Problemen oplossen met SAML op ASA en FTD

Inhoud

Inleiding

Dit document beschrijft de meest voorkomende problemen bij het oplossen van SAML-problemen op Cisco ASA- en FTD-apparaten.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie SAML Identity Provider (IdP)
- Cisco Secure ASA Firewall of Firepower Threat Defence (FTD) Eenmalige aanmeldingsobjectconfiguratie
- Cisco Secure Client AnyConnect VPN

Gebruikte componenten

De handleiding voor best practices is gebaseerd op deze hardware- en softwareversies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

SAML (Security Assertion Markup Language) is een op XML gebaseerd framework voor het uitwisselen van authenticatie- en autorisatiegegevens tussen beveiligingsdomeinen. Het creëert een vertrouwenscirkel tussen de gebruiker, een serviceprovider (SP) en een identiteitsprovider (IdP), waardoor de gebruiker zich in één keer kan aanmelden voor meerdere services. SAML kan worden gebruikt voor Remote Access VPN-verificatie voor Cisco Secure Client-verbindingen met ASA- en FTD VPN-headends, waarbij de ASA of FTD de SP-entiteit in de vertrouwenscirkel is.

De meeste SAML-problemen kunnen worden opgelost door de configuratie op de gebruikte IdP en ASA/FTD te verifiëren. In gevallen waar de oorzaak niet duidelijk is, geven debugs meer duidelijkheid en de voorbeelden in deze gids komen van de debug webvpn saml 255-opdracht.

Het doel van dit document is om een snelle referentie te zijn voor bekende SAML-problemen en mogelijke oplossingen.

Veelvoorkomende problemen:

Probleem 1: Onjuiste entiteitsnaam

verklaring

In het algemeen betekent dit dat de opdracht saml idp [entityID] onder de firewall webvpn-

configuratie niet overeenkomt met de IDp-entiteit die wordt gevonden in de metagegevens van de IdP, zoals weergegeven in het voorbeeld.

Voorbeeld van debug:

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

Van IDP:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

Van ASA/FTD:

<#root>

```
saml idp
```

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

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

Oplossing

Controleer de entiteit-ID van het metagegevensbestand van de IdP en wijzig de opdracht saml idp [entiteit-id] om deze exact aan te passen, inclusief eventuele backslash (/)-tekens.

Probleem 2: Bewering ongeldig

verklaring

Dit betekent dat de firewall niet in staat is om de bewering van de IdP te valideren, omdat de klok van de firewall buiten de geldigheid van de bewering valt.

Voorbeeld van debug:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Voorbeeld:

<#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>

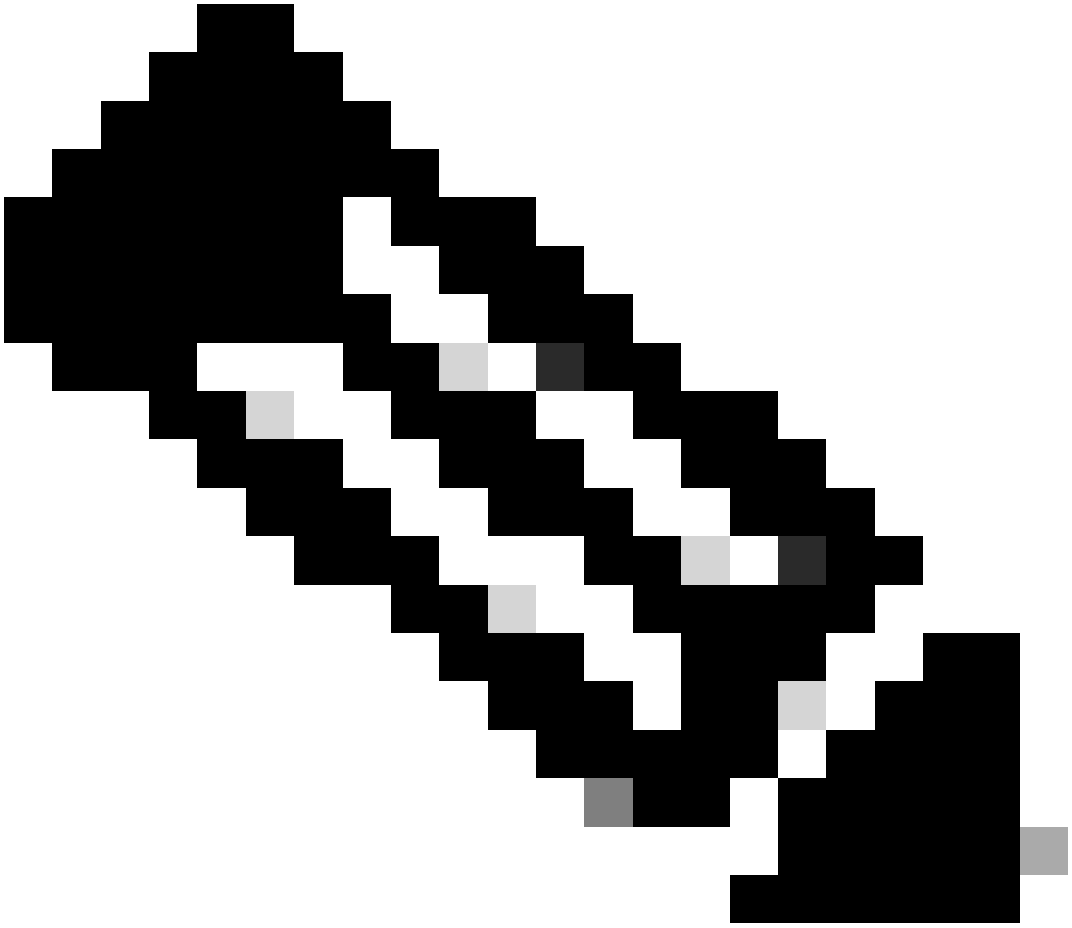
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

