排除ASA和FTD上SAML的常見問題

目錄

簡介

本文檔介紹在對Cisco ASA和FTD裝置上的SAML進行故障排除時遇到的最常見問題。

必要條件

需求

思科建議您瞭解以下主題：

- SAML身份提供程式(IdP)配置
- Cisco Secure ASA防火牆或Firepower威脅防禦(FTD)單一登入對象配置
- Cisco安全使用者端AnyConnect VPN

採用元件

最佳實踐指南基於以下硬體和軟體版本：

- Cisco ASA 9.x
- Firepower威脅防禦7.x/FMC 7.x

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

SAML（Security Assertion Markup Language，安全宣告標籤語言）是一個基於XML的框架，用於在安全域之間交換驗證和授權資料。它在使用者、服務提供商(SP)和身份提供者(IdP)之間建立一個信任圈，允許使用者一次性登入多個服務。SAML可用於遠端訪問VPN身份驗證，用於思科安全客戶端連線到ASA和FTD VPN前端，其中ASA或FTD是信任圈中的SP實體。

大多數SAML問題可通過驗證正在使用的IdP和ASA/FTD上的配置來解決。在原因不明的情況下，debug命令可以更清楚地說明問題，本指南中的示例來自debug webvpn saml 255命令。

本文檔旨在快速參考已知的SAML問題和可能的解決方案。

常見問題：

問題1：實體ID不匹配

說明

通常，表示防火牆webvpn配置下的saml idp [entityID] 命令與IdP後設資料中的IdP實體ID不匹配，如示例所示。

偵錯範例：

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

來自IDP:

<#root>

<EntityDescriptor ID="

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

" entityID="

