ASAおよびFTDでのSAMLの一般的な問題のトラブルシューティング

内容

はじめに

このドキュメントでは、Cisco ASAおよびFTDアプライアンスでSAMLのトラブルシューティングを行う際に発生する最も一般的な問題について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- SAML Identity Provider(IdP)の設定
- Cisco Secure ASA FirewallまたはFirepower Threat Defense(FTD)のシングルサインオンオブジェクトの設定
- CiscoセキュアクライアントAnyConnect VPN

使用するコンポーネント

ベストプラクティスガイドは、次のハードウェアとソフトウェアのバージョンに基づいています。

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

SAML(Security Assertion Markup Language)は、セキュリティドメイン間で認証および許可データを交換するためのXMLベースのフレームワークです。これにより、ユーザ、サービスプロバイダー(SP)、およびユーザが複数のサービスに対して一度にサインインできるアイデンティティプロバイダー(IdP)の間に信頼の輪が作成されます。SAMLは、ASAおよびFTD VPNヘッドエンドへのCisco Secure Client接続のリモートアクセスVPN認証に使用できます。ここで、ASAまたはFTDは、トラストサークル内のSPエンティティです。

ほとんどのSAML問題は、使用されているIdPおよびASA/FTDの設定を確認することで解決できます。原因が不明な場合、デバッグではより明確に示され、このガイドの例はdebug webvpn saml 255コマンドで示されています。

このドキュメントの目的は、既知のSAMLの問題と可能なソリューションのクイックリファレンスを提供することです。

一般的な問題:

問題1:エンティティIDの不一致

説明

一般的に、ファイアウォールwebvpn設定でのsaml idp [entityID]コマンドが、例に示すように、IdPのメタデータ内で見つかったIdPエンティティIDと一致しないことを意味します。

デバッグ例：

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

IDPから：

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

ASA/FTDから：

<#root>

```
saml idp
```

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

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

解決方法

IdPのメタデータファイルのエンティティIDを確認し、saml idp [entity id]コマンドを変更して、バックスラッシュ(/)文字も含めて、このIDと正確に一致するようにします。

問題2：アサーションが有効でない

説明

これは、ファイアウォールのクロックがアサーションの有効範囲外であるため、ファイアウォールはIdPによって提供されるアサーションを検証できないことを意味します。

デバッグ例：

<#root>

[SAML] consume_assertion: assertion is expired or not valid

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>

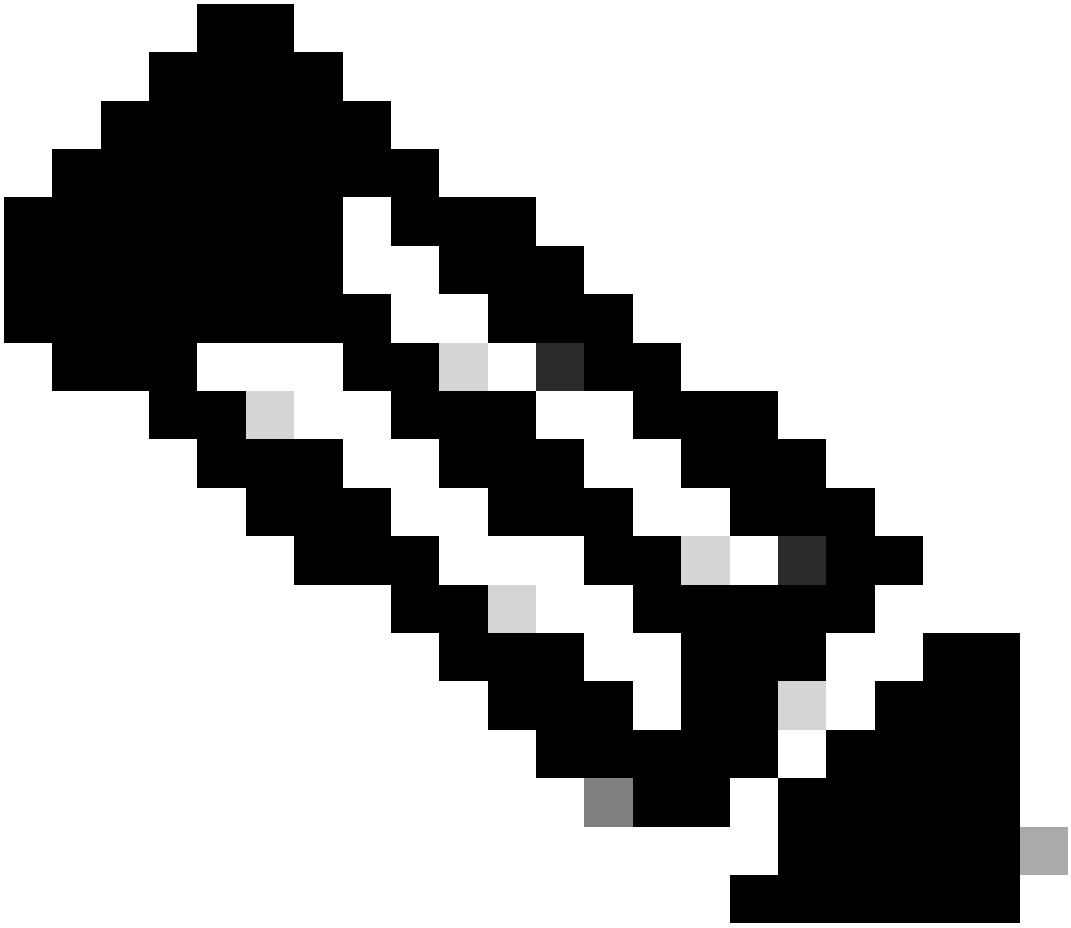
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

