Configurazione di Anyconnect con autenticazione SAML su FTD gestito tramite FMC

Sommario

Introduzione

In questo documento vengono spiegate **Security Assertion Markup Language (SAML)** autenticazione su FTD gestito tramite FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- **AnyConnect** configurazione su FMC
- Valori SAML e metatada.xml

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

> **Nota:** Se possibile, utilizzare un server NTP per sincronizzare l'ora tra FTD e IdP. In caso contrario, verificare che l'ora sia sincronizzata manualmente.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

La configurazione consente agli utenti Anyconnect di stabilire un'autenticazione di sessione VPN con un provider di servizi di identità SAML.

Alcune delle attuali limitazioni di SAML sono:

- SAML su FTD è supportato per l'autenticazione (versione 6.7 successiva) e l'autorizzazione (versione 7.0 successiva).
- Attributi di autenticazione SAML disponibili nella valutazione DAP (simili a **RADIUS** attributi inviati in **RADIUS** la risposta di autorizzazione dal server AAA non è supportata.
- L'ASA supporta i gruppi di tunnel abilitati SAML sui criteri DAP. Tuttavia, non è possibile controllare l'attributo username con l'autenticazione SAML, poiché l'attributo username è mascherato dal provider SAML Identity.

- Perché **AnyConnect** con il browser incorporato utilizza una nuova sessione del browser su ogni tentativo VPN, gli utenti devono riautenticarsi ogni volta se IdP utilizza i cookie della sessione HTTP per tenere traccia dello stato di accesso.
- In questo caso, la **Force Re-Authentication** impostazione **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** non ha effetto su **AnyConnect** autenticazione SAML avviata.

Ulteriori limitazioni o SAML sono descritte nel collegamento fornito qui.

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

Le seguenti limitazioni si applicano ad ASA e FTD: "**Guidelines and Limitations for SAML 2.0**"

> **Nota:** Tutta la configurazione SAML da implementare sull'FTD si trova nel file metadata.xml fornito dall'IdP.

Configurazione

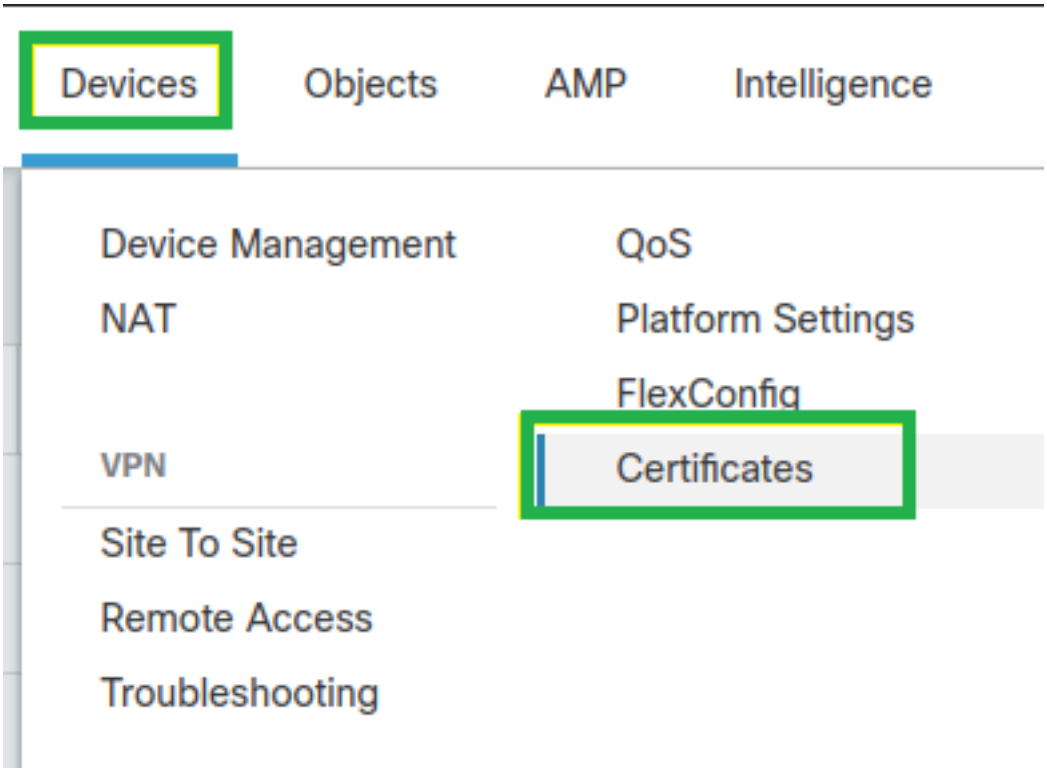
Questa sezione descrive come configurare **AnyConnect** con autenticazione SAML su FTD

