Configure AnyConnect with SAML Authentication on FTD Managed via FMC

Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configuration
Get the SAML IdP Parameters
Configuration on the FTD via FMC
Verify
<u>Froubleshoot</u>

Introduction

This document describes Security Assertion Markup Language (SAML) authentication on FTD managed over FMC.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- AnyConnect configuration on Firepower Management Center (FMC)
- SAML and metatada.xml values

Components Used

The information in this document is based on these software and hardware versions:

- Firepower Threat Defense (FTD) version 6.7.0
- FMC version 6.7.0
- ADFS from AD Server with SAML 2.0

Note: If possible, use an NTP server to synchronize time between the FTD and IdP. Otherwise, verify that the time is manually synchronized between them.

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. If your network is live, ensure that you understand the potential impact of any command.

Background Information

The configuration allows AnyConnect users to establish a VPN session authentication with a SAML Identity Service Provider.

Some of the current limitations for SAML are:

- SAML on FTD is supported for authentication (version 6.7 and higher) and authorization (version 7.0 and higher).
- SAML authentication attributes available in DAP evaluation (similar to RADIUS attributes sent in RADIUS authorization response from AAA server) are not supported.
- ASA supports SAML-enabled tunnel-group on DAP policy. However, you cannot check the username attribute with SAML authentication, because the username attribute is masked by the SAML Identity provider.
- Because AnyConnect with the embedded browser uses a new browser session on every VPN attempt, users must re-authenticate every time if the IdP uses HTTP session cookies to track login state.
- In this case, theForce Re-Authentication setting inConfiguration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servershas no effect on AnyConnect initiated SAML authentication.

More limitations or SAML are described in the link provided here.

Guidelines and Limitations for SAML 2.0

These limitations apply to ASA and FTD: Guidelines and Limitations for SAML 2.0.

Note: All of the SAML configurations to be implemented on the FTD can be found on the metadata.xml file provided by your IdP.

Configuration

This section describes how to configure AnyConnect with SAML authentication on FTD

Get the SAML IdP Parameters

This image shows a SAML IdP metadata.xml file. From the output, you can obtain all values required to configure the AnyConnect profile with SAML:



Configuration on the FTD via FMC

Step 1. Install and enroll the IdP certificate on the FMC. Navigate toDevices > Certificates.



Step 2. Click Add.Select the FTD to enroll in this certificate. Under Cert Enrollment, click the plus + sign.

In theAdd Cert Enrollment section, use any name as a label for the IdP cert. ClickManual.

Check the CA Only and Skip Checkfor CA flag fields.

Paste thebase64 format IdP CA cert.

ClickSave, then clickAdd.

Name	Domain	Enrollment Type	Status	
<=FTDv			Add Cert Enrollment	
Add New Certificate Add a new certificate to the device using cert end generate CA and identify certificate. Device*: FTDv Cert Enrollment*: Select a certificate entrollment object +	rollment object which is Cancel	s used to miy)	Add Cert Enrollment	•
			Carrel Save	•

Step 3. Configure the SAML server settings. Navigate toObjects > Object Management > AAA Servers > Single Sign-on Server, thenselectAdd Single Sign-on Server.

Cisco Firepower Manage Objects / Object Manage	ement Center Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	م
V AAA Server	Single Sign-on Se	rver						Add Single Sign-on Server
RADIUS Server Group Single Sign-on Server	Single Sign-on Server contains	parameters for	SAML based	authenticatio	n. These Sing	le Sign-on	Servers are used to authenticate users logging in throu	gh Remote Access VPN connections.

Step 4. Based on the metadata.xml file already provided by your IdP, configure the SAML values on theNew 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.

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*

▼ | +

Service Provider Certificate

SSL_Wildcard.lab.local +

Request Signature

--No Signature--

Request Timeout

Use the timeout set by the provide

seconds (1-7200)

Save

Step 5. Configure the Connection Profile that uses this authentication method. Navigate to Devices > Remote Access, then edit your current VPN Remote Access configuration.

alialia cisco	Firepower Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		٩	Deploy
Nam	0				Status				Last Modified		
FTD_	RemoteAccess				Targeting 1 devic Up-to-date on all	es I targeted device	05		2020-11-10 11:49:29 Modified by "admin"		∕ ≆

Step 6. Click on the plus + sign and add another Connection Profile.

