Fehlerbehebung bei häufigen Problemen mit SAML auf ASA und FTD

Inhalt

Einleitung

In diesem Dokument werden die häufigsten Probleme bei der Fehlerbehebung für SAML auf Cisco ASA- und FTD-Appliances beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration des SAML Identity Providers (IdP)
- Konfiguration von Cisco Secure ASA Firewall oder FirePOWER Threat Defense (FTD) Single Sign-on Object
- Cisco Secure Client AnyConnect-VPN

Verwendete Komponenten

Der Leitfaden mit Best Practices basiert auf den folgenden Hardware- und Softwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SAML (Security Assertion Markup Language) ist ein XML-basiertes Framework für den Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Sicherheitsdomänen. Es wird ein Vertrauenskreis zwischen dem Benutzer, einem Dienstanbieter (SP) und einem Identitätsanbieter (IdP) erstellt, der es dem Benutzer ermöglicht, sich für mehrere Dienste einmal anzumelden. SAML kann für die VPN-Authentifizierung des Remote-Zugriffs für Cisco Secure Client-Verbindungen zu ASA- und FTD-VPN-Headends verwendet werden, wobei die ASA oder FTD die SP-Einheit im Vertrauenskreis ist.

Die meisten SAML-Probleme können durch Verifizieren der Konfiguration der verwendeten IDp und ASA/FTD behoben werden. In Fällen, in denen die Ursache nicht klar ist, geben debugs mehr Klarheit und die Beispiele in diesem Leitfaden kommen aus dem Befehl debug webvpn saml 255 Befehl.

Dieses Dokument soll als Kurzreferenz für bekannte SAML-Probleme und mögliche Lösungen dienen.

Häufige Probleme:

Problem 1: Objektkennung stimmt nicht überein

Erläuterung

Im Allgemeinen bedeutet dies, dass der Befehl saml idp [entityID] unter der Firewall-Webvpn-Konfiguration nicht mit der IdP-Element-ID übereinstimmt, die in den Metadaten der IdP gefunden wurde, wie im Beispiel gezeigt.

Debug-Beispiel:

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

Von IDP:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

Von ASA/FTD:

<#root>

```
saml idp
```

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

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

Lösung

Überprüfen Sie die Entitäts-ID der Metadatendatei der IdP, und ändern Sie den Befehl saml idp [entity id] genau entsprechend, einschließlich aller umgekehrten Schrägstriche (/).

Problem 2: Assertion ungültig

Erläuterung

Dies bedeutet, dass die Firewall die von der IdP bereitgestellte Assertion nicht validieren kann, da sich die Uhr der Firewall außerhalb der Gültigkeit der Assertion befindet.

Debug-Beispiel:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Beispiel:

<#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>

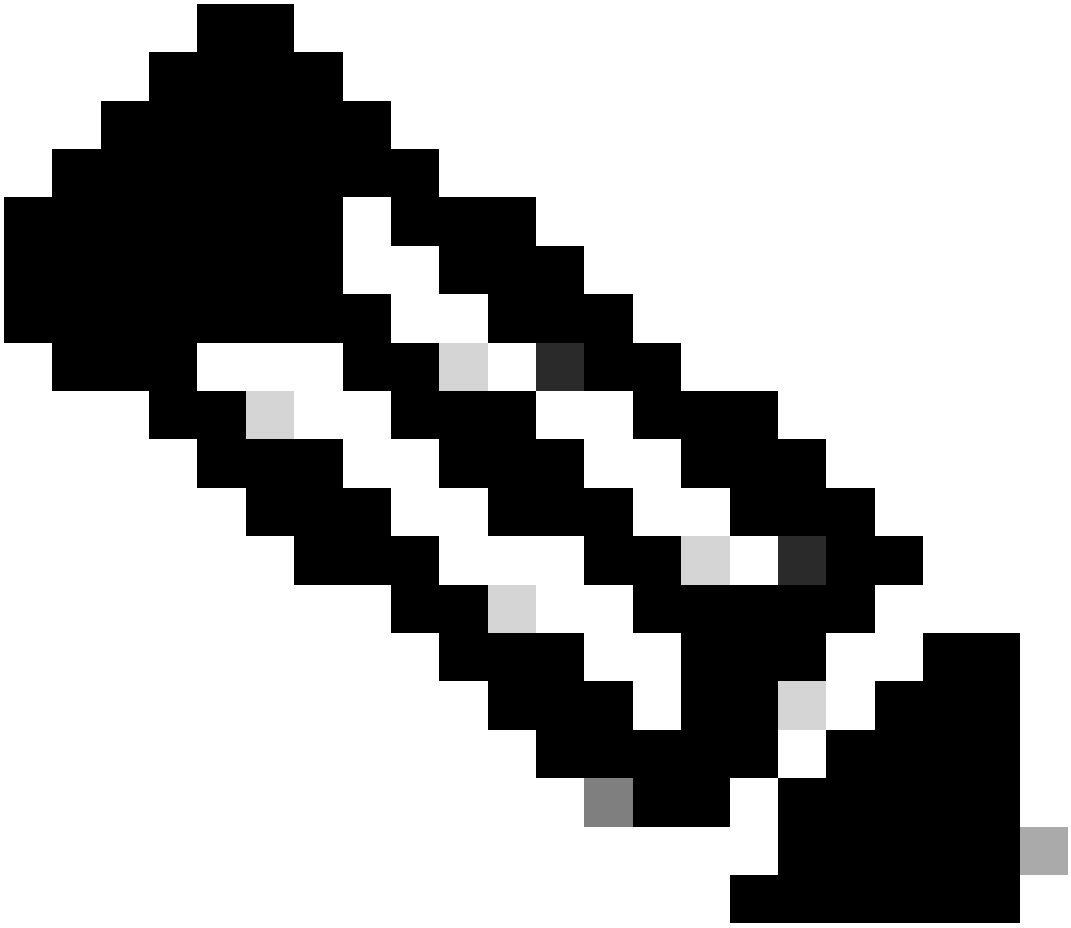
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