Ottiene i parametri IdP SAML

Nell'immagine è illustrato un file metadata.xml di SAML IdP. Dall'output è possibile ottenere tutti i valori necessari per configurare **AnyConnect** profilo con SAML:

Configurazione sul FTD tramite FMC

Passaggio 1. Installare e registrare il certificato del provider di identità nel FMC. Passa a **Devices > Certificates**



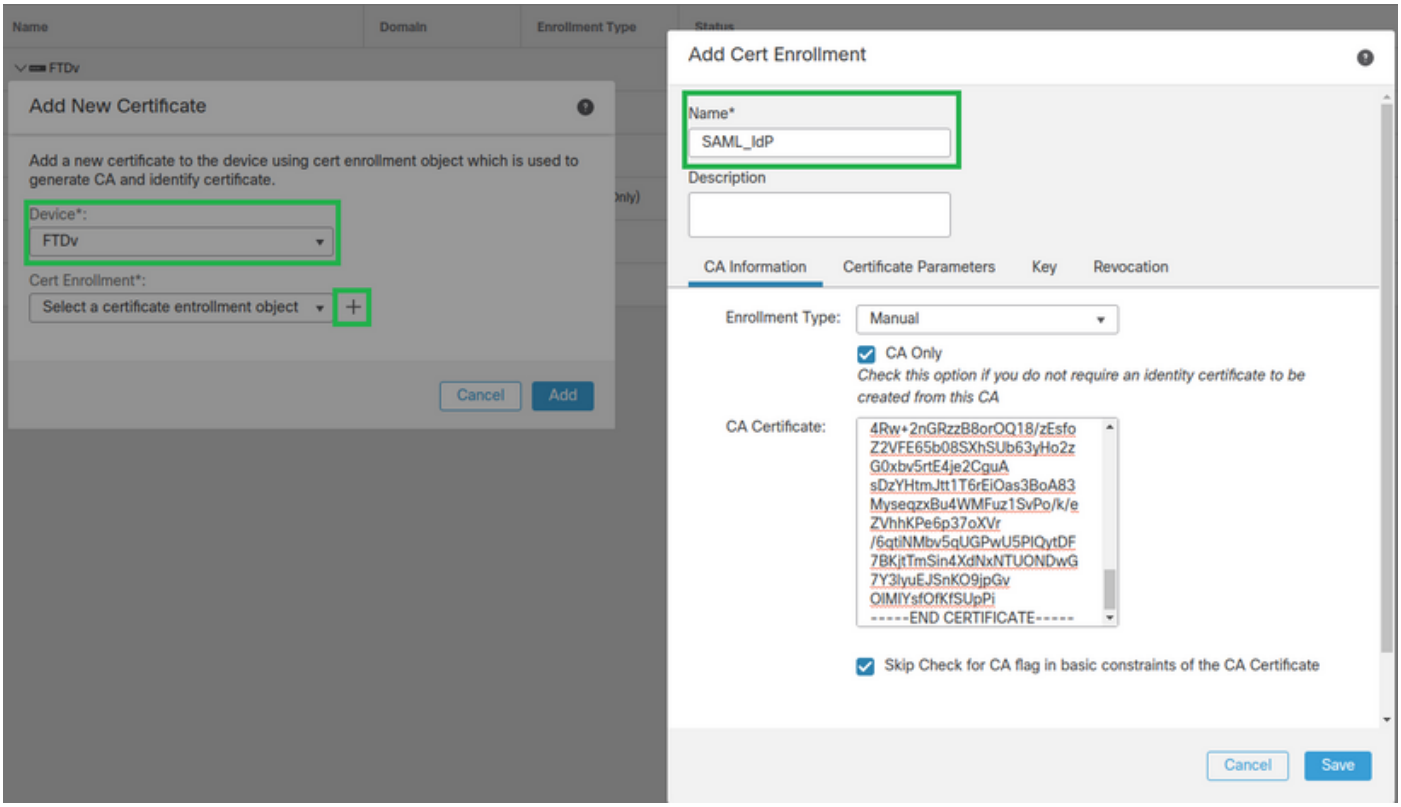
Passaggio 2. Fare clic su **Add**. Selezionare l'FTD da registrare nel certificato. In Registrazione certificato fare clic sul segno **++**

