在通过FMC管理的FTD上配置具有SAML身份验证的Anyconnect

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[获取SAML IdP参数](#)
[通过FMC在FTD上进行配置](#)
[验证](#)
[故障排除](#)

简介

本文档介绍 **Security Assertion Markup Language (SAML)** 通过FMC管理的FTD上的身份验证。

先决条件

要求

建议掌握下列主题的相关知识：

- **AnyConnect** fmc上的配置
- SAML和metatada.xml值

使用的组件

本文档中的信息基于以下软件和硬件版本：

- **Firepower Threat Defense (FTD)** 6.7.0 版
- **Firepower Management Center (FMC)** 6.7.0 版
- 来自 **AD Server** 使用SAML 2.0

> **注意：**如果可能，请使用NTP服务器同步FTD和IdP之间的时间。否则，请验证时间是否已在它们之间手动同步。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

配置允许Anyconnect用户与SAML身份服务提供商建立VPN会话身份验证。

SAML当前的一些限制包括：

- FTD上的SAML支持身份验证（从6.7版本开始）和授权（从7.0版本开始）。
- DAP评估中可用的SAML身份验证属性(类似于 **RADIUS** 属性发送于 **RADIUS** 不支持来自AAA服务器的授权响应。
- ASA在DAP策略上支持启用SAML的隧道组。但是，您无法使用SAML身份验证检查用户名属性，因为用户名属性由SAML身份提供程序进行屏蔽。

- 因为 **AnyConnect** 由于嵌入式浏览器在每次VPN尝试时都会使用新的浏览器会话，因此，如果IdP使用HTTP会话cookie来跟踪登录状态，则用户每次都必须重新进行身份验证。
- 在本例中， **Force Re-Authentication** 设置 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** 对 **AnyConnect** 已启动SAML身份验证。

此处提供的链接中介绍了更多限制或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

以下限制适用于ASA和FTD:"**Guidelines and Limitations for SAML 2.0**"

