Risoluzione dei problemi comuni con SAML su ASA e FTD

Sommario

Introduzione

Questo documento descrive i problemi più comuni incontrati durante la risoluzione dei problemi SAML su appliance Cisco ASA e FTD.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione provider di identità SAML (IdP)
- Configurazione di Cisco Secure ASA Firewall o Firepower Threat Defense (FTD) Single Sign-On Object
- Cisco Secure Client AnyConnect VPN

Componenti usati

La guida alle best practice si basa sulle seguenti versioni hardware e software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

SAML (Security Assertion Markup Language) è un framework basato su XML per lo scambio di dati di autenticazione e autorizzazione tra domini di sicurezza. Crea un circolo di fiducia tra l'utente, un provider di servizi (SP) e un provider di identità (IdP) che consente all'utente di accedere una sola volta a più servizi. SAML può essere utilizzato per l'autenticazione VPN ad accesso remoto per le connessioni Cisco Secure Client agli headend VPN ASA e FTD, dove ASA o FTD è l'entità SP nel cerchio di attendibilità.

La maggior parte dei problemi SAML può essere risolta verificando la configurazione sull'IdP e sull'ASA/FTD in uso. Nei casi in cui la causa non è chiara, i debug offrono maggiore chiarezza e gli esempi in questa guida vengono restituiti dal comando debug webvpn saml 255.

Lo scopo di questo documento è quello di fornire un rapido riferimento ai problemi SAML noti e alle possibili soluzioni.

Problemi comuni:

Problema 1: ID entità non corrispondente

Spiegazione

Generalmente significa che il comando saml idp [entityID] nella configurazione webvpn del firewall non corrisponde all'ID entità IdP trovato nei metadati dell'IdP, come mostrato nell'esempio.

Esempio di debug:

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

Da IDP:

<#root>

```
<EntityDescriptor ID="
```

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

```
" entityID="
```

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

```
">
```

Da ASA/FTD:

<#root>

```
saml idp
```

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

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

Soluzione

Controllare l'ID entità del file di metadati dell'IdP e modificare il comando saml idp [entity id] in modo che corrisponda esattamente a questo, inclusi eventuali caratteri barra rovesciata (/).

Problema 2: Asserzione non valida

Spiegazione

Ciò significa che il firewall non è in grado di convalidare l'asserzione fornita dall'IdP poiché l'orologio del firewall non è valido.

Esempio di debug:

<#root>

[SAML] consume_assertion: assertion is expired or not valid

Esempio:

