

FMCで管理されるFTDでのSAML認証を使用したAnyconnectの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[SAML IdPパラメータの取得](#)

[FMCによるFTDの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

この文書は次のことについて記述しています Security Assertion Markup Language (SAML) fmcを介して管理されるFTDの認証。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AnyConnect FMCでの設定
- SAMLおよびmetatada.xml値

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Threat Defense (FTD) version 6.7.0
- Firepower Management Center (FMC) version 6.7.0
- ADFS from AD Server SAML 2.0を使用

注：可能であれば、NTPサーバを使用してFTDとIdPの間で時刻を同期します。それ以外の場合は、時刻が手動で同期されていることを確認します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

この設定により、AnyconnectユーザはSAML Identity Service ProviderとのVPNセッション認証を確立できます。

SAMLの現在の制限事項には、次のようなものがあります。

- FTDのSAMLは、認証（バージョン6.7以降）と認可（バージョン7.0以降）でサポートされています。
- DAP評価で使用可能なSAML認証属性（SAML Authentication Attributeと類似）RADIUS送信された属性RADIUS AAAサーバからの許可応答はサポートされていません。
- ASAは、DAPポリシーでSAML対応のトンネルグループをサポートします。ただし、username属性はSAML IDプロバイダーによってマスクされるため、SAML認証でusername属性を確認することはできません。
- CAは自分の証明書に署名するので、CA管理者に連絡し、AnyConnect組み込みブラウザでは、VPNが試行されるたびに新しいブラウザセッションが使用されるため、IdPがHTTPセッションCookieを使用してログイン状態を追跡する場合、ユーザは毎回再認証を行う必要があります。
- この場合、Force Re-Authentication 設定 Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers ~ に影響を及ぼさない AnyConnect SAML認証を開始しました。その他の制限またはSAMLについては、ここに記載されているリンクを参照してください。

