

在通過FMC管理的FTD上配置具有SAML身份驗證的Anyconnect

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[組態](#)

[獲取SAML IdP引數](#)

[通過FMC在FTD上進行配置](#)

[驗證](#)

[疑難排解](#)

簡介

本檔案介紹 Security Assertion Markup Language (SAML) 透過FMC管理的FTD上的驗證。

必要條件

需求

思科建議瞭解以下主題：

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

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower Threat Defense (FTD) 版本6.7.0
- Firepower Management Center (FMC) 版本6.7.0
- ADFS來自 AD Server 使用SAML 2.0

附註：如果可能，請使用NTP伺服器同步FTD和IdP之間的時間。否則，請驗證它們之間的時間是否手動同步。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

此配置允許Anyconnect使用者與SAML身份服務提供商建立VPN會話身份驗證。

目前SAML的一些限制包括：

- FTD上的SAML支援驗證（6.7版本以後）和授權（7.0版本以後）。
- DAP評估中可用的SAML身份驗證屬性(類似於 RADIUS 屬性傳送於 RADIUS 不支援來自AAA伺服器的授權響應)。
- ASA在DAP策略上支援啟用SAML的隧道組。但是，您無法使用SAML身份驗證檢查使用者名稱屬性，因為SAML身份提供程式遮蔽了使用者名稱屬性。
- 因為 AnyConnect 由於嵌入式瀏覽器在每次VPN嘗試時都會使用新的瀏覽器會話，因此，如果 IdP使用HTTP會話cookie來跟蹤登入狀態，使用者每次都必須重新進行身份驗證。
- 在本例中， Force Re-Authentication 設定 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers 對 AnyConnect 已啟動SAML身份驗證。

此處提供的連結中介紹了更多限制或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

以下限制適用於ASA和FTD:"Guidelines and Limitations for SAML 2.0"

