Configure AnyConnect met SAML-verificatie configureren op FTD beheerde via FMC

Inhoud

Inleiding

Dit document beschrijft **Security Assertion Markup Language (SAML)** verificatie op FTD beheerd via FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

- **AnyConnect** configuratie op VCC
- SAML- en metatada.xml-waarden

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- **Firepower Threat Defense (FTD)** versie 6.7.0
- **Firepower Management Center (FMC)** versie 6.7.0
- ADFS van **AD Server** met SAML 2.0

  Opmerking: Gebruik indien mogelijk een NTP-server om de tijd tussen de FTD en IdP te synchroniseren. Controleer anders of de tijd handmatig tussen de twee wordt gesynchroniseerd.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Met de configuratie kunnen AnyConnect-gebruikers een VPN-sessieverificatie instellen bij een SAML Identity Service Provider.

Momenteel gelden voor SAML onder meer de volgende beperkingen:

- SAML on FTD wordt ondersteund voor verificatie (versie 6.7 en verder) en autorisatie (versie 7.0 en verder).
- SAML-verificatiekenmerken beschikbaar in DAP-evaluatie (vergelijkbaar met **RADIUS** eigenschappen verzonden **RADIUS** autorisatiereactie van AAA-server) niet ondersteund.
- ASA ondersteunt SAML-enabled tunnelgroep op DAP-beleid. U kunt het kenmerk gebruikersnaam echter niet controleren met SAML-verificatie, omdat het kenmerk gebruikersnaam wordt gemaskeerd door de SAML Identity provider.

- Omdat **AnyConnect** als de ingesloten browser een nieuwe browser sessie gebruikt op elke VPN-poging, moeten gebruikers elke keer opnieuw authenticeren als de IDP HTTP-sessiecookies gebruikt om de inlogstatus bij te houden.
- In dit geval **Force Re-Authentication** instelling **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** heeft geen effect op **AnyConnect** gestart met SAML-verificatie.

Meer beperkingen voor SAML worden beschreven in de link hier.

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

Deze beperkingen zijn van toepassing op ASA en FTD: "**Guidelines and Limitations for SAML 2.0**"

> **Opmerking:** Alle SAML-configuratie die op de FTD moet worden geïmplementeerd, vindt u in het bestand metadata.xml dat door uw IdP wordt geleverd.

Configuratie

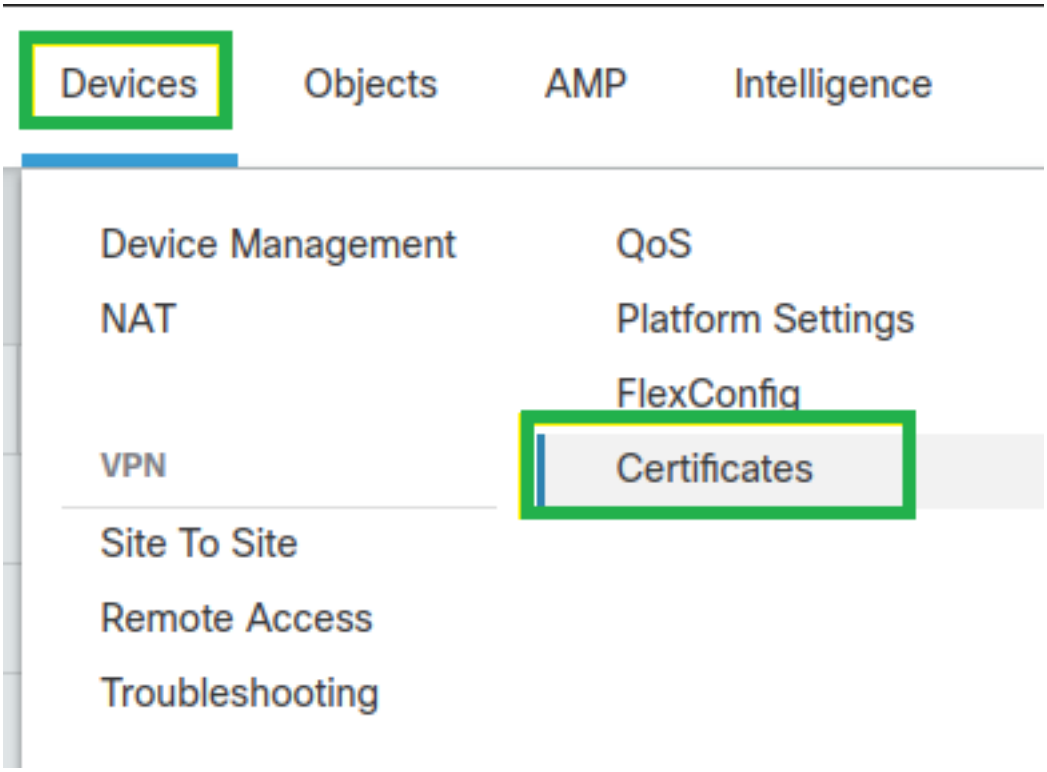
In deze sectie wordt beschreven hoe u **AnyConnect** met SAML-verificatie op FTD