Im Beispiel können wir sehen, dass die Assertion nur zwischen 09:52:10.759 UTC und 10:57:10.759 UTC gültig ist, und die Zeit auf der Firewall außerhalb dieses Gültigkeitsfensters liegt.



Anmerkung: Die Gültigkeitsdauer, die in der Assertion angezeigt wird, ist in UTC angegeben. Wenn die Uhr der Firewall in einer anderen Zeitzone konfiguriert ist, wird die Zeit vor der Validierung in UTC konvertiert.

Lösung

Konfigurieren Sie die korrekte Uhrzeit auf der Firewall manuell oder mithilfe eines NTP-Servers, und vergewissern Sie sich, dass die aktuelle Uhrzeit der Firewall innerhalb der Gültigkeit der Aussage in UTC liegt. Wenn die Firewall in einer anderen Zeitzone als UTC konfiguriert ist, stellen Sie sicher, dass die Zeit in UTC konvertiert wurde, bevor Sie die Gültigkeit der Aussage überprüfen.

Problem 3: Signatur wird nicht verifiziert

Erläuterung

Wenn die Firewall die Signatur der von IdP empfangenen SAML Assertion aufgrund eines falschen IdP-Zertifikats nicht verifiziert, das mithilfe des Befehls trustpoint idp <trustpoint> in der Firewall-Webvpn-Konfiguration konfiguriert wurde.

Debug-Beispiel:

<#root>

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

signature does not verify

Lösung

Laden Sie das Zertifikat von IdP herunter, installieren Sie es auf der Firewall, und weisen Sie den neuen Vertrauenspunkt unter der Firewall-Webvpn-Konfiguration zu. Das IdP-Signaturzertifikat befindet sich in der Regel in den Metadaten der IdP oder in der decodierten SAML-Antwort.

Problem 4: Falsche URL für Assertion Consumer Service

Erläuterung

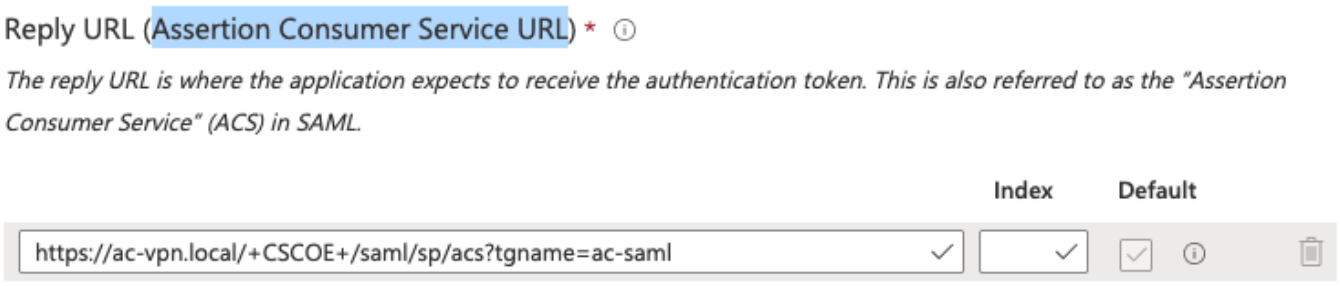
IdP ist mit der falschen Antwort-URL konfiguriert (Assertion Consumer Service-URL).

Beispiele

Debug-Beispiel:

Nach dem Senden der anfänglichen Authentifizierungsanforderung werden keine Debugging-Meldungen angezeigt. Der Benutzer kann Anmeldeinformationen eingeben, schlägt jedoch nach dieser Verbindung fehl, und es werden keine Debugs ausgegeben.