> **注意**：要在FTD上实施的所有SAML配置都可以在IdP提供的metadata.xml文件中找到。

配置

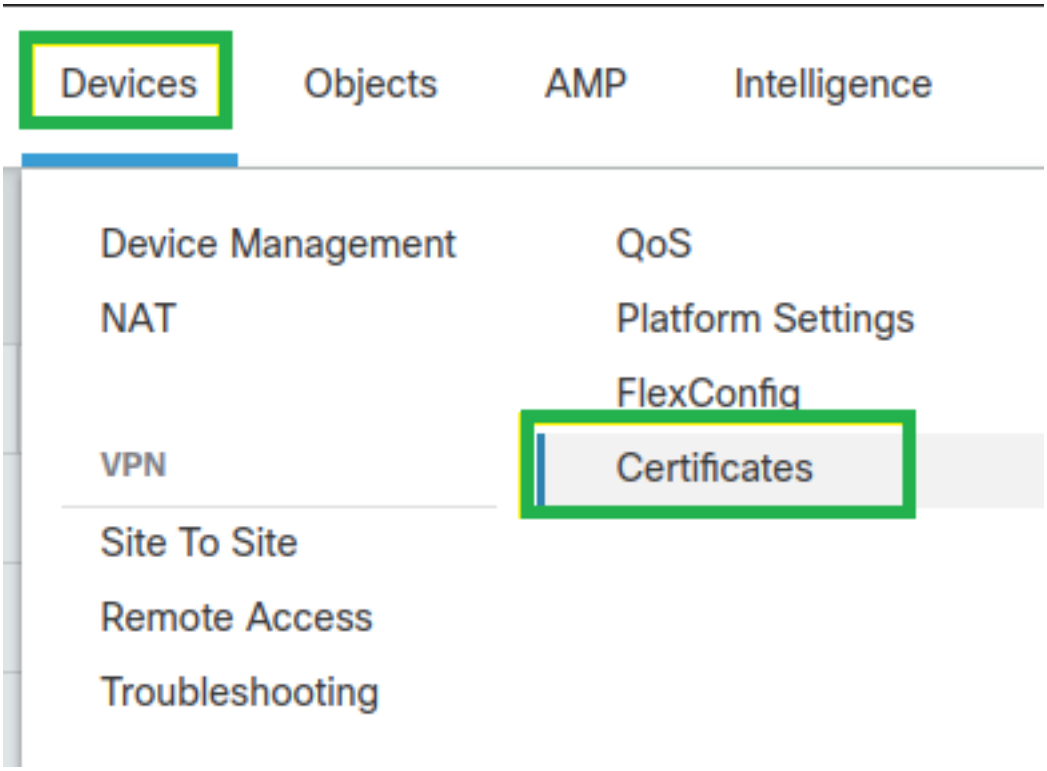
本节介绍如何配置 **AnyConnect** 在FTD上使用SAML身份验证

获取SAML IdP参数

此图像显示SAML IdP metadata.xml文件。从输出中，您可以获得配置 **AnyConnect** 具有SAML的配置文件：

通过FMC在FTD上进行配置

步骤1.在FMC上安装并注册IdP证书。导航至 **Devices > Certificates**



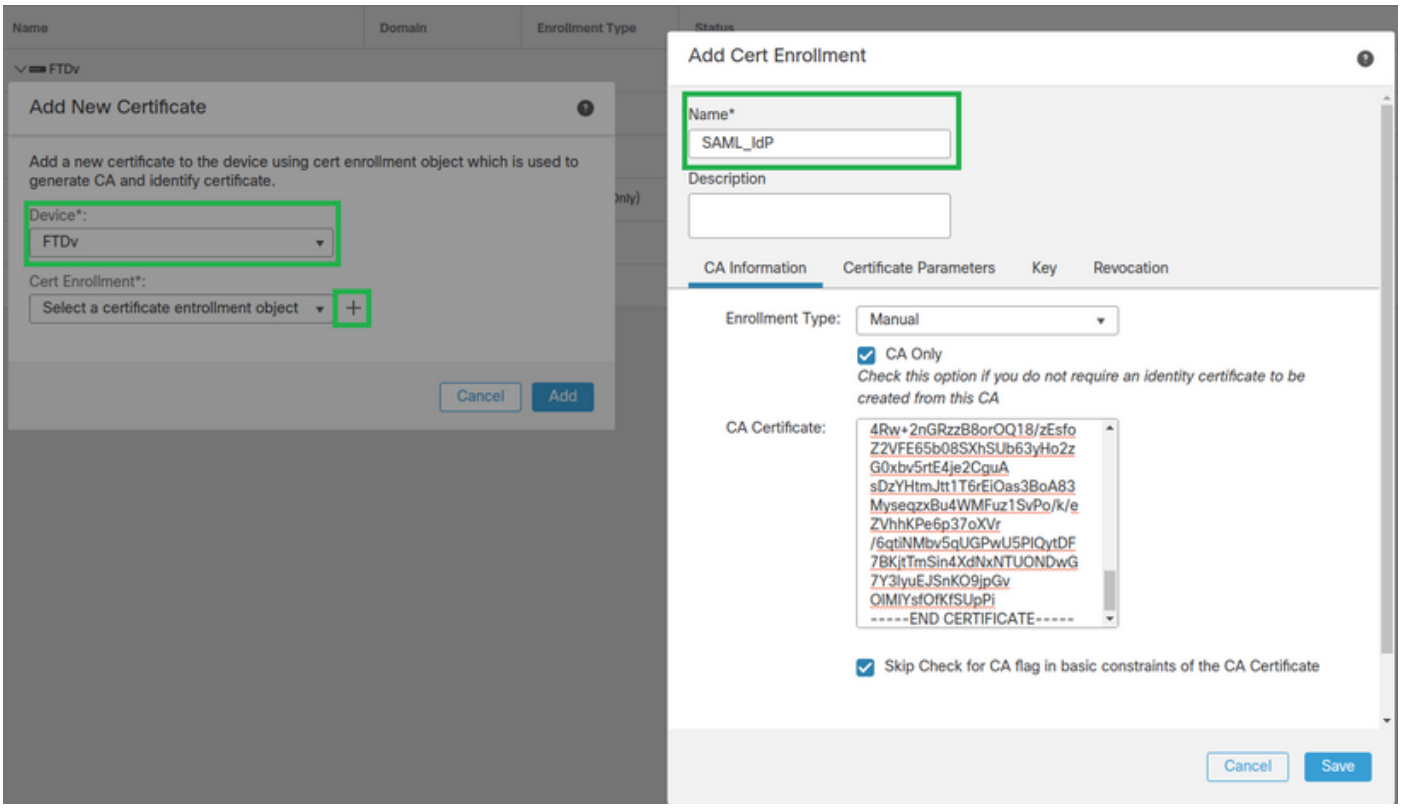
步骤2.单击 **Add**.选择要注册到此证书的FTD。在Cert Enrollment下，点击加号+号

