Solucionar problemas comuns com SAML no ASA e no FTD

Contents

Introdução

Este documento descreve os problemas mais comuns encontrados durante a solução de problemas de SAML em dispositivos Cisco ASA e FTD.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Provedor de Identidade SAML (IdP)
- Configuração do Cisco Secure ASA Firewall ou Firepower Threat Defense (FTD) Single Sign-on Object
- Cisco Secure Client AnyConnect VPN

Componentes Utilizados

O guia de práticas recomendadas baseia-se nas seguintes versões de hardware e software:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

SAML (Security Assertion Markup Language) é uma estrutura baseada em XML para troca de dados de autenticação e autorização entre domínios de segurança. Ele cria um círculo de confiança entre o usuário, um provedor de serviços (SP) e um provedor de identidade (IdP) que permite que o usuário entre uma única vez para vários serviços. O SAML pode ser usado para autenticação de VPN de acesso remoto para conexões do Cisco Secure Client para headends de VPN ASA e FTD, onde o ASA ou FTD é a entidade SP no círculo de confiança.

A maioria dos problemas de SAML pode ser resolvida verificando a configuração no IdP e no ASA/FTD que está sendo usado. Nos casos em que a causa não é clara, as depurações dão mais clareza e os exemplos neste guia vêm do comando debug webvpn saml 255.

A finalidade deste documento é ser uma referência rápida para problemas de SAML conhecidos e possíveis soluções.

Problemas comuns:

Problema 1: Incompatibilidade de ID de entidade

Explicação

Geralmente significa que o comando saml idp [entityID] na configuração do firewall webvpn não corresponde à ID de entidade do IdP encontrada nos metadados do IdP como mostrado no exemplo.

Exemplo de depuração:

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

Do IDP:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

De ASA/FTD:

<#root>

```
saml idp
```

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

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

Solução

Verifique o ID da entidade do arquivo de metadados do IdP e altere o comando saml idp [entity id] para que ele corresponda exatamente a ele, incluindo todos os caracteres de barra invertida (/).

Problema 2: Asserção não válida

Explicação

Isso significa que o firewall não pode validar a asserção fornecida pelo IdP, pois o relógio do firewall está fora da validade da asserção.

Exemplo de depuração:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Exemplo:

<#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>

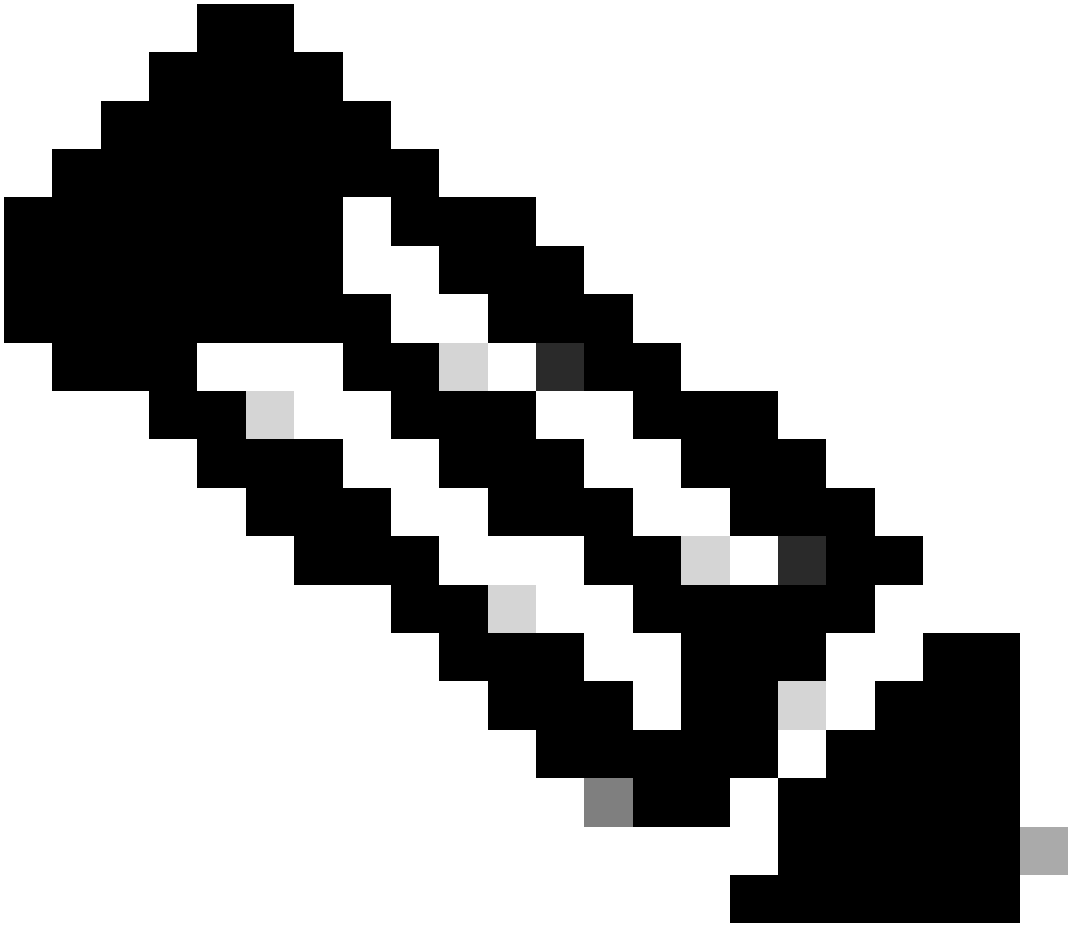
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

