Configurer Anyconnect avec authentification SAML sur FTD géré via FMC

Contenu

Introduction

Ce document décrit **Security Assertion Markup Language (SAML)** authentification sur FTD géré sur FMC.

Conditions préalables

Conditions requises

Cisco recommande de connaître ces sujets :

- **AnyConnect** configuration sur FMC
- Valeurs SAML et metatada.xml

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- **Firepower Threat Defense (FTD)** version 6.7.0
- **Firepower Management Center (FMC)** version 6.7.0
- ADFS de **AD Server** avec SAML 2.0

> **Note**: Si possible, utilisez un serveur NTP pour synchroniser l'heure entre le FTD et l'IdP. Sinon, vérifiez que l'heure est synchronisée manuellement entre eux.

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La configuration permet aux utilisateurs Anyconnect d'établir une authentification de session VPN avec un fournisseur de service d'identité SAML.

Voici quelques-unes des limites actuelles de la LMEA :

- SAML sur FTD est pris en charge pour l'authentification (à partir de la version 6.7) et l'autorisation (à partir de la version 7.0).
- Attributs d'authentification SAML disponibles dans l'évaluation LDAP (similaire à **RADIUS** attributs envoyés **RADIUS** réponse d'autorisation du serveur AAA) ne sont pas prises en charge.
- ASA prend en charge le groupe de tunnels SAML sur la politique DAP. Cependant, vous ne pouvez pas vérifier l'attribut username avec l'authentification SAML, car l'attribut username est masqué par le fournisseur d'identité SAML.

- Parce que **AnyConnect** Lorsque le navigateur intégré utilise une nouvelle session de navigateur à chaque tentative VPN, les utilisateurs doivent s'authentifier à chaque fois si le fournisseur d'identité utilise des cookies de session HTTP pour suivre l'état de connexion.
- Dans ce cas, le **Force Re-Authentication** implantation **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** n'a pas d'effet sur **AnyConnect** a initié l'authentification SAML.

D'autres limitations ou SAML sont décrites dans le lien fourni ici.

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

Ces limitations s'appliquent à ASA et FTD : "**Guidelines and Limitations for SAML 2.0**"

> **Note**: Toute la configuration SAML à implémenter sur le FTD se trouve dans le fichier metadata.xml fourni par votre fournisseur d'identité.

Configuration

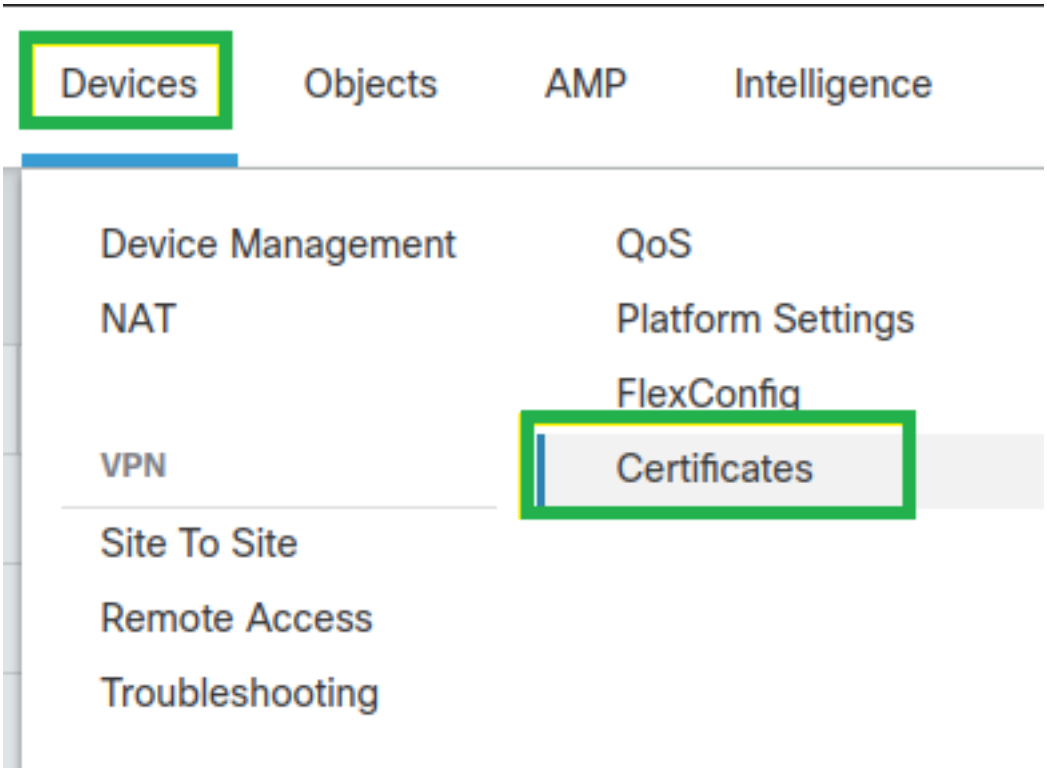
Cette section décrit comment configurer **AnyConnect** avec authentification SAML sur FTD