如果 **Add Cert Enrollment** 部分，使用任意名称作为IdP证书的标签。点击 **Manual**.

查看 **CA Only** 和 **Skip Check** 用于CA标志字段。

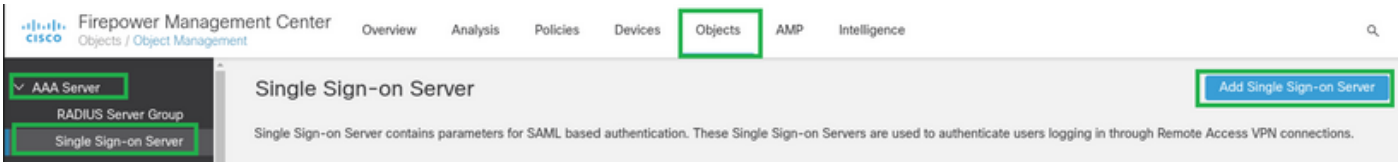
粘贴 **base64** 格式IdP CA证书。

点击 **Save** 然后单击 **Add**.



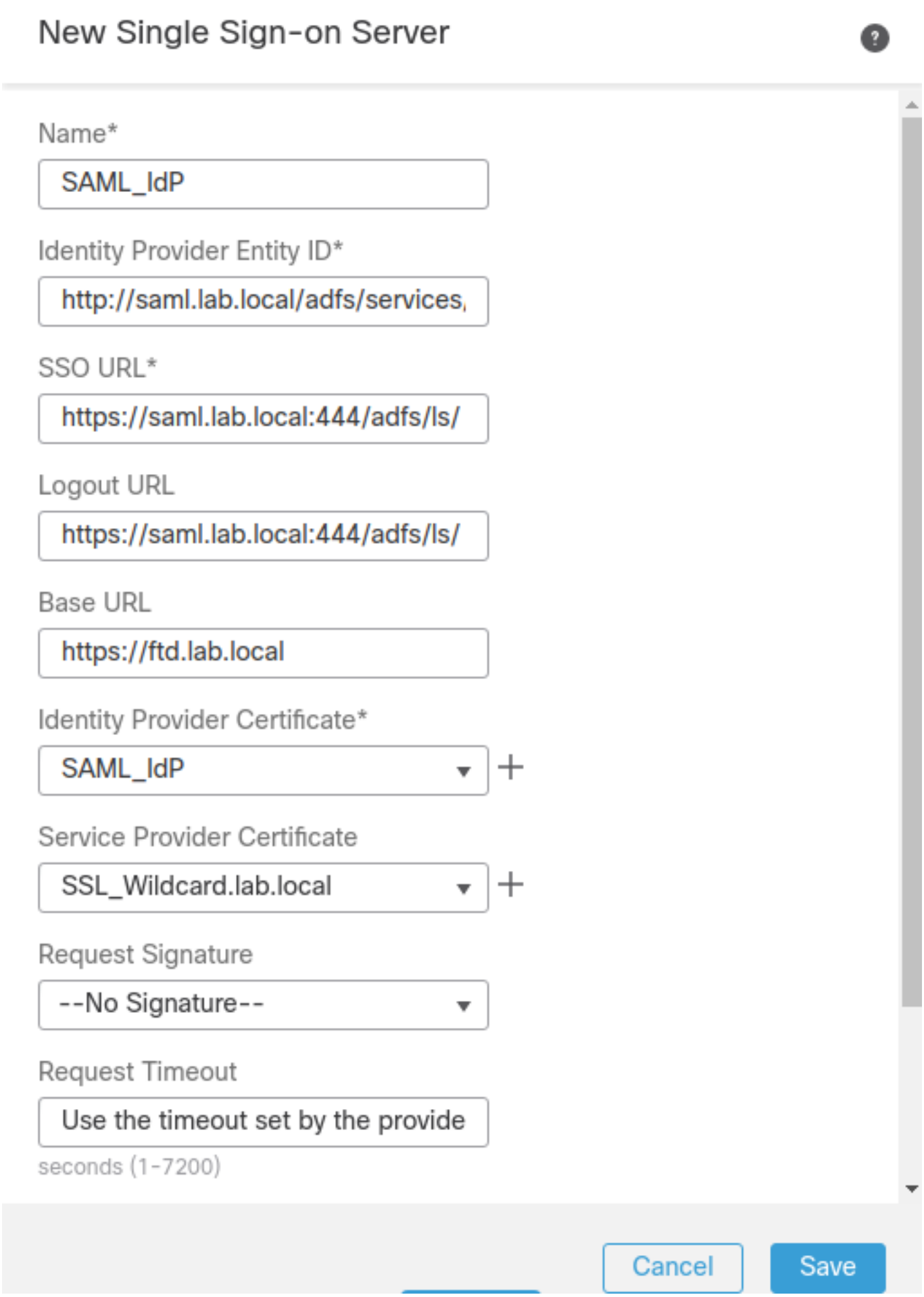
步骤3.配置SAML服务器设置。导航至 **Objects > Object Management > AAA Servers > Single Sign-on Server**.然

