# Configurar o AnyConnect com autenticação SAML no FTD gerenciado via FMC

# Contents

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Configuração
Obter os Parâmetros IdP SAML
Configuração no FTD via FMC
Verificar
Troubleshooting

## Introdução

Este documento descreve a autenticação SAML (Security Assertion Markup Language) no FTD gerenciado no FMC.

## Pré-requisitos

#### Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Configuração do AnyConnect no Firepower Management Center (FMC)
- · Valores SAML e metatada.xml

#### **Componentes Utilizados**

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Threat Defense (FTD) versão 6.7.0
- FMC versão 6.7.0
- ADFS do Servidor AD com SAML 2.0

Observação: Se possível, use um servidor NTP para sincronizar o horário entre o FTD e o IdP. Caso contrário, verifique se a hora é sincronizada manualmente entre eles.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

A configuração permite que os usuários do AnyConnect estabeleçam uma autenticação de sessão VPN com um provedor de serviço de identidade SAML.

Algumas das limitações atuais do SAML são:

- O SAML no FTD é suportado para autenticação (versão 6.7 e superior) e autorização (versão 7.0 e superior).
- Os atributos de autenticação SAML disponíveis na avaliação DAP (semelhante aos atributos RADIUS enviados na resposta de autorização RADIUS do servidor AAA) não são suportados.
- O ASA oferece suporte ao grupo de túneis habilitado para SAML na política DAP. No entanto, você não pode verificar o atributo de nome de usuário com a autenticação SAML, pois o atributo de nome de usuário é mascarado pelo provedor de identidade SAML.
- Como o AnyConnect com o navegador incorporado usa uma nova sessão do navegador em cada tentativa de VPN, os usuários devem reautenticar sempre que o IdP usar cookies de sessão HTTP para rastrear o estado de login.
- Neste caso, o Force Re-Authentication definição em Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers não tem efeito na autenticação SAML iniciada pelo AnyConnect.

Mais limitações para SAML são descritas no link fornecido aqui.

#### Diretrizes e Limitações do SAML 2.0

Essas limitações se aplicam ao ASA e ao FTD: Diretrizes e Limitações para SAML 2.0.

Observação: todas as configurações SAML a serem implementadas no FTD podem ser encontradas no arquivo metadata.xml fornecido pelo seu IdP.

## Configuração

Esta seção descreve como configurar o AnyConnect com autenticação SAML no FTD

Obter os Parâmetros IdP SAML

Esta imagem mostra um arquivo metadata.xml do IdP SAML. Na saída, você pode obter todos os valores necessários para configurar o perfil do AnyConnect com SAML:

c2mit version="1.0"?> <exit(bes 0bit="" adfs="" cde="" entitvid="" eritryid_http:="" saml.ab.local="" services="" straines="LicsAML12.0:metadata" trust"="" url<br=""><i:sitydes 0bit="" adfs="" cde="" entitvid="" eritryid_http:="" saml.ab.local="" services="" straines="LicsAML12.0:metadata" trust"="" url<br=""><i:sitydes 0bit="" adfs="" cde="" entitvid="" eritryid_http:="" saml.ab.local="" services="" straines="LicsAML12.0:metadata" trust"="" url<br=""><i:sitydes 0bit="" adfs="" cde="" entitvid="" eritryid_http:="" saml.ab.local="" services="" straines="LicsAML12.0:metadata" trust"="" url<br=""><i:sitydes 0bit="" docs.oasis-<br="" eritryid_http:="" straines="LicsAML12.0:metadata">open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust="http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust="http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust="http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust="http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust="http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/0bit/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/trust.http://docs.oasis- open.org/vs:Xust=trust".200312 http://docs.oasis-open.org/vs/2007/trust.http://docs.oasis- open.org/vs:Xust=trust".200312</i:sitydes></i:sitydes></i:sitydes></i:sitydes></exit(bes>
< <kr></kr> (Kr/Descriptor usa "Joining's
<ul> <li>&lt; cost track structure and the stru</li></ul>
CXS99Certificate>MIIC2DCCAcCgAw18AgIQVMpbH3X81cxEUm/yofrLTTANBgkqhkiG9w08AQsFADAoMSYwJAYDVQQDEx18REZTIFNpZ25pbmcgL58zYW1sLmxbYiSsb2NhbDAeFw0yMDA2MTYwMTU0MjiaFw0yMTA2MTYwMTU0MjiaMCgx2jAk8gNVBAM
(/X97084) (X99084)
+ <fed:tokentypesoffered></fed:tokentypesoffered>
+ <fed:claimtypesoffered></fed:claimtypesoffered>
<fed:securitytokenserviceendpoint> IGF Signifing Certificate</fed:securitytokenserviceendpoint>
* <endpointreference xmins="http://www.w3.org/2005/08/addressing"></endpointreference>
(/fed.SecurityTokenServiceEndpoint>)
<pre>+ <fed:passiverequestorendpoint></fed:passiverequestorendpoint></pre>
+ <spssdbecriptor **true*="" **um:oasis="" mames="" protocol="" saml2.0.protocol*="" supportenumeration="" tc="" wangasertionssigned=""></spssdbecriptor>
<ul> <li>CDPSSODescriptor protocolsupportmenention="um:oesist:names/tclsAMLI2.0:protocol"&gt;</li> </ul>
* <keyvescriptor use="secryption"> a <keyvescriptor use="secryption"></keyvescriptor></keyvescriptor>
< Copyright the significant of the second se
Compression Control in the provide state of the state
Compression of the control in the second distribution of the second dist
< NameDFormat > um;oasis;names:tc:SANL:2.0;nameId=format;persistent
<nameidformat>um:oasis:namaa:tr=SAMI=3.0:namaid.format=transiant</nameidformat>
<singlesignonservice =="" location="https://samil.tab.local:444/adfs/ls/*"> Uri sign-in (sign-on)</singlesignonservice>
<singlesignonservice binding="um:oasis:naffeestc:SAME2.0:bindings:HTTP-POST" location="https://samLlab.local:444/adfs/ls/"></singlesignonservice>

Configuração no FTD via FMC

Etapa 1. Instalar e registrar o certificado IdP no FMC. Navegue até Devices > Certificates.



Etapa 2. Clique em Add. Selecione o FTD para se inscrever neste certificado. Em Cert Enrollment, clique no sinal de mais +.

No Add Cert Enrollment use qualquer nome como rótulo para o certificado IdP. Clique em Manual.

Marque a caixa CA Only e Skip Check para campos de flag CA.

Cole o base64 formatar certificado IdP CA.

Clique em save e clique em Add.

Name	Domain	Enrollment Type	Status	
∼ 📾 FTDv			Add Cert Enrollment	
Add New Certificate Add a new certificate to the device using cert en generate CA and identify certificate. Device*: FTDv Cert Enrollment*: Select a certificate entrollment object +	rollment object which i Cancel	Add	Name*         SAML_IdP         Description         CA Information       Certificate Parameters       Key       Revocation         Enrollment Type:       Manual           C A Only             Check this option if you do not require an identity certificate to be created from this CA         CA Certificate: <pre></pre>	
			Cancel Save	

Etapa 3. Defina as configurações do servidor SAML. Navegue até Objects > Object Management > AAA Servers > Single Sign-on Server. Em seguida, selecione Add Single Sign-on Server.



Etapa 4. Com base na metadata.xml arquivo já fornecido pelo IdP, configure os valores SAML no 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.

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)

Cancel

Save

Etapa 5. Configurar o Connection Profile que usa esse método de autenticação. Navegue até Devices > Remote Access e, em seguida, edite seu VPN Remote Access Configuração.

altalta cisco	Firepower Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence		٩	Deploy
Name					Status				Last Modified		
FTD_F	temoteAccess				Targeting 1 devic Up-to-date on all	es targeted device	15		2020-11-10 11:49:29 Modified by "admin"		∕ ≆

Etapa 6. Clique no sinal de mais + e adicione outro Perfil de conexão.