De SAML IDP-parameters ophalen

Dit beeld toont een SAML IdP metadata.xml bestand. Van de output, kunt u alle waarden verkrijgen die worden vereist om te vormen **AnyConnect** profiel met SAML:

Configuratie op het FTD via het VCC

Stap 1. Installeer en registreer het IDp-certificaat in het VCC. Navigeer naar **Devices > Certificates**



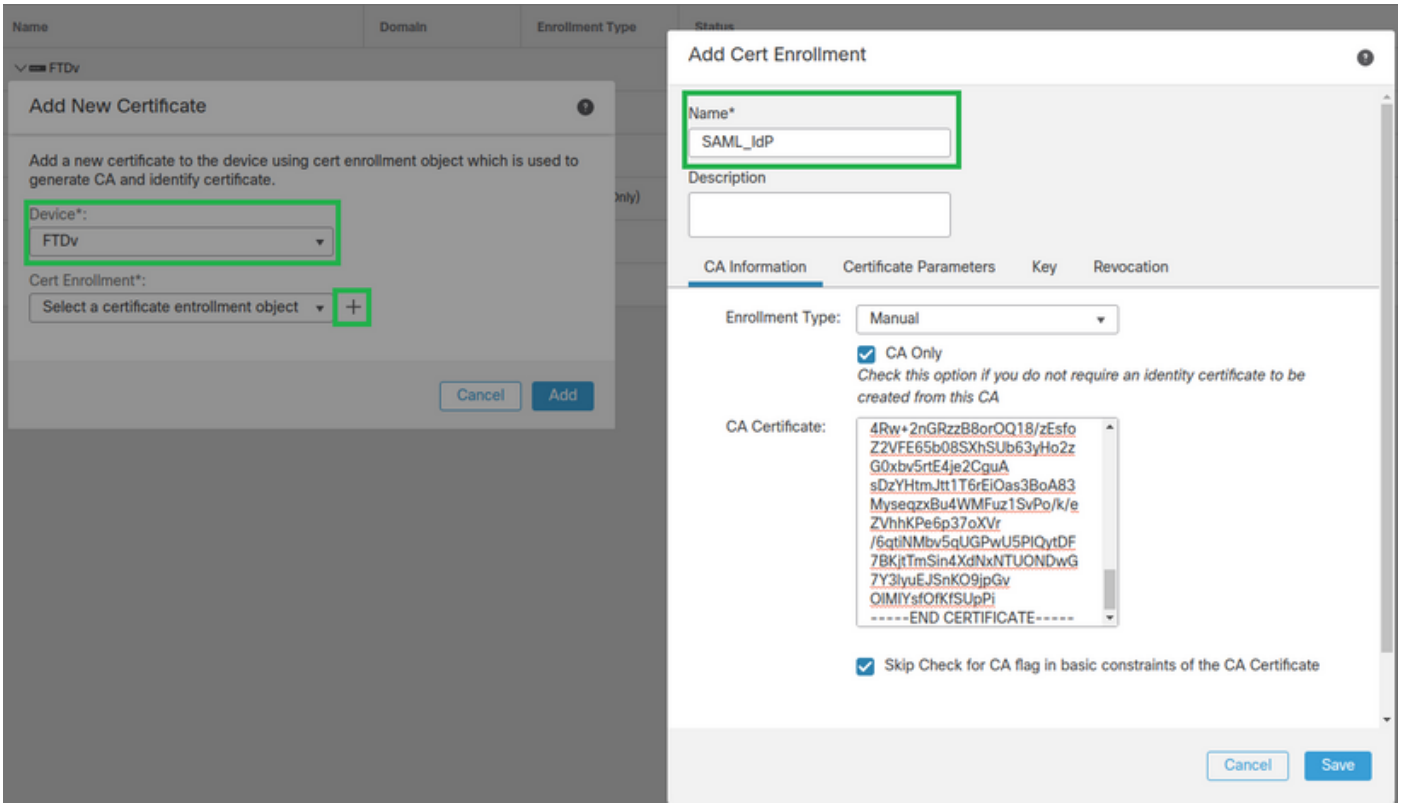
Stap 2. Klik op **Add**. Selecteer de FTD om in te schrijven op dit certificaat. Klik onder Inschrijving behouden op het plusteken **+**.