Obtenir les paramètres IDp SAML

Cette image présente un fichier metadata.xml IdP SAML. Vous pouvez obtenir toutes les valeurs requises pour configurer le **AnyConnect** profil avec SAML :

Configuration sur le FTD via FMC

Étape 1 : installation et inscription du certificat IdP sur le FMC Naviguez jusqu'à **Devices > Certificates**



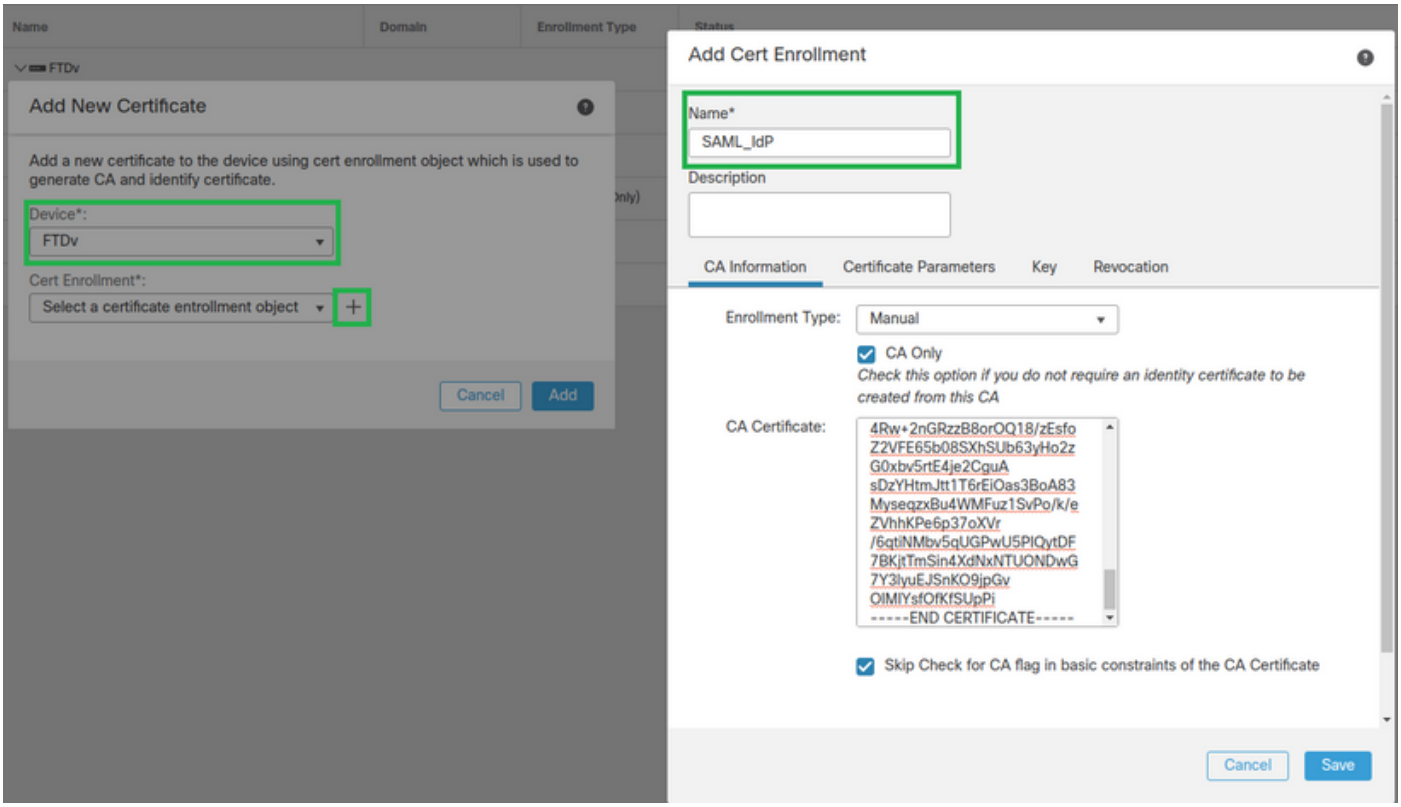
Étape 2. Cliquez sur **Add**. Sélectionnez le FTD à inscrire dans ce certificat. Sous Inscription au certificat, cliquez sur le signe plus **+**.