Von IDP:



Aus FW- oder SP-Metadaten:

<#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"
 />
```

Im Beispiel ist zu sehen, dass die Assertion Consumer Service URL auf IdP nicht mit dem Speicherort auf den Metadaten von SP übereinstimmt.

Lösung

Ändern Sie die Assertion Consumer Service-URL für die IdP, wie in den Metadaten des SP angezeigt. Die Metadaten des SP können mit dem Befehl show saml metadaten <tunnel-group-name> abgerufen werden.

Problem 5: assertion audience is invalid (Assertion-Zielgruppe ist ungültig)

Erläuterung

Wenn das IdP ein falsches Ziel in der SAML-Antwort sendet, z. B. die falsche Tunnelgruppe.

Debug-Beispiel:

<#root>

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

Von SAML-Ablaufverfolgung:

<#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>
```

Von Firewall- oder SP-Metadaten:

```
<#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"
 />
```

Lösung

Korrigieren Sie die Konfiguration auf dem IDP, da Ziel und Empfänger in der SAML-Antwort mit dem Speicherort übereinstimmen müssen, der in den Firewall-/SP-Metadaten in der Ausgabe von show sam metadates <tunnel-group-name> angezeigt wird.

Problem 6: SAML-Konfigurationsänderungen treten nicht in Kraft

Erläuterung

Nach jeder Änderung der SAML-Konfiguration unter webvpn wird empfohlen, den Befehl saml identity-provider <IDP-Entity-ID> unter der Tunnelgruppe zu entfernen und neu hinzuzufügen.

Lösung

Entfernen Sie den Befehl saml identity-provider <IDP-Entity-ID> unter der Tunnelgruppe, und fügen Sie ihn erneut hinzu.

Problem 7: So verwenden Sie denselben IDP unter Mehrere Tunnelgruppen-/Verbindungsprofile

Erläuterung

Um die SAML-Authentifizierung so zu konfigurieren, dass dieselbe IdP-SSO-Anwendung für mehrere Tunnelgruppen verwendet wird, führen Sie die unten aufgeführten Konfigurationsschritte aus.

Lösungen

Option 1 für ASA 9.16 und frühere Versionen, FDM Managed FTD oder FMC/FTD 7.0 und frühere

Versionen:

- Erstellen Sie auf dem IdP separate SSO-Anwendungen, eine für jede Tunnelgruppe bzw. jedes Verbindungsprofil.
- Erstellen Sie eine CSR-Anfrage unter Verwendung der von der IDP verwendeten Standard-CN.
- Signieren Sie den CSR von einer internen/externen Zertifizierungsstelle.
- Installieren Sie dasselbe signierte Identitätszertifikat auf den Anwendungen, die für separate Tunnelgruppen oder Verbindungsprofile verwendet werden sollen.

Option 2 für ASA 9.17.1 und höher oder FTD/FMC 7.1 und höher:

- Erstellen Sie auf dem IdP separate SSO-Anwendungen, eine für jede Tunnelgruppe/jedes Verbindungsprofil.
- Laden Sie die Zertifikate jeder Anwendung herunter und laden Sie sie auf die ASA oder FTD hoch.
- Weisen Sie für jedes Tunnelgruppen-/Verbindungsprofil den Vertrauenspunkt zu, der der IdP-Anwendung entspricht.

Problem 8: Fehler bei der Authentifizierung aufgrund des Problems beim Abrufen des Cookies für die einmalige Anmeldung

Erläuterung

Dies ist in der Secure Client-Software auf dem Client-Gerät aus verschiedenen Gründen zu sehen, darunter:

- Die Gültigkeit der Aussage liegt außerhalb der aktuellen Zeit der FW.
- Die Entitäts-ID oder die Assertion Consumer Service-URL ist für den IDP falsch definiert.

Lösung

- Führen Sie Debug-Vorgänge für die FW aus, und überprüfen Sie, ob spezifische Fehler vorliegen.
- Überprüfen Sie die auf dem IDP konfigurierte Entitäts-ID und Assertion Consumer Service-URL anhand der aus der FW erhaltenen Metadaten.

Problem 9: Relaystatus-Hash-Diskrepanz

Erläuterungen

- Der RelayState-Parameter dient dazu, dass IdP den Benutzer nach erfolgreicher SAML-Authentifizierung an die ursprüngliche Ressource zurückleitet, die angefordert wurde. Die RelayState-Informationen der Assertion müssen mit den RelayState-Informationen am Ende der Authentifizierungsanforderungs-URL übereinstimmen.
- Dies kann ein Hinweis auf einen MitM-Angriff sein, kann aber auch durch Änderungen des RelayState auf der IdP-Seite verursacht werden.

Debug-Beispiel:

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

Lösung

- Umstellung auf eine feste Version, wie in Cisco Bug-ID CSCwf85757 beschrieben
- Vergewissern Sie sich, dass die IdP die RelayState-Informationen nicht ändert.

Weitere Fehlerbehebungsmaßnahmen

Während die meisten SAML-Fehlerbehebungen nur mit der Ausgabe des Webvpn-Saml-Debugging durchgeführt werden können, gibt es jedoch Zeiten, in denen zusätzliche Debugging-Vorgänge beim Ermitteln der Ursache eines Problems hilfreich sein können.

<#root>

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

Zugehörige Informationen

- Technischer Support und Downloads von Cisco
- ASA-Konfigurationsanleitungen
- FMC/FDM-Konfigurationsanleitungen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.