后，选择 **Add Single Sign-on Server**.

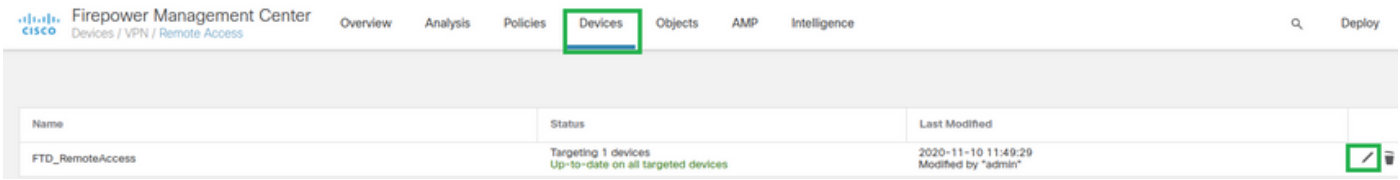


步骤4.基于 **metadata.xml** 文件，请配置 **New Single Sign-on Server**.

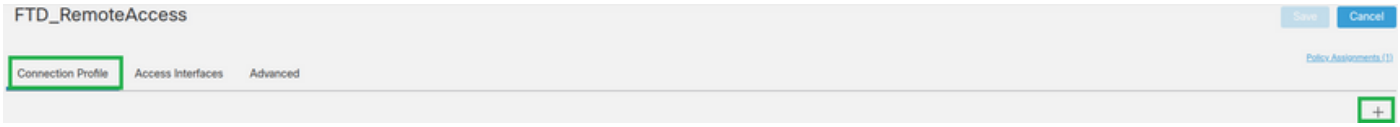
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



