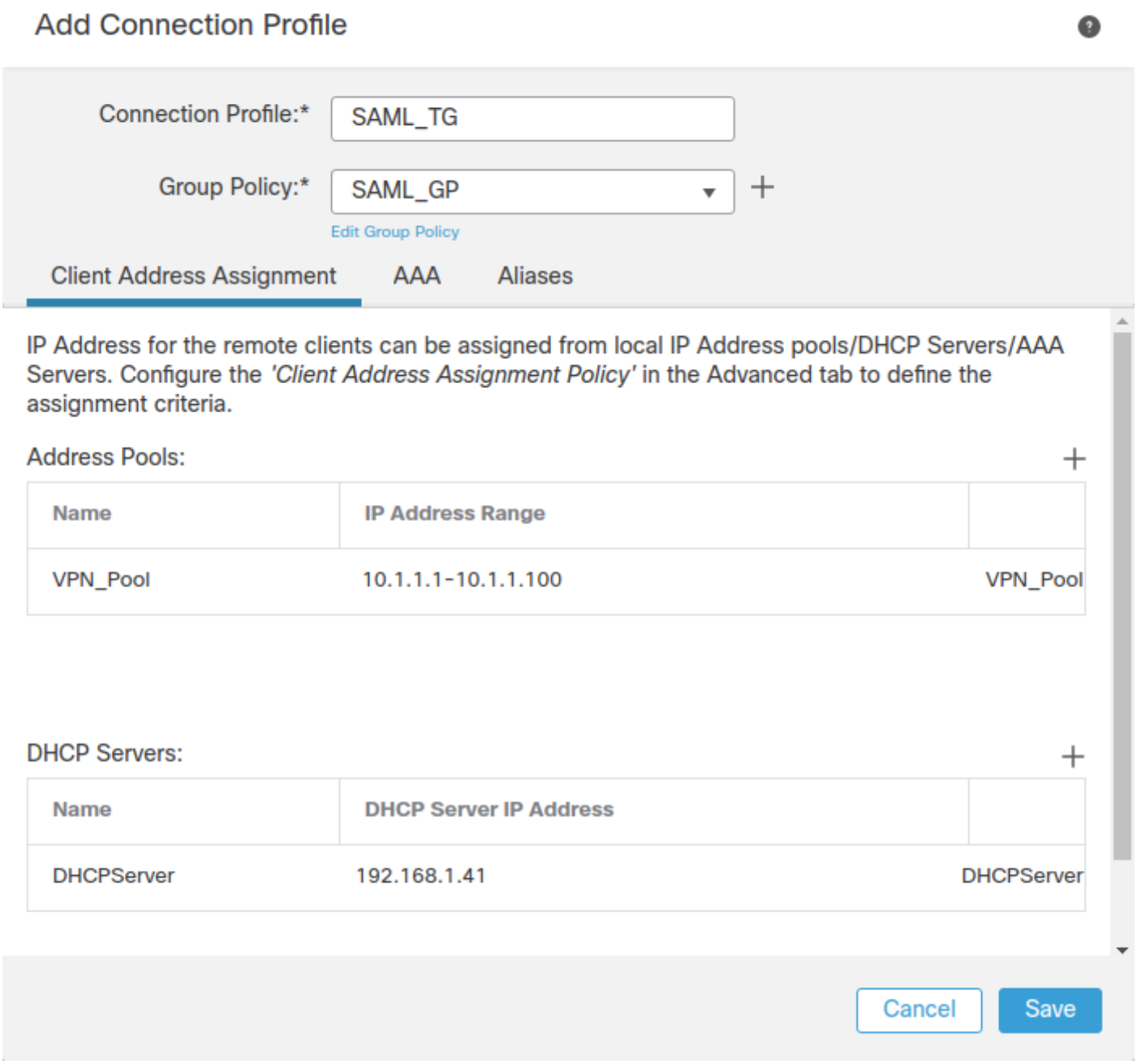
Paso 5. Configuración del **Connection Profile** que utiliza este método de autenticación. Vaya a **Devices > Remote Access** y, a continuación, editar el **VPN Remote Access** configuración.



Paso 6. Haga clic en el **signo** más**+** y agregue otro **Connection Profile**.

