Konfiguration von AnyConnect mit SAML-Authentifizierung auf FTD, die über FMC verwaltet wird

Inhalt

Einleitung

Dieses Dokument beschreibt **Security Assertion Markup Language (SAML)** Authentifizierung auf FTD über FMC verwaltet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- **AnyConnect** Konfiguration auf FMC
- SAML- und metatada.xml-Werte

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- **Firepower Threat Defense (FTD)** Version 6.7.0
- **Firepower Management Center (FMC)** Version 6.7.0
- ADFS von **AD Server** mit SAML 2.0

Anmerkung: Wenn möglich, verwenden Sie einen NTP-Server, um die Zeit zwischen FTD und IdP zu synchronisieren. Überprüfen Sie andernfalls, ob die Uhrzeit manuell zwischen den Teilnehmern synchronisiert wurde.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Die Konfiguration ermöglicht es AnyConnect-Benutzern, eine VPN-Sitzungsauthentifizierung mit einem SAML Identity Service Provider einzurichten.

Einige der derzeitigen Einschränkungen für SAML sind:

- SAML auf FTD wird für Authentifizierung (ab Version 6.7) und Autorisierung (ab Version 7.0) unterstützt.
- SAML-Authentifizierungsattribute in DAP-Bewertung verfügbar (ähnlich **RADIUS** Attribute gesendet in **RADIUS** Autorisierungsantwort vom AAA-Server) werden nicht unterstützt.
- ASA unterstützt SAML-fähige Tunnelgruppen gemäß DAP-Richtlinie. Sie können das Attribut "username" jedoch nicht mit der SAML-Authentifizierung überprüfen, da das Attribut "username" vom SAML-Identitätsanbieter maskiert wird.

- Weil **AnyConnect** Wenn der eingebettete Browser bei jedem VPN-Versuch eine neue Browsersitzung verwendet, müssen sich die Benutzer jedes Mal erneut authentifizieren, wenn die IdP HTTP-Sitzungscookies verwendet, um den Anmeldestatus zu verfolgen.
- In diesem Fall **Force Re-Authentication** Einstellung **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** hat keine Auswirkungen auf **AnyConnect** initiierte SAML-Authentifizierung.

Weitere Einschränkungen für SAML sind in dem hier bereitgestellten Link beschrieben.

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

Diese Einschränkungen gelten für ASA und FTD: "**Guidelines and Limitations for SAML 2.0**"

> **Anmerkung:** Sämtliche auf dem FTD zu implementierende SAML-Konfiguration finden Sie in der Datei metadaten.xml, die von Ihrem IdP bereitgestellt wird.

Konfiguration

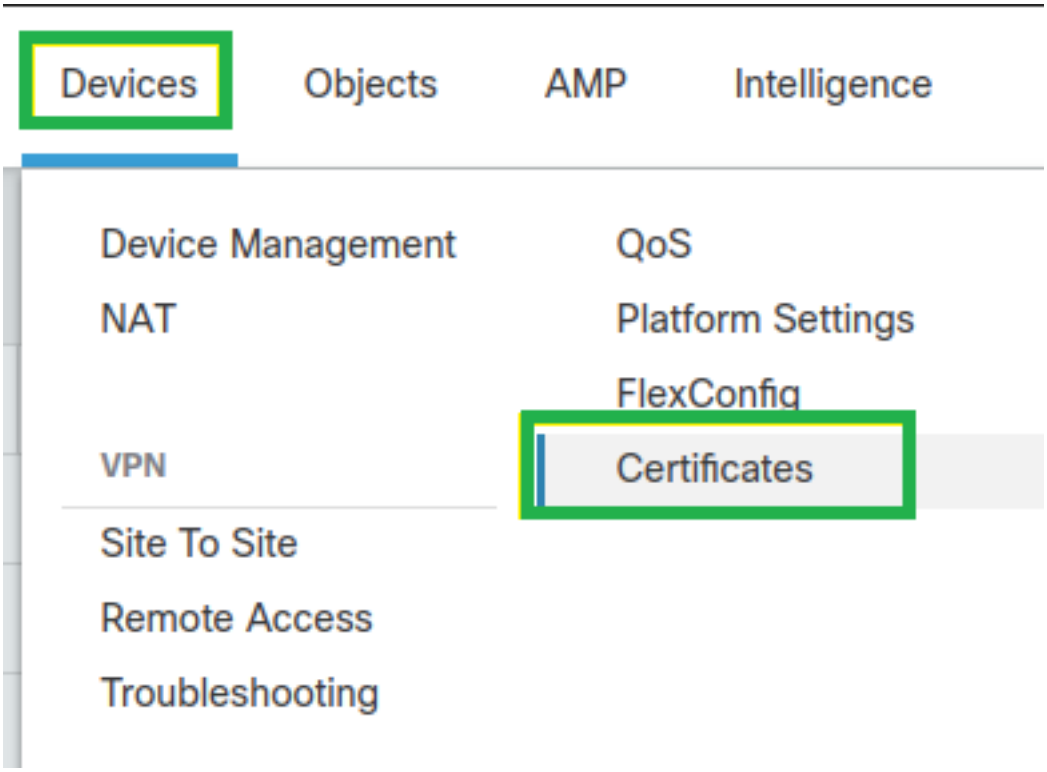
In diesem Abschnitt wird die Konfiguration **AnyConnect** mit SAML-Authentifizierung auf FTD

