FMC를 통해 관리되는 FTD에서 SAML 인증을 사용하여 Anyconnect 구성

목차

소개

이 문서에서는 **Security Assertion Markup Language (SAML)** fmc를 통해 관리되는 FTD에 대한 인증

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- **AnyConnect** fmc의 컨피그레이션
- SAML 및 metatada.xml 값

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- **Firepower Threat Defense (FTD)** 버전 6.7.0
- **Firepower Management Center (FMC)** 버전 6.7.0
- AD FS 보낸 사람 **AD Server** SAML 2.0 사용

  참고: 가능하면 NTP 서버를 사용하여 FTD와 IdP 간의 시간을 동기화합니다. 그렇지 않으면 시간이 수동으로 동기화되어 있는지 확인합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 컨피그레이션을 통해 Anyconnect 사용자는 SAML ID 서비스 공급자를 사용하여 VPN 세션 인증을 설정할 수 있습니다.

SAML에 대한 현재 제한 사항은 다음과 같습니다.

- FTD의 SAML은 인증(버전 6.7 이후) 및 권한 부여(버전 7.0 이후)에 지원됩니다.
- DAP 평가에서 사용 가능한 SAML 인증 특성(과 유사) **RADIUS** 보낸 특성 **RADIUS** AAA 서버의 권한 부여 응답은 지원되지 않습니다.
- ASA는 DAP 정책에서 SAML 지원 터널 그룹을 지원합니다. 그러나 사용자 이름 특성은 SAML ID 공급자에 의해 마스킹되므로 SAML 인증에서는 사용자 이름 특성을 확인할 수 없습니다.

- 왜냐하면 **AnyConnect** 임베디드 브라우저는 모든 VPN 시도에서 새로운 브라우저 세션을 사용하므로, IdP가 HTTP 세션 쿠키를 사용하여 로그인 상태를 추적하는 경우 사용자는 매번 재인증해야 합니다.
- 이 경우 **Force Re-Authentication** 설정 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers** 에 영향을 미치지 않음 **AnyConnect** SAML 인증을 시작했습니다.

SAML에 대한 더 많은 제한 사항은 여기에 제공된 링크에 설명되어 있습니다.

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

이러한 제한은 ASA 및 FTD에 적용됩니다. "**Guidelines and Limitations for SAML 2.0**"

> **참고:** FTD에 구현할 모든 SAML 컨피그레이션은 IdP에서 제공하는 metadata.xml 파일에서 찾을 수 있습니다.

설정

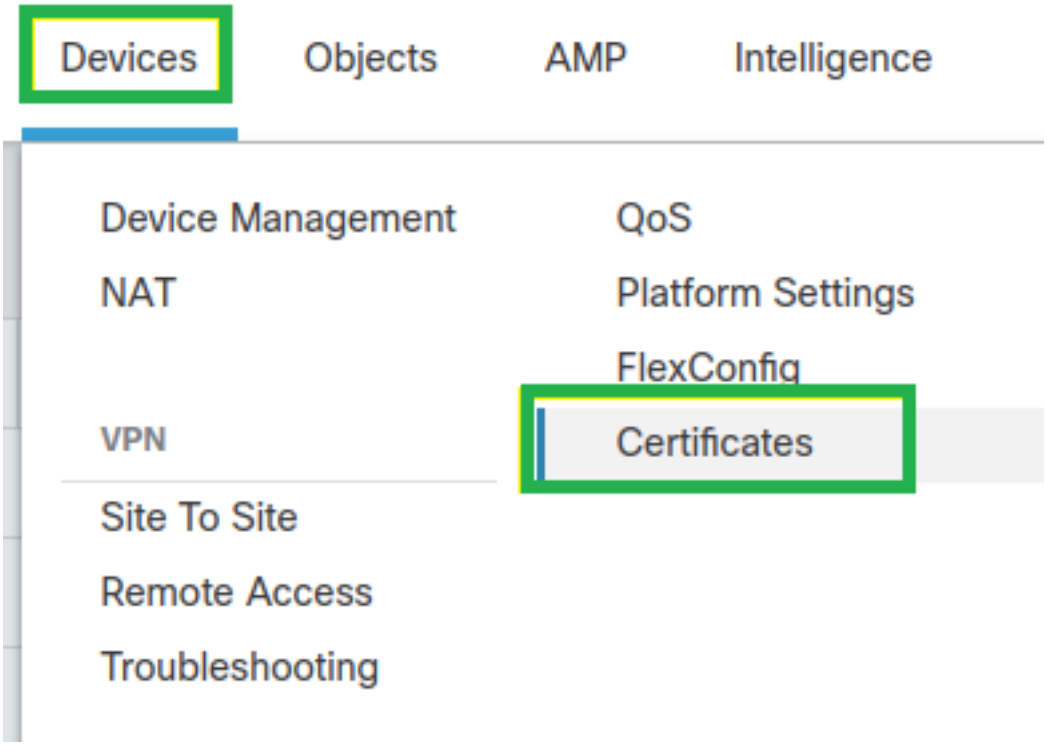
이 섹션에서는 구성 방법에 대해 설명합니다 **AnyConnect** FTD에서 SAML 인증 사용