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

ASAおよびFTDには次の制限事項があります。「 」 Guidelines and Limitations for SAML 2.0 「 」

注：FTDに実装されるすべてのSAML設定は、IdPによって提供されるmetadata.xmlファイルにあります。

コンフィギュレーション

このセクションでは、WLCを設定するための AnyConnect FTDでのSAML認証を使用する場合

SAML IdPパラメータの取得

次の図に、SAML IdP metadata.xmlファイルを示します。この出力から、AnyConnect samlのプロファイル：

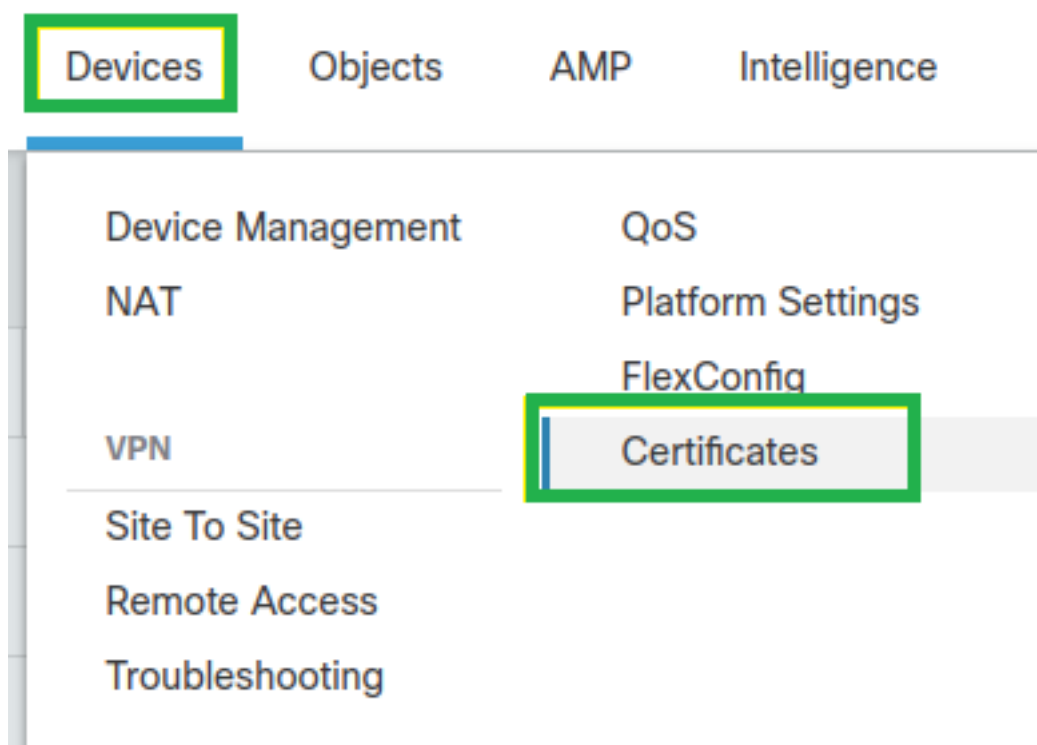
```

<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://saml.lab.local/adfs/services/trust" >> EntityID url
+ <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
+ <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsrfed/federation/200706" xmlns:xs="http://www.w3.org/2001/XMLSchema-instance" ServiceDisplayName="Josue Brenes - SAML Server - Lab.Local" protocolSupportEnumeration="http://docs.oasis-
open.org/ws-xf/ws-trust/200512 http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsrfed/federation/200706" xsi:type="fed:ApplicationServiceType">
- <RoleDescriptor xmlns:fed="http://docs.oasis-open.org/wsrfed/federation/200706" xmlns:xs="http://www.w3.org/2001/XMLSchema-instance" ServiceDisplayName="Josue Brenes - SAML Server - Lab.Local" protocolSupportEnumeration="http://docs.oasis-
open.org/ws-xf/ws-trust/200512 http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsrfed/federation/200706" xsi:type="fed:SecurityTokenServiceType">
- <KeyDescriptor use="signing">
+ <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#" >
- <X509Data >
+ <X509Certificate>MIICTDCCAcCgAwIBAgIQVqMpb4I3X3I0xUxm/Yofr1TTANBglqkqkiC9wBDAQsFADAoMSYwJAYDVQQDEx1BREZTIFNpZ225bmcglSBzrYW1sl.mshYi5sb2hhbDAeFw0yMDAxMjYwMTU0MjEafw0yMTAxMjYwMTU0MjEaMCgxJAkBgNVBAM
/<X509Data>
+ <KeyInfo>
+ <KeyDescriptor>
+ <fed:TokenTypesOffered>
+ <fed:ClaimTypesOffered>
+ <fed:SecurityTokenServiceEndpoint>
+ <EndpointReference xmlns="http://www.w3.org/2005/08/addressing">
+ <fed:SecurityTokenServiceEndpoint>
+ <fed:PassiveRequestorEndpoint>
+ <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="signing">
+ <KeyDescriptor use="signature">
+ <SingleLogoutService Location="https://saml.lab.local:444/adfs/ls/" >> Url sign-out
+ <SingleLogoutService Location="https://saml.lab.local:444/ads/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
+ <NameIDFormat urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress </NameIDFormat>
+ <NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:persistent </NameIDFormat>
+ <NameIDFormat urn:oasis:names:tc:SAML:2.0:nameid-format:transient </NameIDFormat>
+ <SingleSignOnService Location="https://saml.lab.local:444/adfs/ls/" >> Url sign-in (sign-on)
+ <SingleSignOnService Location="https://saml.lab.local:444/ads/ls/" binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>