SAML IdP-Parameter abrufen

Dieses Bild zeigt eine SAML-IdP-Datei "metadaten.xml". Aus der Ausgabe können Sie alle Werte abrufen, die zum Konfigurieren des **AnyConnect** Profil mit SAML:

Konfiguration auf FTD über FMC

Schritt 1: Installation und Registrierung des IdP-Zertifikats beim FMC Navigieren Sie zu **Devices > Certificates**



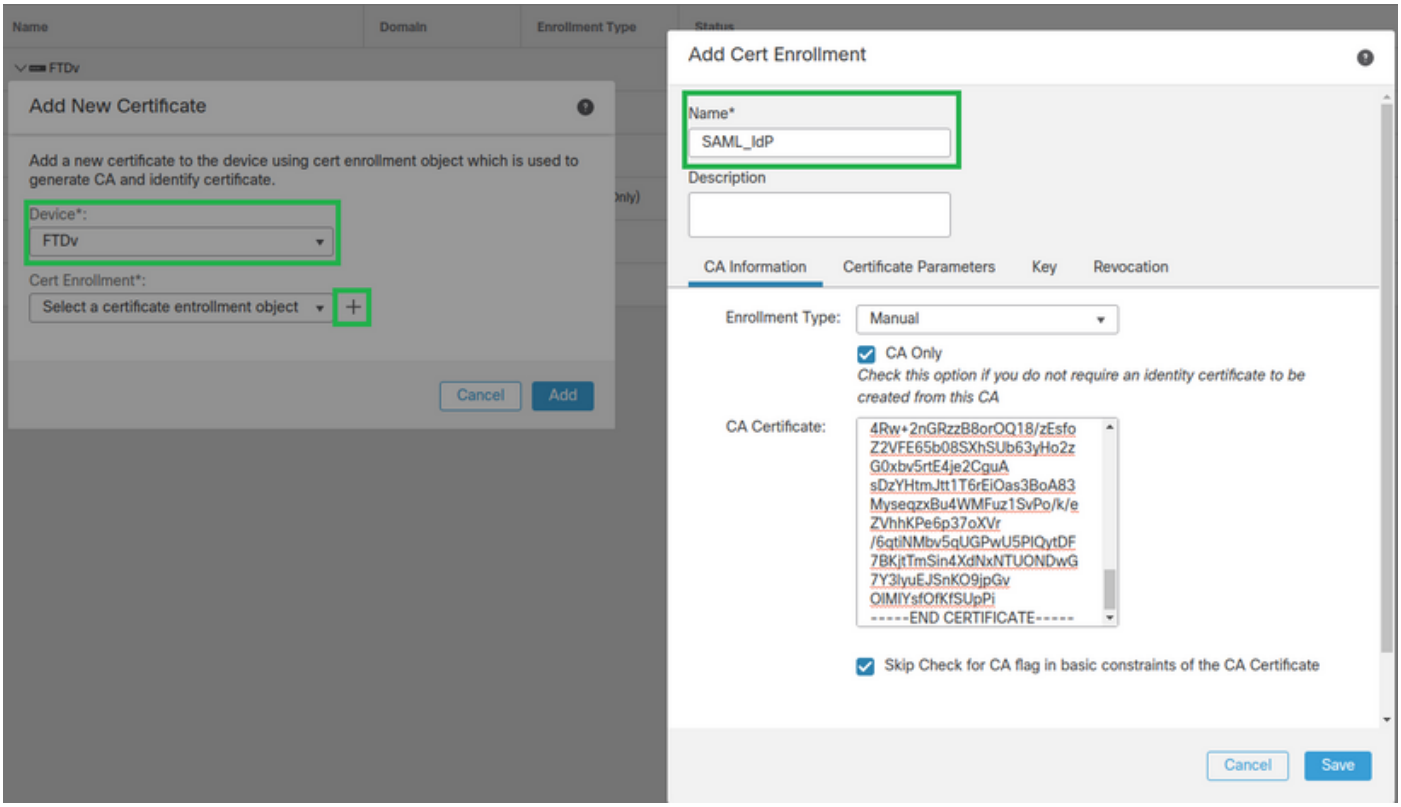
Schritt 2. Klicken Sie auf **Add**. Wählen Sie das FTD aus, um sich für dieses Zertifikat anzumelden. Klicken Sie unter Zertifikatregistrierung auf das Pluszeichen **+**.