附註：要在FTD上實施的所有SAML配置都可以在IdP提供的metadata.xml檔案中找到。

組態

本節介紹如何配置 AnyConnect 在FTD上使用SAML驗證

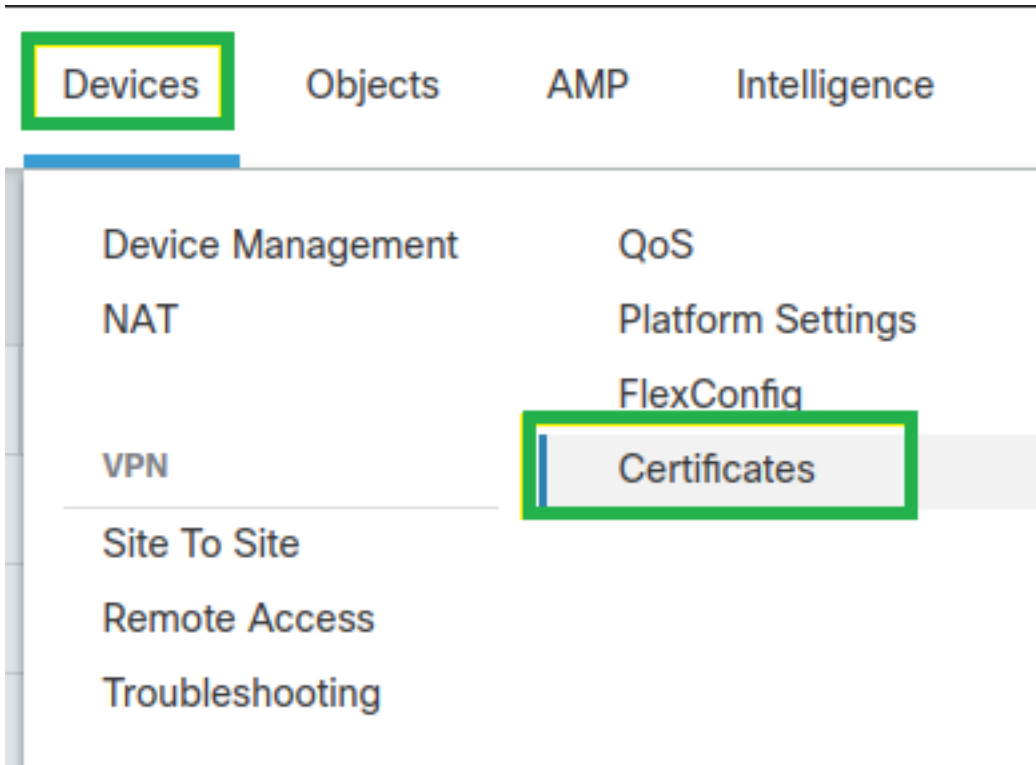
獲取SAML IdP引數

此圖顯示SAML IdP metadata.xml檔案。從輸出中，您可以獲取配置 AnyConnect 使用SAML的配置檔案：

```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://saml.lab.local/adfs/services/trust" EntityID uri="http://saml.lab.local/adfs/services/trust" />
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
  <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsfed/federation/2007/06" xmlns:sc="http://www.w3.org/2001/XMLSchema-instance" ServiceDisplayName="Josue Brenes - SAML Server - Lab.Local" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sec/trust/2005/12 http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/2007/06" xsi:type="fed:ApplicationServiceType" />
  <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsfed/federation/2007/06" xmlns:sc="http://www.w3.org/2001/XMLSchema-instance" ServiceDisplayName="Josue Brenes - SAML Server - Lab.Local" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sec/trust/2005/12 http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/2007/06" xsi:type="fed:SecurityTokenServiceType" />
  <KeyDescriptor use="signing">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#" />
    <X509Data />
    <X509Certificate>MIIC2DCCAccgAwIBAgIQW4pbH3XB1oxtUm/yofrL1TANBgkqhkiG9w0BAQsFAADAoH5YwJAYDVQQDExlBREZlIFNpZDZ3bmcgcj58Zl9Y1slmohY15sb2NhbG9AeFw0yMDA2MTYwHTU0HjlaFw0yMDA2MTYwHTU0HjlaMCGxJAKBghNVBAM
    </X509Data>
  </KeyDescriptor>
  <fed:TokenTypesOffered />
  <fed:ClaimTypesOffered />
  <fed:SecurityTokenServiceEndpoint />
  <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
    <fed:SecurityTokenServiceEndpoint />
    <fed:PassiveRequestorEndpoint />
  </EndpointReference>
  <RoleDescriptor />
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" />
  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" />
  <KeyDescriptor use="encryption">
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#" />
  </KeyDescriptor>
  <SingleLogoutService Location="https://saml.lab.local:444/adfs/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  <SingleLogoutService Location="https://saml.lab.local:444/adfs/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress />
  <NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
  <NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
  <NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient />
  <SingleSignOnService Location="https://saml.lab.local:444/adfs/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  <SingleSignOnService Location="https://saml.lab.local:444/adfs/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
```