SAML IdP 매개변수 가져오기

이 그림에서는 SAML IdP metadata.xml 파일을 보여 줍니다. 출력에서 를 구성하는 데 필요한 모든 값을 가져올 수 있습니다. **AnyConnect** SAML을 사용한 프로파일:

FMC를 통한 FTD 컨피그레이션

1단계. FMC에 IdP 인증서를 설치하고 등록합니다. 탐색 **Devices > Certificates**



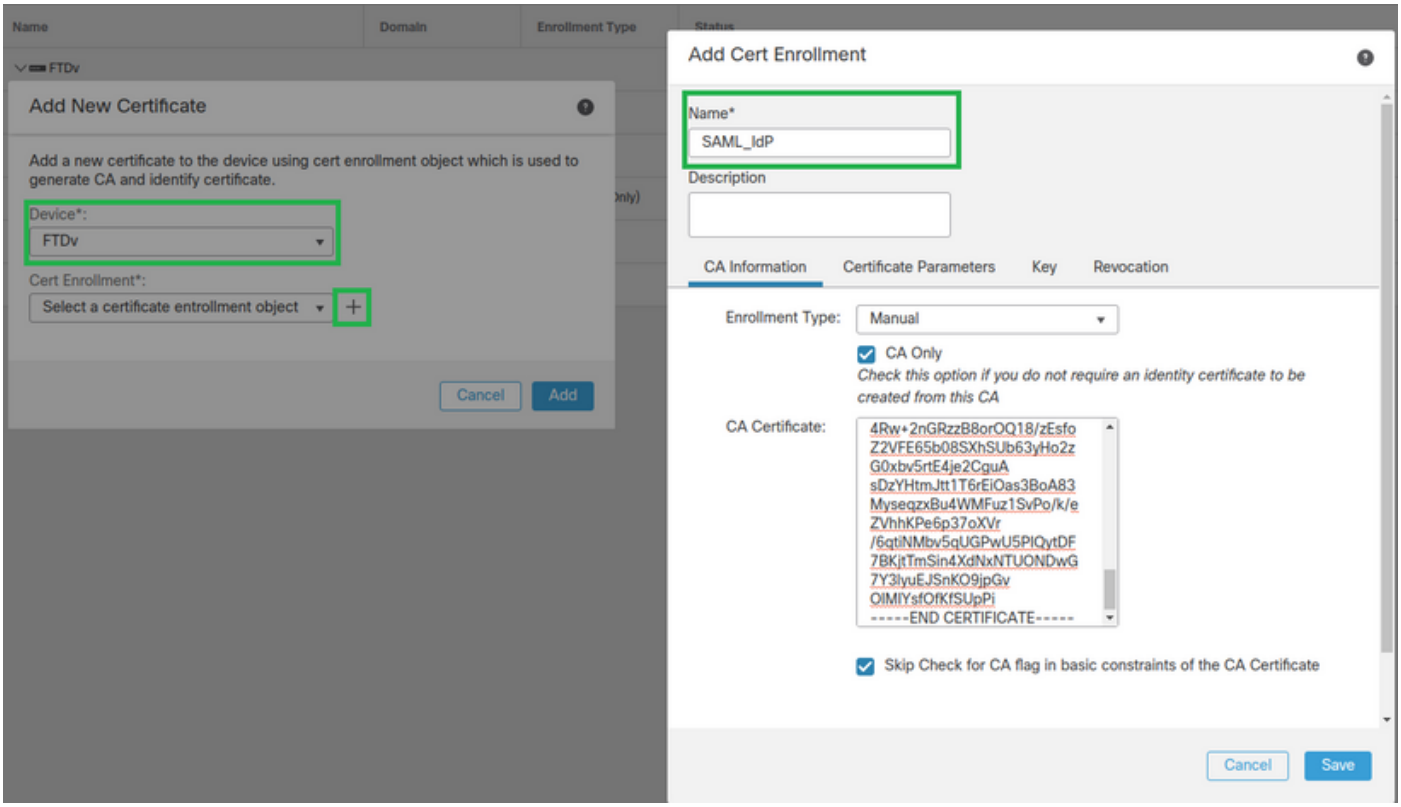
2단계. 클릭 **Add**. 이 인증서에 등록할 FTD를 선택합니다. Cert Enrollment(인증서 등록)에서 더하기 **+** 기호를 클릭합니다.