In het **Add Cert Enrollment** deel, gebruik om het even welke naam als etiket voor de cert IdP. Klik **Manual**.

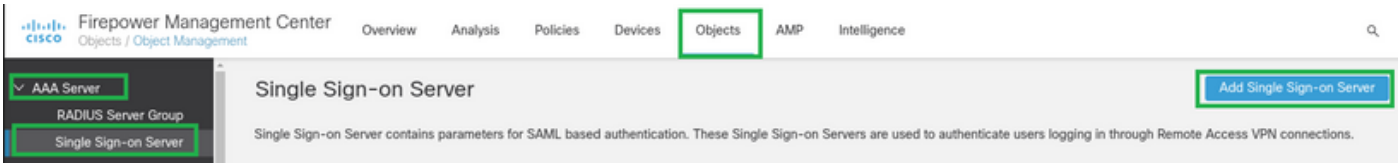
Controleer de **CA Only** en **Skip Check** voor CA-vlagvelden.

Plakt het **base64** formaat IDp CA cert.

Klik **Save** en klik vervolgens op **Add**.

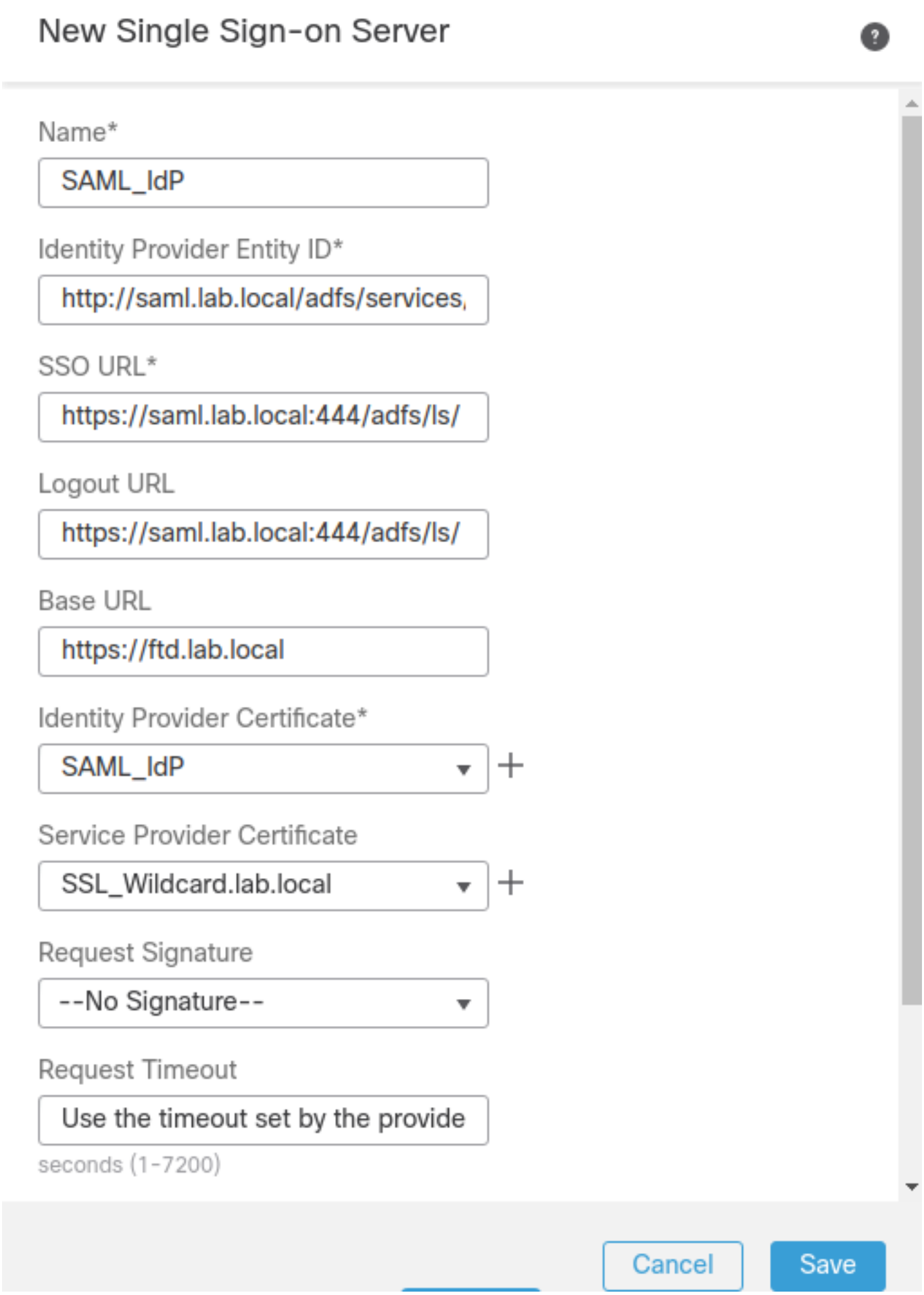