通過FMC在FTD上進行配置

步驟1.在FMC上安裝並註冊IdP證書。 導航至 Devices > Certificates



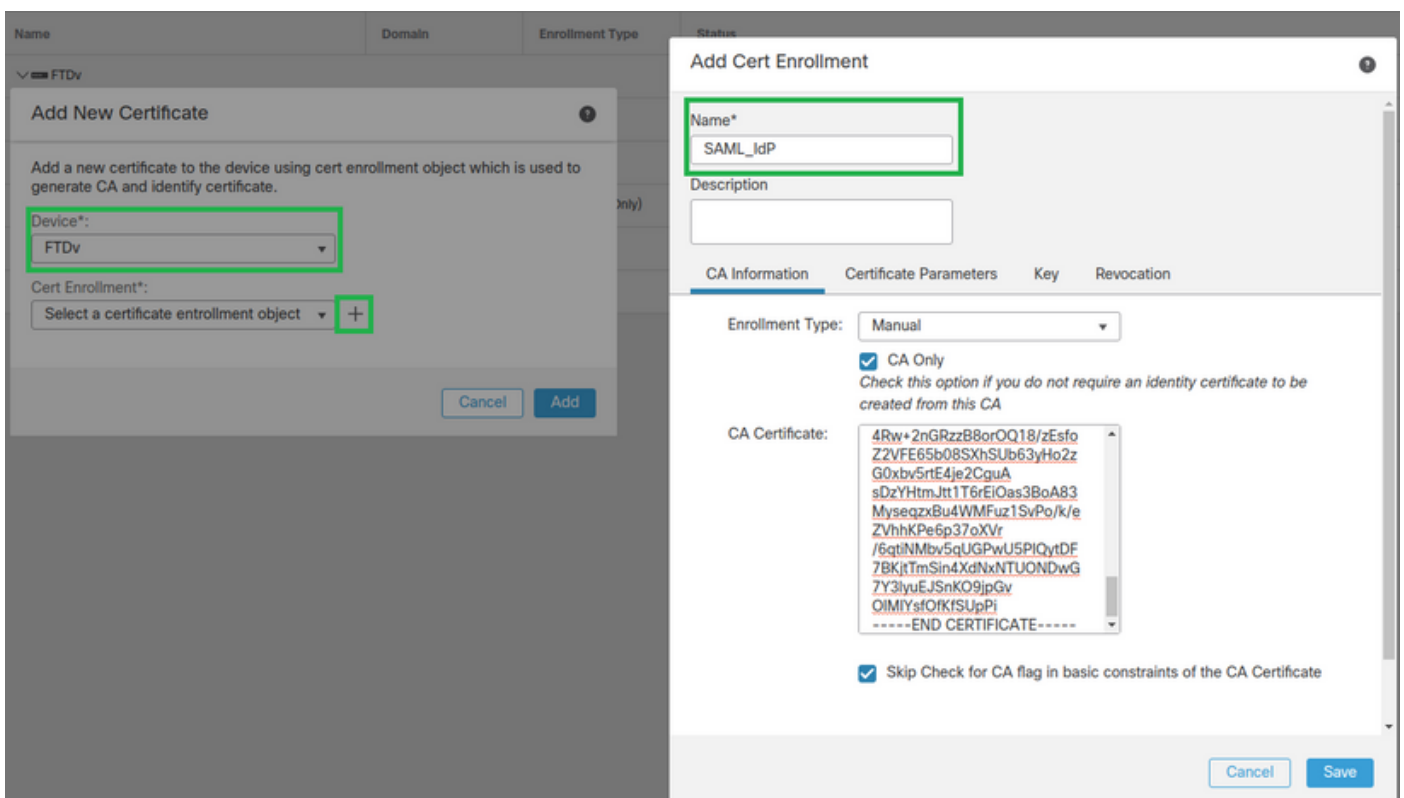
步驟2.單擊 Add.選擇要註冊到此證書的FTD。在「Cert Enrollment (證書註冊)」下，按一下加號 +號

在 Add Cert Enrollment 部分，使用任何名稱作為IdP證書的標籤。按一下 Manual.

檢查 CA Only 和 Skip Check 用於CA標誌欄位。

貼上 base64 格式IdP CA證書。

按一下 Save 然後按一下 Add.



步驟3.配置SAML伺服器設定。導航至 Objects > Object Management > AAA Servers > Single Sign-on Server.然後，選擇 Add Single Sign-on Server.



步驟4.根據 metadata.xml 檔案，請配置 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.

New Single Sign-on Server



Name*

Identity Provider Entity ID*

SSO URL*

Logout URL

Base URL

Identity Provider Certificate*



Service Provider Certificate



Request Signature

Request Timeout

seconds (1-7200)

Cancel

Save

步驟5.設定 Connection Profile 使用此身份驗證方法。導航至 **Devices > Remote Access** 然後編輯當前的 VPN Remote Access 組態。

Firepower Management Center Overview Analysis Policies **Devices** Objects AMP Intelligence

Name	Status	Last Modified
FTD_RemoteAccess	Targeting 1 devices Up-to-date on all targeted devices	2020-11-10 11:49:29 Modified by "admin"

步驟6.按一下加號+並添加另一個 Connection Profile.