Dans la **Add Cert Enrollment** , utilisez n'importe quel nom comme étiquette pour le certificat IdP. Cliquer **Manual**.

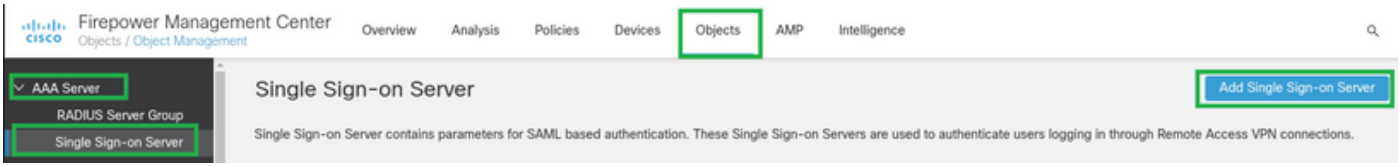
Vérifiez la **CA Only** et **Skip Check** pour les champs d'indicateur CA.

Collez le **base64** format IdP CA cert.

Cliquer **Save** puis cliquez sur **Add**.

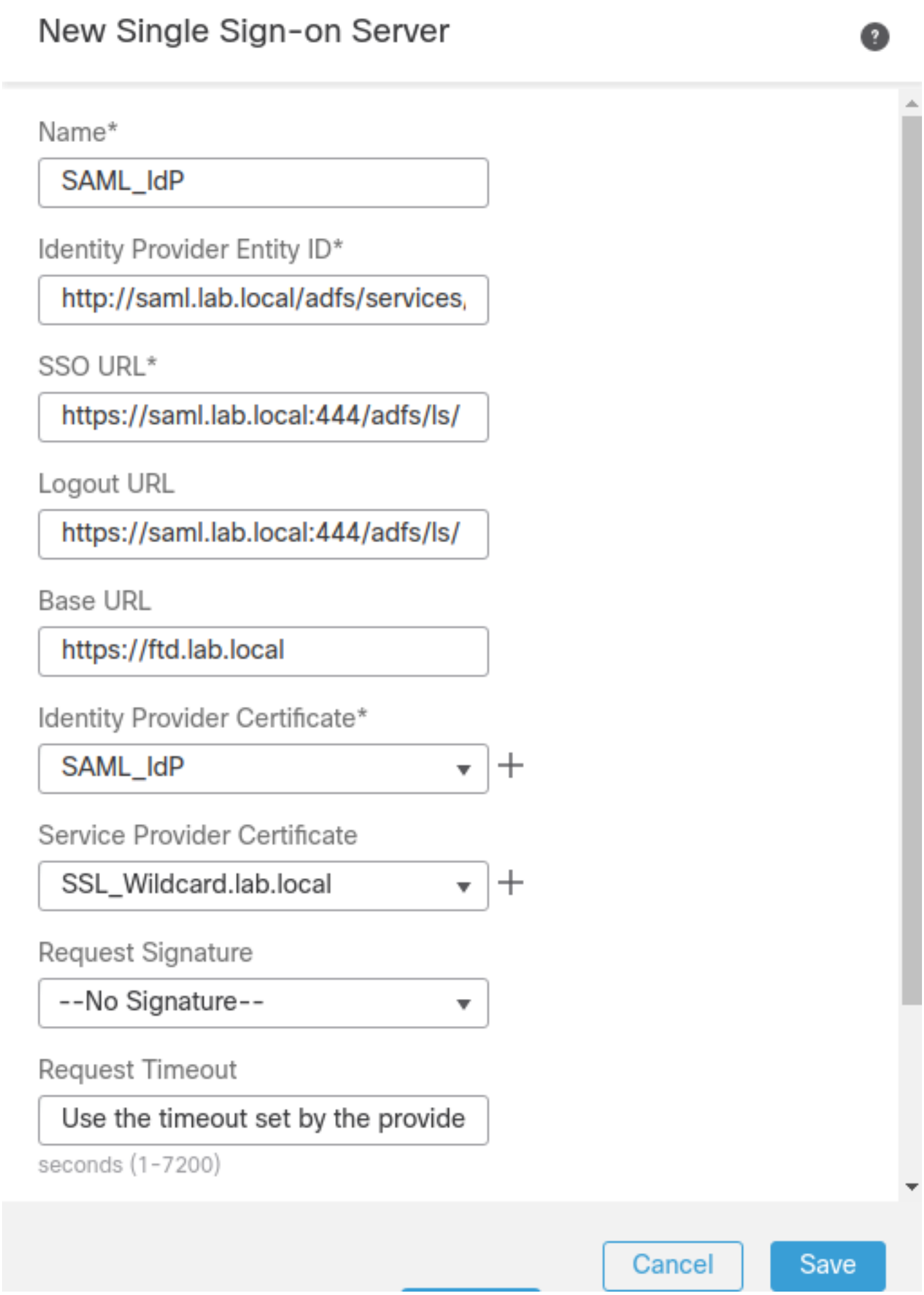