의 **Add Cert Enrollment** 섹션에서 임의의 이름을 IdP 인증서의 레이블로 사용합니다. 클릭 **Manual.**

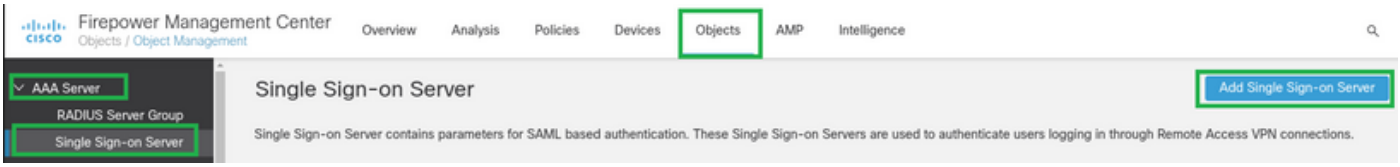
확인 **CA Only** 및 **Skip Check** CA 플래그 필드

붙여넣기 **base64** IdP CA 인증서 형식

클릭 **Save** 다음을 클릭합니다. **Add.**

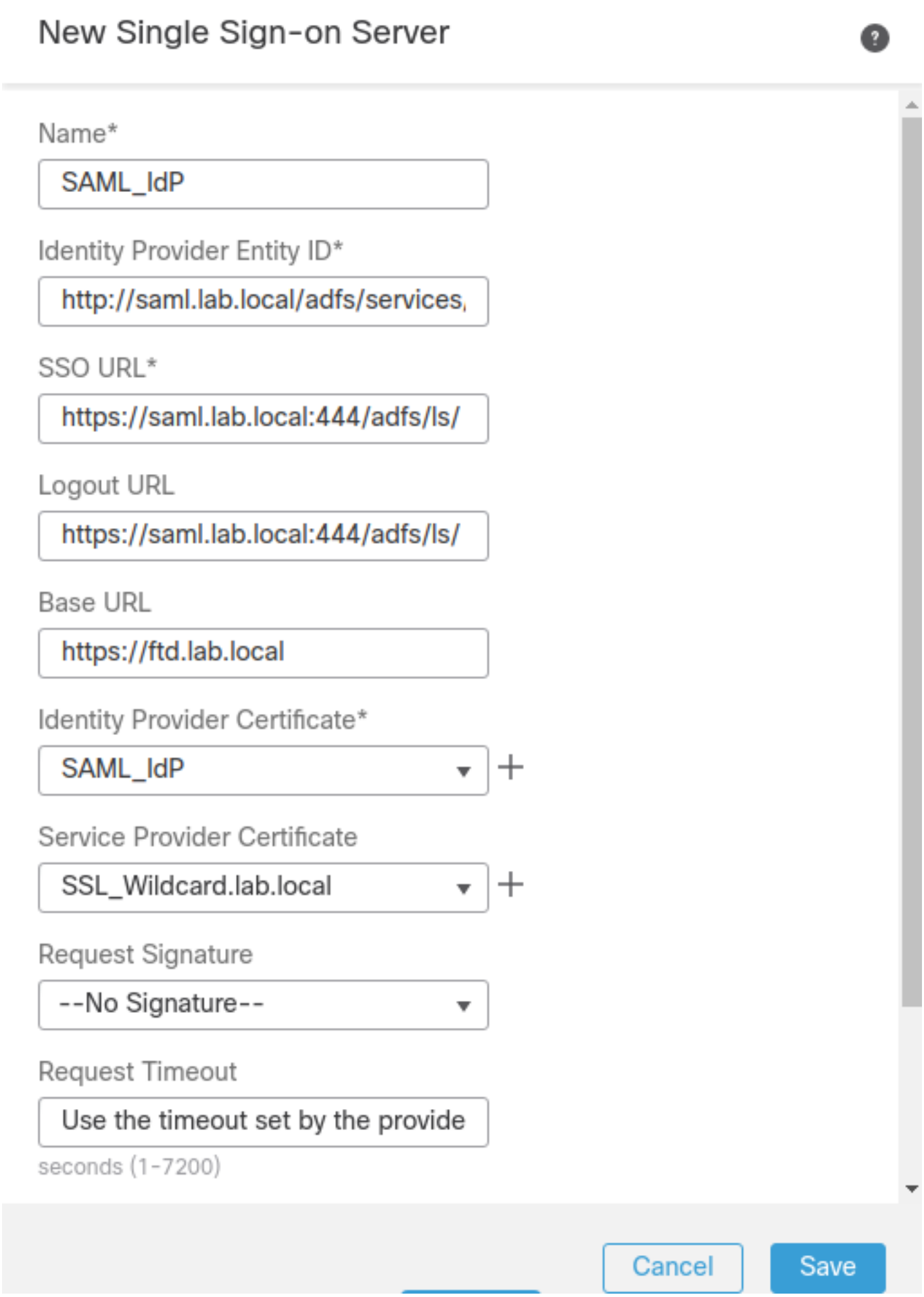


3단계. SAML 서버 설정을 구성합니다. 탐색 **Objects > Object Management > AAA Servers > Single Sign-on Server**. 그런 다음 **Add Single Sign-on Server**.

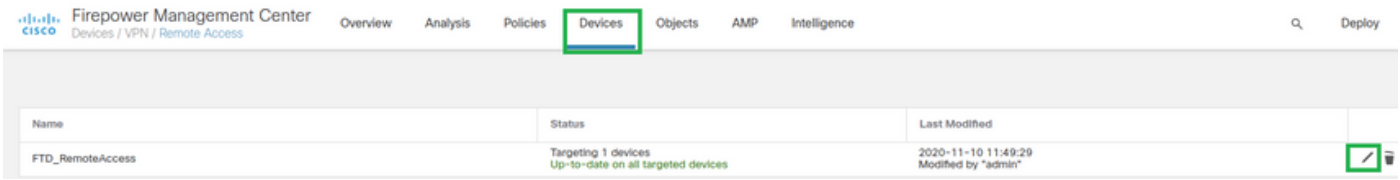


4단계. **metadata.xml** IdP에서 이미 제공한 파일이므로 **New Single Sign-on Server**.