FTD_RemoteAccess Save Cancel

Connection Profile Access Interfaces Advanced Policy Assignments (1)

+

步驟7.建立新的 Connection Profile 新增正確的VPN , Pool或DHCP伺服器。

Add Connection Profile

Connection Profile:* SAML_TG

Group Policy:* SAML_GP +
[Edit Group Policy](#)

Client Address Assignment AAA Aliases

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools: +

Name	IP Address Range	
VPN_Pool	10.1.1.1-10.1.1.100	VPN_Pool

DHCP Servers: +

Name	DHCP Server IP Address	
DHCPServer	192.168.1.41	DHCPServer

Cancel Save

步驟8.選擇AAA頁籤。在 Authentication Method 選項，選擇SAML。

在 Authentication Server 選項，選擇在步驟4中建立的SAML對象。

Connection Profile:* SAML_TG

Group Policy:* SAML_GP +

[Edit Group Policy](#)

Client Address Assignment **AAA** Aliases

Authentication

Authentication Method: SAML

Authentication Server: SAML_IdP (SSO)

Authorization

Authorization Server:

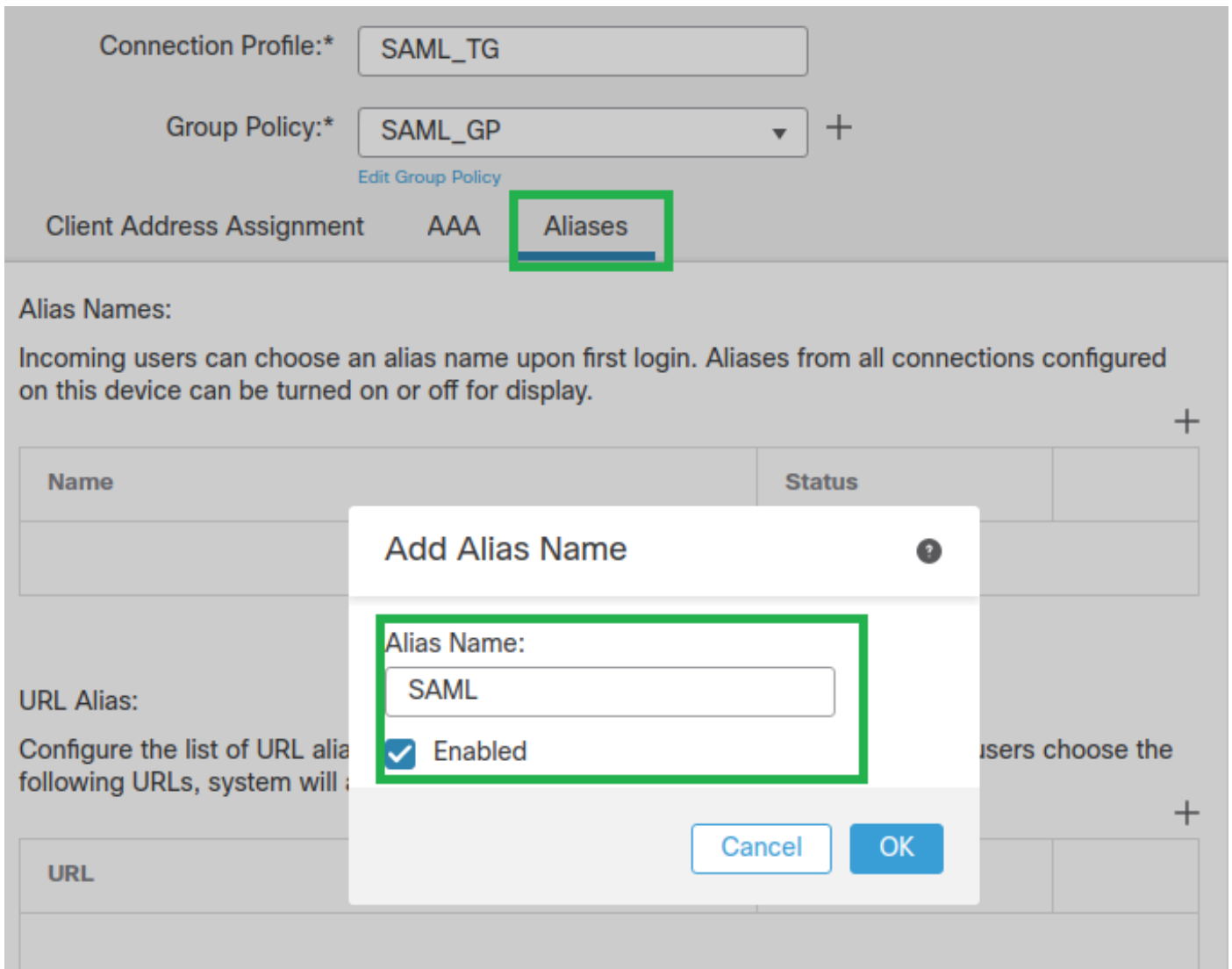
Allow connection only if user exists in authorization database