Im **Add Cert Enrollment** -Abschnitt einen beliebigen Namen als Label für das IdP-Zertifikat verwenden. Klicken Sie auf **Manual**.

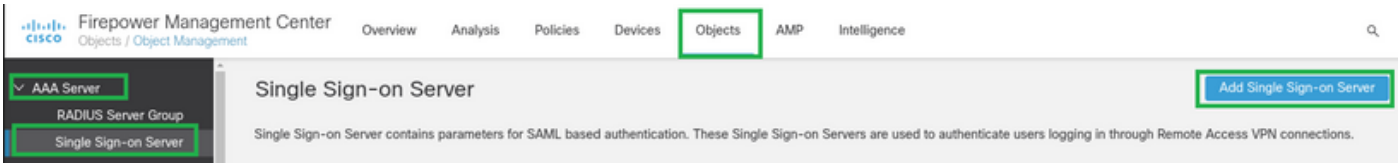
Überprüfen Sie **CA Only** und **Skip Check** für CA-Markierungsfelder.

Einfügen des **base64** Format IDP CA Zertifikat.

Klicken Sie auf **Save** und dann auf **Add**.

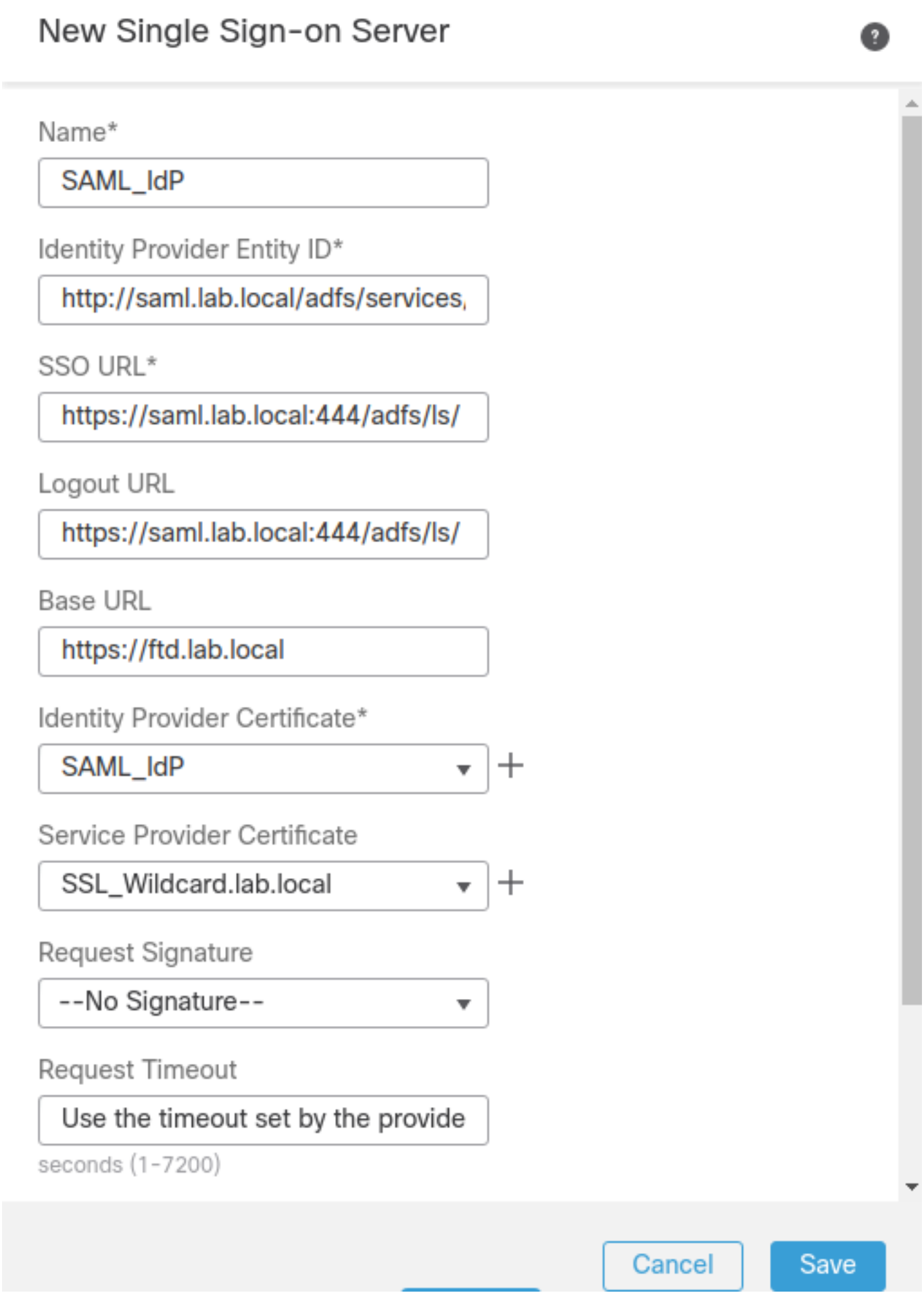