Nella **Add Cert Enrollment** utilizzare qualsiasi nome come etichetta per il certificato IdP. Clic **Manual**.

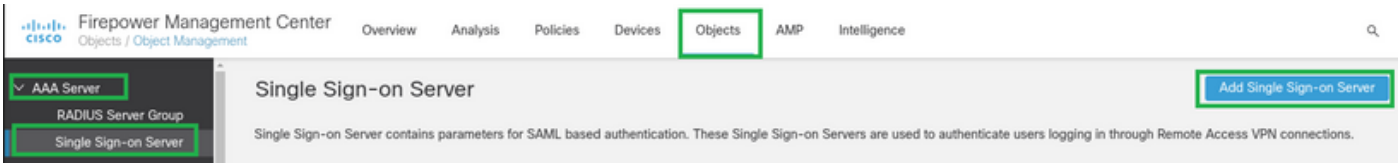
Controllare la **CA Only** e **Skip Check** per i campi contrassegno CA.

Incolla **base64** formato certificato CA IdP.

Clic **Save** e fare clic su **Add**.

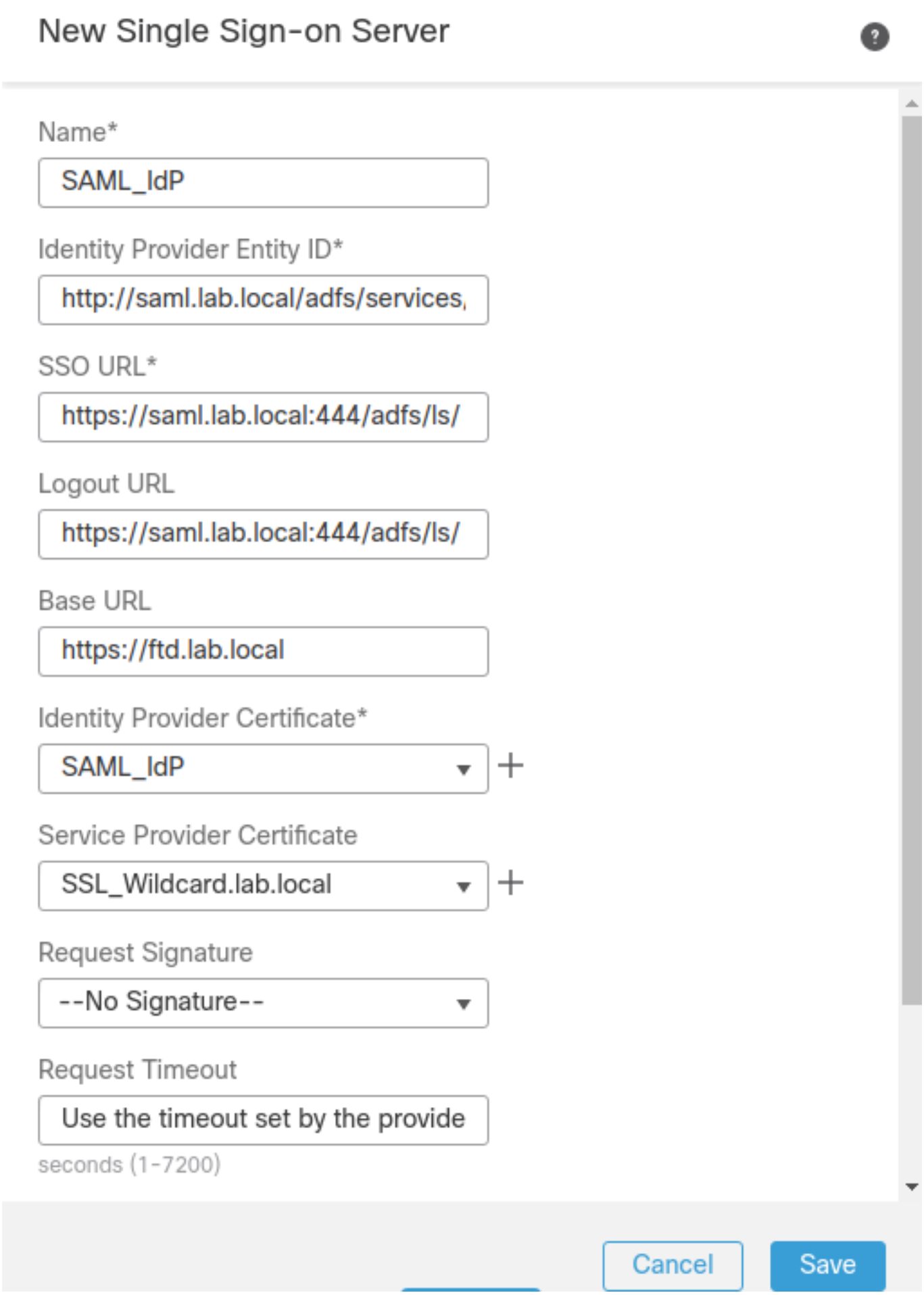