Étape 3. Configuration des paramètres du serveur SAML Naviguez jusqu'à **Objects > Object Management > AAA Servers > Single Sign-on Server**. Sélectionnez ensuite **Add Single Sign-on Server**.

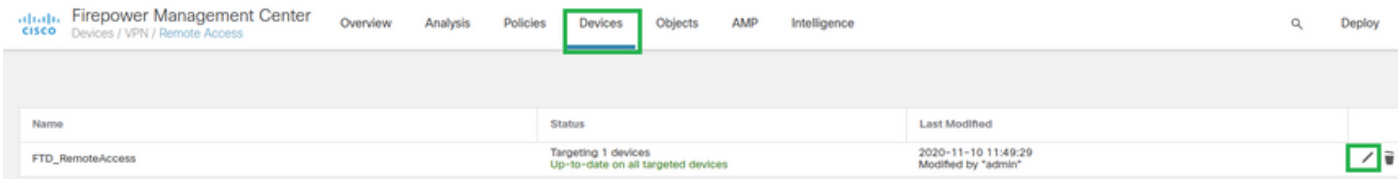


Étape 4. En fonction de la **metadata.xml** déjà fourni par votre fournisseur d'identité, configurez les valeurs SAML sur le **New Single Sign-on Server**.

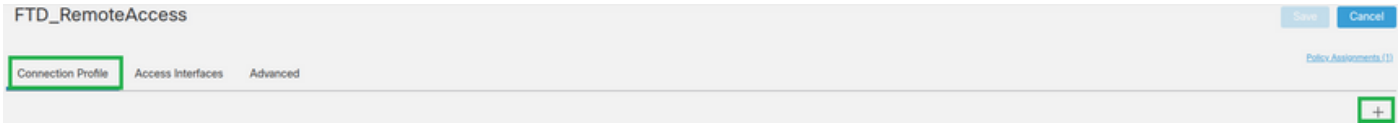
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