FTD_RemoteAccess	Sive Cancel
Connection Profile Access Interfaces Advanced	Euler-Assistment,/1
	+

Step 7. Create the new Connection Profile and add the proper VPN, Pool, or DHCP Server.

Add Connection Profile

Connection Profile:*	SAML_TG]	
Group Policy:*	SAML_GP		•) +	
E	dit Group Policy				
Client Address Assignment	AAA	Aliases			

0

+

+

Save

Cancel

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

Step 8. Select the AAA tab. Under the Authentication Methodoption, select SAML.

Under the Authentication Serveroption, select the SAML object created in Step 4.

Connection Profile:* SAML_TG
Group Policy:* SAML_GP +
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:

Step 9. Create a group alias to map the connections to this Connection Profile. This is the tag that users can see on the AnyConnect Software drop-down menu.

When this is configured, click **OK** and **save** the complete SAML Authentication VPN configuration.

Connection Profile:*	SAML_TG]
Group Policy:*	SAML_GP		•] +
	Edit Group Policy			
Client Address Assignmen	t AAA	Aliases		

Alias Names:

Incoming users can choose an alias name upon first login. Aliases from all connections configured on this device can be turned on or off for display.

Name		Status		
	Add Alias Name		0	
URL Alias: Configure the list of URL alia following URLs, system will a	Alias Name: SAML C Enabled	Cancel	OK	users choose the +

Step 10. Navigate to **Deploy > Deployment** and select the proper FTD to apply the SAML Authentication VPN changes.

Step 11. Provide the FTD metadata.xml file to the IDP so they add the FTD as a trusted device.

On the FTD CLI, run the commandshow saml metadata SAML_TG where SAML_TG is the name of the Connection Profile created on Step 7.

This is the expected output:

<#root>

```
> 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
```

```
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="ur
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
<ds:KeyInfo xmins:ds="nttp://www.w3.org/2000/09/xmidsig#">
<ds:X509Data>
```

 $<\!\!ds:\!X509Certificate\!>\!MIIF1zCCBL+gAwIBAgITYAAAABN6dX+H0cOFYwAAAAAAEzANBgkqhkiG9w0BAQsFactored and the second second$

```
ADBAMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IsZAEZFgNsYWIx
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMT1aFw0yMjA0MTEwMTQy
MT1aMCMxCzAJBgNVBAYTAkNSMRQwEgYDVQQDDAsqLmxhYi5sb2NhbDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfWk+V1f+Y1sIE4hyY6+Qr1yKf
g1wEqLOFHtGVM3re/WmFuD+4sCyU1VkoiJhf2+X8tG7x2WTpKKtZM3N7bHpb7oPc
uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAygz6JJdK0CNjNEdEkYcaG8
PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdic7bt1QQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44051BEcv
OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwqqLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDqQWBBR0kmTIhXT/
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWH1Hqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V010LTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWM1MjBLZXk1MjBTZXJ2aWN1
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1z
dHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMIGmBggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWM1MjBLZXk1MjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv
bkF1dGhvcm10eTA0BgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR01
BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG
AQUFBwMFBggrBgEFBQcDAgYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADggEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYFtSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG
5EQSC1YqS31sTuarm4WPDJyMShc6h1UpswnCokGRMMqpx2GmDqv4Zf8SzJJ0NI4y
DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidp1+V9kp1RYamyjFUo+agx0E+L1zp8C
i0YEwYKXgKk3CZdwJfnYQuCWjmapYw1LGt5S59Uwegwro6AsUXY335+Z0rY/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</pre>
<SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://ftd</pre>
</EntityDescriptor>
```

After the metadata.xml from the FTD is provided to the IdP and it is as a trusted device, a test under the VPN connection can be performed.

Verify

Verify that the VPN AnyConnect connection was established with SAML as an authentication method with the commands seen here:

<#root>

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

Troubleshoot

Some verification commands on the FTD CLI can be used to troubleshoot SAML, and Remote Access VPN connection as seen in the bracket:

<#root>
firepower#
show run webvpn
firepower#
show run tunnel-group
firepower#
show crypto ca certificate
firepower#
debug webvpn saml 25

Note: You can troubleshoot DART from the AnyConnect user PC as well.