Resolución de problemas comunes con SAML en ASA y FTD

Contenido

Introducción

Este documento describe los problemas más comunes encontrados al resolver problemas de SAML en dispositivos Cisco ASA y FTD.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del proveedor de identidad SAML (IdP)
- Configuración del firewall Cisco Secure ASA o del objeto de registro único Firepower Threat Defense (FTD)
- VPN AnyConnect de Cisco Secure Client

Componentes Utilizados

La guía de prácticas recomendadas se basa en las siguientes versiones de hardware y software:

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

SAML (lenguaje de marcado de aserción de seguridad) es un marco basado en XML para intercambiar datos de autenticación y autorización entre dominios de seguridad. Crea un círculo de confianza entre el usuario, un proveedor de servicios (SP) y un proveedor de identidad (IdP) que permite al usuario iniciar sesión una sola vez para varios servicios. SAML se puede utilizar para la autenticación VPN de acceso remoto para conexiones de Cisco Secure Client a cabeceras ASA y FTD VPN, donde ASA o FTD es la entidad SP en el círculo de confianza.

La mayoría de los problemas de SAML se pueden resolver verificando la configuración en el IdP y el ASA/FTD que se está utilizando. En los casos en que la causa no es clara, las depuraciones dan más claridad y los ejemplos de esta guía provienen del comando debug webvpn saml 255.

El propósito de este documento es ser una referencia rápida para problemas conocidos de SAML y posibles soluciones.

Problemas Comunes:

Problema 1: Discordancia de ID de entidad

Explicación

Generalmente significa que el comando saml idp [entityID] bajo la configuración de firewall webvpn no coincide con el IdP Entity ID encontrado en los metadatos del IdP como se muestra en el ejemplo.

Ejemplo de depuración:

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

Desde IDP:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

Desde ASA/FTD:

<#root>

```
saml idp
```

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

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

Solución

Verifique el ID de entidad del archivo de metadatos del IdP y cambie el comando saml idp [entity id] para que coincida exactamente con esto, incluyendo cualquier carácter de barra diagonal inversa (/).

Problema 2: Afirmación no válida

Explicación

Esto significa que el firewall no puede validar la afirmación proporcionada por el IdP ya que el

reloj del firewall está fuera de la validez de la afirmación.

Ejemplo de depuración:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Ejemplo:

<#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>

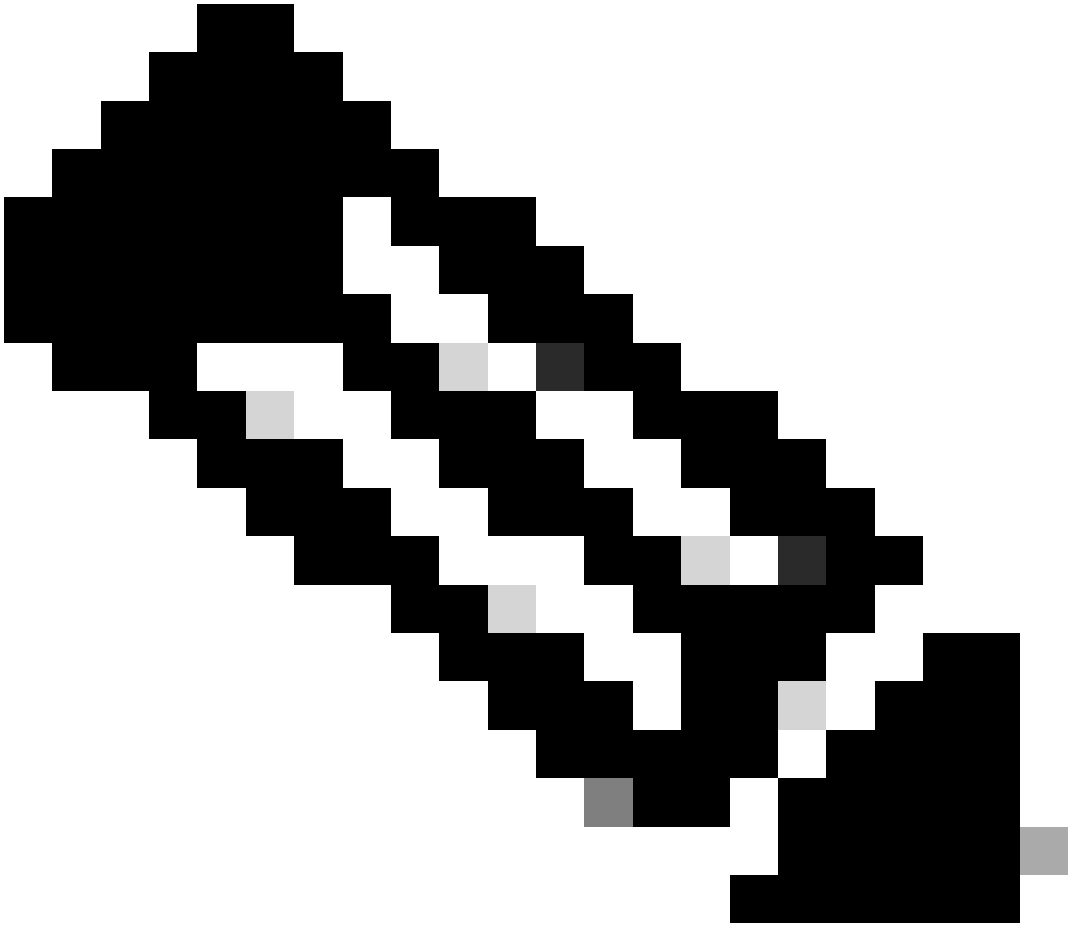
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