Stap 3. Configureer de SAML-serverinstellingen. Navigeer naar **Objects > Object Management > AAA Servers > Single Sign-on Server**. Selecteer vervolgens **Add Single Sign-on Server**.

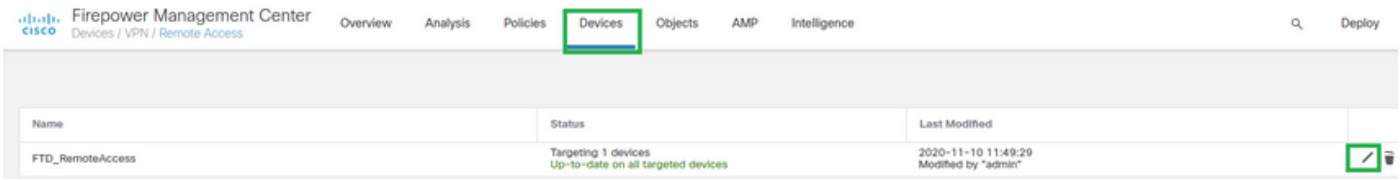


Stap 4. Gebaseerd op de **metadata.xml** bestand reeds verstrekt door uw IDp, de SAML-waarden configureren op de **New Single Sign-on Server**.

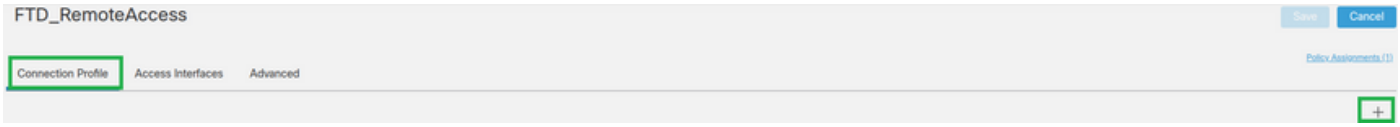
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