<#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>

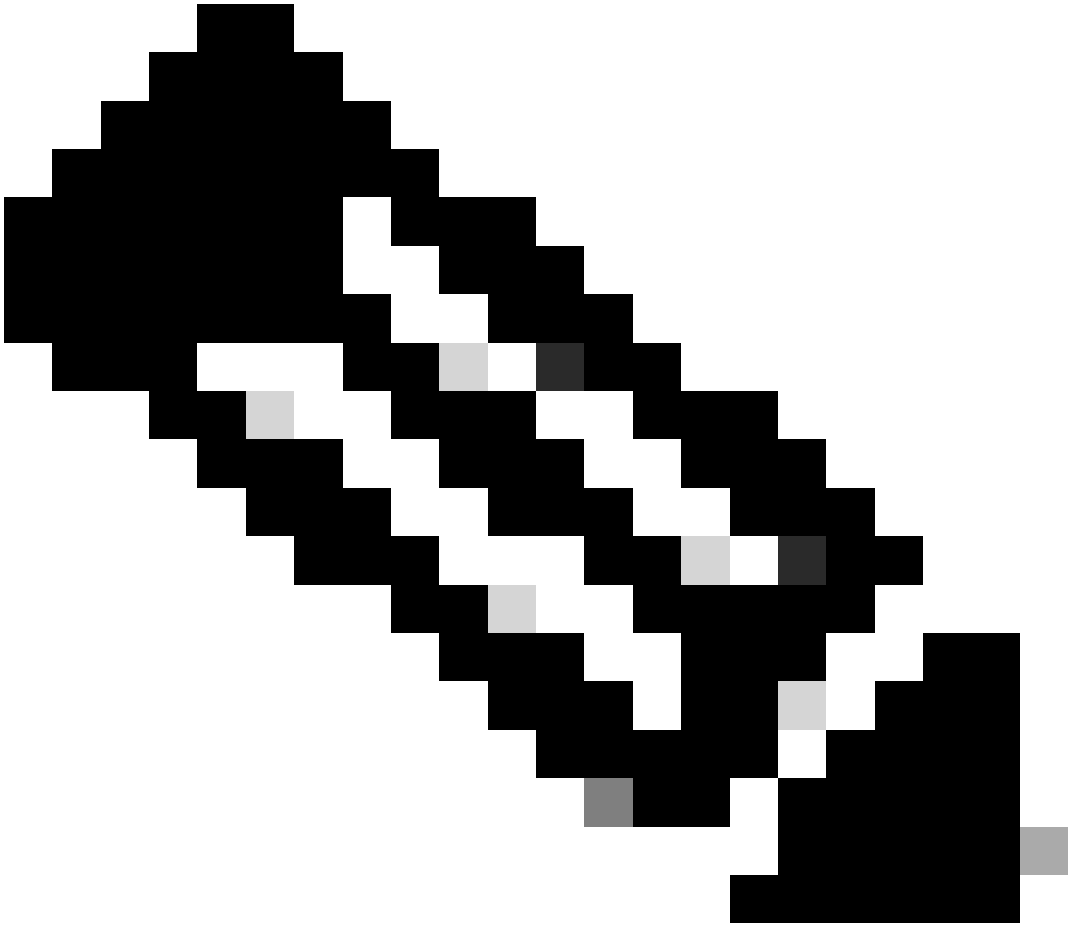
```
firepower#
```

show clock

15:26:49.240 UTC Tue Jun 21 2022

```
 >>>> Current time on the firewall
```

Nell'esempio, è possibile vedere che l'asserzione è valida solo tra le 09:52:10.759 UTC e le 10:57:10.759 UTC e l'ora sul firewall è esterna a questa finestra di validità.



Nota: Il tempo di validità visualizzato nell'asserzione è in UTC. Se l'orologio del firewall è configurato in un fuso orario diverso, l'ora verrà convertita in UTC prima della convalida.

Soluzione

Configurare l'ora corretta sul firewall manualmente o utilizzando un server NTP e verificare che l'ora corrente del firewall rientri nella validità dell'asserzione in UTC. Se il firewall è configurato in un fuso orario diverso da quello UTC, verificare che l'ora sia convertita in UTC prima di verificare la validità dell'asserzione.

Problema 3: firma non verificata

Spiegazione

Quando il firewall non riesce a verificare la firma dell'asserzione SAML ricevuta dal provider di identità a causa di un certificato del provider di identità non corretto configurato nella

configurazione webvpn del firewall con il comando trustpoint idp<trustpoint>.

Esempio di debug:

<#root>

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

signature does not verify

Soluzione

Scaricare e installare il certificato dal provider di identità sul firewall e assegnare il nuovo trust point nella configurazione webvpn del firewall. Il certificato di firma IdP si trova in genere nei metadati dell'IdP o nella risposta SAML decodificata.

Problema 4: URL non corretto per il servizio consumer di asserzione

Spiegazione

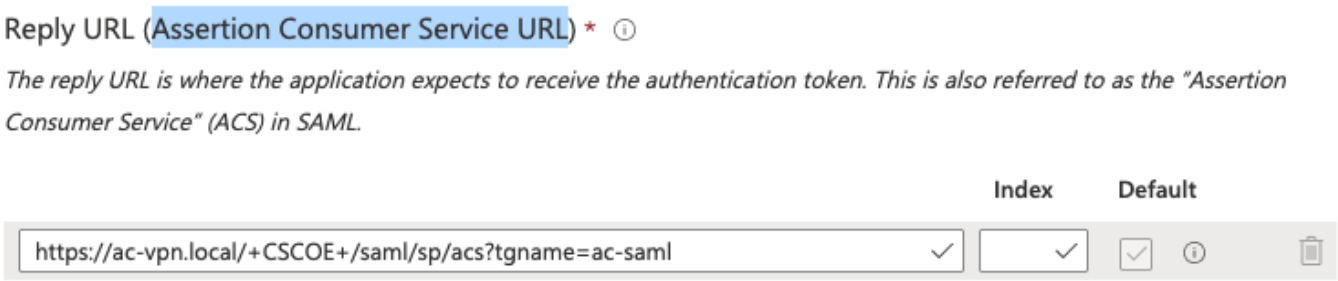
Il provider di identità è configurato con l'URL di risposta errato (URL servizio consumer di asserzione).

Esempi

Esempio di debug:

Dopo l'invio della richiesta di autenticazione iniziale, non viene visualizzato alcun debug. L'utente può immettere le credenziali, ma dopo tale connessione non riesce e non viene stampato alcun debug.