Accounting

Accounting Server:

步驟9. 創建組別名以將連線對映到此組 Connection Profile.這是使用者可以在上看到的標籤 AnyConnect 軟體下拉選單。

配置此配置後，按一下「確定」並儲存完整的 SAML Authentication VPN 組態。



步驟10. 導航至 **Deploy > Deployment** 並選擇適當的FTD以應用 **SAML Authentication VPN** 更改。

步驟11. 提供FTD **metadata.xml** 檔案至IdP，因此他們會將FTD新增為受信任裝置。

在FTD CLI上，執行命令 **show saml metadata SAML_TG** 其中SAML_TG是 **Connection Profile** 建立於Step 7。

這是預期輸出：

```
> 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
```



```
ADBAMRUwEwYKcZImiZPyLQBGryFbG9jYwWxEzARBgoJkiaJk/IsZAEZFgNsYWIxEjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQyMTlaMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQDDAsqLmxhYi5sb2NhbDCCASlwDQYJKoZIhvcNAQEBBQADgGEPADCCAQoCggEBAKfRmbCfWk+V1f+Y1sIE4hyY6+Qr1yKfg1wEqLOFhtGVM3re/WmFuD+4sCyU1Vkoijhf2+X8tG7x2WtpKktZM3N7bHpb7oPcuz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JjdK0CNjNedEKYcaG8PFRfUy31UPmCqQnEy+GYZipErrWtpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMYEY4F8sdc7bt1QQPKG9JIAWny9RvHBmLgj0px2i5Rp5k1JIECD9KHGj44051BEcvOFY6ecAPv4CkZB6C1oftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC AuUwggLhMBYGA1UdEQPMA2CCyoubGFilmxvY2FsMBOGA1UdDgQWBROkmTihXT/EjkMdpC4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWH1Hqxd11VIRYSCSCuHTa4TCBzQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049V01OLTVMEM5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9jZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNOQ2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbmQwgbkGCCsGAQUFBwEBBIIgSMIGpMIGmBggrBgEFBQcwAoBmWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWN1cyxDTj1TZXJ2aWN1cyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWNOQ2xhc3M9Y2VydGlmawNhdGlvbkF1dGhvcml0eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBAGCNxUHBDawLgYmKwYBAGCNxUIgYKsboLeU6B4ZUthLbxToW+yFILLh4iaWYXgpQUCAWQAQMwSwYDVR01BEQwQgYIKwYBBQUHAWEGCCsGAQUFBwMHBGgrBgEFBQcDBGyIKwYBBQUIAgIGCCsGAQUFBwMFBGgrBgEFBQcDQAgYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUFBwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUFBwMFMAoGCCsGAQUFBwMCMAYGBFUDJQAwdQYJKoZIhvcNAQELBQADggEBAKQnqcaUfz3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V Lmq04X1goaAs6obHrYftSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG5EQSCL1YqS31sTuarm4WPDJYmShc6hlUpswnCokGRMMgpx2GmDgv4Zf8SszJJ0NI4y 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 從FTD提供給IdP且它作為可信裝置，可以執行VPN連線下的測試。

驗證

驗證 VPN AnyConnect 已使用SAML建立連線，作為身份驗證方法，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

疑難排解

FTD CLI上的某些驗證命令可用於排除SAML和 Remote Access VPN 連線如括弧所示：

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

附註： 您可以進行疑難排解 DART 從 AnyConnect 使用者PC。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。