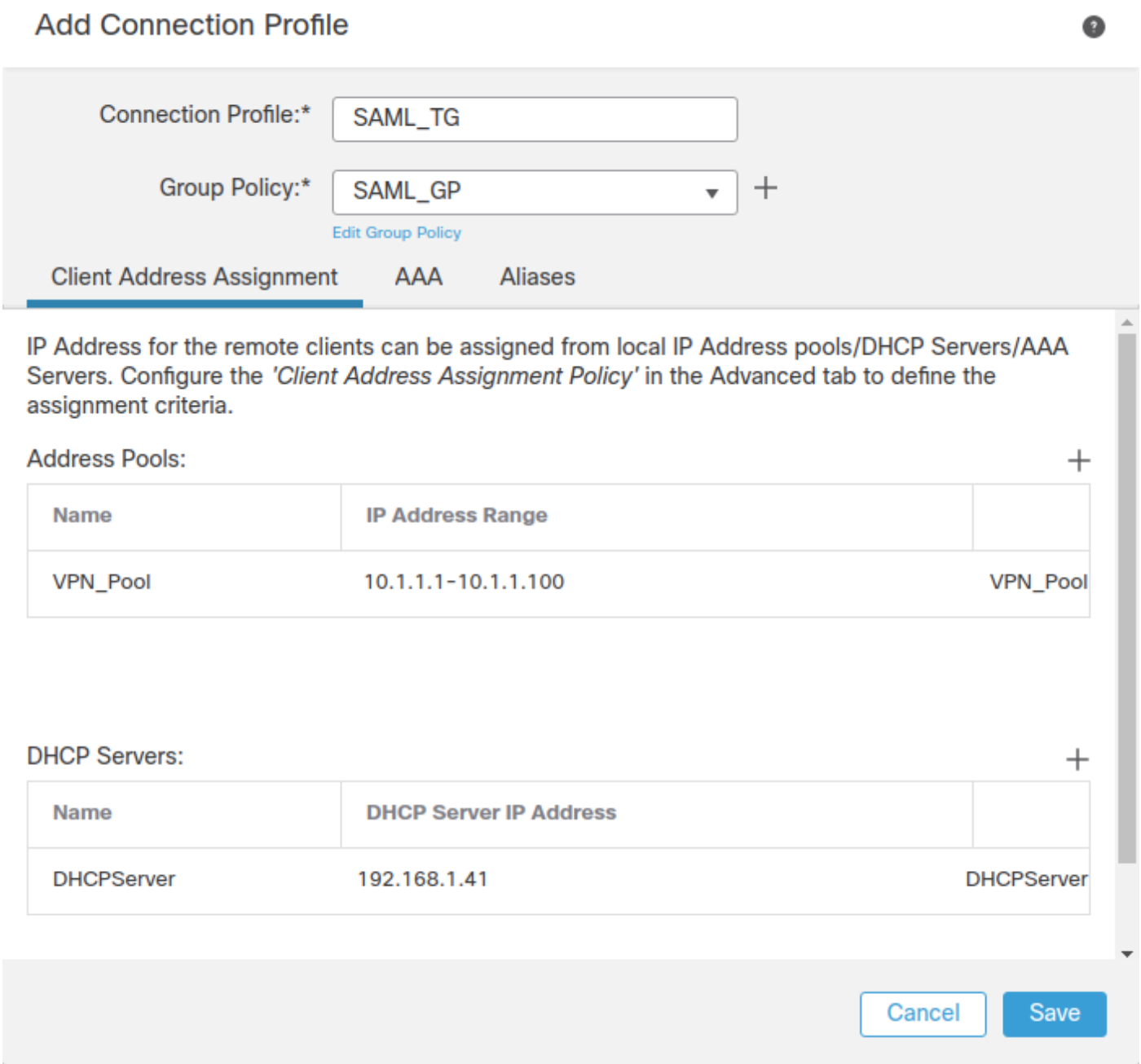
Étape 5 : configuration du **Connection Profile** qui utilise cette méthode d'authentification. Naviguez jusqu'à **Devices > Remote Access** puis modifiez votre **VPN Remote Access** configuration.



Étape 6. Cliquez sur le signe plus **+** et ajoutez un autre **Connection Profile**.