```

FMCによるFTDの設定

ステップ1:FMCにIdP証明書をインストールして登録します。 移動先 **Devices > Certificates**



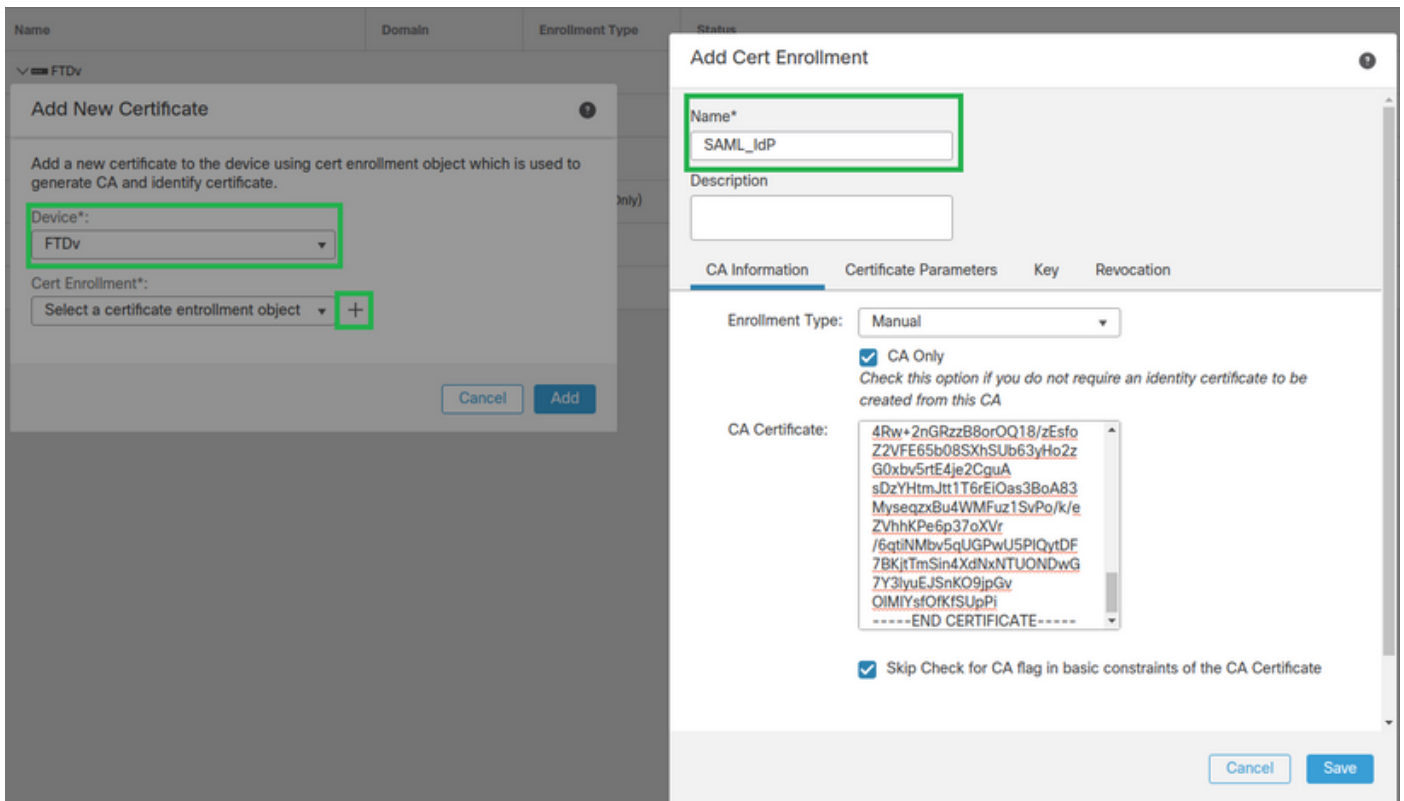
ステップ2:[Click] Add. この証明書に登録するFTDを選択します。 [Cert Enrollment]で、プラス記号 (+) をクリックします

内 Add Cert Enrollment IdP証明書のラベルとして任意の名前を使用します。クリック **Manual**.

次を確認します。 **CA Only** と **Skip Check CA**フラグフィールドの場合。

貼り付け **base64 format IdP CA cert**

クリック **Save** 次に、 **Add**.



ステップ3:SAMLサーバの設定を行います。移動先 **Objects > Object Management > AAA Servers > Single Sign-on Server**.次に、 **Add Single Sign-on Server**.



ステップ4:次に基づく **metadata.xml** ファイルはIdPによってすでに提供されています。 **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*

SAML_IdP

Identity Provider Entity ID*

http://saml.lab.local/adfs/services,

SSO URL*

https://saml.lab.local:444/adfs/ls/

Logout URL

https://saml.lab.local:444/adfs/ls/

Base URL

https://ftd.lab.local

Identity Provider Certificate*

SAML_IdP



Service Provider Certificate

SSL_Wildcard.lab.local



Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

Cancel

Save

ステップ5:設定 Connection Profile この認証方式を使用します。移動先 Devices > Remote Access 現在の設定を編集します VPN Remote Access ありません。

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"

ステップ6:プラス記号(+)をクリックし、別の記号を追加します。 Connection Profile.