In het voorbeeld kunnen we zien dat de bewering alleen geldig is tussen 09:52:10.759 UTC tot 10:57:10.759 UTC, en de tijd op de firewall bevindt zich buiten dit geldigheidsvenster.



Opmerking: De geldigheidstermijn in de bewering is in UTC. Als de klok op de firewall in een andere tijdzone is geconfigureerd, wordt de tijd in UTC vóór validatie omgezet.

Oplossing

Configureer de juiste tijd op de firewall handmatig of met behulp van een NTP-server en controleer of de huidige tijd van de firewall binnen de geldigheid van de bewering in UTC valt. Als de firewall is geconfigureerd in een andere tijdzone dan UTC, moet u ervoor zorgen dat de tijd wordt geconverteerd naar UTC voordat u de geldigheid van de bewering controleert.

Probleem 3: Handtekening wordt niet gecontroleerd

verklaring

Wanneer de firewall de handtekening van de SAML-bevestiging die is ontvangen van de IdP niet verifieert vanwege een onjuist IdP-certificaat dat is geconfigureerd onder de firewall webvpn-

configuratie met de opdracht trustpoint idp <trustpoint>.

Voorbeeld van debug:

<#root>

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

signature does not verify

Oplossing

Download en installeer het certificaat van de IdP op de firewall en wijs het nieuwe trustpoint toe onder de firewall webvpn-configuratie. Het IdP-ondertekeningscertificaat is meestal te vinden in de metagegevens van de IdP of de gedecodeerde SAML-respons.

Probleem 4: Onjuiste URL voor Bewering Consumentenservice

verklaring

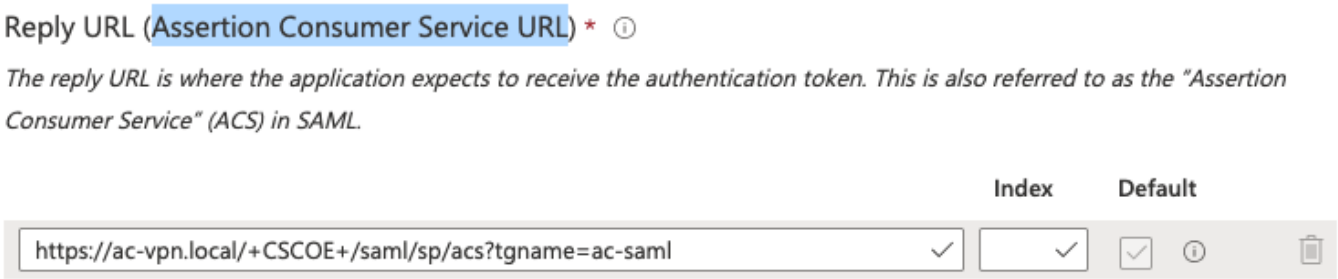
IdP is geconfigureerd met de verkeerde Reply URL (Assertion Consumer Service URL).

Voorbeelden

Voorbeeld van debug:

Er worden geen foutmeldingen weergegeven nadat de eerste verificatieaanvraag is verzonden. Gebruiker kan inloggegevens invoeren, maar nadat die verbinding mislukt en er geen fouten worden afgedrukt.

Van IDP:



Van FW- of SP-metagegevens:

<#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**"

/>

In het voorbeeld is te zien dat de "Assertion Consumer Service URL" op IdP niet overeenkomt met de locatie op de metadata van SP.

