Dépannage des problèmes courants avec SAML sur ASA et FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Problèmes courants
  - Problème 1 : Non-concordance ID entité
    - Solution :
  - Problème 2 : Assertion non valide
    - Explication
    - Solution
  - Problème 3 : La signature ne vérifie pas
    - Explication
    - Solution
  - Problème 4 : URL incorrecte pour le service client d'assertion
    - Explication
    - Exemples
    - Solution
  - Problème 5 : L'audience d'assertions est incorrecte
    - Explication
    - Solution
  - Problème 6 : Les modifications de configuration SAML ne prennent pas effet
    - Explication
    - Solution
  - Problème 7 : Comment utiliser le même IDP sous plusieurs profils de groupe de tunnels/connexion
    - Explication
    - Solutions
  - Problème 8 : Échec de l'authentification en raison d'un problème de récupération du cookie d'authentification unique
    - Explication
    - Solution
  - Problème 9 : Discordance de hachage d'état de relais
    - Explications
    - Solution
- Dépannage supplémentaire
- Informations connexes

Introduction

Ce document décrit les problèmes les plus courants rencontrés lors du dépannage de SAML sur les appareils Cisco ASA et FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- VPN AnyConnect Cisco Secure Client
- Configuration du fournisseur d'identité (IdP) SAML
- Configuration d'un objet d'authentification unique Cisco Secure ASA Firewall ou Firepower Threat Defense (FTD)

Composants utilisés

Les guides des meilleures pratiques sont basés sur les versions matérielles et logicielles suivantes :

- Cisco ASA 9.x
- Firepower Threat Defense 7.x / FMC 7.x

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

SAML (Security Assertion Markup Language) est un cadre XML d'échange de données d'authentification et d'autorisation entre domaines de sécurité. Il crée un cercle de confiance entre l'utilisateur, un fournisseur de services (SP) et un fournisseur d'identité (IdP), ce qui permet à l'utilisateur de se connecter une seule fois pour plusieurs services. SAML peut être utilisé pour l'authentification VPN d'accès à distance pour les connexions du client sécurisé Cisco aux têtes de réseau VPN ASA et FTD, où ASA ou FTD est l'entité SP dans le cercle de confiance.

La plupart des problèmes SAML peuvent être résolus en vérifiant la configuration sur l'IdP et l'ASA/FTD utilisés. Dans les cas où la cause n'est pas claire, les débogages fournissent plus de clarté et les exemples dans ce guide dérivent de la commande debug webvpn saml 255.

Le présent document a pour but de fournir une référence rapide sur les problèmes connus liés au SAML et sur les solutions possibles.

Problèmes courants

Problème 1 : Non-concordance ID entité

Cela signifie généralement que la commande saml idp [entityID] sous la configuration webvpn du pare-feu ne correspond pas à l'ID d'entité du fournisseur d'identité trouvé dans les métadonnées du fournisseur d'identité, comme indiqué dans l'exemple suivant.

Exemple de débogage :

```
Sep 05 23:54:02 [SAML] consume_assertion: The identifier of a provider is unknown to #LassoServer. To r
```

De IDP :

<#root>

```
<EntityDescriptor ID="
```

```
_7e53f3f3-7c79-444a-b42d-d60ae13f0948
```

```
" entityID="
```

```
https://sts.example.net/69c69fff-03f6-4c9c-be73-9ed4f5f894c/
```

```
">
```

À partir de ASA/FTD :

<#root>

```
saml idp
```

```
https://sts.example.net/69c69fff-03f6-4c9c-be73-9ed4f5f894
```

```
>>>> The entity ID is missing characters at the end
```

Solution :

Vérifiez l'ID d'entité du fichier de métadonnées du fournisseur d'identité et modifiez la commande saml idp [entity id] pour qu'elle corresponde exactement à ceci ; y compris les barres obliques inverses (/).

Problème 2 : Assertion non valide

Explication

Le pare-feu ne peut pas valider l'assertion fournie par le fournisseur d'identité, car l'horloge du pare-feu est en dehors de la validité de l'assertion.

