排除ASA和FTD上SAML的常见问题

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

常见问题

- 问题 1：实体ID不匹配
  - 解决方案：
- 问题 2：断言无效
  - 说明
  - 解决方案
- 问题 3：签名无法验证
  - 说明
  - 解决方案
- 问题 4：断言使用者服务的URL不正确
  - 说明
  - Examples
  - 解决方案
- 问题 5：断言受众无效
  - 说明
  - 解决方案
- 问题 6：SAML配置更改未生效
  - 说明
  - 解决方案
- 问题 7：如何在多个隧道组/连接配置文件下使用相同的IDP
  - 说明
  - 解决方案
- 问题 8：由于检索单点登录Cookie时出现问题，身份验证失败
  - 说明
  - 解决方案
- 问题 9：中继状态哈希不匹配
  - 说明
  - 解决方案

进一步排除故障

相关信息

简介

本文档介绍在对Cisco ASA和FTD设备上的SAML进行故障排除时遇到的最常见问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全客户端AnyConnect VPN
- SAML身份提供程序(IdP)配置
- 思科安全ASA防火墙或Firepower威胁防御(FTD)单点登录对象配置

使用的组件

最佳实践指南基于以下硬件和软件版本：

- 思科ASA 9.x
- Firepower威胁防御7.x/FMC 7.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SAML（Security Assertion Markup Language，安全声明标记语言）是一个基于XML的框架，用于在安全域之间交换身份验证和授权数据。它在用户、服务提供商(SP)和身份提供者(IdP)之间创建信任圈，允许用户一次性登录多个服务。SAML可用于思科安全客户端连接到ASA和FTD VPN头端的远程访问VPN身份验证，其中ASA或FTD是信任圈中的SP实体。

大多数SAML问题可以通过验证正在使用的IdP和ASA/FTD上的配置来解决。在原因不明的情况下，调试会更加清晰，本指南中的示例源自debug webvpn saml 255命令。

本文档旨在快速参考已知的SAML问题和可能的解决方案。

常见问题

问题 1：实体ID不匹配

这通常意味着防火墙webvpn配置下的saml idp [entityID] 命令与IdP元数据中的IdP实体ID不匹配，如下例所示。

调试示例：

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

从IDP:

```
<#root>

<EntityDescriptor ID="

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

" entityID="

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

">
```

从ASA/FTD:

```
<#root>

saml idp

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

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

解决方案：

检查IdP的元数据文件的实体ID，并更改saml idp [entity id]命令以完全匹配此项；包括任何反斜杠(/)字符。

问题 2：断言无效

说明

防火墙无法验证IdP提供的断言，因为防火墙的时钟超出了断言的有效范围。

调试示例：

<#root>

[SAML] consume_assertion: assertion is expired or not valid

示例：

<#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

在上一示例中，您可以看到断言仅在09:52:10.759 UTC到10:57:10.759 UTC之间有效，并且防火墙上的时间在有效性窗口之外。

注意：断言中显示的有效时间以UTC表示。如果防火墙的时钟配置在不同时区，则它在验证之前会以UTC格式转换时间。

解决方案

手动或使用NTP服务器在防火墙上配置正确的时间，并验证防火墙的当前时间是否在UTC中声明的有效范围内。如果防火墙配置在不同于UTC的时区，请确保时间转换为UTC，然后检查断言的有效性。

问题 3：签名无法验证

说明

当防火墙由于使用trustpoint idp <trustpoint>命令在防火墙webvpn下不正确的IdP证书配置而未能验证从IdP接收的SAML断言的签名时。

调试示例：

