Configurer Anyconnect avec authentification SAML sur FTD géré via FMC

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Obtenir les paramètres IDp SAML Configuration sur le FTD via FMC Vérification Dépannage

Introduction

Ce document décrit Security Assertion Markup Language (SAML) authentification sur FTD géré sur FMC.

Conditions préalables

Conditions requises

Cisco recommande de connaître ces sujets :

- AnyConnect configuration sur FMC
- Valeurs SAML et metatada.xml

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Threat Defense (FTD) Version 6.7.0
- Firepower Management Center (FMC) Version 6.7.0
- ADFS de AD Server avec SAML 2.0

Note: Si possible, utilisez un serveur NTP pour synchroniser l'heure entre le FTD et l'IdP. Sinon, vérifiez que l'heure est synchronisée manuellement entre eux.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La configuration permet aux utilisateurs Anyconnect d'établir une authentification de session VPN avec un fournisseur de service d'identité SAML.

Voici quelques-unes des limites actuelles de la LMEA :

- SAML sur FTD est pris en charge pour l'authentification (à partir de la version 6.7) et l'autorisation (à partir de la version 7.0).
- Attributs d'authentification SAML disponibles dans l'évaluation LDAP (similaire à RADIUS attributs envoyés RADIUS réponse d'autorisation du serveur AAA) ne sont pas prises en charge.
- ASA prend en charge le groupe de tunnels SAML sur la politique DAP. Cependant, vous ne pouvez pas vérifier l'attribut username avec l'authentification SAML, car l'attribut username est masqué par le fournisseur d'identité SAML.
- Parce que AnyConnect Lorsque le navigateur intégré utilise une nouvelle session de navigateur à chaque tentative VPN, les utilisateurs doivent s'authentifier à chaque fois si le fournisseur d'identité utilise des cookies de session HTTP pour suivre l'état de connexion.
- Dans ce cas, le Force Re-Authentication implantation Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Single Sign On Servers n'a pas d'effet sur AnyConnect a initié l'authentification SAML.

D'autres limitations ou SAML sont décrites dans le lien fourni ici.

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

Ces limitations s'appliquent à ASA et FTD : "Guidelines and Limitations for SAML 2.0"

Note: Toute la configuration SAML à implémenter sur le FTD se trouve dans le fichier metadata.xml fourni par votre fournisseur d'identité.

Configuration

Cette section décrit comment configurer AnyConnect avec authentification SAML sur FTD

Obtenir les paramètres IDp SAML

Cette image présente un fichier metadata.xml IdP SAML. Vous pouvez obtenir toutes les valeurs requises pour configurer le AnyConnect profil avec SAML :

| chord version="1.0"> Chord version="1.0" Chord version="1 | |
|--|-----|
| <keydescriptor li="" signing's<="" use*=""> <keydescriptor li="" signing's<="" use*=""> <keydescriptor li="" signing's<="" use*=""> </keydescriptor></keydescriptor></keydescriptor> | Т |
| <\$3000ata> | |
| <3599Certificate>MIIC2DCCAcCgAw1BAgIQVMpbH3X81cxEUm/yofrLTTANBgkqhkiG9w0BAQsFADAoHSYw)AYDVQQDEx1BREZTIFNpZ2SpbmcgL5BzYW1sLmxhYi5sb2NhbDAeFw0yMDA2HTYwMTU0MjiaFw0yMTA2MTYwMTU0MjiaMCgx)JAkBgNVBA | м |
| | |
| | |
| < cfed: Tokon Types Offered> | - 1 |
| + <fed:claimtypesoffered></fed:claimtypesoffered> | - 1 |
| <pre>- <fed:securitytokenserviceendpoint> IQP Signing Certificate</fed:securitytokenserviceendpoint></pre> | - 1 |
| * <endpointreference xmins="http://www.w3.org/2005/08/addressing"></endpointreference> | |
| | |
| + <ted:passiverequestorendpoint></ted:passiverequestorendpoint> | - 1 |
| | |
| CPSSUPerceptor protocosportmuneration - umicasis names it: SAMEL2.0 protocol - university - united - uni | |
| Consistence protocomponent mene and sum constrained a | - 1 |
| + Keybereiden um "deningen | |
| Sindel courtService Location Datass//samilab.local:444/adfs/is/1 | - 1 |
| <singlelogoutservice 15="" adms="" binding="uncoasis.names.tc:SAML:2.0.bindings:HTTP-POST" location="" mttps:="" samutab.socar:444=""></singlelogoutservice> | |
| <namedformat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</namedformat> | |
| <namedformat>umioasis:namesitc:SAMLi2.0:nameid-format:persistent</namedformat> | - 1 |
| <nameidformat>um:oosis:namaa:tc=SAML+2.0:nameId.format:transfent</nameidformat> | - 1 |
| csanglesignovservice tocation = intrps://samil.tab.locat/44/adfs/its/1021100 StER-IDL ST STER-IDL STER-IDL S | |
| comprogrammer account in the constraints of a second se | |