この例では、アサーションが09:52:10.759 UTC ~ 10:57:10.759 UTCの間でのみ有効であり、ファイアウォールの時刻がこの有効期間外であることを確認できます。



注：アサーションに表示される有効期間はUTCです。ファイアウォールのクロックが異なるタイムゾーンで設定されている場合は、検証前にUTCで時刻が変換されます。

解決方法

ファイアウォールで正しい時刻を手動またはNTPサーバを使用して設定し、ファイアウォールの現在の時刻がUTCのアサーションの有効期間内であることを確認します。ファイアウォールがUTC以外のタイムゾーンで設定されている場合は、アサーションの有効性を確認する前に、時刻がUTCに変換されていることを確認します。

問題3:シグニチャが確認しない

説明

trustpoint idp <trustpoint>コマンドによりファイアウォールwebvpn設定で設定されたIdP証明書が正しくないために、ファイアウォールがIdPから受信したSAMLアサーションの署名の検証に失敗

した場合。

デバッグ例：

<#root>

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

signature does not verify

解決方法

IdPからファイアウォールに証明書をダウンロードしてインストールし、ファイアウォールwebvpn設定で新しいトラストポイントを割り当てます。通常、IdP署名証明書は、IdPのメタデータまたはデコードされたSAML応答に含まれています。

問題4:アサーションコンシューマサービスのURLが正しくない

説明

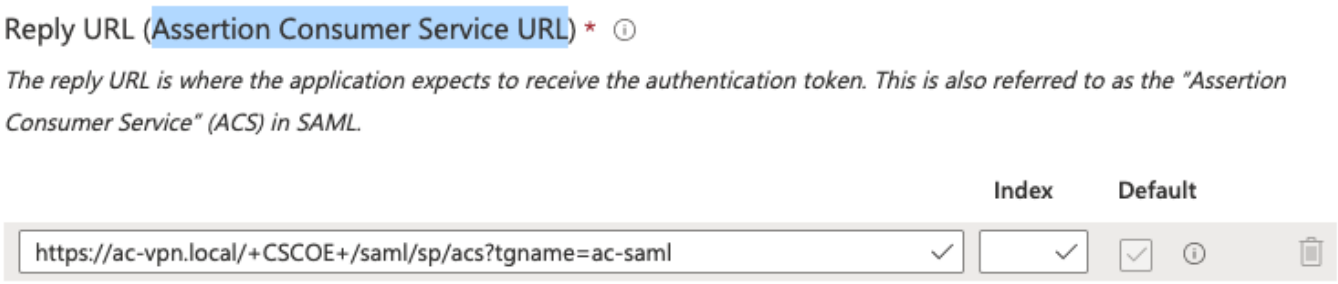
IdPに誤った応答URL（アサーションコンシューマサービスURL）が設定されています。