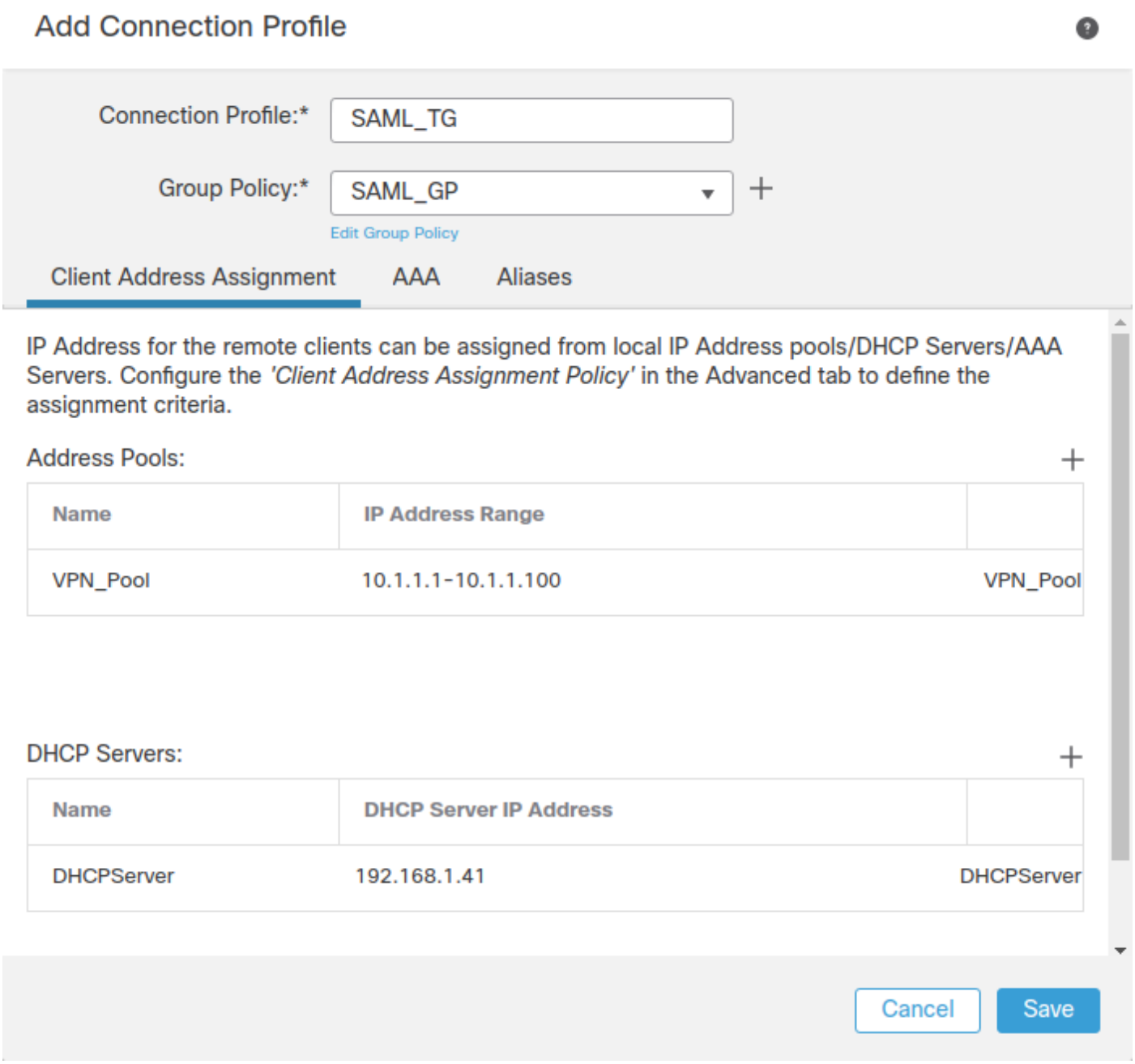
Stap 5. Configureer de **Connection Profile** die deze verificatiemethode gebruikt. Navigeer naar **Devices > Remote Access** en bewerk vervolgens uw huidige **VPN Remote Access** configuratie.



Stap 6. Klik op het plusteken **+** en voeg er een toe **Connection Profile**.