Exemple de débogage :

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Exemple :

<#root>

```
[SAML]
```

NotBefore:2022-06-21T09:52:10.759Z NotOnOrAfter:2022-06-21T10:57:10.759Z

```
 timeout: 0    >>>>> Validity of the saml assertion provided by the IDP
Jun 21 15:20:46 [SAML] consume_assertion: assertion is expired or not valid
```

<#root>

```
firepower#
```

show clock

15:26:49.240 UTC Tue Jun 21 2022

```
>>>> Current time on the firewall
```

Dans l'exemple précédent, vous pouvez voir que l'assertion n'est valide qu'entre 09:52:10.759 UTC et 10:57:10.759 UTC, et que l'heure sur le pare-feu est en dehors de la fenêtre de validité.

Remarque : Le temps de validité vu dans l'assertion est en UTC. Si l'horloge du pare-feu est configurée dans un fuseau horaire différent, elle convertit l'heure en UTC avant validation.

Solution

Configurez l'heure correcte sur le pare-feu manuellement ou à l'aide d'un serveur NTP et vérifiez que l'heure actuelle du pare-feu est dans la validité de l'assertion dans UTC. Si le pare-feu est configuré dans un fuseau horaire différent de UTC, assurez-vous que l'heure est convertie en UTC avant de vérifier la validité de l'assertion.

Problème 3 : La signature ne vérifie pas

Explication

Lorsque le pare-feu ne parvient pas à vérifier la signature de l'assertion SAML reçue du fournisseur d'identité en raison d'une configuration de certificat de fournisseur d'identité incorrecte sous le webvpn de pare-feu avec la commande trustpoint idp <trustpoint>.

Exemple de débogage :

<#root>

```
[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=evp_signatures.c:line=372:obj=rsa-sha256:subj=unknown
```

signature does not verify

Solution

Téléchargez et installez le certificat à partir du fournisseur d'identité sur le pare-feu et attribuez le nouveau point de confiance sous la configuration webvpn du pare-feu. Le certificat de signature du fournisseur d'identité se trouve généralement dans les métadonnées du fournisseur d'identité ou dans la réponse SAML décodée.

Problème 4 : URL incorrecte pour le service client d'assertion

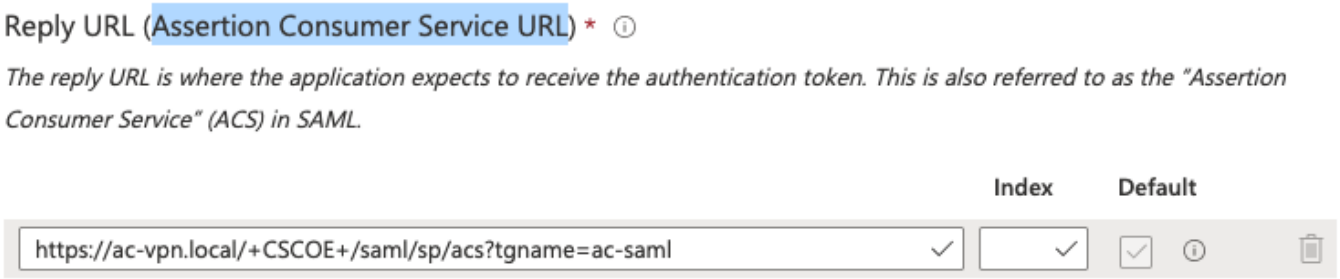
Explication

IdP est configuré avec une URL de réponse incorrecte (URL du service client d'assertion).

Exemples

Exemple de débogage : Aucun débogage n'est affiché après l'envoi de la demande d'authentification initiale. L'utilisateur ne peut pas entrer d'informations d'identification, mais après cette connexion échoue et aucun débogage n'est imprimé.

De IDP :



À partir des métadonnées FW ou SP :

<#root>

```
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

"https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=acvpn"

 />
```

Dans cet exemple, vous pouvez voir que l'« URL du service client d'assertion » sur le fournisseur d'identité ne correspond pas à l'emplacement sur les métadonnées du fournisseur de services.

Solution

Modifiez l'URL du service client d'assertion sur le fournisseur d'identité comme indiqué dans les métadonnées du fournisseur de services. Les métadonnées du SP peuvent être obtenues à l'aide de la commande show saml metadata <tunnel-group-name>.

Problème 5 : L'audience d'assertions est incorrecte

Explication

Lorsque le fournisseur d'identité envoie une destination incorrecte dans la réponse SAML, telle que le groupe de tunnels incorrect.