No exemplo, podemos ver que a asserção só é válida entre 09:52:10.759 UTC a 10:57:10.759 UTC, e a hora no firewall está fora dessa janela de validade.



Note: O tempo de validade visto na asserção está em UTC. Se o relógio no firewall estiver configurado em um fuso horário diferente, ele converte a hora em UTC antes da validação.

Solução

Configure a hora correta no firewall manualmente ou usando um servidor NTP e verifique se a hora atual do firewall está dentro da validade da asserção em UTC. Se o firewall estiver configurado em um fuso horário diferente do UTC, verifique se a hora foi convertida em UTC antes de verificar a validade da asserção.

Problema 3: A assinatura não é verificada

Explicação

Quando o firewall falha ao verificar a assinatura da asserção SAML recebida do IdP devido a um

certificado IdP incorreto configurado na configuração de firewall webvpn com o comando trustpoint idp <trustpoint>.

Exemplo de depuração:

<#root>

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

signature does not verify

Solução

Baixe e instale o certificado do IdP no firewall e atribua o novo ponto de confiança na configuração do firewall webvpn. O certificado de assinatura IdP geralmente pode ser encontrado nos metadados do IdP ou na resposta SAML decodificada.

Problema 4: URL incorreta para o serviço de consumidor de asserção

Explicação

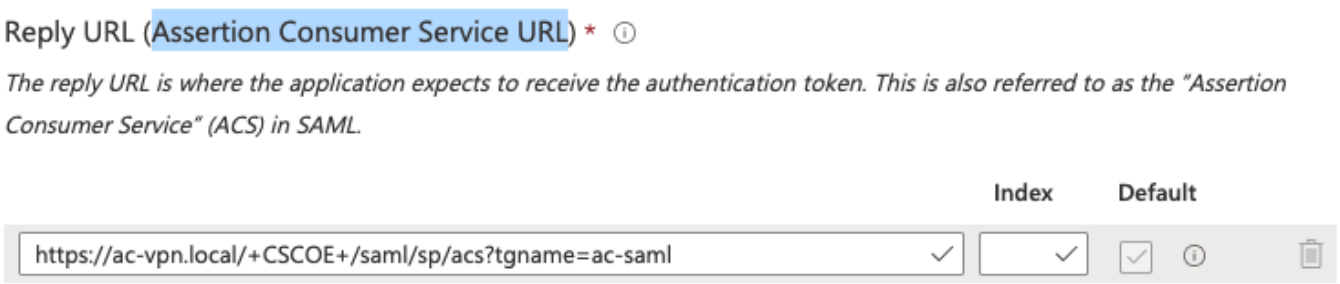
O IdP está configurado com a URL de Resposta incorreta (URL do Serviço de Consumidor de Asserção).