En el ejemplo, podemos ver que la aserción sólo es válida entre 09:52:10.759 UTC y 10:57:10.759 UTC, y la hora del firewall está fuera de esta ventana de validez.



Nota: El tiempo de validez visto en la afirmación está en UTC. Si el reloj del firewall está configurado en una zona horaria diferente, convierte la hora en UTC antes de la validación.

Solución

Configure la hora correcta en el firewall manualmente o mediante un servidor NTP y verifique que la hora actual del firewall esté dentro de la validez de la afirmación en UTC. Si el firewall está configurado en una zona horaria distinta a UTC, asegúrese de que la hora se convierte a UTC antes de comprobar la validez de la afirmación.

Problema 3: La firma no se verifica

Explicación

Cuando el firewall no puede verificar la firma de la afirmación SAML recibida del IdP debido a un

certificado IdP incorrecto configurado bajo la configuración de firewall webvpn con el comando trustpoint idp <trustpoint>.

Ejemplo de depuración:

<#root>

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

signature does not verify

Solución

Descargue e instale el certificado del IdP en el firewall y asigne el nuevo punto de confianza en la configuración de firewall webvpn. El certificado de firma IdP se puede encontrar generalmente en los metadatos del IdP o en la respuesta SAML decodificada.

Problema 4: URL incorrecta para el servicio de aserción al consumidor

Explicación

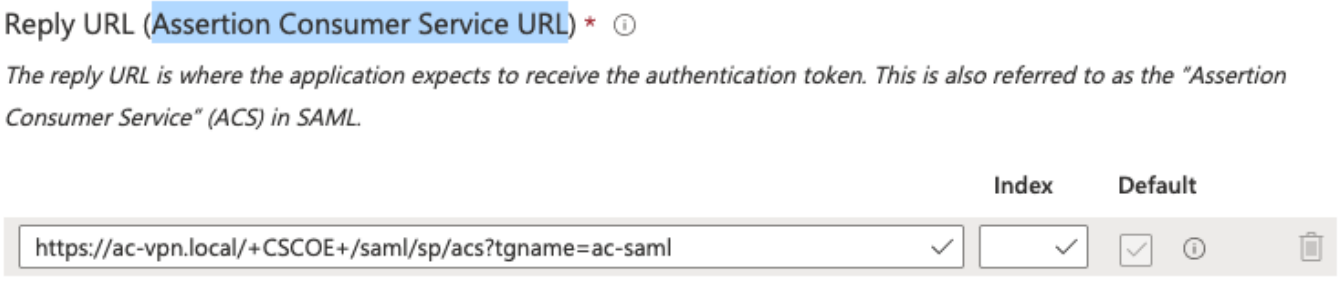
IdP está configurado con la URL de respuesta incorrecta (URL de servicio de consumidor de aserción).

Examples

Ejemplo de depuración:

No se muestran depuraciones después de enviar la solicitud de autenticación inicial. El usuario puede ingresar las credenciales pero después de que la conexión falle y no se impriman depuraciones.