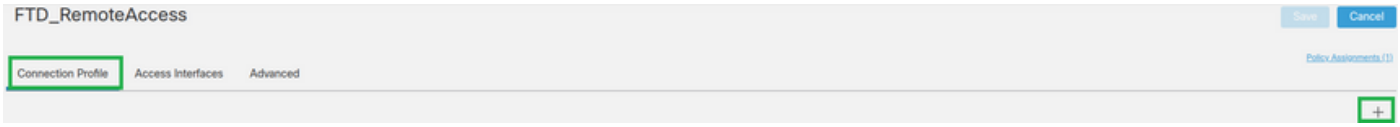
```
SAML Provider Entity ID: entityID from metadata.xml
SSO URL: SingleSignOnService from metadata.xml.
Logout URL: SingleLogoutService from metadata.xml.
BASE URL: FQDN of your FTD SSL ID Certificate.
Identity Provider Certificate: IdP Signing Certificate.
Service Provider Certificate: FTD Signing Certificate.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



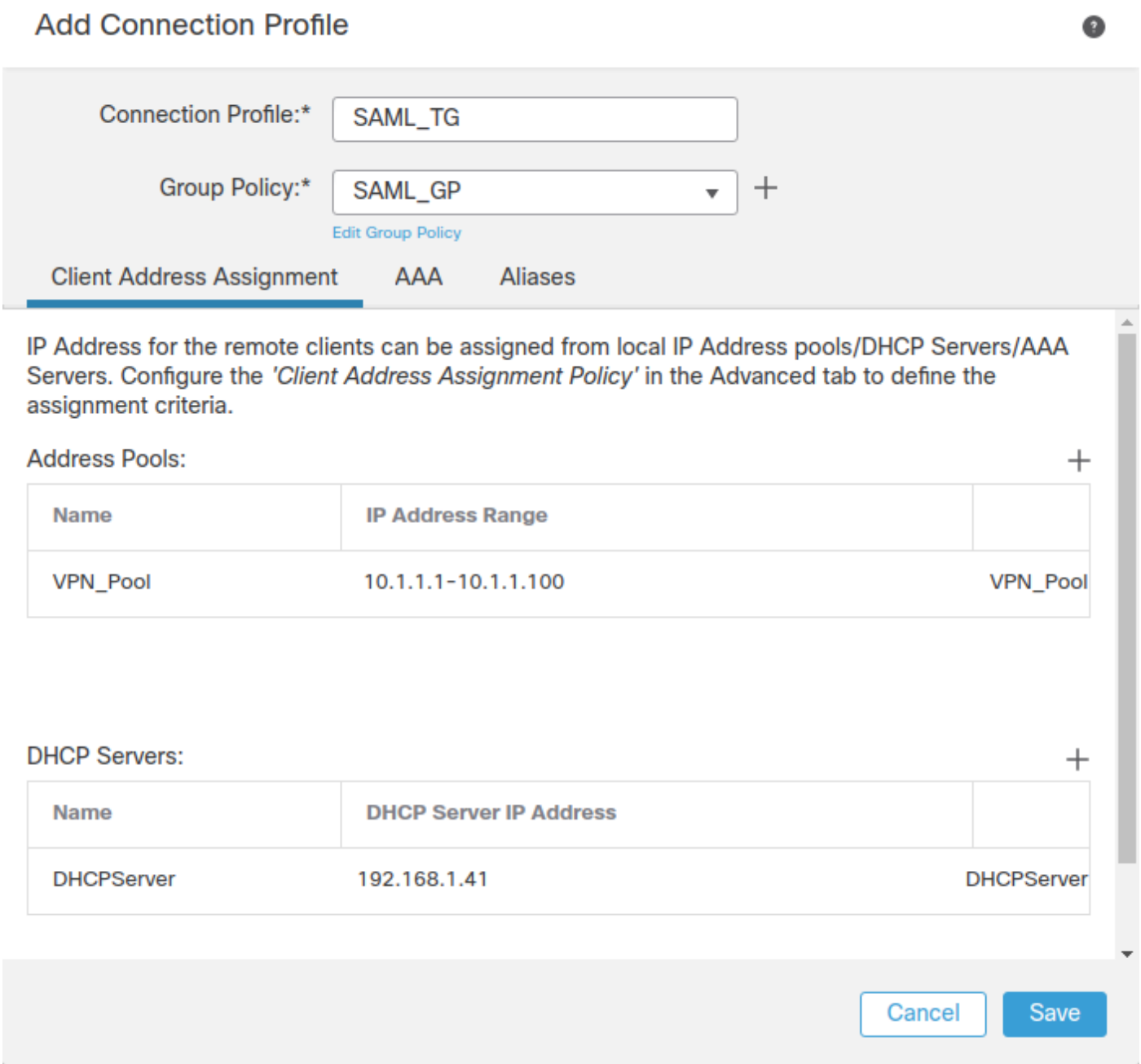
5단계. 구성 **Connection Profile** 이 인증 방법을 사용합니다. 탐색 **Devices > Remote Access** 현재 **VPN Remote Access** 설정.



6단계. 더하기 **+** 기호를 클릭하고 다른 기호를 추가합니다. **Connection Profile**.