Schritt 3: Konfigurieren der SAML-Servereinstellungen Navigieren Sie zu **Objects > Object Management > AAA Servers > Single Sign-on Server**. Wählen Sie anschließend **Add Single Sign-on Server**.

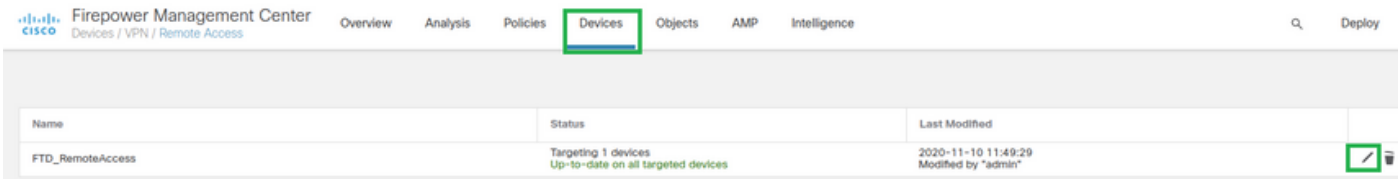


Schritt 4: Basierend auf dem **metadata.xml** Datei, die bereits von Ihrem IdP bereitgestellt wurde, konfigurieren Sie die SAML-Werte auf dem **New Single Sign-on Server**.

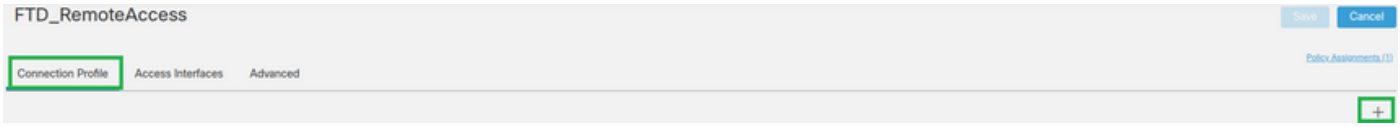
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



