ESA/SMA SAML SSO를 위한 자체 서명 인증서 생성 및 구성

목차

소개

이 문서에서는 SAML(Security Assertion Markup Language) SP(Service Provider) 컨피그레이션을 위한 자체 서명 인증서를 만드는 방법에 대해 설명합니다.

사전 요구 사항

이 문서를 사용하여 ESA(Email Security Appliance) 및 SMA(Security Management Appliance)의 SAML(Security Assertion Markup Language) 2.0 SSO(Single Sign-On) SP(Service Provider) 컨피그레이션에 대한 자체 서명 인증서를 생성합니다.

요구 사항

방법 1(ESA 웹 UI): 웹 UI의 ESA 관리 액세스 및 인증서 관리 권한

방법 2(OpenSSL 명령): OpenSSL이 설치되고 명령줄에서 사용 가능합니다.

창: OpenSSL을 설치합니다.

macOS, Linux 또는 Unix: OpenSSL은 일반적으로 기본적으로 또는 운영 체제 패키지 관리자를 통

해 사용할 수 있습니다.

사용되는 구성 요소

구체적인 하드웨어 및 소프트웨어 요구 사항은 없습니다.

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

이 문서는 SAML(Security Assertion Markup Language) 2.0 SSO(Single Sign-On)를 사용하는 ESA(Email Security Appliance) 및 SMA(Security Management Appliance) 구축에 적용됩니다. SAML SP 구성에는 서비스 공급자 설정을 위한 SSL(Secure Sockets Layer) 인증서가 필요합니다. 인증서는 내부 인증서 도구, CA(인증 기관) 또는 자체 서명 인증서에서 가져올 수 있습니다.

문제

ESA 및 SMA를 위한 일부 SAML SP 구축에는 자체 서명 인증서가 필요합니다. 이 문서에서는 인증서 및 개인 키를 만들고 선택적으로 개인 키를 암호로 암호화하는 방법에 대해 설명합니다.

해결

- Windows에서 Windows용 OpenSSL을 설치합니다. 이 방법에 대한 지침이 있는 온라인 자습서가 있습니다.
- Unix, macOS 및 Linux에서는 일반적으로 OpenSSL을 기본적으로 사용할 수 있습니다.
- ESA에서 이미 인증서를 관리하고 SAML SP 사용을 위해 인증서를 내보내야 하는 경우 ESA 웹 UI 방법을 사용합니다.
- 명령줄에서 인증서 및 키 쌍을 직접 생성해야 하는 경우 OpenSSL 명령 방법을 사용합니다.

방법 1: ESA 웹 UI에서 자체 서명 인증서 생성 및 내보내기

ESA에서 이미 인증서를 관리하고 SAML SP 사용을 위해 인증서를 내보내야 하는 경우 이 방법을

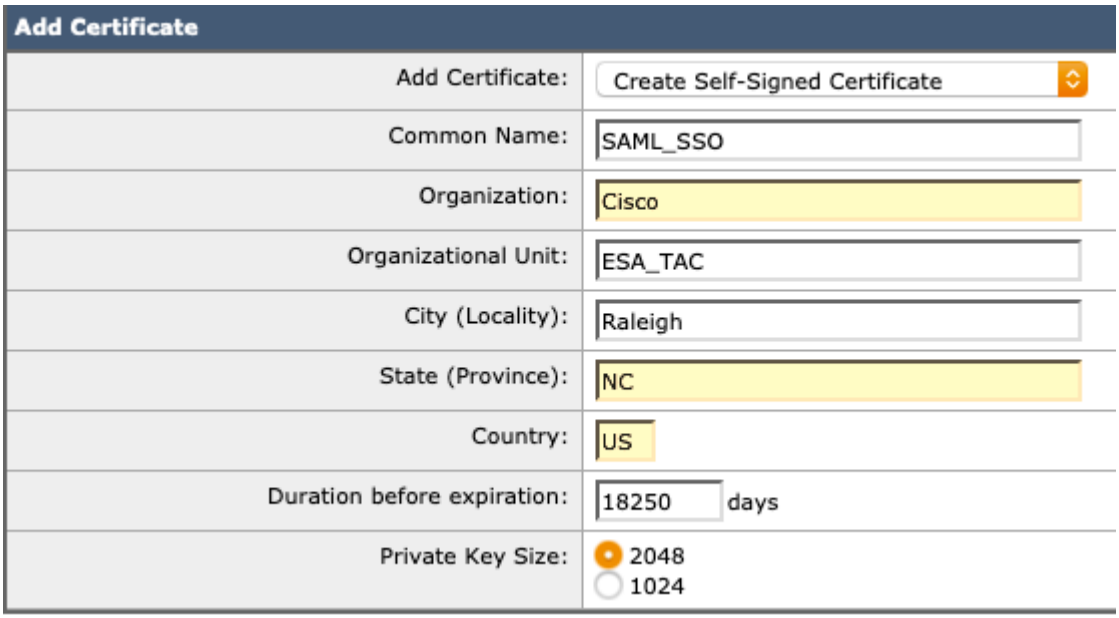
사용합니다.

인증서를 만듭니다.

1. ESA Web UI에서 Network(네트워크) > Certificates(인증서)로 이동합니다. Add Certificate(인증서 추가)를 선택한 다음 Create Self-Signed Certificate(셀프 서명 인증서 생성)를 선택합니다.