Passaggio 3. Configurare le impostazioni del server SAML. Passa a **Objects > Object Management > AAA Servers > Single Sign-on Server**. Quindi, selezionare **Add Single Sign-on Server**.

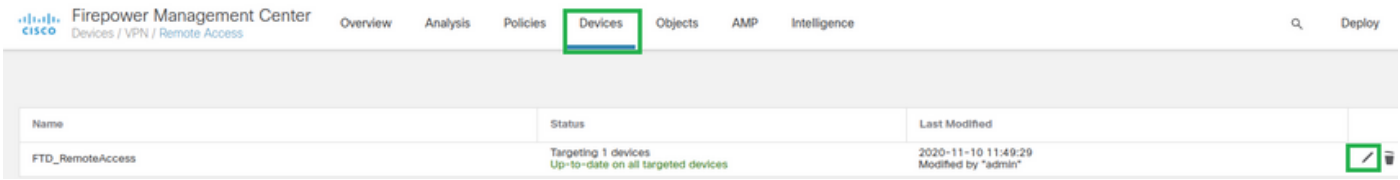


Passaggio 4. In base al **metadata.xml** già fornito dal provider di identità, configurare i valori SAML nel **New Single Sign-on Server**.

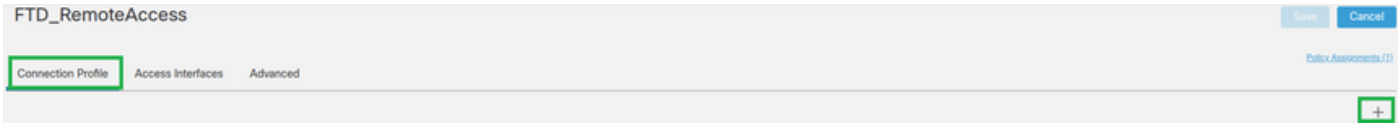
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