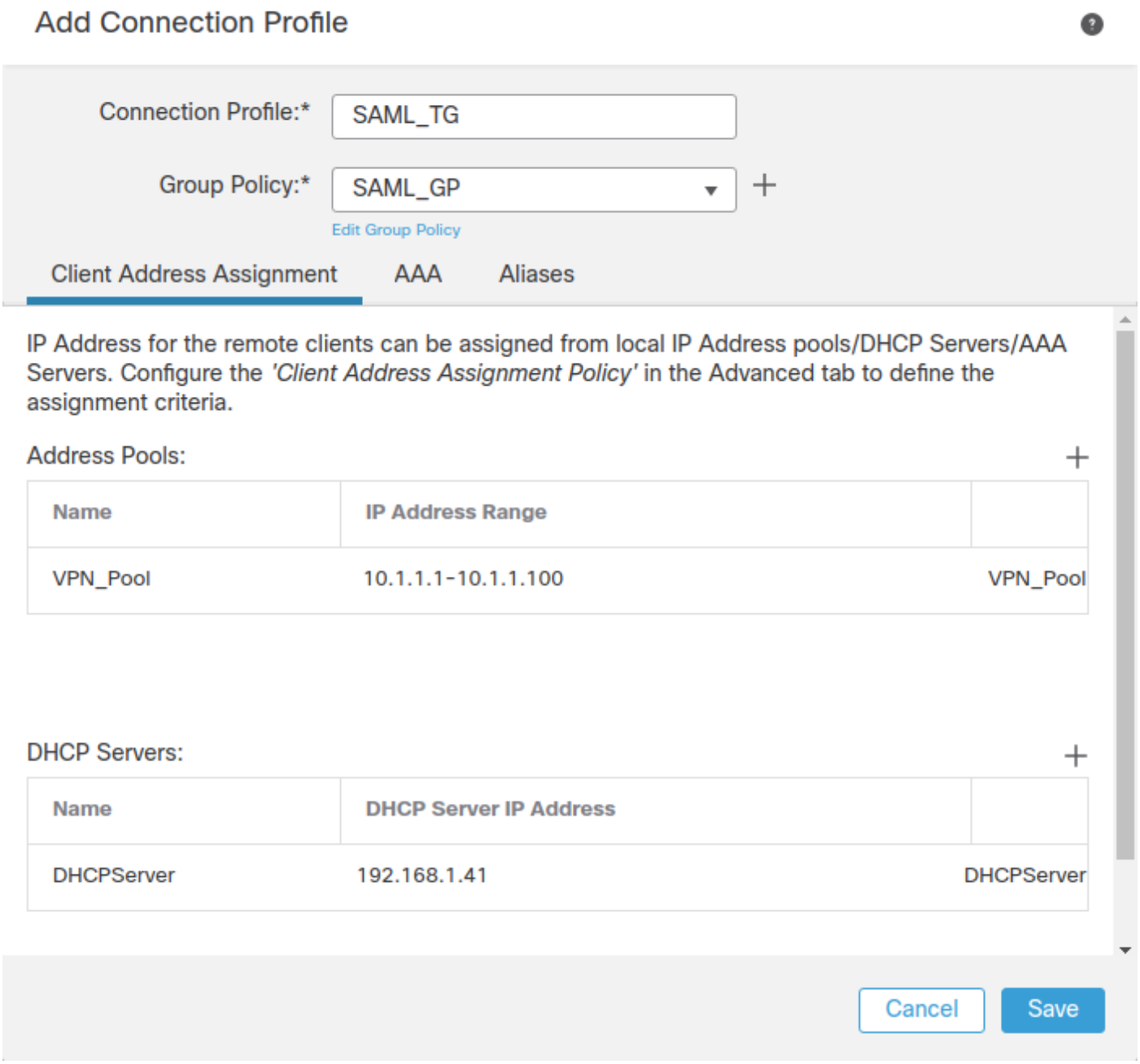
Schritt 5: Konfigurieren des **Connection Profile** , der diese Authentifizierungsmethode verwendet. Navigieren Sie zu **Devices > Remote Access** und dann die aktuelle **VPN Remote Access** konfiguration.



Schritt 6. Klicken Sie auf das Pluszeichen **+** und fügen Sie ein weiteres hinzu **Connection Profile**.