FTD_RemoteAccess Save Cancel

Connection Profile Access Interfaces Advanced Policy Assignments (1)

+

ステップ7 : 新しいVLANを Connection Profile 適切なVPNを追加します Pool、またはDHCPサーバ。

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

ステップ8:[AAA]タブを選択します。下 Authentication Method [SAML]を選択します。

下 Authentication Server オプションで、手順4で作成したSAMLオブジェクトを選択します。

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:

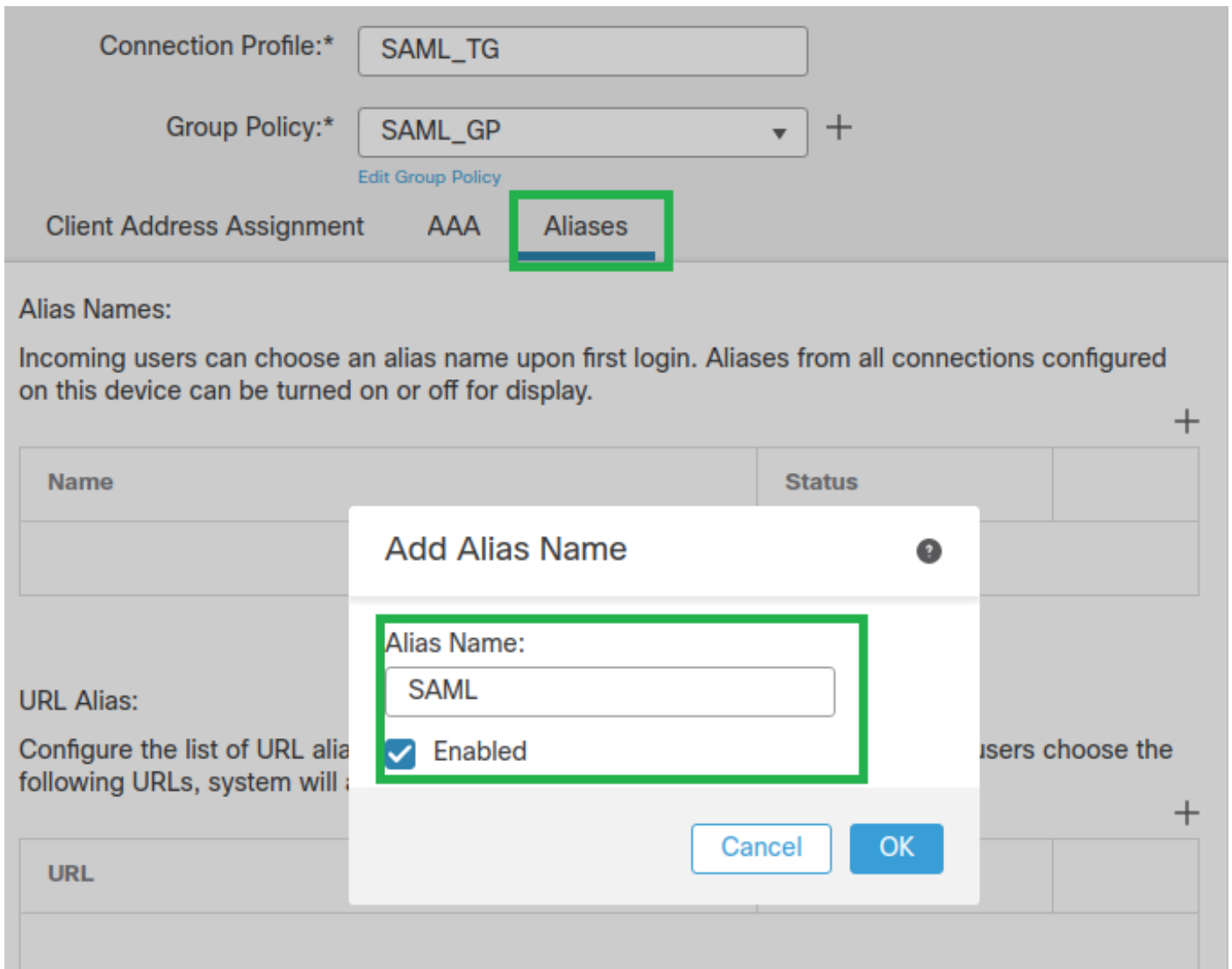
Allow connection only if user exists in authorization database