Da IDP:



Da metadati 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"

/>

Nell'esempio, è possibile notare che l'"URL del servizio consumer di asserzione" in IdP non corrisponde alla posizione nei metadati di SP.

Soluzione

Modificare l'URL del servizio consumer di asserzione nell'IdP come mostrato nei metadati dell'SP. I metadati dell'SP possono essere ottenuti usando il comando show saml metadata <tunnel-group-name>.

Problema 5: assertion audience is invalid (Il destinatario dell'asserzione non è valido)

Spiegazione

Quando l'IdP invia una destinazione errata nella risposta SAML, ad esempio un gruppo di tunnel errato.

Esempio di debug:

<#root>

[SAML] consume_assertion: assertion audience is invalid

Da traccia 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>
```

Da metadati 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"
 />
```

Soluzione

Correggere la configurazione nell'IDP in modo che la destinazione e il destinatario nella risposta SAML corrispondano al percorso indicato nei metadati firewall/SP nell'output show saml metadata <tunnel-group-name>.

Problema 6: modifiche alla configurazione SAML non effettive

Spiegazione

Dopo aver apportato modifiche alla configurazione SAML in webvpn, si consiglia di rimuovere e aggiungere nuovamente il comando saml identity-provider <IDP-Entity-ID> nel gruppo di tunnel.

Soluzione

Rimuovere e aggiungere nuovamente il comando saml identity-provider <IDP-Entity-ID> nel gruppo di tunnel.

Problema 7: Come utilizzare lo stesso IDP in più profili di connessione/gruppo di tunnel

Spiegazione

Per configurare l'autenticazione SAML in modo da utilizzare la stessa applicazione SSO IdP per più gruppi di tunnel, eseguire la procedura di configurazione seguente.

Soluzioni

Opzione 1 per ASA 9.16 e versioni precedenti, FTD gestito da FDM o FMC/FTD 7.0 e versioni

precedenti:

- Creare applicazioni SSO separate nell'IdP, una per ogni gruppo di tunnel/profilo di connessione.
- Create un CSR utilizzando il CN predefinito utilizzato dall'IDP.
- Firmare il CSR da una CA interna/esterna.
- Installare lo stesso certificato di identità firmato nelle applicazioni da utilizzare per gruppi di tunnel o profili di connessione separati.

Opzione 2 per ASA 9.17.1 e versioni successive o FTD/FMC 7.1 e versioni successive:

- Creare applicazioni SSO separate nell'IdP, una per ogni gruppo di tunnel/profilo di connessione.
- Scaricare i certificati da ciascuna applicazione e caricarli sull'appliance ASA o FTD.
- Assegnare il trust point corrispondente all'applicazione IdP per ogni gruppo di tunnel/profilo di connessione.

Problema 8: autenticazione non riuscita a causa di un problema durante il recupero del cookie Single Sign-On

Spiegazione

Questa condizione può essere rilevata sul software Secure Client sul dispositivo client per diversi motivi, tra cui:

- La validità dell'asserzione è al di fuori dell'ora corrente del firmware.
- L'ID entità o l'URL del servizio consumer di asserzione non è definito correttamente nell'IDP.

Soluzione

- Eseguire i debug sul firmware e verificare la presenza di errori specifici.
- Verificare l'ID entità e l'URL del servizio consumer di asserzione configurati nell'IDP in base ai metadati ottenuti dal firmware.

Problema 9: Hash stato inoltro non corrispondente

Spiegazioni

- Il parametro RelayState consente di reindirizzare l'utente tramite IdP alla risorsa originale richiesta dopo l'autenticazione SAML. Le informazioni RelayState nell'asserzione devono corrispondere alle informazioni RelayState alla fine dell'URL della richiesta di autenticazione.
- Ciò può indicare un attacco MitM, ma può essere causato anche da modifiche a RelayState sul lato IdP.

Esempio di debug:

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

Soluzione

- Passare a una versione fissa, come descritto nell'ID bug Cisco CSCwf85757
- Verificare che l'IdP non stia modificando le informazioni RelayState.

Ulteriori suggerimenti per la risoluzione dei problemi

Sebbene la maggior parte delle operazioni di risoluzione dei problemi SAML possa essere eseguita solo con l'output del debug saml webvpn, in alcuni casi è possibile eseguire debug aggiuntivi per individuare la causa di un problema.

<#root>

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

Informazioni correlate

- Supporto tecnico Cisco e download
- Guide alla configurazione dell'ASA
- Guide alla configurazione di FMC/FDM

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).