Configuration sur le FTD via FMC

Étape 1 : installation et inscription du certificat IdP sur le FMC Naviguez jusqu'à Devices > Certificates



Étape 2. Cliquez sur Add. Sélectionnez le FTD à inscrire dans ce certificat. Sous Inscription au certificat, cliquez sur le signe plus +.

Dans la Add Cert Enrollment , utilisez n'importe quel nom comme étiquette pour le certificat IdP. Cliquer Manual.

Vérifiez la CA Only et Skip Check pour les champs d'indicateur CA.

Collez le base64 format IdP CA cert.

Cliquer Save puis cliquez sur Add.



Étape 3. Configuration des paramètres du serveur SAML Naviguez jusqu'à Objects > Object Management > AAA Servers > Single Sign-on Server. Sélectionnez ensuite Add Single Sign-on Server.



Étape 4. En fonction de la metadata.xml déjà fourni par votre fournisseur d'identité, configurez les valeurs SAML sur le 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*

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)

Étape 5 : configuration du Connection Profile qui utilise cette méthode d'authentification. Naviguez jusqu'à Devices > Remote Access puis modifiez votre VPN Remote Access configuration.

Save

Cancel

| cisco | Firepower Management Center Devices / VPN / Remote Access | Overview Analy | lysis Policies | Devices | Objects | AMP | Intelligence | | ٩ | Deploy |
|-------|--|----------------|----------------|---|----------------------|-----|--------------|--|---|------------|
| | | | | | | | | | | |
| Nam | 0 | | | Status | | | | Last Modified | | |
| FTD, | RemoteAccess | | | Targeting 1 device Up-to-date on all | es targeted devic | es | | 2020-11-10 11:49:29 Modified by "admin" | | ∕ ∎ |

Étape 6. Cliquez sur le signe plus + et ajoutez un autre Connection Profile.

| FTD_RemoteAccess | Sive Cancel |
|---|------------------------|
| Connection Profile Access Interfaces Advanced | Patice Assistants, (3) |
| | + |

Étape 7. Créez le nouveau Connection Profile et ajoutez le VPN approprié, Poolou serveur DHCP.

| Add Connection Profile |) | 0 |
|--|---|-----------------------|
| Connection Profile:* | SAML_TG | |
| Client Address Assignment | dit Group Policy AAA Aliases | |
| IP Address for the remote client Servers. Configure the 'Client assignment criteria. | nts can be assigned from local IP Address pools/DHCP S Address Assignment Policy' in the Advanced tab to defin | Servers/AAA te the |
| 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 |
| | Cano | el Save |

Étape 8. Sélectionnez l'onglet AAA. Sous la Authentication Method , sélectionnez SAML.

Sous la Authentication Server, sélectionnez l'objet SAML créé à l'étape 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: |

Étape 9. Créez un alias de groupe pour mapper les connexions à ce Connection Profile. Il s'agit de la balise que les utilisateurs peuvent voir sur le AnyConnect Menu déroulant Logiciel.

Lorsque cette option est configurée, cliquez sur OK et enregistrez le 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 ; | Alias Name: SAML Chabled | | users choose the |
| URL | | Cancel OK | |

Étape 10. Accédez à Deploy > Deployment et sélectionnez le FTD approprié pour appliquer le SAML Authentication VPN modifications.

Étape 11. Fournissez le FTD metadata.xml au fournisseur d'identifiants afin qu'il ajoute le FTD en tant que périphérique approuvé.

Sur l'interface de ligne de commande FTD, exécutez la commande show sami metadata SAML_TG où SAML_TG est le nom du Connection Profile créé à l'étape 7.