Accounting

Accounting Server:

手順9 : 接続をここにマッピングするためのグループエイリアスを作成します Connection Profile. これは、ユーザが AnyConnect [ソフトウェア]ドロップダウンメニュー

これが設定されたら、[OK]をクリックして完了を保存します SAML Authentication VPN ありません。



ステップ10:次に移動 **Deploy > Deployment** 適切なFTDを選択して、 **SAML Authentication VPN** 保存します。

ステップ11:FTDの提供 **metadata.xml** ファイルをIdPに保存し、FTDを信頼できるデバイスとして追加します。

FTD CLIで、次のコマンドを実行します **show saml metadata SAML_TG** ここで、SAML_TGは **Connection Profile** ステップ7で作成します。

予想される出力を次に示します。

```
> 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>MIIFlzCCBL+gAWIBAgITyAAAAABN6dX+H0cOFyWAAAAAAEzANBqkqhkiG9w0BAQsF
ADBAMRUwEwYKcZImiZPyLQBGryFbG9jYwWxEzARBgoJkiaJk/IsZAEZFgNsYWIxEjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQy
MTlaMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQQDDAsqLmxhYi5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBBAKfRmbCfWk+V1f+Y1sIE4hyY6+QrlyKf
glwEqLOFhtGVM3re/WmFuD+4sCyU1Vkoijhf2+X8tG7x2WTPkKtZM3N7bHpb7oPcuz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JjdK0CNjNedEkYcaG8
PFRfUy31UPmCqQnEy+GYZipErrWTPwWbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMyEY4F8sdc7btlQQPKG9JIAwNy9RvHBmLgj0px2i5Rp5k1JIECD9KHGj44051BEcv
OFY6ecAPv4CkZB6C1oftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwggLhMBYGA1UdEQQPMAC2CCyoubGFILmxvY2FsMBOGA1UdDgQWBROkmTIhXT/
EjkmDpc4aM6PTnyKpZafBgNVHSMEGDAWgBTEPQVWHlHqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMiHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V01OLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWNl
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz
dHJpYnV0aW9uUG9pbmQwgbkGCCsGAQUFBwEBBIBGSMIGpMIGmBggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmawNhdGlv
bkF1dGhvcml0eTA0BgNVHQ8BAf8EBAMCBaAwPQYJKwYBAGCNxUHBDawLgYmKwYB
BAGCNxUIgYKsboLeOU6B4ZUthLbxToW+yFILLh4iaWYXgpQUCAWQAQMwSwYDVR01
BEQwQgYIKwYBBQUHAWEGCCsGAQUFBwMHBGgrBgEFBQcDBGyIKwYBBQUIAgIGCCsG
AQUFBwMFBGgrBgEFBQcDAGYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUDJQAwdQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYftSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG
5EQSCL1YqS31sTuarm4WPDJyMShc6hlUpswnCokGRMMgpx2GmDgv4Zf8SzJJ0NI4y
DgMozuObwKNUXuhbiLuoXwvb2Whm1lysidpl+v9kplRYamyjFUo+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>
```

その後 metadata.xml ftdからIdPに提供され、信頼できるデバイスとしてVPN接続の下でテストを実行できます。

確認

次のことを確認します。VPN AnyConnect 次に示すコマンドを使用して、SAMLを認証方式として接続が確立されました。

```
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

トラブルシューティング

FTD CLIの一部の検証コマンドを使用して、SAMLおよびSAML Remote Access VPN ブラケットに表示される接続:

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

注：トラブルシューティングが可能 DART AnyConnect ユーザPCも同様です

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。