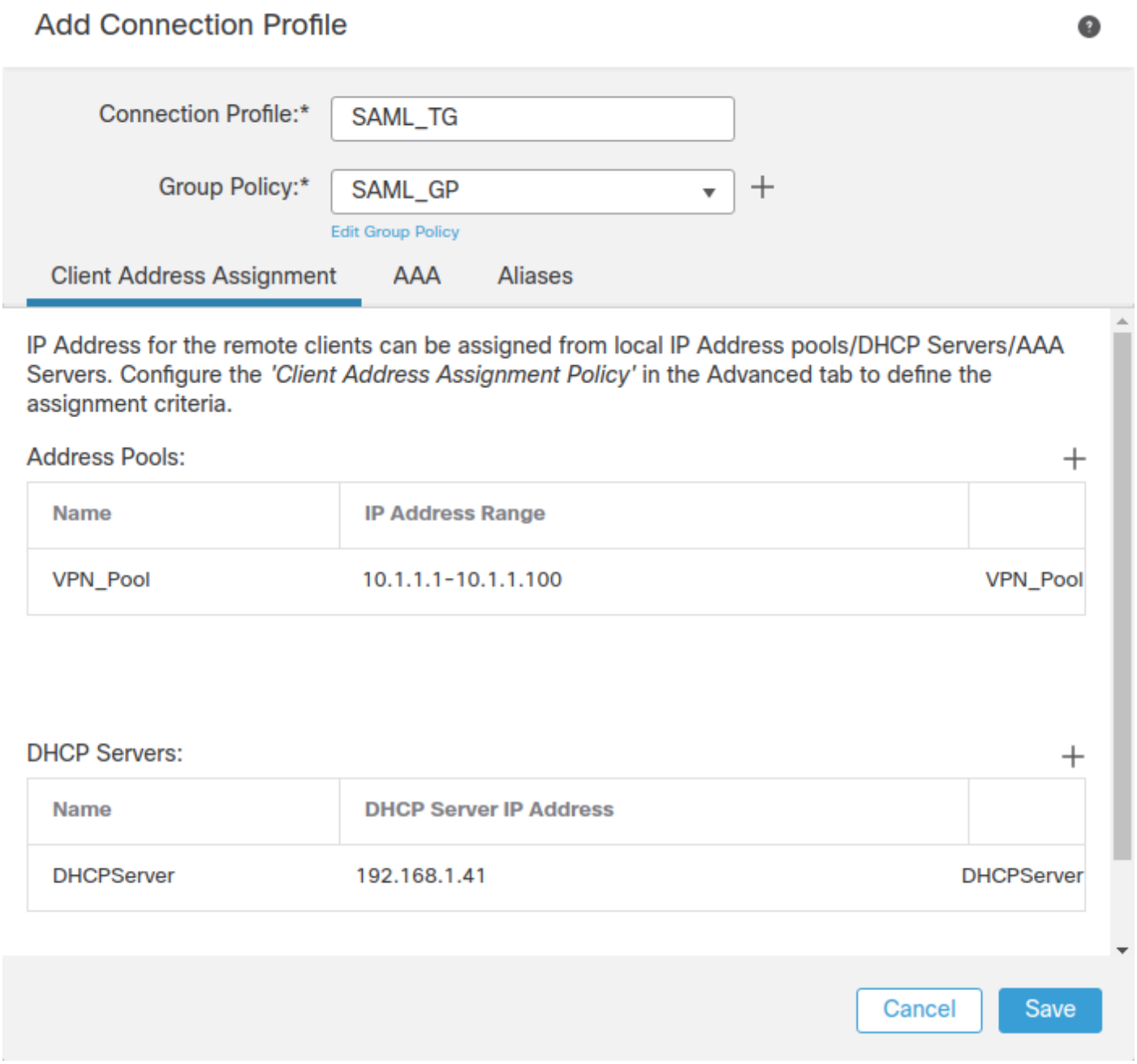
Passaggio 5. Configurare **Connection Profile** che utilizza questo metodo di autenticazione. Passa a **Devices > Remote Access** e quindi modificare il **VPN Remote Access** configurazione.



Passaggio 6. Fare clic sul segno più **+** e aggiungere un altro **Connection Profile**.