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

">

在ASA/FTD上：

<#root>

saml idp

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

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

解決方案

檢查IdP的後設資料檔案的實體ID，並更改saml idp [entity id]命令以完全匹配此項，包括任何反斜槓(/)字元。

問題2:斷言無效

說明

這表示防火牆無法驗證IdP提供的斷言，因為防火牆的時鐘超出斷言的有效性。

偵錯範例：

<#root>

[SAML] consume_assertion: assertion is expired or not valid

範例：

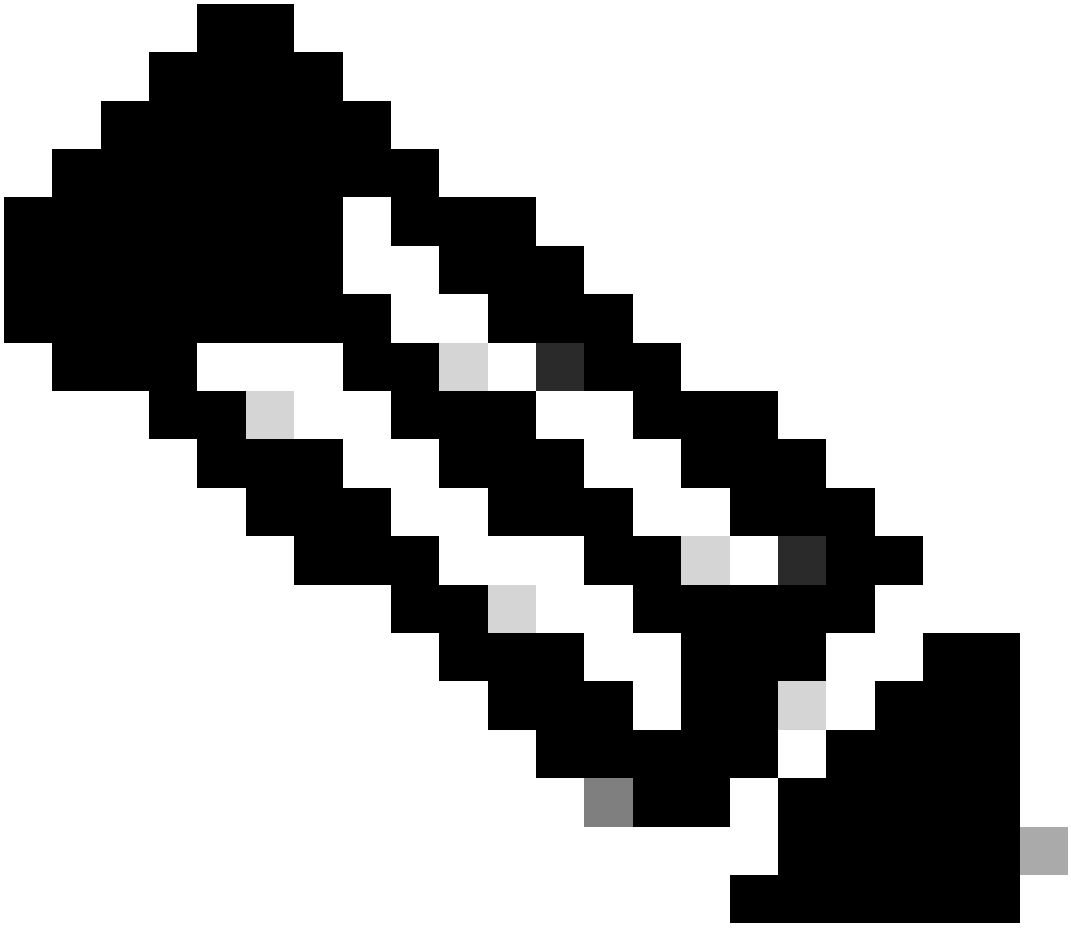
<#root>

[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
```

在示例中，我們可以看到斷言僅在09:52:10.759 UTC到10:57:10.759 UTC之間有效，並且防火牆上的時間超出了此有效性窗口。



附註：斷言中看到的有效期為UTC。如果防火牆上的時鐘配置在不同的時區，則在驗證之前會以UTC格式轉換時間。

解決方案

手動或使用NTP伺服器配置防火牆的正確時間，並驗證防火牆的當前時間是否在UTC中宣告的有效範圍內。如果防火牆配置在與UTC不同的時區，請確保時間轉換為UTC，然後再檢查宣告的有效性。

問題3：簽名無法驗證

說明

由於使用trustpoint idp <trustpoint>命令在防火牆webvpn配置下配置的IdP證書不正確，防火牆無法驗證從IdP接收的SAML斷言的簽名。

偵錯範例：

<#root>

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

signature does not verify

解決方案

從防火牆上的IdP下載並安裝證書，並在防火牆webvpn配置下分配新的信任點。IdP簽名證書通常可在IdP的後設資料或解碼的SAML響應中找到。

問題4：斷言使用者服務的URL不正確

說明

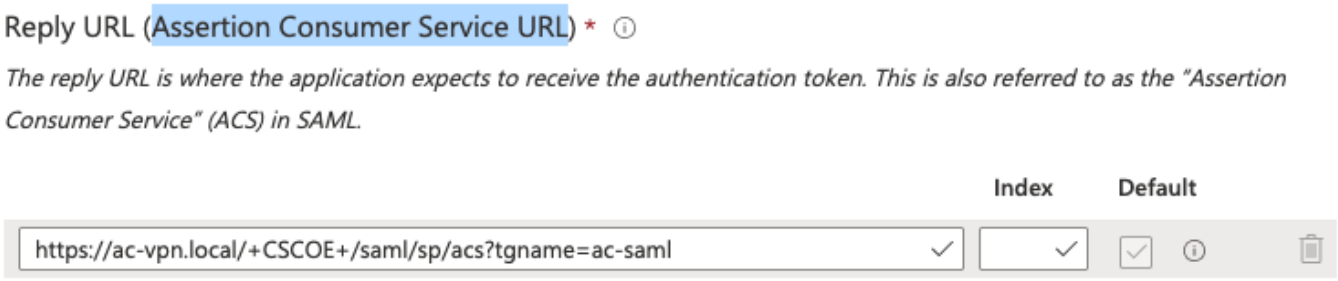
IdP配置了錯誤的Reply URL(Assertion Consumer Service URL)。

範例

偵錯範例：

傳送初始身份驗證請求後，不顯示調試。使用者可以輸入憑證，但在連線失敗且未列印調試之後。

來自IDP:



從FW或SP後設資料：

<#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"

/>

在示例中，可以看到IdP上的「斷言使用者服務URL」與SP後設資料上的位置不匹配。

解決方案

更改IdP上的斷言使用者服務URL，如SP的後設資料中所示。可以使用show saml metadata <tunnel-group-name> 命令獲取SP的後設資料。

問題5:斷言受眾無效

說明

當IdP在SAML響應中傳送不正確的目標（例如錯誤的隧道組）時。

偵錯範例：

<#root>

[SAML] consume_assertion: assertion audience is invalid

在SAML跟蹤中：

<#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>

從防火牆或SP後設資料：

<#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"
 />
```