Voici le résultat attendu :

```
> 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 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+Y1sIE4hyY6+Qr1yKf g1wEqLOFHtGVM3re/WmFuD+4sCyU1VkoiJhf2+X8tG7x2WTpKKtzM3N7bHpb7oPc uz8N4GabfAIw287soLM521h6ZM01bWGQ0vxXR+xtCAyqz6JJdK0CNjNEdEkYcaG8 PFrFUy31UPmCqQnEy+GYZipErrWTpWwbF7FWr5u7efhTtmdR6Y8vjAZqFddigXMy EY4F8sdic7btlQQPKG9JIaWny9RvHBmLgj0px2i5Rp5k1JIECD9kHGj44051BEcv OFY6ecAPv4CkZB6CloftaHjUGTSeVeBAvXBK24Ci9e/ynIUNJ/CM9pcCAwEAAaOC AuUwggLhMBYGA1UdEQQPMA2CCyoubGFiLmxvY2FsMB0GA1UdDgQWBBR0kmTIhXT/ $\verb"EjkMdpc4aM6PTnyKPzAfBgNVHSMEGDAWgBTEPQVWHlHqxd11VIRYSCSCuHTa4TCB"$ zQYDVR0fBIHFMIHCMIG/oIG8oIG5hoG2bGRhcDovLy9DTj1NUzIwMTItQ0EsQ049 V0lOLTVBME5HNDkxQURCLENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNl cyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1sb2NhbD9j ZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Q2xhc3M9Y1JMRGlz dHJpYnV0aW9uUG9pbnQwqbkGCCsGAQUFBwEBBIGsMIGpMIGmBqqrBqEFBQcwAoaB mWxkYXA6Ly8vQ049TVMyMDEyLUNBLENOPUFJQSxDTj1QdWJsaWMlMjBLZXklMjBT ZXJ2aWNlcyxDTj1TZXJ2aWNlcyxDTj1Db25maWd1cmF0aW9uLERDPWxhYixEQz1s b2NhbD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlv bkFldGhvcml0eTAOBgNVHQ8BAf8EBAMCBaAwPQYJKwYBBAGCNxUHBDAwLgYmKwYB BAGCNxUIgYKsboLe0U6B4ZUthLbxToW+yFILh4iaWYXgpQUCAWQCAQMwSwYDVR01 ${\tt BEQwQgYIKwYBBQUHAwEGCCsGAQUFBwMHBggrBgEFBQcDBgYIKwYBBQUIAgIGCCsG}$ AQUFBwMFBggrBgEFBQcDAgYEVR01ADBfBgkrBgEEAYI3FQoEUjBQMAoGCCsGAQUF BwMBMAoGCCsGAQUFBwMHMAoGCCsGAQUFBwMGMAoGCCsGAQUFCAICMAoGCCsGAQUF BwMFMAoGCCsGAQUFBwMCMAYGBFUdJQAwDQYJKoZIhvcNAQELBQADqqEBAKQnqcaU fZ3kdeoE8v2Qz+3Us8tXxXaXVhS3L5heiwr1IyUgsZm/+RLJL/zGE3AprEiITW2V Lmq04X1goaAs6obHrYFtSttz/9X1TAe1KbZ0G1RVg9Lb1PiF17kZAxALjLJH1CTG 5EQSC1YqS31sTuarm4WPDJyMShc6hlUpswnCokGRMMqpx2GmDqv4Zf8SzJJ0NI4y DgMozuObwkNUXuHbiLuoXwvb2Whm11ysidp1+V9kp1RYamyjFUo+agx0E+L1zp8C i0YEwYKXgKk3CZdwJfnYQuCWjmapYwlLGt5S59Uwegwro6AsUXY335+ZOrY/kuLF tzR3/S90jDq6dqk= </ds:X509Certificate> </ds:X509Data> </ds:KeyInfo> </KeyDescriptor> <AssertionConsumerService index="0" isDefault="true"</pre> 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"</pre> 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>

Après le metadata.xmi à partir du FTD est fourni au fournisseur d'identité et il est comme un périphérique de confiance, un test sous la connexion VPN peut être effectué.

Vérification

Vérifiez que le **VPN AnyConnect** La connexion a été établie avec SAML comme méthode d'authentification avec les commandes présentées ici :

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

Dépannage

Certaines commandes de vérification de l'interface de ligne de commande FTD peuvent être utilisées pour dépanner SAML et Remote Access VPN connexion comme indiqué dans le support :

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

Note: Vous pouvez dépanner DART a partir des versions AnyConnect PC utilisateur également.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.