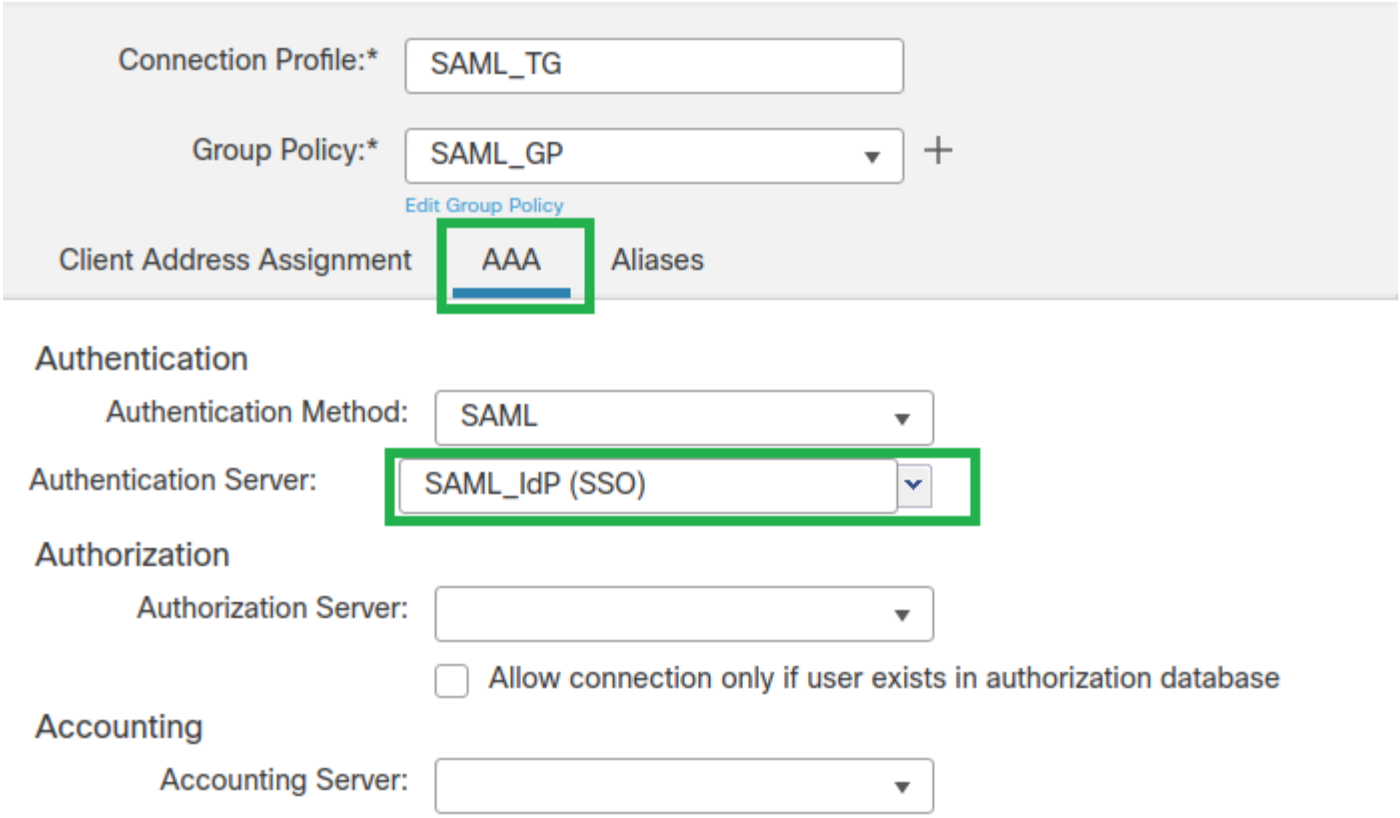


Passaggio 7. Creare il nuovo **Connection Profile** e aggiungere la VPN corretta, **Pool**o server DHCP.