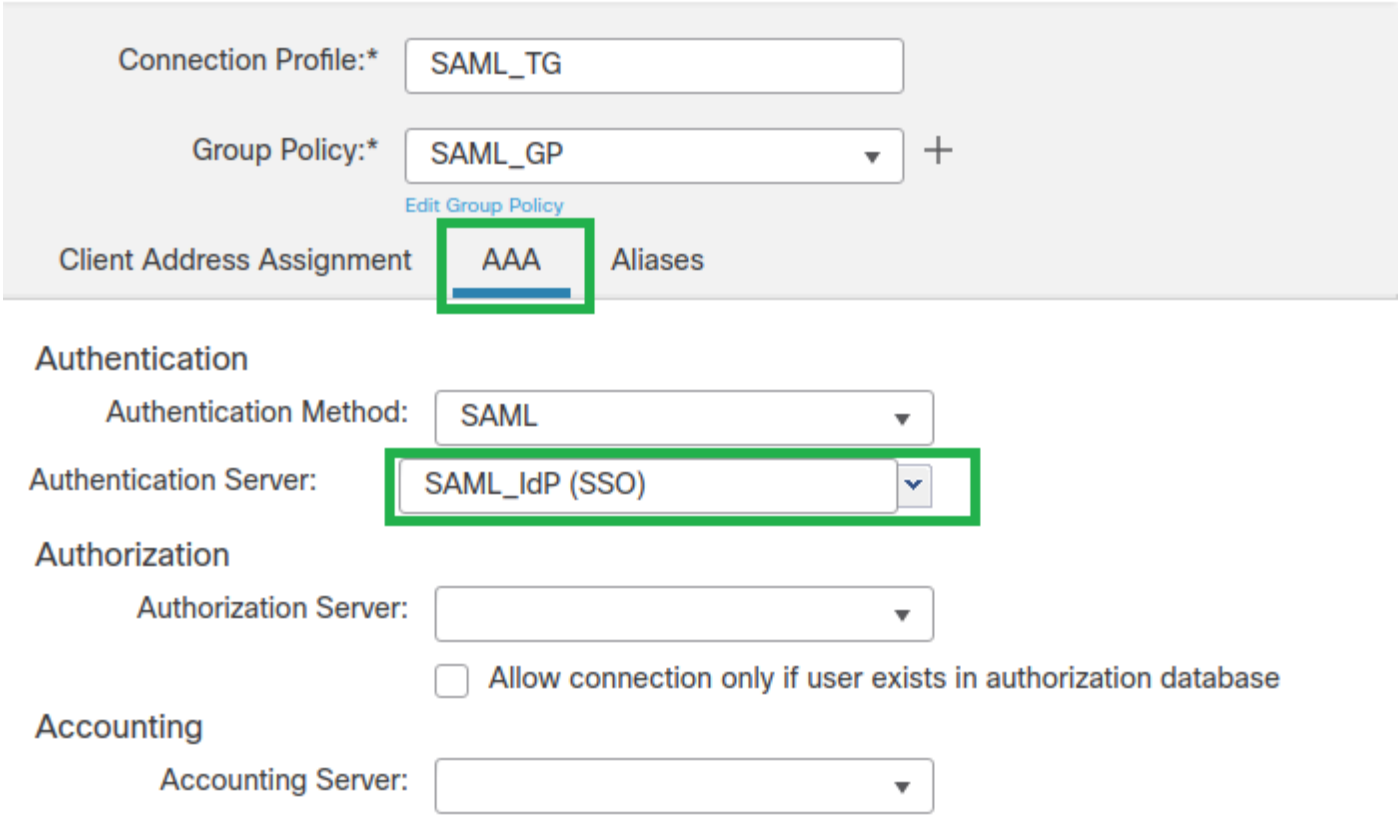


Étape 7. Créez le nouveau **Connection Profile** et ajoutez le VPN approprié, **Pool**ou serveur DHCP.