FTD_RemoteAccess	Save Cancel
Connection Profile Access Interfaces Advanced	Euler-Assionment/13
	+

Passo 7. Crie o novo Perfil de Conexão e adicione a VPN, o Pool ou o Servidor DHCP apropriados.

#### 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

Etapa 8. Selecione a guia AAA. Sob o comando Authentication Method selecione SAML.

Sob o comando Authentication Server selecione o objeto SAML criado na Etapa 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:

Etapa 9. Crie um alias de grupo para mapear as conexões para este Perfil de Conexão. Essa é a marca que os usuários podem ver no menu suspenso Software AnyConnect.

Quando isso estiver configurado, clique em OK e salve a configuração completa da VPN de Autenticação SAML.

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 URL	Alias Name: SAML Control Enabled	Cancel OK	users choose the +

Etapa 10. Navegue até Deploy > Deployment e selecione o FTD apropriado para aplicar as alterações de VPN de autenticação SAML.

Etapa 11. Forneça o arquivo metadata.xml do FTD ao IDP para que ele adicione o FTD como um dispositivo confiável.

Na CLI do FTD, execute o comando show saml metadata SAML\_TG onde SAML\_TG é o nome do Perfil de Conexão criado na Etapa 7.

Esta é a saída esperada:

<#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

```
<?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:S
<SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="ur</pre>
<KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>MIIF1zCCBL+gAwIBAgITYAAAABN6dX+H0cOFYwAAAAAAEzANBgkqhkiG9w0BAQsF
ADBAMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxEzARBgoJkiaJk/IsZAEZFgNsYWIx
EjAQBgNVBAMTCU1TMjAxMi1DQTAeFw0yMDA0MTEwMTQyMTlaFw0yMjA0MTEwMTQy
MT1aMCMxCzAJBqNVBAYTAkNSMRQwEqYDVQQDDAsqLmxhYi5sb2NhbDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAKfRmbCfWk+V1f+Y1sIE4hyY6+Qr1yKf
g1wEqLOFHtGVM3re/WmFuD+4sCyU1VkoiJhf2+X8tG7x2WTpKKtZM3N7bHpb7oPc
uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8
PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy
EY4F8sdic7bt1QQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44051BEcv
OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC
AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWBBR0kmTIhXT/
EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWH1Hqxd11VIRYSCSCuHTa4TCB
zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049
V0]OLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWM]MjBLZXk]MjBTZXJ2aWN]
cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j
ZXJ0aWZpY2F0ZVJ1dm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRG1z
dHJpYnV0aW9uUG9pbnQwgbkGCCsGAQUFBwEBBIGsMIGpMIGmBggrBgEFBQcwAoaB
mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWM1MjBLZXk1MjBT
ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s
b2NhbD9jQUN1cnRpZm1jYXR1P2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydG1maWNhdG1v
bkF1dGhvcm10eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB
BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR01
BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG
AQUFBwMFBggrBgEFBQcDAgYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF
BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF
BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADqqEBAKQnqcaU
fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V
Lmq04X1goaAs6obHrYFtSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG
5EQSC1YqS31sTuarm4WPDJyMShc6h1UpswnCokGRMMgpx2GmDgv4Zf8SzJJONI4y
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>
```

Depois que o metadata.xml do FTD é fornecido ao IdP e é como um dispositivo confiável, um teste na conexão VPN pode ser executado.

### Verificar

Verifique se a conexão VPN AnyConnect foi estabelecida com SAML como um método de autenticação com os comandos vistos aqui:

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

### Troubleshooting

Alguns comandos de verificação na CLI de FTD podem ser usados para solucionar problemas de SAML e conexão de VPN de acesso remoto, conforme visto no parêntese:

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

Solutionar problemas do DART no PC do usuário do AnyConnect.

#### Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.