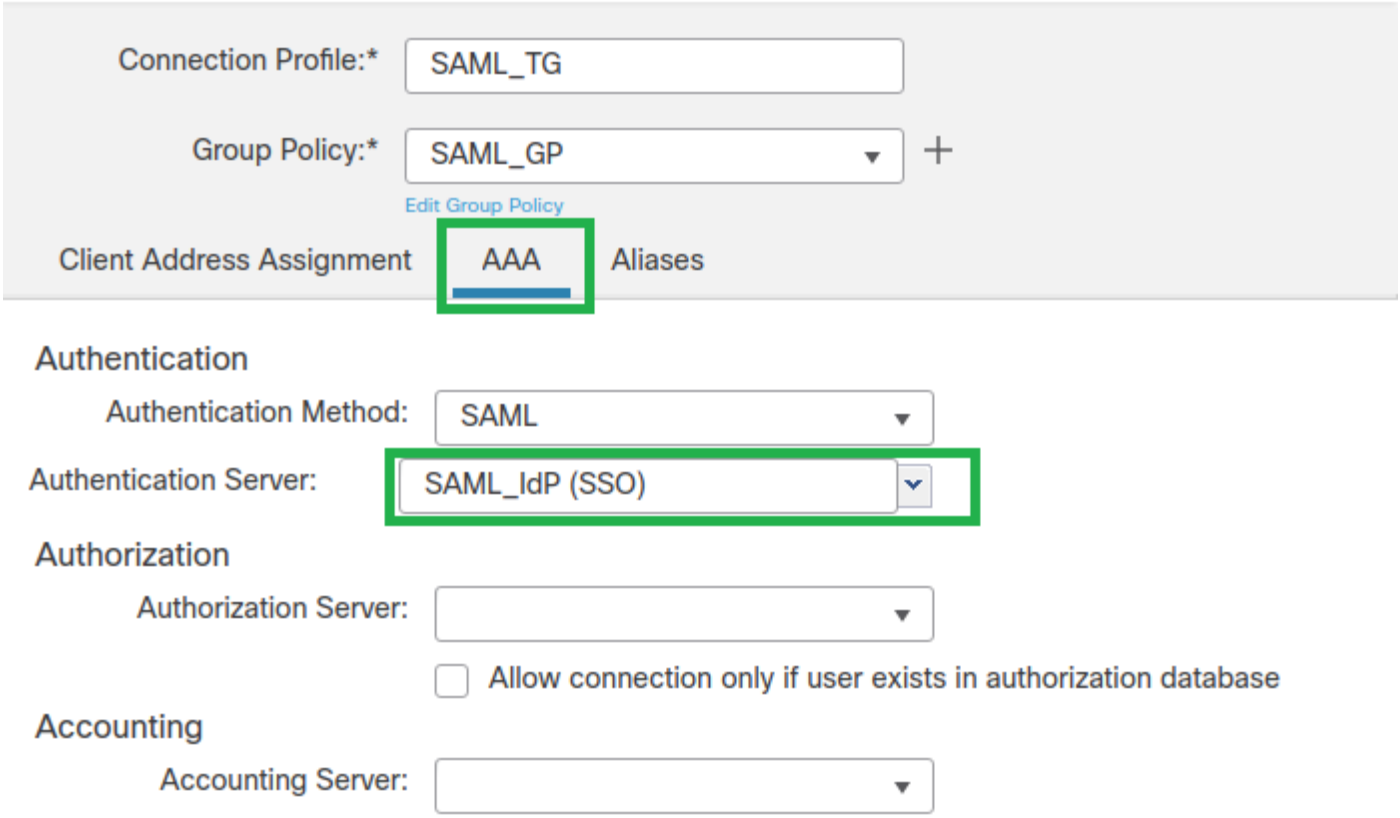


Stap 7. Maak de nieuwe **Connection Profile** en de juiste VPN toevoegen, **Pool**of DHCP-server.