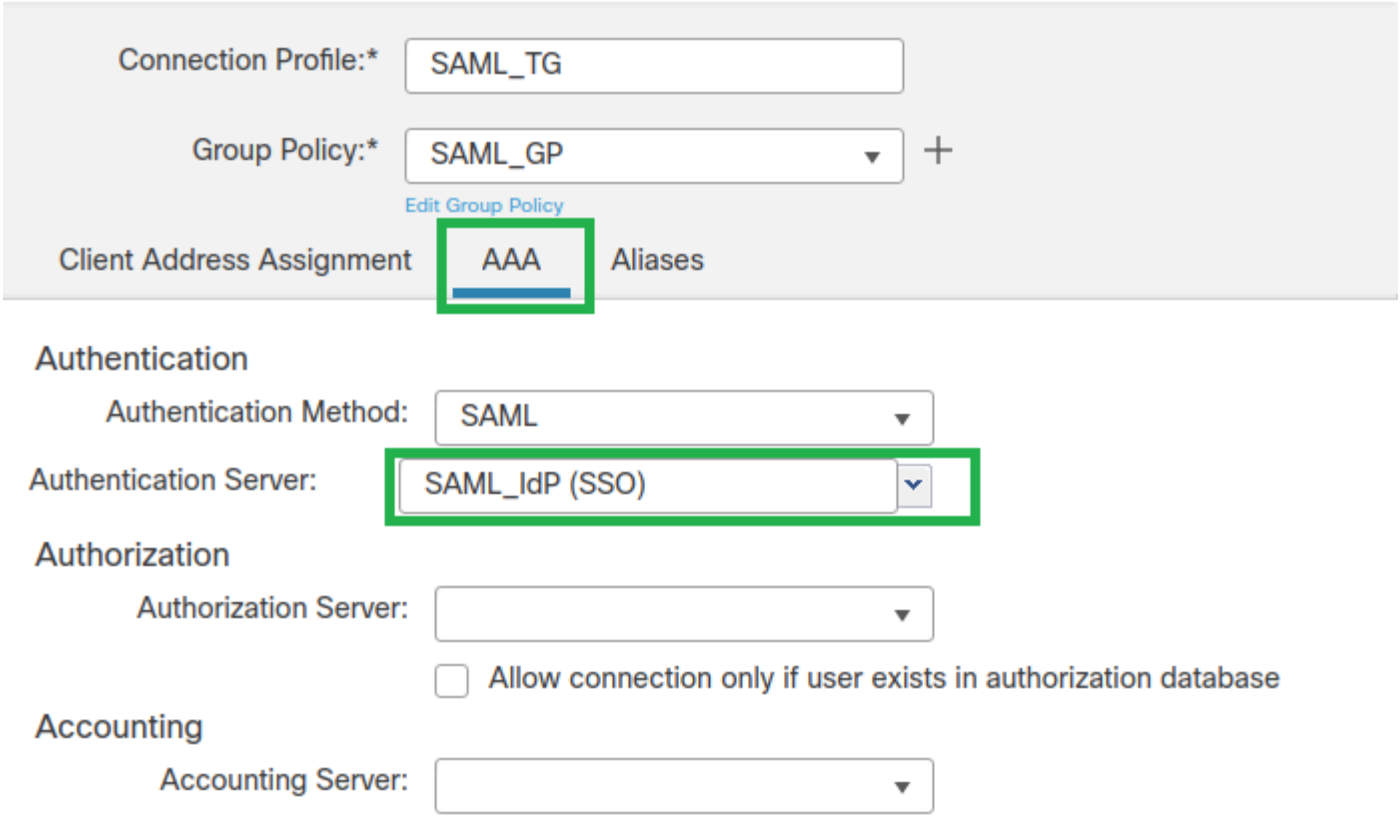


Schritt 7: Erstellen Sie die neue **Connection Profile** und fügen Sie das entsprechende VPN hinzu, **Pool**oder DHCP-Server.