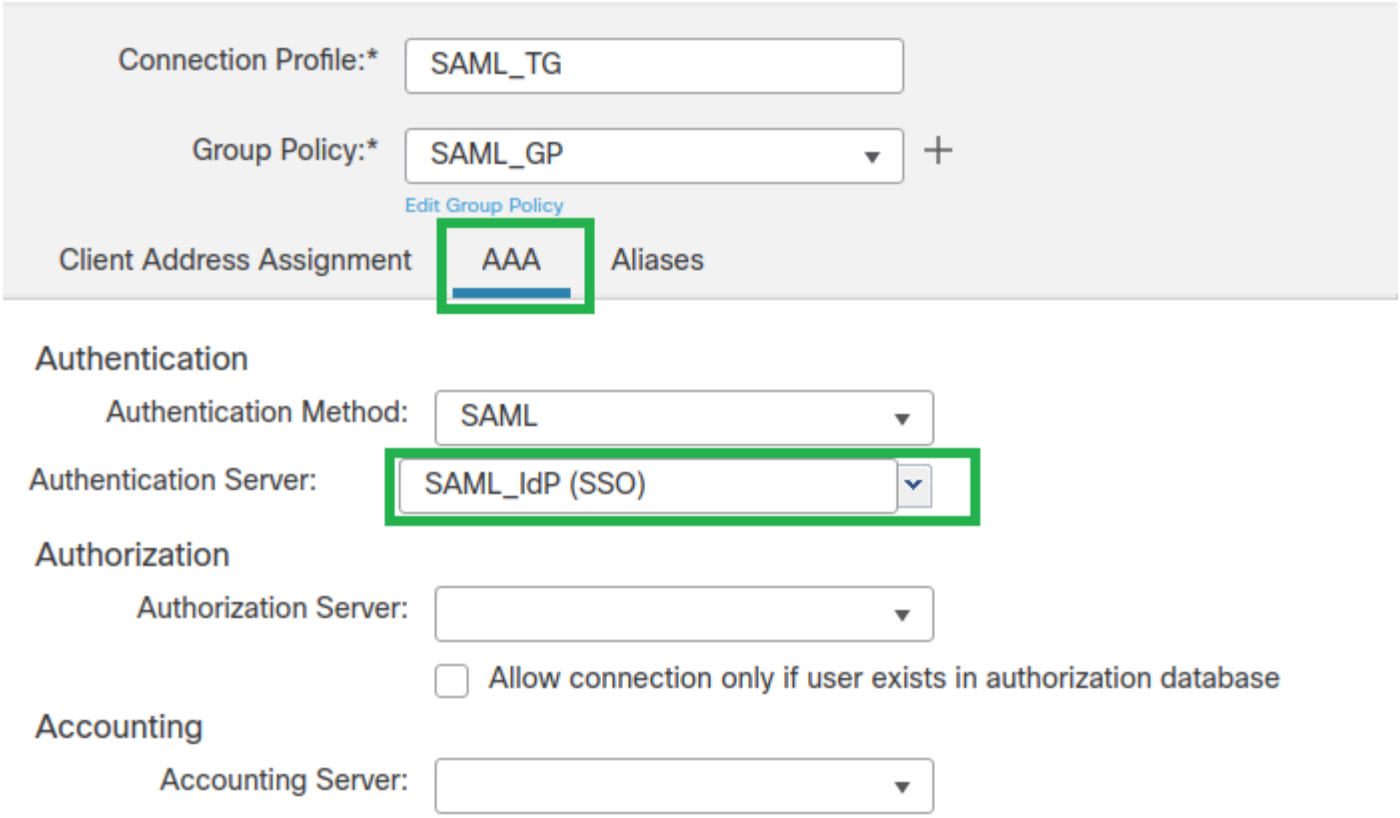


Paso 7. Cree el nuevo **Connection Profile** y agregue la VPN adecuada, **Pool**o servidor DHCP.