2. 템플리트 필드를 입력합니다. 일반 이름, 조직, 조직 단위, 시, 도, 국가 및 기간(1-18250일).

3. 개인 키 크기를 2048로 설정합니다.



자체 서명 인증서 템플릿 완료

4. 인증서를 제출하고, 결과를 검토하고, 변경사항 커밋을 선택합니다.

Certificate Name:	SAML_SSO
Common Name:	SAML_SSO
Organization:	Cisco
Organization Unit:	ESA_TAC
City (Locality):	Raleigh
State (Province):	NC
Country:	US
Signature Issued By:	Common Name (CN): SAML_SSO Organization (O): Cisco Organizational Unit (OU): ESA_TAC Issued On: Sep 20 15:50:27 2019 GMT Expires On: Sep 7 15:50:27 2069 GMT

구성 후 보기

인증서 내보내기

1. ESA Web UI에서 Network(네트워크) > Certificates(인증서) > Export Certificate(인증서 내보내기)로 이동합니다.

2. 내보낼 인증서를 선택하고 패스프레이즈를 생성한 다음 Export를 선택하고 파일을 디렉토리에 저장합니다.

참고: 관리용 SAML SSO는 PKCS#12(PFX) 인증서를 가져올 수 있습니다. 개인 키 암호화가 필요하지 않은 경우 나머지 변환 단계는 선택 사항입니다.

인증서를 변환합니다.

내보낸 인증서는 PKCS#12/PFX 형식이며 PEM(Privacy-Enhanced Mail)로 변환해야 합니다.

이 OpenSSL 명령을 실행하여 PFX 파일을 PEM 형식으로 변환합니다.

<#root>

openssl

```
 pkcs12 -in <certname>.pfx -nokeys -out cert.pem -nodes
```

<#root>

openssl

```
 pkcs12 -in SAML_SSO.pfx -out UNIX_FULL.pem -nodes
```

내용을 편집하고 출력을 두 개의 파일로 분할합니다.

1. 새로 변환된 파일은 약간의 수정이 필요합니다.

2. 텍스트 편집기에서 두 개의 빈 파일을 열고 이름을<name>.crt 및 <name>.key로 지정합니다.

3. 변환된 파일에서 -----BEGIN CERTIFICATE-----~-----END CERTIFICATE----- 섹션을 복사합니다
.

4. 내용을 <name>.crt 파일에 붙여넣고 저장합니다.

5. 변환된 파일에서 -----BEGIN PRIVATE KEY-----~-----END PRIVATE KEY----- 섹션을 복사합니다
.

6. 내용을 <name>.key 파일에 붙여 넣고 저장합니다.

7. 이제 인증서 및 키를 구성의 SAML SP 부분에 로드할 수 있습니다.

방법 2: OpenSSL 명령을 사용하여 자체 서명 인증서 및 키 쌍 생성

명령줄에서 인증서 및 키 쌍을 직접 생성해야 하는 경우 이 방법을 사용합니다.

인증서 및 키 쌍을 만듭니다.

Unix, Linux 또는 macOS 명령줄 인터페이스에서 OpenSSL 명령을 실행합니다. 도메인을 필요한 이름으로 바꿉니다.

<#root>

openssl

```
 req -newkey rsa:2048 -nodes -keyout domain.key -x509 -days 1095 -out domain.crt
```

작성 중에 나열된 필드에 대한 프롬프트가 표시됩니다.

명령이 실행되는 디렉토리에는 다음과 같은 두 개의 파일이 생성됩니다. saml_ssl.crt 및 saml_ssl.key.

```
$ openssl req -newkey rsa:2048 -nodes -keyout saml_sso.key -x509 -days 1095 -out saml_sso.crt
Generating a 2048 bit RSA private key
..........+++
.....................................................................................................
writing new private key to 'saml_sso.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:NC
Locality Name (for example, city) []:Raleigh
Organization Name (for example, company) []:Cisco
Organizational Unit Name (for example, section) []:ESA_TAC
Common Name (for example, fully qualified host name) []:SAML_SSO
Email Address []:user@example.com
```

개인 키 암호화(선택 사항, (컨피그레이션에는 필요하지 않음)

참고: 예제 패스프레이즈를 재사용하지 마십시오. 이 키는 예제 용도로만 사용됩니다.

이 OpenSSL 명령은 암호화되지 않은 개인 키(unencrypted.key)를 가져와 암호화된 키(encrypted.key)를 출력합니다.

<#root>

openssl

```
 rsa -des3 -in unencrypted.key -out encrypted.key
```

<#root>

openssl

```
 rsa -des3 -in saml_sso.key -out saml_secure.key
```

```
$ openssl rsa -des3 -in saml_sso.key -out saml_secure.key
writing RSA key
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

```
$ ls

saml_sso.crt
saml_sso.key
saml_secure.key
```

인증서 및 키가 SAML SSO SP 또는 스팸 SSO SP 설정에 대해 준비되었습니다.

관련 정보

Cisco Email Security Appliance – 엔드 유저 가이드

Cisco Content Security Management Appliance - 최종 사용자 가이드

Cisco Web Security - 최종 사용자 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.