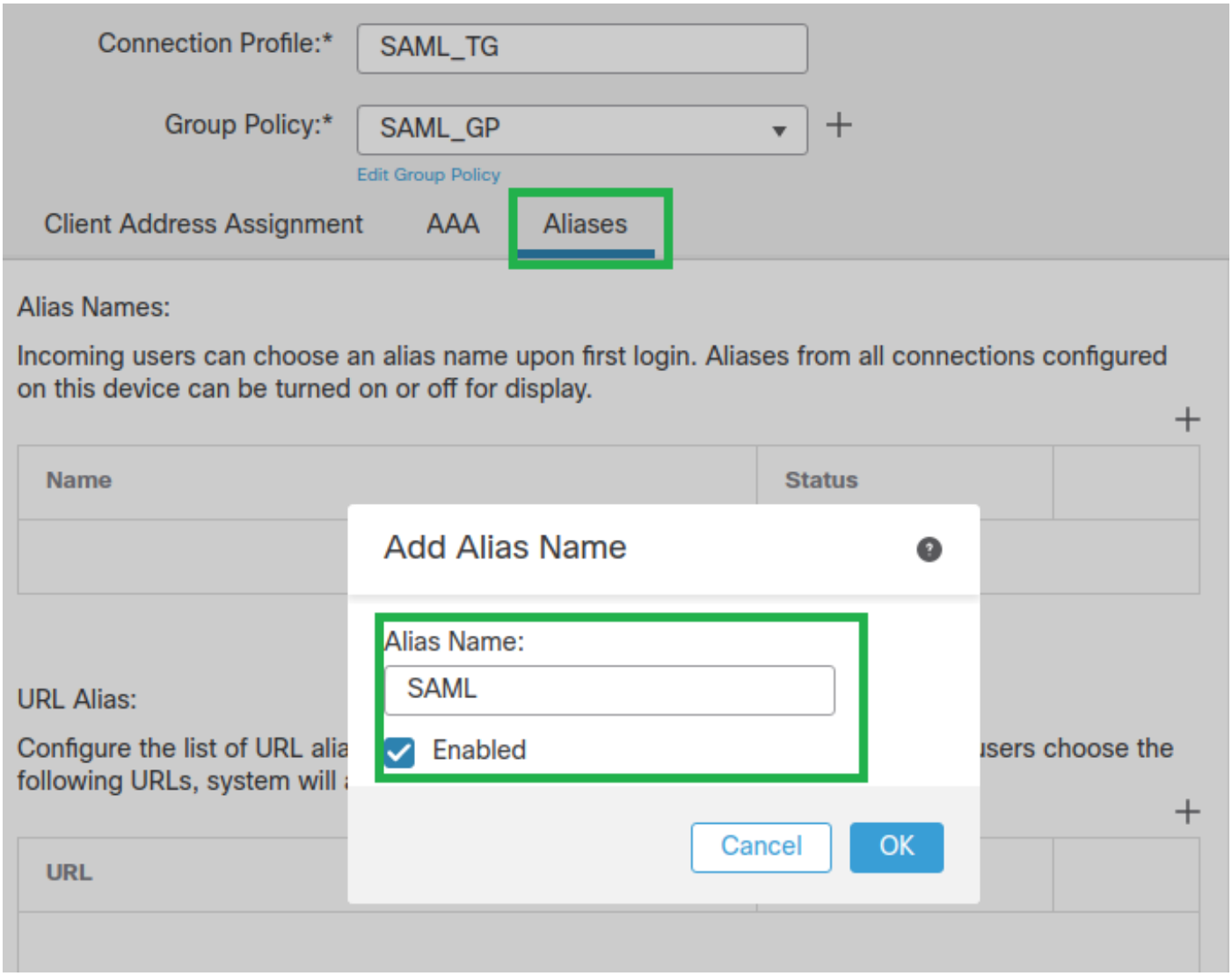
Schritt 8: Wählen Sie die Registerkarte AAA aus. Im **Authentication Method** wählen Sie SAML aus.

Im **Authentication Server** wählen Sie das SAML-Objekt, das in Schritt 4 erstellt wurde.



Schritt 9: Erstellen Sie einen Gruppenalias, um die Verbindungen mit diesem **Connection Profile**. Dies ist der Tag, den Benutzer auf dem **AnyConnect** Software-Dropdown-Menü.

Klicken Sie nach der Konfiguration auf OK, und speichern Sie die vollständige **SAML Authentication VPN** konfiguration.



Schritt 10: Navigieren Sie zu **Deploy > Deployment** und wählen Sie die passende FTD aus, um die **SAML Authentication VPN** Änderungen.

Schritt 11: FTD angeben **metadata.xml** in den **IdP** eintragen, sodass der FTD als vertrauenswürdiges Gerät hinzugefügt wird.

Führen Sie in der FTD-CLI den Befehl **show saml metadata SAML_TG** wobei SAML_TG der Name des **Connection Profile** in Schritt 7 erstellt.

Dies ist die erwartete Ausgabe:

```
> 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>
```

Nach dem **metadata.xml** aus dem FTD an den IdP übermittelt und als vertrauenswürdiges Gerät verwendet wird, kann ein Test unter der VPN-Verbindung durchgeführt werden.

Überprüfung

Prüfen Sie, ob **VPN AnyConnect** -Verbindung wurde mit SAML als Authentifizierungsmethode mit den hier gezeigten Befehlen hergestellt:

```
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
```

Fehlerbehebung

Einige Verifizierungsbefehle der FTD-CLI können zur Fehlerbehebung bei SAML und **Remote Access VPN** Anschluss in der Halterung:

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

Anmerkung: Sie können Fehler beheben **DART** von **AnyConnect** Benutzer-PC.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.