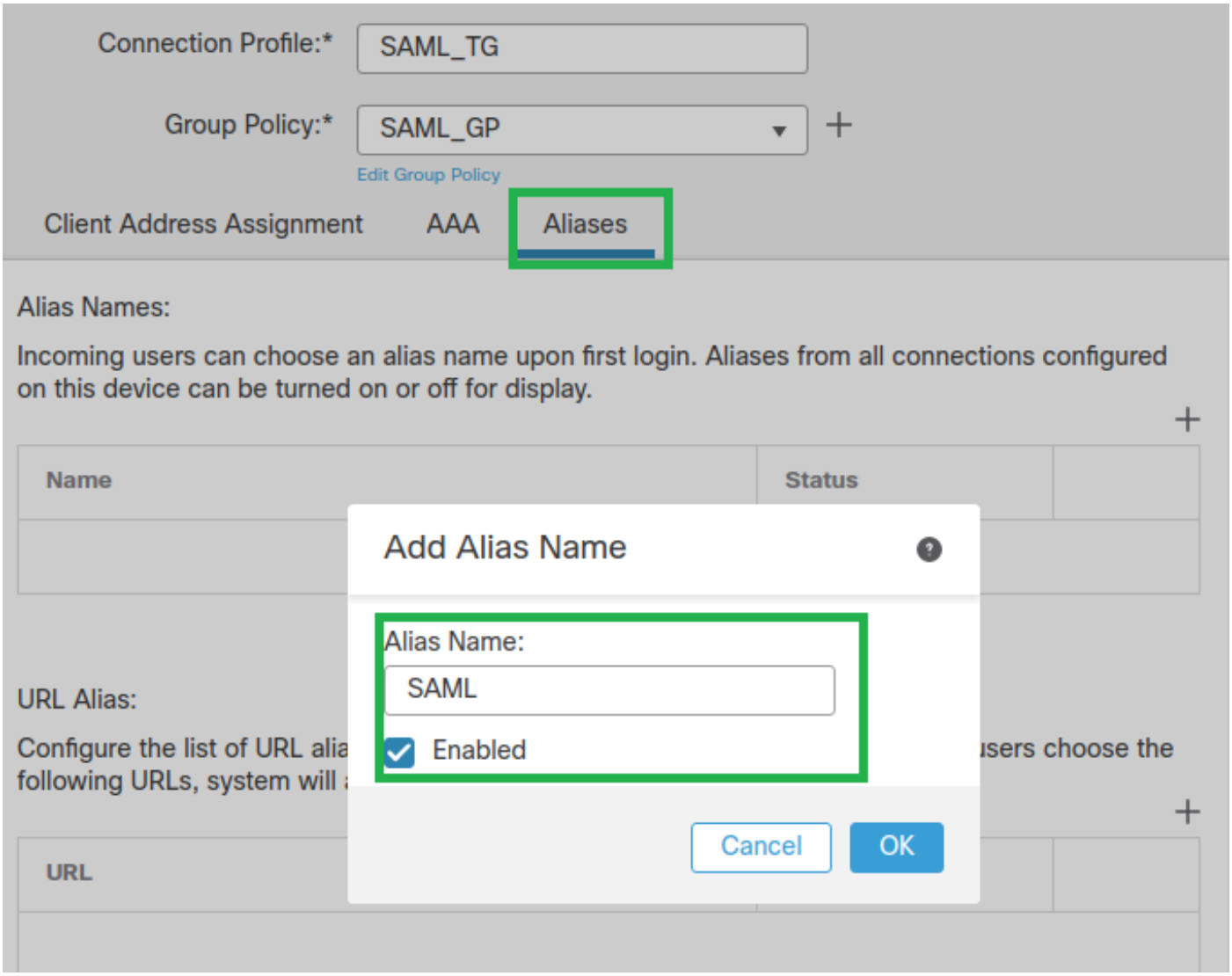
Passaggio 8. Selezionare la scheda AAA. Sotto la **Authentication Method** selezionare SAML.

Sotto la **Authentication Server** selezionare l'oggetto SAML creato al punto 4.



Passaggio 9. Creare un alias di gruppo per mappare le connessioni a questo **Connection Profile**. Questo è il tag che gli utenti possono visualizzare sul **AnyConnect** Menu a discesa Software.

Una volta configurato, fare clic su OK e salvare la **SAML Authentication VPN** configurazione.



Passaggio 10. Passare a **Deploy > Deployment** e selezionare l'FTD appropriato per applicare **SAML Authentication VPN** modifiche.

Passaggio 11. Fornire l'FTD **metadata.xml** all'**IdP** in modo da aggiungere l'FTD come dispositivo attendibile.

Dalla CLI FTD, eseguire il comando **show saml metadata SAML_TG** dove SAML_TG è il nome del **Connection Profile** creato nel passo 7.

Questo è l'output previsto:

```
> 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>
```

Dopo il **metadata.xml** dall'FTD viene fornito all'IdP ed è come dispositivo attendibile, è possibile eseguire un test sotto la connessione VPN.

Verifica

Verificare che **VPN AnyConnect** connessione stabilita con SAML come metodo di autenticazione con i comandi seguenti:

```
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 : c0a801090000400005faad9a1
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
```

Risoluzione dei problemi

Alcuni comandi di verifica della CLI FTD possono essere utilizzati per risolvere i problemi di SAML e **Remote Access VPN** come indicato sulla staffa:

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

Nota: Risoluzione dei problemi **DART** dal **AnyConnect** anche il PC dell'utente.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).