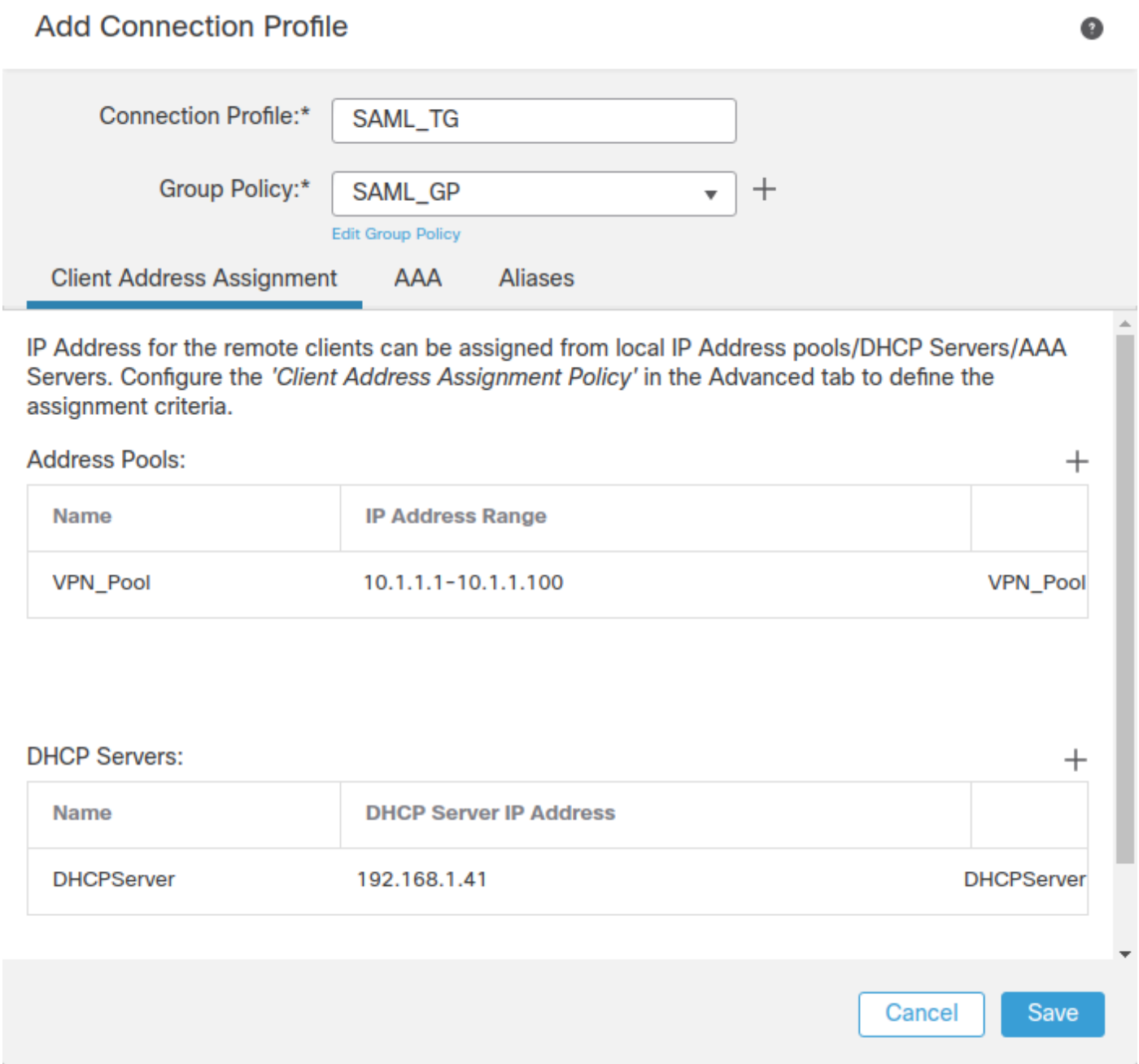
步骤5.配置 **Connection Profile** 使用此身份验证方法。导航至 **Devices > Remote Access** 然后编辑当前的 **VPN Remote Access** 配置.