例

デバッグ例：

初期認証要求の送信後は、デバッグは表示されません。ユーザはクレデンシャルを入力できますが、その接続が失敗し、デバッグは出力されません。

IDPから：



FWまたはSPメタデータから：

<#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"

/>

この例では、IdPの「Assertion Consumer Service URL」がSPのメタデータの場所と一致しないことがわかります。

解決方法

SPのメタデータに示されているように、IdPのAssertion Consumer Service URLを変更します。SPのメタデータは、show saml metadata <tunnel-group-name>コマンドを使用して取得できます。

問題5:アサーションオーディエンスが無効である

説明

IdPが誤ったトンネルグループなど、SAML応答で誤った宛先を送信した場合。

デバッグ例：

<#root>

[SAML] consume_assertion: assertion audience is invalid

SAMLトレース：

<#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>

ファイアウォールまたはSPメタデータから：

<#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"

/>

解決方法

SAML応答の宛先および受信者が、show saml metadata <tunnel-group-name>出力のファイアウォール/SPメタデータに示されている場所と一致する必要があるため、IDPの設定を修正します。

問題6:SAML設定の変更が有効にならない

説明

webvpnでSAML設定を変更した後は、tunnel-groupの下でsaml identity-provider <IDP-Entity-ID>コマンドを削除し、再度追加することをお勧めします。

解決方法

tunnel-groupの下にあるsaml identity-provider <IDP-Entity-ID>コマンドを削除してから再度追加します。

問題7:複数のトンネルグループまたは接続プロファイルで同じIDPを使用する方法

説明

複数のトンネルグループで同じIdP SSOアプリケーションを使用するようにSAML認証を設定するには、次の設定手順に従います。

解決方法

ASA 9.16以前、FDM管理対象FTDまたはFMC/FTD 7.0以前のオプション1:

- IdPで、トンネルグループまたは接続プロファイルごとに1つずつ、個別のSSOアポレーションを作成します。
- IDPで使用されるデフォルトのCNを使用してCSRを作成します。
- 内部/外部CAからのCSRの署名
- 個別のトンネルグループまたは接続プロファイルに使用するアプリケーションに、同じ署名付きID証明書をインストールします。

ASA 9.17.1以降またはFTD/FMC 7.1以降の場合はオプション2:

- IdPで、トンネルグループ/接続プロファイルごとに1つずつ、個別のSSOアプリケーションを作成します。
- 各アプリケーションから証明書をダウンロードし、ASAまたはFTDにアップロードします。
- 各トンネルグループ/接続プロファイルのIdPアプリケーションに対応するトラストポイントを割り当てます。

問題8：シングルサインオンクッキーの取得中に問題が発生したため、認証に失敗しました

説明

この問題は、クライアントデバイスのセキュアクライアントソフトウェアで発生する可能性があります。これには、次のような複数の原因が考えられます。

- アサーションの有効性がFWの現在の時刻外である。
- エンティティIDまたはアサーションコンシューマサービスURLがIDPで正しく定義されていません。

解決方法

- FWでデバッグを実行し、特定のエラーを確認します。
- IDPで設定されているエンティティIDとアサーションコンシューマサービスURLを、FWから取得したメタデータと照合して確認します。

問題9：リレー状態ハッシュの不一致

説明

- RelayStateパラメータは、SAML認証が成功した後、要求された元のリソースにユーザをリダイレクトして戻すことを目的としています。アサーションのRelayState情報は、認証要求URLの末尾にあるRelayState情報と一致する必要があります。
- これはMitM攻撃を示している可能性もありますが、IdP側のRelayStateの変更が原因で発生する可能性もあります。

デバッグ例：

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

解決方法

- Cisco Bug ID CSCwf85757に記載されているように、修正済みリリースに移行する
- IdPがRelayState情報を変更していないことを確認します。

さらなるトラブルシューティング

ほとんどのSAMLトラブルシューティングは、webvpn samlデバッグの出力だけで実行できますが、問題の原因を特定するために追加のデバッグが役立つ場合があります。

<#root>

firepower#

debug webvpn saml 255

firepower#

debug webvpn 255

firepower#

debug webvpn session 255

firepower#

debug webvpn request 255

関連情報

- シスコテクニカルサポートおよびダウンロード
- ASA設定ガイド
- FMC/FDM構成ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。