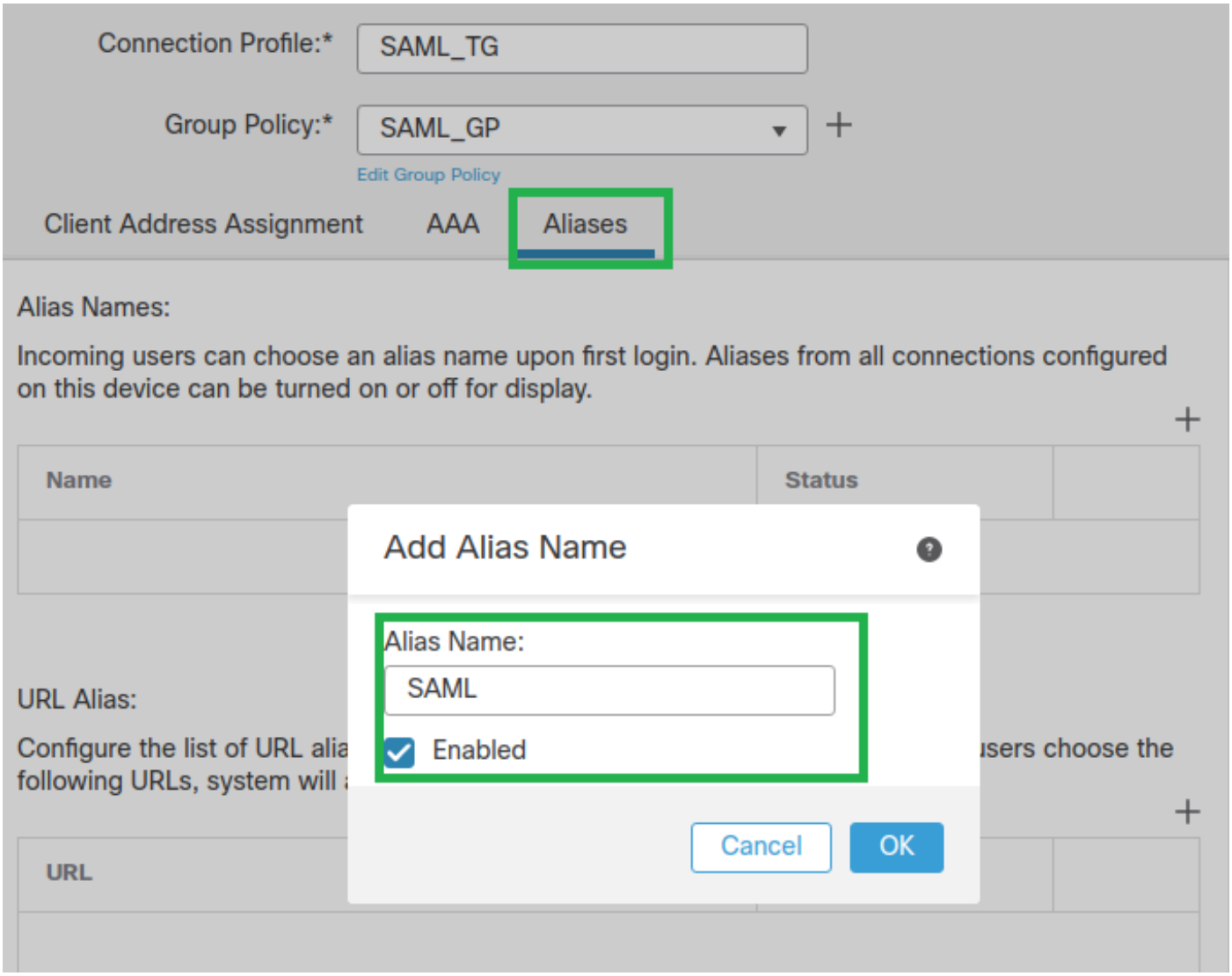
Paso 8. Seleccione la pestaña AAA. En la **Authentication Method** seleccione SAML.

En la **Authentication Server** seleccione el objeto SAML creado en el paso 4.



Paso 9. Cree un alias de grupo para asignar las conexiones a este **Connection Profile**. Esta es la etiqueta que los usuarios pueden ver en el **AnyConnect** Menú desplegable Software (Software).

Una vez configurado, haga clic en Aceptar y guarde el **SAML Authentication VPN** configuración.



Paso 10. Vaya a **Deploy > Deployment** y seleccione el FTD adecuado para aplicar el **SAML Authentication VPN** cambios.

Paso 11. Proporcionar el FTD **metadata.xml** al **IdP** para que agreguen el FTD como dispositivo de confianza.

En la CLI de FTD, ejecute el comando **show saml metadata SAML_TG** donde SAML_TG es el nombre del **Connection Profile** creado en el paso 7.

Este es el resultado esperado:

```
> 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:SAML:2.0:metadata">
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<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
uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8
PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdic7btlQQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44O5lBEcv
OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWBBROkmTIhXT/
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWHlHqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V0lOLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNl
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMIGmBggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
bkF1dGhvcml0eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR0l
BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG
AQUFBwMFBggrBgEFBQcDAgYEVR0lADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYFtSttz/9XlTAe1KbZ0GlRVg9LblPiF17kZAxALjLJHlCTG
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-POST"
Location="https://ftd.lab.local/+CSCOE+/saml/sp/acs?tgname=SAML_TG" />
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://ftd.lab.local/+CSCOE+/saml/sp/logout"/><SingleLogoutService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://ftd.lab.local/+CSCOE+/saml/sp/logout"/></SPSSODescriptor>
</EntityDescriptor>
```

Después del **metadata.xml** desde el FTD se proporciona al IdP y es como un dispositivo de confianza, se puede realizar una prueba bajo la conexión VPN.

Verificación

Compruebe que el **VPN AnyConnect** se estableció una conexión con SAML como método de autenticación con los comandos aquí vistos:

```
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
```

Troubleshoot

Algunos comandos de verificación en la CLI de FTD se pueden utilizar para solucionar problemas de SAML y **Remote Access VPN** conexión tal como se ve en el soporte:

```
firepower# show run webvpn
firepower# show run tunnel-group
firepower# show crypto ca certificate
firepower# debug webvpn saml 25
```

Nota: Puede solucionar problemas **DART** desde **AnyConnect** del usuario.

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).