Desde IDP:



Desde metadatos de FW o SP:

<#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"

/>

En el ejemplo, se puede ver que la "URL de Assertion Consumer Service" en IdP no coincide con la ubicación en los metadatos de SP.

Solución

Cambie la URL de Assertion Consumer Service en el IdP como se muestra en los metadatos del SP. Los metadatos del SP se pueden obtener mediante el comando show saml metadata <tunnel-group-name>.

Problema 5: La audiencia de afirmación no es válida

Explicación

Cuando el IdP envía un destino incorrecto en la respuesta SAML, como el grupo de túnel incorrecto.

Ejemplo de depuración:

<#root>

[SAML] consume_assertion: assertion audience is invalid

Desde seguimiento SAML:

<#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>
```

Desde metadatos de firewall o SP:

<#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"
 />
```

Solución

Corrija la configuración en el IDP ya que el Destino y el Destinatario en la respuesta SAML deben coincidir con la ubicación como se muestra en los metadatos del firewall/SP en la salida show saml metadata <tunnel-group-name>.

Problema 6: Los cambios de configuración de SAML no tienen efecto

Explicación

Después de cualquier modificación con la configuración SAML bajo webvpn, se sugiere quitar y volver a agregar el comando saml identity-provider <IDP-Entity-ID> bajo el grupo de túnel.

Solución

Quite y vuelva a agregar el comando saml identity-provider <IDP-Entity-ID> bajo el grupo de túnel.

Problema 7: Cómo Utilizar el Mismo IDP bajo Múltiples Perfiles de Grupo de Túnel/Conexión

Explicación

Para configurar la autenticación SAML para utilizar la misma aplicación SSO IdP para varios grupos de túnel, siga los pasos de configuración a continuación.

Soluciones

Opción 1 para ASA 9.16 y versiones anteriores, FTD gestionado por FDM o FMC/FTD 7.0 y versiones anteriores:

- Cree aplicaciones SSO separadas en el IdP, una para cada grupo de túnel/perfil de conexión.
- Cree un CSR utilizando el CN predeterminado que utiliza el IDP.
- Firmar el CSR desde una CA interna o externa.
- Instale el mismo certificado de identidad firmado en las aplicaciones que se utilizarán para grupos de túnel o perfiles de conexión independientes.

Opción 2 para ASA 9.17.1 y posteriores o FTD/FMC 7.1 y posteriores:

- Cree aplicaciones SSO separadas en el IdP, una para cada grupo de túnel/perfil de conexión.
- Descargue los certificados de cada aplicación y cárguelos en el ASA o FTD.
- Asigne el punto de confianza que corresponde a la aplicación IdP para cada grupo de túnel/perfil de conexión.

Problema 8: Error de autenticación debido a un problema al recuperar la cookie de inicio de sesión único

Explicación

Esto se puede ver en el software Secure Client en el dispositivo del cliente debido a múltiples razones, incluyendo pero no limitado a:

- La validez de la afirmación está fuera de la hora actual del firmware.
- El ID de entidad o URL de servicio de consumidor de aserción no está definido correctamente en el IDP.

Solución

- Ejecute los debugs en el FW y verifique si hay errores específicos.
- Verifique el ID de entidad y la URL de servicio de consumidor de aserción configurados en el IDP con los metadatos obtenidos del FW.

Problema 9: Discordancia de Hash de estado de retransmisión

Explicaciones

- El parámetro RelayState sirve para que IdP redirija al usuario al recurso original solicitado después de una autenticación SAML exitosa. La información de RelayState en la afirmación debe coincidir con la información de RelayState al final de la URL de solicitud de autenticación.
- Esto puede ser una indicación de un ataque MitM pero también puede ser causado por cambios en el estado de retransmisión en el lado IdP.

Ejemplo de depuración:

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

Solución

- Pase a una versión corregida como se detalla en el Id. de bug Cisco CSCwf85757
- Verifique que el IdP no esté cambiando la información de RelayState.

Solución de problemas adicional

Mientras que la mayoría de la resolución de problemas de SAML se puede realizar con solo la salida de la depuración saml de webvpn, sin embargo, hay momentos en los que las depuraciones adicionales pueden ser útiles para identificar la causa de un problema.

<#root>

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

Información Relacionada

- Soporte técnico y descargas de Cisco
- Guías de configuración de ASA
- Guías de configuración de FMC/FDM

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).