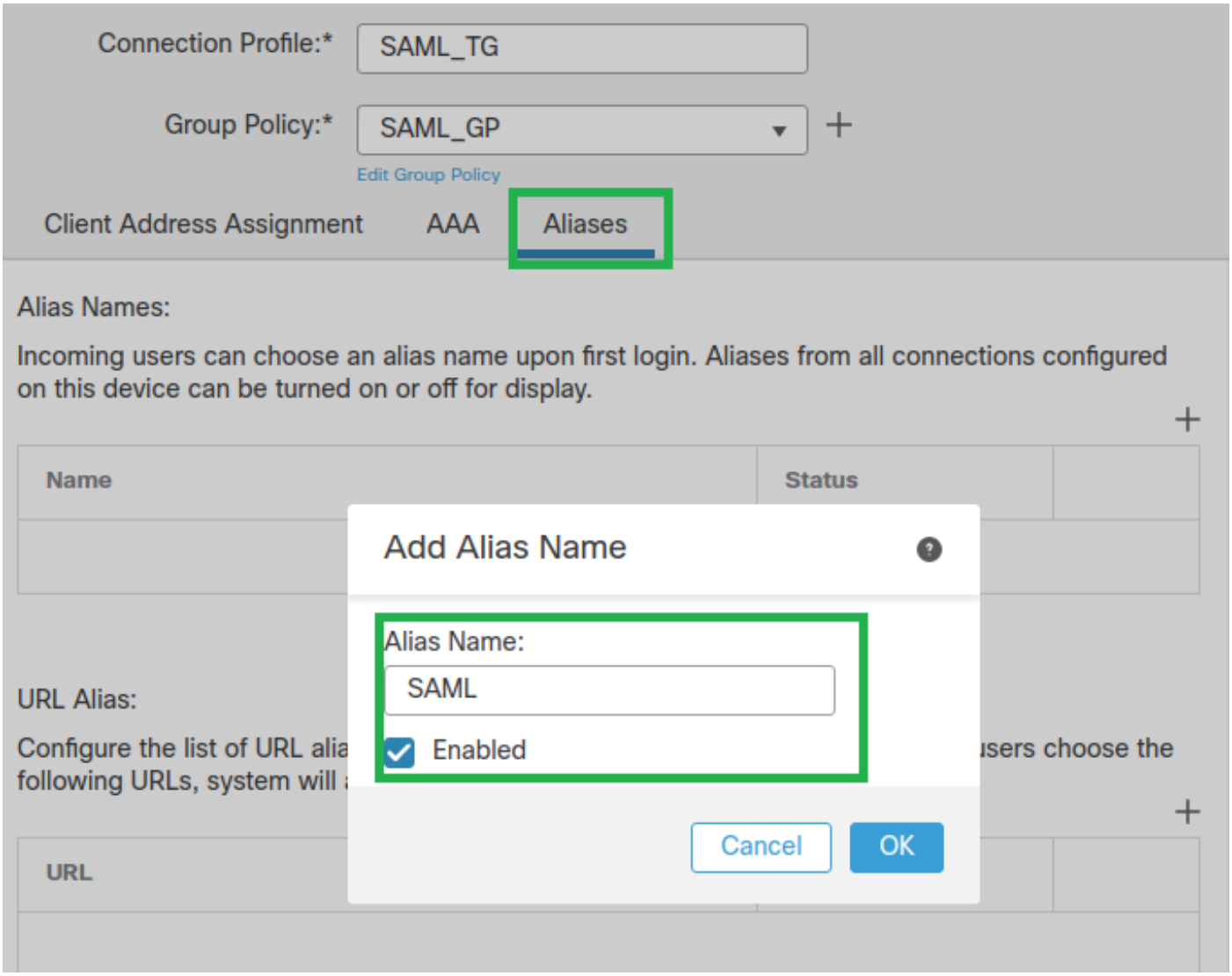
Stap 8. Selecteer het tabblad AAA. In het **Authentication Method** Selecteer SAML.

In het **Authentication Server** Selecteer in deze optie het SAML-object dat in stap 4 is gemaakt.



Stap 9. Maak een groepsalias om de verbindingen met dit **Connection Profile**. Dit is de tag die gebruikers kunnen zien op het **AnyConnect** Software vervolgkeuzemenu.

Wanneer dit is ingesteld, klikt u op OK en slaat u het volledige bestand op **SAML Authentication VPN** configuratie.



Stap 10. Navigeer naar **Deploy > Deployment** en selecteer het juiste FTD om de **SAML Authentication VPN** wijzigingen.

Stap 11. Verstrek de FTD **metadata.xml** bestand aan de **IdP** zodat ze de FTD als een vertrouwd apparaat toevoegen.

Voer op de FTD CLI de opdracht uit **show saml metadata SAML_TG** waarbij SAML_TG de naam is van de **Connection Profile** gemaakt op Stap 7.

Dit is de verwachte output:

```
> 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>
```

Na de **metadata.xml** van de FTD wordt verstrekt aan de IDp en het is als vertrouwd apparaat, kan een test onder de verbinding van VPN worden uitgevoerd.

Verifiëren

Controleer of **VPN AnyConnect** Er is verbinding met SAML tot stand gebracht als een verificatiemethode met de opdrachten die hier te zien zijn:

```
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
```

Problemen oplossen

Sommige verificatieopdrachten op de FTD CLI kunnen worden gebruikt voor het oplossen van problemen met SAML en **Remote Access VPN** verbinding tussen haakjes:

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

Opmerking: U kunt problemen oplossen **DART** van de **AnyConnect** gebruikers-pc ook.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.