步骤6.点击加号+**并添**加另一个 **Connection Profile.**

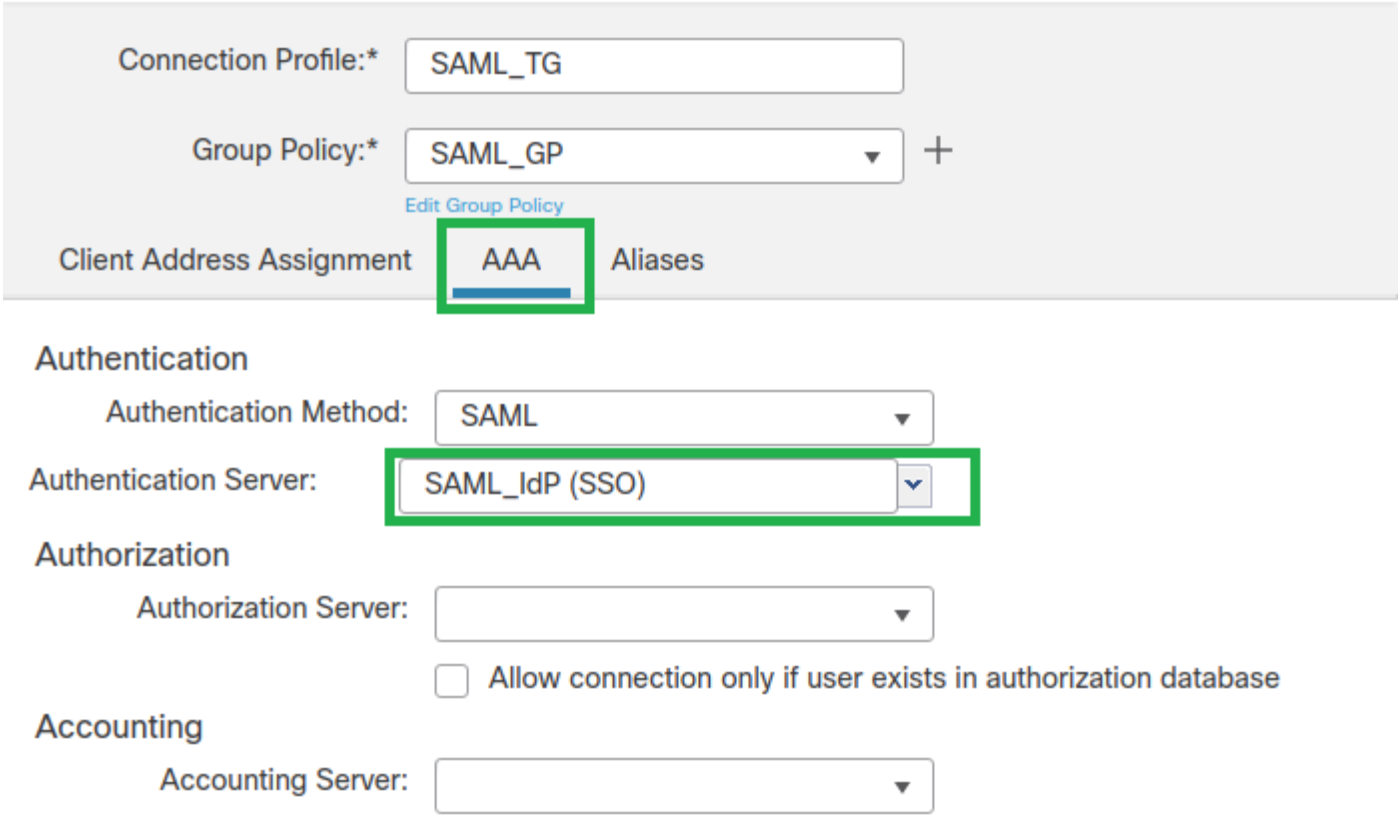


步骤7.创建新的 **Connection Profile** 并添加适当的VPN， **Pool**或DHCP服务器。



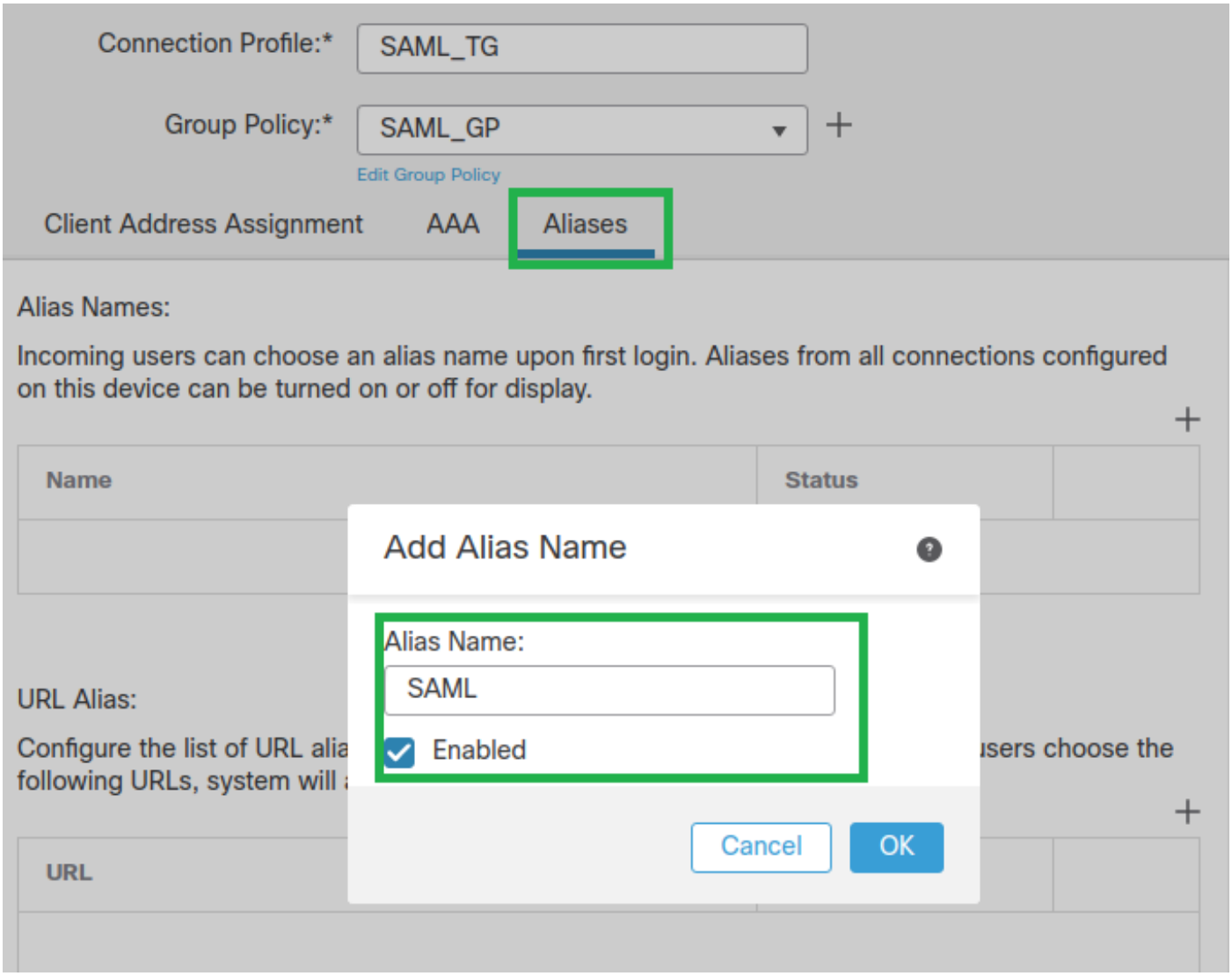
步骤8.选择AAA选项卡。在 **Authentication Method** 选项，选择SAML。

在 **Authentication Server** 选项，选择在第4步中创建的SAML对象。



步骤9.创建组别名以将连接映射到此组 **Connection Profile**.这是用户可以在 **AnyConnect** 软件下拉菜单。

配置完成后，点击OK并保存完整的 **SAML Authentication VPN** 配置.



步骤10.导航至 **Deploy > Deployment** 并选择适当的FTD **SAML Authentication VPN** 更改。

步骤11.提供FTD **metadata.xml** 将文件添加到**IdP**，以便将FTD添加为受信任设备。

在FTD CLI上，运行命令 **show saml metadata SAML_TG** 其中SAML_TG是 **Connection Profile** 创建时间：

这是预期输出：

```
> 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>
```

在 **metadata.xml** 从FTD提供给IdP，它作为受信任设备，可以执行VPN连接下的测试。

验证

验证 **VPN AnyConnect** 已使用SAML建立连接，作为身份验证方法，命令如下所示：

```
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 : c0a80109000040005faad9a1
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
```

故障排除

FTD CLI上的某些验证命令可用于排除SAML和 **Remote Access VPN** 如括号所示的连接：

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

注意：您可以进行故障排除 **DART** 从 **AnyConnect** 用户PC。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。