ASA 및 FTD에서 SAML의 일반적인 문제 해결

목차

소개

이 문서에서는 Cisco ASA 및 FTD 어플라이언스에서 SAML을 트러블슈팅하는 동안 발생하는 가장 일반적인 문제에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SAML IdP(Identity Provider) 컨피그레이션
- Cisco Secure ASA Firewall 또는 FTD(Firepower Threat Defense) Single Sign-on Object 컨피그레이션
- Cisco Secure Client AnyConnect VPN

사용되는 구성 요소

모범 사례 가이드는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SAML(Security Assertion Markup Language)은 보안 도메인 간에 인증 및 권한 부여 데이터를 교환하기 위한 XML 기반 프레임워크입니다. 사용자, 서비스 공급자(SP) 및 IDP(Identity Provider) 간에 신뢰 범위를 생성하여 여러 서비스에 대해 한 번에 로그인할 수 있습니다. SAML은 ASA 및 FTD VPN 헤드엔드에 대한 Cisco Secure Client 연결을 위한 원격 액세스 VPN 인증에 사용할 수 있습니다. 여기서 ASA 또는 FTD는 신뢰 서클의 SP 엔터티입니다.

대부분의 SAML 문제는 사용 중인 IdP 및 ASA/FTD의 컨피그레이션을 확인하여 해결할 수 있습니다. 원인이 명확하지 않은 경우 디버그는 더 명확한 설명을 제공하며 이 설명서의 예는 debug webvpn saml 255 명령에서 나옵니다.

이 문서의 목적은 알려진 SAML 문제 및 가능한 해결책을 신속하게 참조하는 것입니다.

일반적인 문제:

문제 1: 엔터티 ID 불일치

설명

일반적으로 방화벽 webvpn 컨피그레이션의 saml idp [entityID] 명령이 예에 표시된 대로 IdP 메타데이터에 있는 IdP 엔티티 ID와 일치하지 않음을 의미합니다.

디버그 예:

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

IDP에서:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

ASA/FTD에서:

<#root>

```
saml idp
```

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

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

솔루션

IdP 메타데이터 파일의 엔티티 ID를 확인하고 이와 정확히 일치하도록 saml idp [entity id] 명령을 백슬래시(/) 문자로 변경합니다.

문제 2: 어설션이 잘못되었습니다.

설명

이는 방화벽의 시계가 어설션의 유효성을 벗어났기 때문에 방화벽이 IdP에서 제공한 어설션의 유효성을 검사할 수 없음을 의미합니다.

디버그 예:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

예:

<#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>

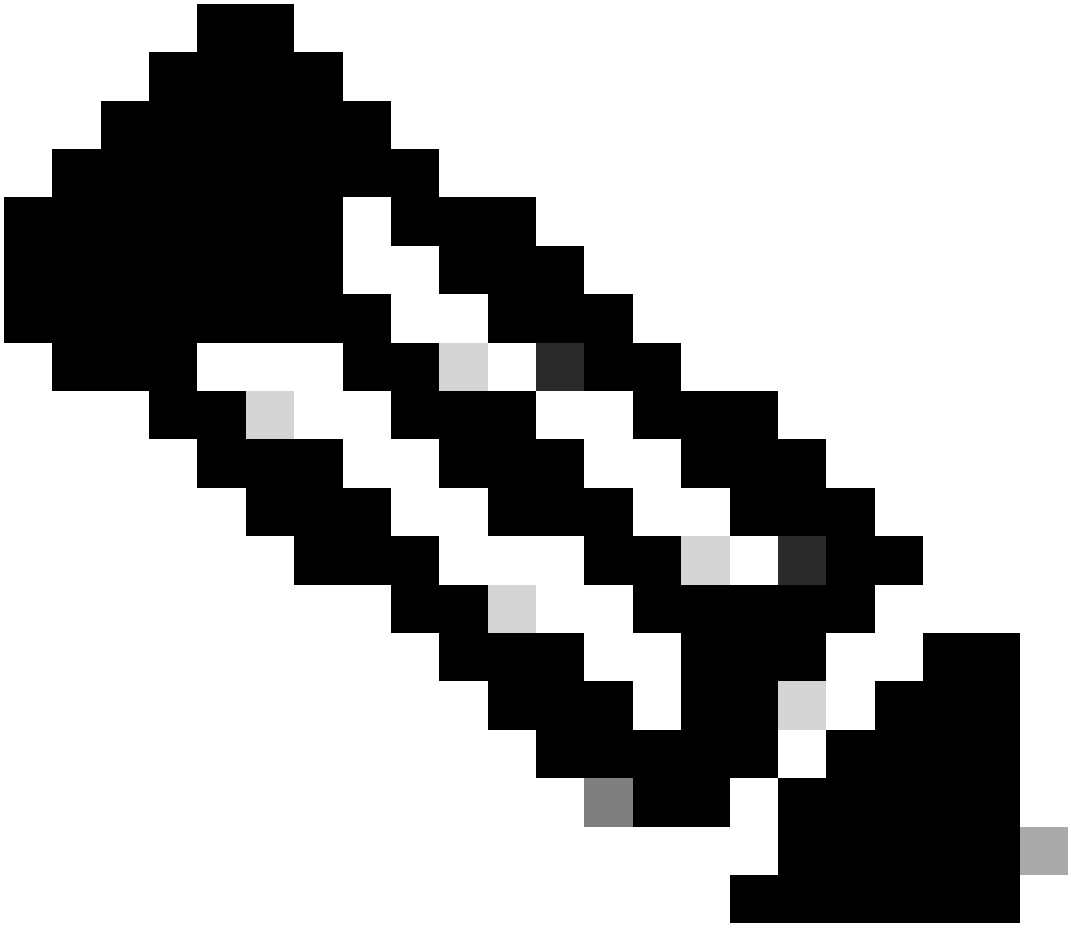
firepower#

 show clock

15:26:49.240 UTC Tue Jun 21 2022

 >>>> Current time on the firewall

이 예에서는 어설션이 09:52:10.759 UTC에서 10:57:10.759 UTC 사이에서만 유효하며 방화벽의 시간이 이 유효성 창을 벗어났음을 알 수 있습니다.



참고: 어설션에 표시되는 유효 기간은 UTC입니다. 방화벽의 시계가 다른 표준 시간대에 구성된 경우 유효성 검사 전 시간을 UTC로 변환합니다.

솔루션

수동으로 또는 NTP 서버를 사용하여 방화벽의 올바른 시간을 구성하고 방화벽의 현재 시간이 UTC의 어설션에 대한 유효성 내에 있는지 확인합니다. 방화벽이 UTC와 다른 표준 시간대에 구성된 경우 검증의 유효성을 확인하기 전에 시간이 UTC로 변환되었는지 확인합니다.

문제 3: 서명이 확인되지 않음

설명

trustpoint idp <trustpoint> 명령을 사용하여 방화벽 webvpn 컨피그레이션에 구성된 잘못된 IdP 인증서로 인해 방화벽이 IdP에서 수신한 SAML assertion의 서명을 확인하지 못할 경우

디버그 예:

<#root>

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

signature does not verify

솔루션

방화벽의 IdP에서 인증서를 다운로드하여 설치하고 방화벽 webvpn 컨피그레이션 아래에 새 신뢰 지점을 할당합니다. IdP 서명 인증서는 일반적으로 IdP의 메타데이터 또는 디코딩된 SAML 응답에서 찾을 수 있습니다.

문제 4: 어설션 소비자 서비스의 URL이 잘못되었습니다.

설명

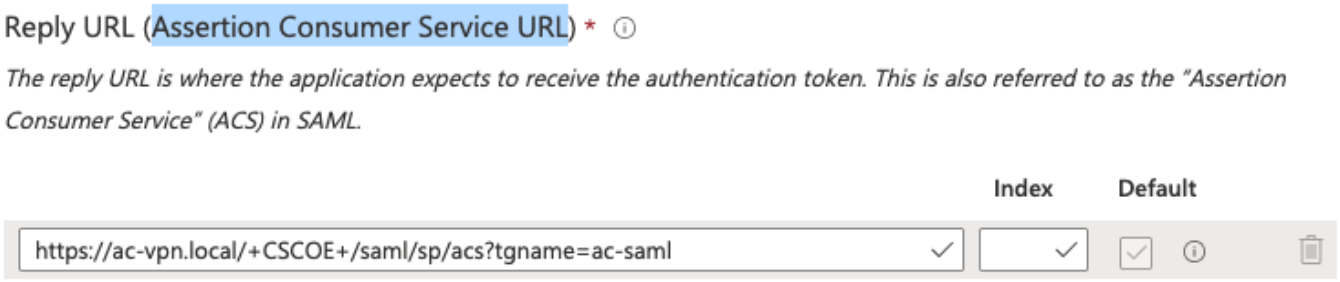
IdP가 잘못된 회신 URL(Assertion Consumer Service URL)로 구성되어 있습니다.

예

디버그 예:

초기 인증 요청을 보낸 후에는 디버그가 표시되지 않습니다. 사용자는 자격 증명을 입력할 수 있지만 연결이 실패하고 디버그가 인쇄되지 않은 후입니다.