Exemple de débogage :

<#root>

```
[SAML] consume_assertion: assertion audience is invalid
```

À partir de la trace SAML :

<#root>

```
<samlp:Response ID="_36585f72-f813-471b-b4fd-3663fd24ffe8"
Version="2.0"
IssueInstant="2022-06-21T11:36:26.664Z"
Destination=

"https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=acvpn1

"

Recipient="https://ac-vpn.local/+CSCOE+/saml/sp/acs?

tgname=acvpn1

"

<AudienceRestriction> <Audience>

https://ac-vpn.local/saml/sp/metadata/acvpn
```

```
</Audience> </AudienceRestriction>
```

À partir du pare-feu ou des métadonnées SP :

<#root>

```
<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP

Location="https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=acvpn"

 />
```

Solution

Corrigez la configuration sur le fournisseur d'identité en tant que destination et destinataire. La réponse SAML doit correspondre à l'emplacement tel qu'indiqué dans les métadonnées de pare-feu/SP dans la sortie show saml metadata **<**tunnel-group-name**>**.

Problème 6 : Les modifications de configuration SAML ne prennent pas effet

Explication

Après toute modification avec la configuration SAML sous webvpn, il est suggéré de supprimer et de rajouter la commande saml identity-provider **<**IDP-Entity-ID**>** sous le tunnel-group.

Solution

Supprimez et ajoutez à nouveau la commande saml identity-provider <IDP-Entity-ID> sous le tunnel-group.

Problème 7 : Comment utiliser le même IDP sous plusieurs profils de groupe de tunnels/connexion

Explication

Pour configurer l'authentification SAML afin d'utiliser la même application SSO IdP pour plusieurs groupes de tunnels, passez en revue les étapes de configuration ci-dessous.

Solutions

Option 1 pour ASA 9.16 et versions antérieures, FTD géré par FDM ou FMC/FTD 7.0 et versions antérieures :

- Créez des applications SSO distinctes sur l'IdP, une pour chaque groupe de tunnels/profil de connexion.
- Créez un CSR à l'aide du CN par défaut utilisé par l'IDP.
- Signez le CSR auprès d'une autorité de certification interne/externe.
- Installez le même certificat d'identité signé sur les applications à utiliser pour des groupes de tunnels ou des profils de connexion distincts.

Option 2 pour ASA 9.17.1 et versions ultérieures ou FTD/FMC 7.1 et versions ultérieures :

- Créez des applications SSO distinctes sur l'IdP, une pour chaque groupe de tunnels/profil de connexion.
- Téléchargez les certificats de chaque application et téléchargez-les sur l'ASA ou le FTD.
- Attribuez le point de confiance qui correspond à l'application IdP pour chaque groupe de tunnels/profil de connexion.

Problème 8 : Échec de l'authentification en raison d'un problème de récupération du cookie d'authentification unique

Explication

Ceci peut être vu sur le logiciel Secure Client sur le périphérique client pour plusieurs raisons, notamment, mais sans s'y limiter :

- La validité de l'assertion est en dehors de l'heure actuelle du FW.
- L'ID d'entité ou l'URL du service client d'assertion est incorrectement défini sur l'IDP.

Solution

- Exécutez des débogages sur le pare-feu et recherchez des erreurs spécifiques.
- Vérifiez l'ID d'entité et l'URL du service client d'assertion configurés sur l'IDP par rapport aux métadonnées obtenues du FW.

Problème 9 : Discordance de hachage d'état de relais

Explications

- Le paramètre RelayState a pour but de permettre au protocole d'identification de rediriger l'utilisateur vers la ressource d'origine demandée après une authentification SAML réussie. Les informations RelayState de l'assertion doivent correspondre aux informations RelayState à la fin de l'URL de la demande d'authentification.
- Cela peut être une indication d'une attaque MitM, mais peut également être provoqué par des modifications de l'état du relais du côté IdP.

Exemple de débogage :

```
[SAML] relay-state hash mismatch.
```

Solution

- Passez à une version fixe comme détaillé dans l'ID de bogue Cisco CSCwf85757
- Vérifiez que l'IdP ne modifie pas les informations RelayState

Dépannage supplémentaire

Bien que la plupart des dépannages SAML puissent être effectués avec le résultat du débogage SAML webvpn, il peut arriver que des débogages supplémentaires soient utiles pour identifier la cause d'un problème.

<#root>

```
firepower#
```

debug webvpn saml 255

```
firepower#
```

debug webvpn 255

```
firepower#
```

debug webvpn session 255

```
firepower#
```

debug webvpn request 255

Informations connexes

- Assistance technique de Cisco et téléchargements
- Guides de configuration ASA
- Guides de configuration FMC/FDM

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.