```
<#root>

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

signature does not verify
```

解决方案

从防火墙上的IdP下载并安装证书，并在防火墙webvpn配置下分配新的信任点。IdP签名证书通常可在IdP的元数据或解码的SAML响应中找到。

问题 4：断言使用者服务的URL不正确

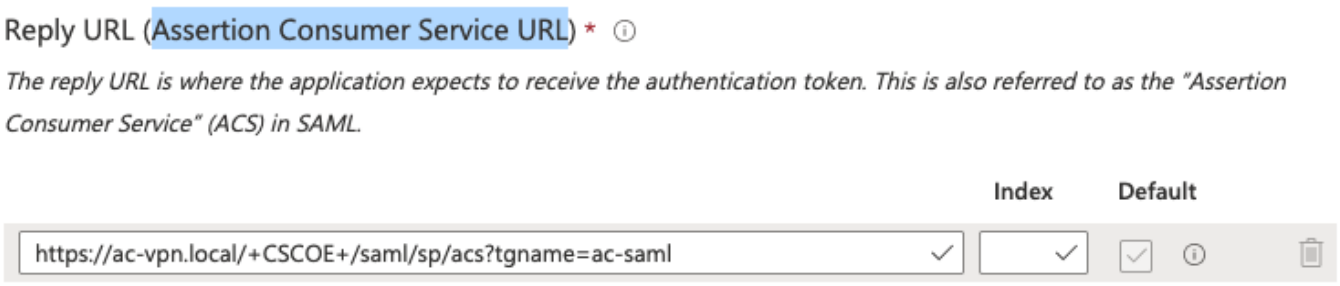
说明

IdP配置了错误的回复URL（断言消费者服务URL）。

Examples

调试示例：发送初始身份验证请求后，不会显示调试。用户无法输入凭证，但在连接失败后，不会打印调试。

从IDP:



从FW或SP元数据：

<#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"

/>

在此示例中，您可以看到IdP上的“断言消费者服务URL”与SP元数据上的位置不匹配。

解决方案

更改IdP上的断言使用者服务URL，如SP的元数据中所示。可以使用show saml metadata <tunnel-group-name>命令获取SP的元数据。

问题 5：断言受众无效

说明

当IdP在SAML响应中发送不正确的目标（例如错误的隧道组）时。

调试示例：

<#root>

[SAML] consume_assertion: assertion audience is invalid

从SAML跟踪：

<#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>

从防火墙或SP元数据：

<#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"

/>

解决方案

更正IdP上作为目标和收件人的配置。SAML响应必须与show saml metadata <tunnel-group-name>输出中的防火墙/SP元数据中所示的位置匹配。

问题 6：SAML配置更改未生效

说明

在webvpn下对SAML配置进行任何修改后，建议删除并重新添加tunnel-group下的saml identity-provider <IDP-Entity-ID>命令。

解决方案

在tunnel-group下删除并重新添加saml identity-provider <IDP-Entity-ID>命令。

问题 7：如何在多个隧道组/连接配置文件下使用相同的IDP

说明

要将SAML身份验证配置为对多个隧道组使用相同的IdP SSO应用，请查看以下配置步骤。

解决方案

选项1，适用于ASA 9.16及更低版本、FDM管理的FTD或FMC/FTD 7.0及更低版本：

- 在IdP上创建单独的SSO应用，每个隧道组/连接配置文件对应一个。
- 使用IDP使用的默认CN创建CSR。
- 从内部/外部CA签署CSR。
- 在要用于独立隧道组或连接配置文件的应用上安装相同的签名身份证书。

ASA 9.17.1及更高版本或FTD/FMC 7.1及更高版本的选项2:

- 在IdP上创建单独的SSO应用，每个隧道组/连接配置文件对应一个。
- 从每个应用下载证书并上传到ASA或FTD。
- 为每个隧道组/连接配置文件分配与IdP应用对应的信任点。

问题 8：由于检索单点登录Cookie时出现问题，身份验证失败

说明

由于多种原因（包括但不限于），可以在客户端设备上的安全客户端软件上看到这种情况：

- 断言的有效性超出了防火墙的当前时间。
- 在IDP上错误地定义了实体ID或断言消费者服务URL。

解决方案

- 在FW上运行调试并检查特定错误。
- 对照从FW获取的元数据，验证在IDP上配置的实体ID和声明使用者服务URL。

问题 9：中继状态哈希不匹配

说明

- RelayState参数的作用是使IdP将用户重新定向到SAML身份验证成功后请求的原始资源。断言的RelayState信息必须与身份验证请求URL末尾的RelayState信息匹配。
- 这可能表示MitM攻击，但也可能是由IdP端的RelayState更改引起的。

调试示例：

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

解决方案

- 根据Cisco Bug ID CSCwf85757中的详细信息迁移到固定版本
- 验证IdP是否未更改RelayState信息

进一步排除故障

虽然大多数SAML故障排除都可以通过webvpn SAML调试的输出进行，但有时候，额外的调试有助

于查明问题的原因。

<#root>

```
firepower#

debug webvpn saml 255

firepower#

debug webvpn 255

firepower#

debug webvpn session 255

firepower#

debug webvpn request 255
```

相关信息

- 思科技术支持和下载
- ASA配置指南
- FMC/FDM配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。