Examples

Exemplo de depuração:

Nenhuma depuração é mostrada após o envio da solicitação de autenticação inicial. O usuário pode inserir credenciais, mas depois que a conexão falhar e nenhuma depuração for impressa.

Do IDP:



De metadados de FW ou 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"

/>

No exemplo, pode-se ver que o "URL do serviço de consumidor de asserção" no IdP não corresponde ao local nos metadados do SP.

Solução

Altere a URL do Serviço de Consumidor de Asserção no IdP conforme mostrado nos metadados do SP. Os metadados do SP podem ser obtidos com o comando show saml metadata <tunnel-group-name>.

Problema 5: Audiência de Asserção é Inválida

Explicação

Quando o IdP envia um destino incorreto na resposta SAML, tal como o grupo de túneis errado.

Exemplo de depuração:

<#root>

[SAML] consume_assertion: assertion audience is invalid

Do rastreamento 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>
```

Dos metadados do Firewall ou 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"

 />
```

Solução

Corrija a configuração no IDP, pois o Destino e o Destinatário na resposta SAML devem corresponder ao local conforme mostrado nos metadados do firewall/SP na saída de show saml metadata <tunnel-group-name>.

Problema 6: As alterações de configuração SAML não entram em vigor

Explicação

Após qualquer modificação com a configuração SAML em webvpn, sugere-se remover e adicionar novamente o comando saml identity-provider <IDP-Entity-ID> no tunnel-group.

Solução

Remova e adicione novamente o comando saml identity-provider <IDP-Entity-ID> no tunnel-group.

Problema 7: Como usar o mesmo IDP em vários perfis tunnel-group/connection

Explicação

Para configurar a autenticação SAML para usar o mesmo aplicativo IdP SSO para vários grupos de túneis, siga as etapas de configuração abaixo.

Soluções

Opção 1 para o ASA 9.16 e anterior, FDM gerenciado FTD ou FMC/FTD 7.0 e anterior:

- Crie aplicações SSO separadas no IdP, uma para cada perfil de grupo de túneis/conexão.
- Crie um CSR usando o CN padrão usado pelo IDP.
- Assine o CSR de uma CA interna/externa.

- Instale o mesmo certificado de identidade assinado nos aplicativos a serem usados para grupos de túneis separados ou perfis de conexão.

Opção 2 para o ASA 9.17.1 e posterior ou FTD/FMC 7.1 e posterior:

- Crie aplicativos SSO separados no IdP, um para cada perfil de grupo de túneis/conexão.
- Faça o download dos certificados de cada aplicativo e carregue-os no ASA ou no FTD.
- Atribua o ponto confiável que corresponde ao aplicativo IdP para cada perfil tunnel-group/connection.

Problema 8: Falha na autenticação devido a um problema na recuperação do cookie de logon único

Explicação

Isso pode ser visto no software Secure Client no dispositivo cliente devido a vários motivos, incluindo, mas não limitado a:

- A validade da asserção está fora da hora atual do FW.
- A ID da entidade ou a URL do serviço do consumidor de asserção está definida incorretamente no IDP.

Solução

- Execute depurações no FW e verifique se há erros específicos.
- Verifique a ID da entidade e a URL do serviço do consumidor de asserção configuradas no IDP em relação aos metadados obtidos do FW.

Problema 9: Incompatibilidade de Hash de Relay-state

Explicações

- O parâmetro RelayState serve para que o IdP redirecione o usuário de volta para o recurso original solicitado após a autenticação SAML bem-sucedida. As informações de RelayState na asserção devem corresponder às informações de RelayState no final da URL de solicitação de autenticação.
- Isso pode ser uma indicação de um ataque MitM, mas também pode ser causado por alterações no RelayState no lado do IdP.

Exemplo de depuração:

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

Solução

- Mude para uma versão fixa conforme detalhado na ID de bug Cisco CSCwf85757
- Verifique se o IdP não está alterando as informações de RelayState.

Mais soluções de problemas

Embora a maioria das soluções de problemas de SAML possa ser realizada apenas com a saída da depuração webvpn saml, no entanto, há momentos em que depurações adicionais podem ser úteis para identificar a causa de um problema.

<#root>

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

Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Guias de configuração do ASA
- Guias de configuração do FMC/FDM

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.