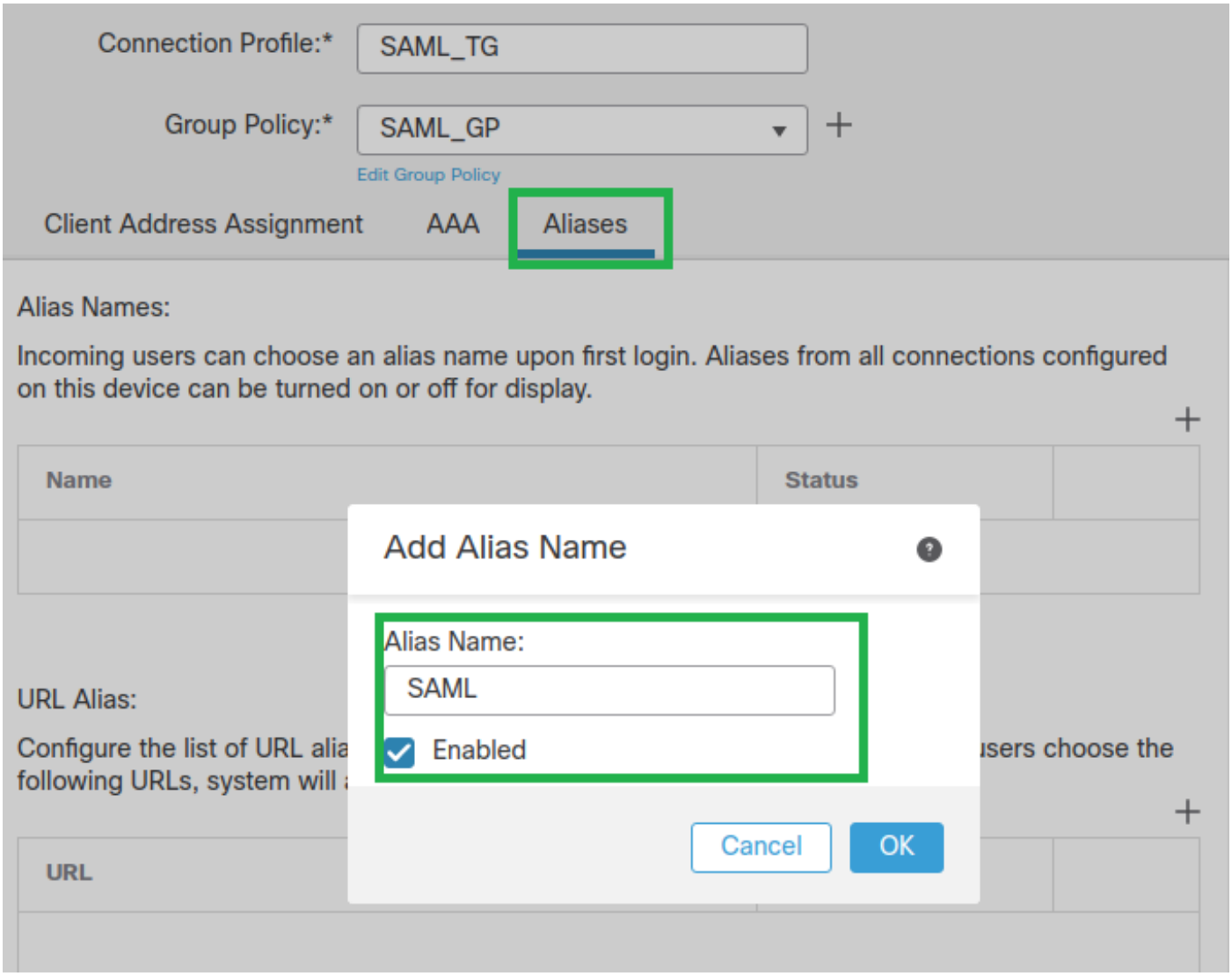
Étape 8. Sélectionnez l'onglet AAA. Sous la **Authentication Method** , sélectionnez SAML.

Sous la **Authentication Server** , sélectionnez l'objet SAML créé à l'étape 4.



Étape 9. Créez un alias de groupe pour mapper les connexions à ce **Connection Profile**. Il s'agit de la balise que les utilisateurs peuvent voir sur le **AnyConnect** Menu déroulant Logiciel.

Lorsque cette option est configurée, cliquez sur OK et enregistrez le **SAML Authentication VPN** configuration.



Étape 10. Accédez à **Deploy > Deployment** et sélectionnez le FTD approprié pour appliquer le **SAML Authentication VPN** modifications.

Étape 11. Fournissez le FTD **metadata.xml** au **fournisseur** d'**identifiants** afin qu'il ajoute le FTD en tant que périphérique approuvé.

Sur l'interface de ligne de commande FTD, exécutez la commande **show saml metadata SAML_TG** où SAML_TG est le nom du **Connection Profile** créé à l'étape 7.

Voici le résultat attendu :

```
> 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>
```

Après le **metadata.xml** à partir du FTD est fourni au fournisseur d'identité et il est comme un périphérique de confiance, un test sous la connexion VPN peut être effectué.

Vérification

Vérifiez que le **VPN AnyConnect** La connexion a été établie avec SAML comme méthode d'authentification avec les commandes présentées ici :

```
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
```

Dépannage

Certaines commandes de vérification de l'interface de ligne de commande FTD peuvent être utilisées pour dépanner SAML et **Remote Access VPN** connexion comme indiqué dans le support :

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

Note: Vous pouvez dépanner **DART** a partir des versions **AnyConnect** PC utilisateur également.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.