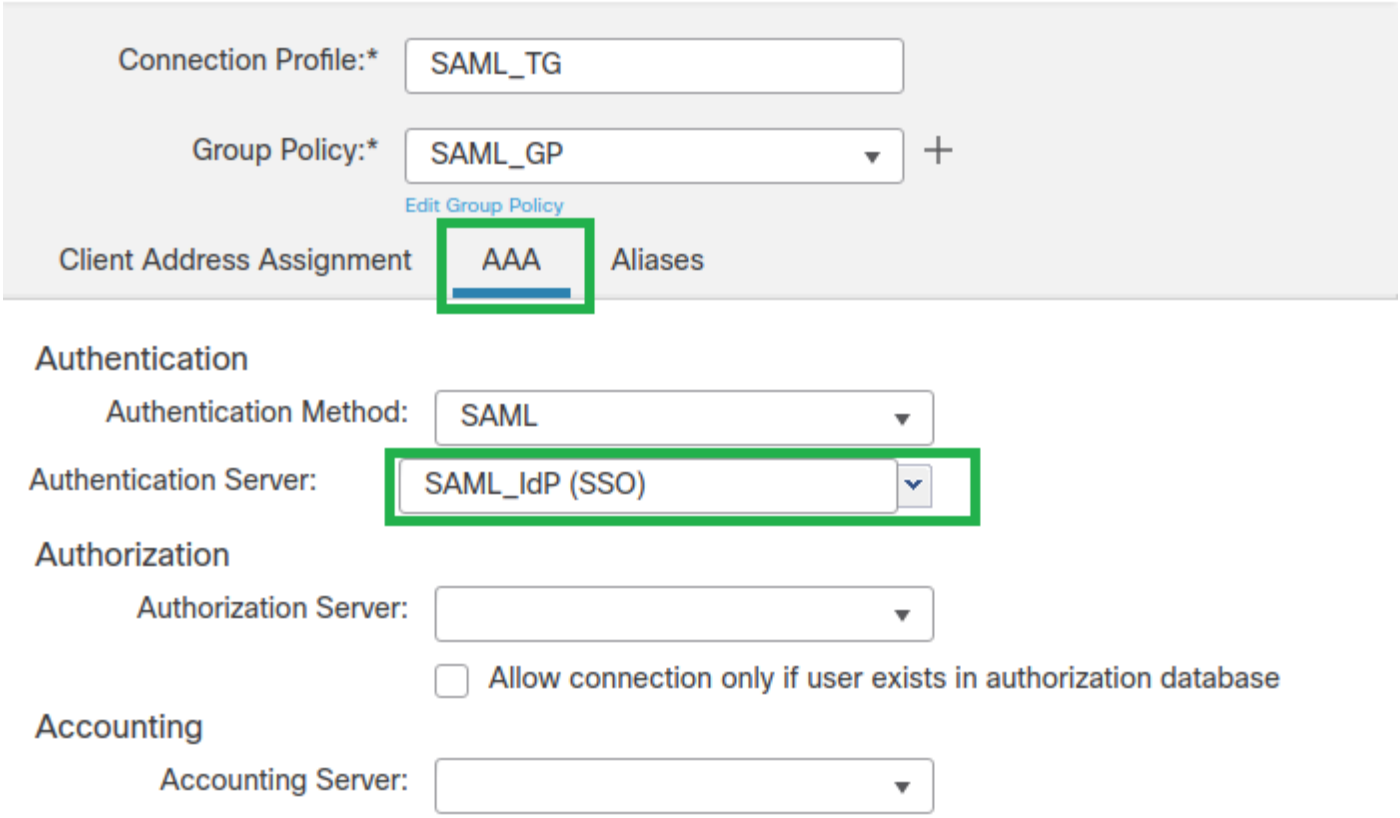


7단계. 새 **Connection Profile** 올바른 VPN을 추가하면 **Pool**또는 DHCP 서버입니다.



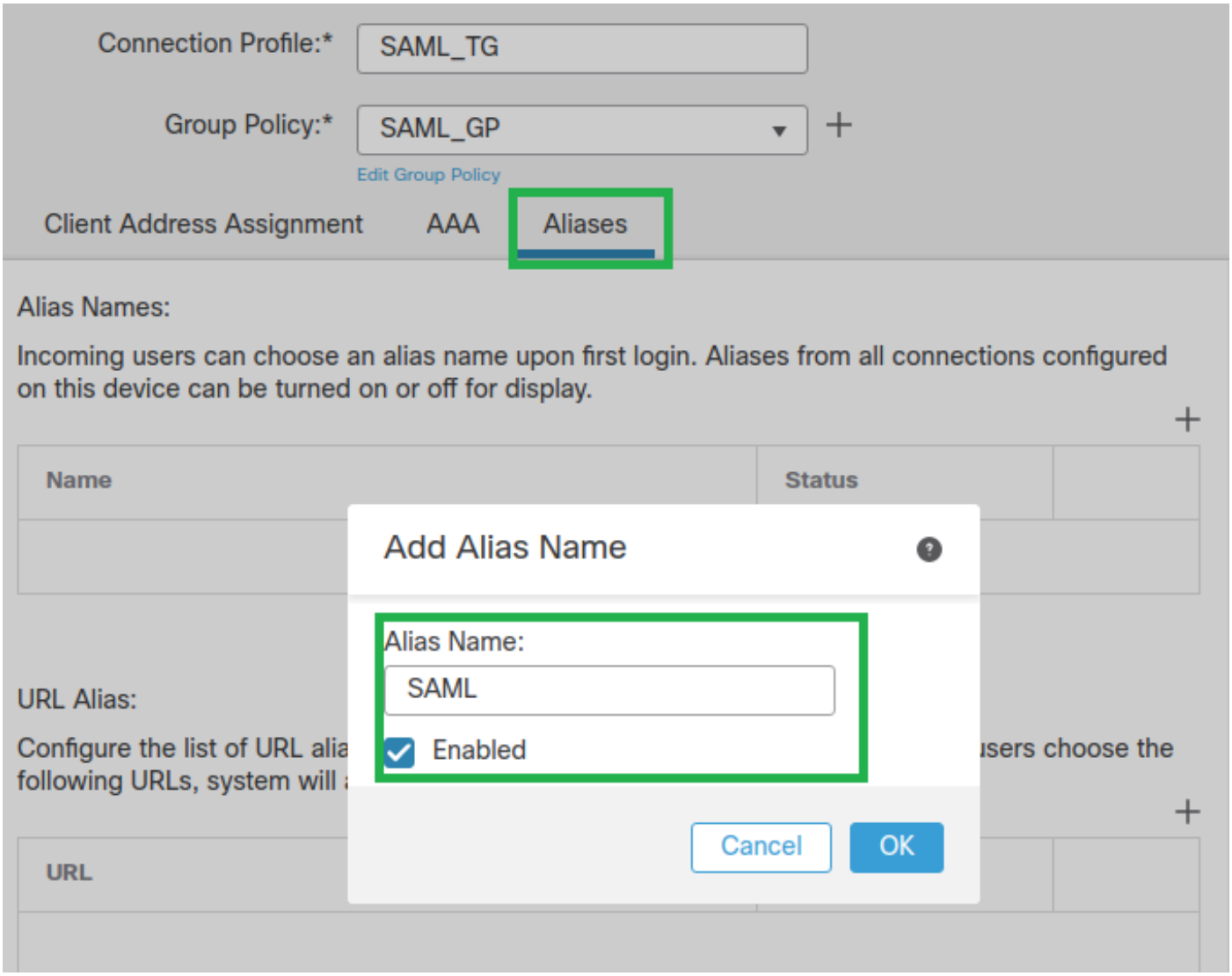
8단계. AAA 탭을 선택합니다. 아래 **Authentication Method** 옵션을 선택하고 SAML을 선택합니다.

아래 **Authentication Server** 4단계에서 생성한 SAML 객체를 선택합니다.



9단계. 그룹 별칭을 만들어 연결을 여기에 매핑합니다. **Connection Profile.** 사용자가 **AnyConnect** 소프트웨어 드롭다운 메뉴

구성이 완료되면 OK(확인)를 클릭하고 전체 내용을 저장합니다 **SAML Authentication VPN** 설정.



10단계. 다음으로 이동 **Deploy > Deployment** 올바른 FTD를 선택하여 **SAML Authentication VPN** 변경.

11단계. FTD 제공 **metadata.xml** 파일을 IdP에 **추가하여** FTD를 신뢰할 수 있는 디바이스로 추가합니다.

FTD CLI에서 명령을 실행합니다 **show saml metadata SAML_TG** 여기서 SAML_TG는 **Connection Profile** 7단계에서 생성되었습니다.

이는 예상 출력입니다.

```
> 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>
```

이후 **metadata.xml** ftd에서 IdP로 제공되며 신뢰할 수 있는 디바이스로서 VPN 연결 하의 테스트를 수행할 수 있습니다.

다음을 확인합니다.

다음을 확인합니다. **VPN AnyConnect** 다음 명령을 사용하여 인증 방법으로 SAML에 연결이 설정되었습니다.

```
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
```

문제 해결

FTD CLI의 일부 확인 명령을 사용하여 SAML 및 **Remote Access VPN** 대괄호에 표시된 연결:

```
firepower# show run webvpn
```

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

참고: 문제 해결 가능 **DART** 에서 **AnyConnect** 사용자 PC도 포함됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.