IDP에서:



FW 또는 SP 메타데이터에서:

<#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"

```
 />
```

이 예에서는 IdP의 "Assertion Consumer Service URL"이 SP의 메타데이터 위치와 일치하지 않음

을 알 수 있습니다.

솔루션

SP의 메타데이터에 표시된 대로 IdP에서 Assertion Consumer Service URL을 변경합니다. SP의 메타데이터는 show saml metadata <tunnel-group-name> 명령을 사용하여 가져올 수 있습니다.

문제 5: 어설션 대상이 잘못되었습니다.

설명

IdP가 SAML 응답에서 잘못된 터널 그룹 등의 잘못된 대상을 전송하는 경우

디버그 예:

<#root>

[SAML] consume_assertion: assertion audience is invalid

SAML 추적에서:

<#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>

방화벽 또는 SP 메타데이터에서:

<#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"

/>

솔루션

SAML 응답의 대상 및 수신자가 show saml metadata <tunnel-group-name> 출력의 방화벽/SP 메타데이터에 표시된 위치와 일치해야 하므로 IDP의 컨피그레이션을 수정합니다.

문제 6: SAML 컨피그레이션 변경 사항이 적용되지 않음

설명

webvpn에서 SAML 컨피그레이션을 수정한 후, saml identity-provider <IDP-Entity-ID> 명령을 제거하고 tunnel-group 아래에 다시 추가하는 것이 좋습니다.

솔루션

터널 그룹 아래의 saml identity-provider <IDP-Entity-ID> 명령을 제거하고 다시 추가합니다.

문제 7: 여러 터널 그룹/연결 프로파일에서 동일한 IDP를 사용하는 방법

설명

여러 터널 그룹에 대해 동일한 IdP SSO 애플리케이션을 사용하도록 SAML 인증을 구성하려면 다음 컨피그레이션 단계를 수행합니다.

솔루션

ASA 9.16 이하, FDM 관리 FTD 또는 FMC/FTD 7.0 이하 버전의 옵션 1:

- 각 터널 그룹/연결 프로파일에 대해 하나씩 IdP에 별도의 SSO 어포메이션을 생성합니다.
- IDP에서 사용하는 기본 CN을 사용하여 CSR을 생성합니다.
- 내부/외부 CA에서 CSR에 서명합니다.
- 별도의 터널 그룹 또는 연결 프로파일에 사용할 애플리케이션에 동일한 서명 ID 인증서를 설치합니다.

ASA 9.17.1 이상 또는 FTD/FMC 7.1 이상에 대한 옵션 2:

- 각 터널 그룹/연결 프로파일에 대해 하나씩 IdP에 별도의 SSO 애플리케이션을 생성합니다.
- 각 애플리케이션에서 인증서를 다운로드하고 ASA 또는 FTD에 업로드합니다.
- 각 터널 그룹/연결 프로파일에 대해 IdP 애플리케이션에 해당하는 신뢰 지점을 할당합니다.

문제 8: Single Sign-On 쿠키를 검색하는 동안 문제가 발생하여 인증에 실패했습니다

.

설명

클라이언트 장치의 Secure Client 소프트웨어에서 다음과 같은 여러 가지 이유로 인해 볼 수 있습니다.

- 어설션의 유효성이 FW의 현재 시간을 벗어납니다.
- 엔터티 ID 또는 어설션 소비자 서비스 URL이 IDP에 잘못 정의되어 있습니다.

솔루션

- FW에서 디버그를 실행하고 특정 오류를 확인합니다.
- FW에서 가져온 메타데이터에 대해 IDP에 구성된 Entity ID 및 Assertion Consumer Service URL을 확인합니다.

문제 9: 릴레이 상태 해시 불일치

설명

- RelayState 매개 변수는 IdP가 사용자를 SAML 인증에 성공한 후 요청된 원래 리소스로 다시 리디렉션하도록 하는 목적을 수행합니다. 어설션의 RelayState 정보는 인증 요청 URL의 끝에 있는 RelayState 정보와 일치해야 합니다.
- 이는 MitM 공격을 나타낼 수 있지만 IdP 측에서 RelayState가 변경되었기 때문일 수도 있습니다.

디버그 예:

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

솔루션

- Cisco 버그 ID CSCwf에 설명된 대로 고정 릴리스로 이동합니다85757
- IdP가 RelayState 정보를 변경하지 않는지 확인합니다.

추가 문제 해결

대부분의 SAML 문제 해결은 webvpn saml debug의 출력만으로 수행할 수 있지만, 문제의 원인을 파악하는 데 추가 디버그가 도움이 될 수 있는 경우가 있습니다.

<#root>

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

관련 정보

- Cisco 기술 지원 및 다운로드
- ASA 컨피그레이션 가이드
- FMC/FDM 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.