解決方案

更正IDP上的配置，因為SAML響應中的目標和收件人必須與在show saml metadata <tunnel-group-name>輸出中的防火牆/SP後設資料中所顯示的位置相匹配。

問題6:SAML配置更改未生效

說明

在webvpn下對SAML配置進行任何修改後，建議刪除並重新新增tunnel-group下的saml identity-provider <IDP-Entity-ID>命令。

解決方案

刪除並重新新增tunnel-group下的saml identity-provider <IDP-Entity-ID>命令。

問題7:如何在多個隧道組/連線配置檔案下使用相同的IDP

說明

要將SAML身份驗證配置為對多個隧道組使用相同的IdP SSO應用程式，請按照以下配置步驟操作。

解決方案

選項1（適用於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上建立單獨的SSO應用，每個隧道組/連線配置檔案一個。
- 使用IDP使用的預設CN建立CSR。
- 從內部/外部CA簽署CSR。
- 在要用於單獨隧道組或連線配置檔案的應用程式上安裝相同的簽名身份證書。

ASA 9.17.1及更高版本或FTD/FMC 7.1及更高版本的選項2:

- 在IdP上建立單獨的SSO應用程式，每個隧道組/連線配置檔案各一個。
- 從每個應用下載證書並上傳到ASA或FTD上。
- 為每個隧道組/連線配置檔案分配與IdP應用程式對應的信任點。

問題8:由於檢索單一登入Cookie時出現問題，身份驗證失敗

說明

由於多種原因（包括但不限於），可以在客戶端裝置上的安全客戶端軟體上看到這種情況：

- 斷言的有效性超出了防火牆的當前時間。
- 在IDP上錯誤地定義了實體ID或斷言使用者服務URL。

解決方案

- 對防火牆運行調試並檢查特定錯誤。
- 根據從FW獲取的後設資料，驗證IDP上配置的實體ID和宣告使用者服務URL。

問題9:中繼狀態雜湊不匹配

說明

- RelayState引數的作用是使IdP將使用者重定向回成功SAML身份驗證後請求的原始資源。斷言的RelayState資訊必須與身份驗證請求URL末尾的RelayState資訊匹配。
- 這可能表示MitM攻擊，但也可能是由IdP端的RelayState更改引起的。

偵錯範例：

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

解決方案

- 移轉至固定版本，如思科錯誤ID CSCwf85757中所述
- 驗證IdP是否未更改RelayState資訊。

其他疑難排解

雖然大多數SAML故障排除可以僅使用webvpn saml debug的輸出進行，但有時額外的調試有助於查明問題的原因。

<#root>

```
firepower#
debug webvpn saml 255
firepower#
debug webvpn 255
firepower#
debug webvpn session 255
firepower#
debug webvpn request 255
```

相關資訊

- 思科技術支援和下載
- ASA配置指南
- FMC/FDM配置指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。