Oplossing

Wijzig de URL van de Assertion Consumer Service op de IdP zoals weergegeven in de metagegevens van de SP. De metagegevens van de SP kunnen worden verkregen met behulp van de opdracht show saml metadata **<**tunnel-group-name**>**.

Probleem 5: Bewering Publiek is ongeldig

verklaring

Wanneer de IdP een onjuiste bestemming verzendt in de SAML-reactie, zoals de verkeerde tunnelgroep.

Voorbeeld van debug:

<#root>

[SAML] consume_assertion: assertion audience is invalid

Van SAML trace:

<#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>
```

Van Firewall- of SP-metagegevens:

<#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"

/>

Oplossing

Corrigeer de configuratie op de IDP omdat de bestemming en ontvanger in SAML-reactie moeten overeenkomen met de locatie zoals weergegeven in de firewall/SP-metagegevens in de uitvoer toon kleine metagegevens <tunnel-group-name>.

Probleem 6: wijzigingen in SAML-configuratie worden niet van kracht

verklaring

Na elke wijziging met SAML-configuratie onder webvpn, wordt voorgesteld om de saml identity-provider <IDP-Entity-ID> opdracht onder de tunnelgroep te verwijderen en opnieuw toe te voegen.

Oplossing

Verwijder en voeg de opdracht saml identity-provider <IDP-Entity-ID> onder de tunnelgroep opnieuw toe.

Probleem 7: Dezelfde IDP gebruiken onder meerdere tunnelgroep / verbindingsprofielen

verklaring

Als u SAML-verificatie wilt configureren om dezelfde IdP SSO-toepassing voor meerdere tunnelgroepen te gebruiken, volgt u de onderstaande configuratiestappen.

Oplossingen

Optie 1 voor ASA 9.16 en eerder, FDM beheerde FTD, of FMC/FTD 7.0 en eerder:

- Maak afzonderlijke SSO-toepassingen op de IdP, één voor elke

tunnelgroep/verbindingsprofiel.
- Maak een CSR met behulp van de standaard CN die wordt gebruikt door de IDP.
- Onderteken de CSR van een interne/externe CA.
- Installeer hetzelfde ondertekende identiteitscertificaat op de toepassingen die moeten worden gebruikt voor afzonderlijke tunnelgroepen of verbindingsprofielen.

Optie 2 voor ASA 9.17.1 en hoger of FTD/FMC 7.1 en hoger:

- Maak afzonderlijke SSO-toepassingen op de IdP, één voor elke tunnelgroep/verbindingsprofiel.
- Download de certificaten van elke applicatie en upload op de ASA of FTD.
- Wijs het vertrouwenspunt toe dat overeenkomt met de IdP-toepassing voor elk tunnelgroep/verbindingsprofiel.

Probleem 8: Verificatie mislukt vanwege probleem met ophalen van de Single Sign-On-cookie

verklaring

Dit is te zien op de Secure Client-software op het clientapparaat om meerdere redenen, waaronder maar niet beperkt tot:

- De geldigheid van de bewering valt buiten de huidige tijd van de FW.
- De Entiteit-ID of de Assertion Consumer Service-URL is onjuist gedefinieerd op de IDP.

Oplossing

- Voer foutmeldingen uit op de FW en controleer op specifieke fouten.
- Verifieer de Entiteit-ID en de Assertion Consumer Service-URL die is geconfigureerd op de IDP aan de hand van de metagegevens die zijn verkregen uit de FW.

Probleem 9: Hash-mismatch van relaisstatus

Toelichting

- De parameter RelayState dient om de gebruiker door middel van IdP terug te leiden naar de oorspronkelijke bron die is aangevraagd na succesvolle SAML-verificatie. De RelayState-informatie over de bewering moet overeenkomen met de RelayState-informatie aan het einde van de URL voor het authenticatieverzoek.
- Dit kan een indicatie zijn van een MitM-aanval, maar kan ook worden veroorzaakt door wijzigingen in de RelayState aan de IdP-kant.

Voorbeeld van debug:

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

Oplossing

- Ga naar een vaste release zoals beschreven in Cisco bug ID CSCwf85757
- Controleer of de IdP de RelayState-gegevens niet wijzigt.

Verdere probleemoplossing

Hoewel de meeste SAML-probleemoplossing kan worden uitgevoerd met alleen de uitvoer van de webvpn-foutopsporing, zijn er echter momenten waarop extra foutopsporing nuttig kan zijn om de oorzaak van een probleem aan te wijzen.

<#root>

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

Gerelateerde informatie

- Technische ondersteuning en downloads van Cisco
- ASA-configuratiehandleidingen
- Configuratiehandleidingen voor FMC/FDM

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.