SMA에 인증서를 생성 및 설치하는 방법

목차

소개

이 문서에서는 Cisco SMA(Security Management Appliance)에서 구성 및 사용할 인증서를 생성하고 설치하는 방법에 대해 설명합니다.

사전 요구 사항

로컬로 명령 openssl을 실행하려면 액세스 권한이 있어야 합니다.

ESA(Email Security Appliance)에 대한 관리자 계정 액세스 및 SMA의 CLI에 대한 관리자 액세스 권한이 필요합니다.

다음 항목을 .pem 형식으로 사용할 수 있어야 합니다.

- X.509 인증서
- 인증서와 일치하는 개인 키
- CA(Certificate Authority)에서 제공하는 중간 인증서

SMA에 인증서를 생성 및 설치하는 방법

> **팁**:신뢰할 수 있는 CA에서 서명한 인증서를 사용하는 것이 좋습니다.Cisco에서는 특정 CA를 권장하지 않습니다. 작업할 CA에 따라 여러 형식으로 서명된 인증서, 개인 키 및 중간 인증서(해당하는 경우)를 다시 받을 수 있습니다. 인증서를 설치하기 전에 CA에서 제공하는 파일 형식을 직접 조사하거나 CA와 상의하십시오.

현재 SMA는 로컬 인증서 생성을 지원하지 않습니다. 대신 ESA에서 자체 서명 인증서를 생성할 수 있습니다.이를 해결 방법으로 사용하여 SMA에 대한 인증서를 생성하여 가져오고 구성할 수 있습니다.

ESA에서 인증서 생성 및 내보내기

1. ESA GUI에서 Network(네트워크) > Certificates(인증서) **> Add Certificate(인증서 추가)**에서 자체 서명 인증서**를 생성합니다**. 자체 서명 인증서를 생성할 때 인증서가 제대로 사용될 수 있도록 ESA가 아닌 SMA의 호스트 이름을 "CN(Common Name)"에서 사용하는 것이 중요합니다.
2. 변경 사항을 제출하고 커밋합니다.
3. Network(네트워크) **> Certificates(인증서) > Export Certificates(인증서 내보내기)**에서 생성된 인증서**를 내보냅니다**. (1) 자체 서명 인증서로 내보내기 및 저장/사용 또는 (2) 인증서 서명 요청 다운로드(외부에서 서명된 인증서가 필요한 경우) 두 가지 옵션이 있습니다. 자체 서명 인증서로 저장/사용: 인증서 **내보내기 선택**인증서를 변환할 때 사용할 파일 이름(예: mycert.pfx) 및 암호를 지정합니다.그러면 파일을 로컬로 저장하라는 메시지가 자동으로 표시됩니다."내보낸 인증서 변환"으로 진행합니다.인증서 서명 요청 다운로드 **네트워크 > 인증서**생성한 인증서 이름을 클릭합니다."Signature Issued By(서명 발급자)" 섹션에서 **Download Certificate Signing Request(인증서 서명 요청 다운로드...)를** 클릭합니다..pem 파일을 로컬로 저장하고 CA에 제출합니다.

내보낸 인증서 변환

ESA에서 만들고 내보낸 인증서는 .pfx 형식입니다.SMA는 가져오기에 .pem 형식만 지원하므로 이 인증서를 변환해야 합니다. .pfx 형식에서 .pem 형식으로 인증서를 변환하려면 다음 openssl 명령**예**를 사용하십시오.

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

ESA에서 인증서를 생성하는 동안 사용된 패스프레이즈를 입력하라는 메시지가 표시됩니다. OpenSSL 명령으로 만든 .pem 파일에는 인증서와 키가 모두 .pem 형식으로 포함됩니다. 이제 SMA에서 인증서를 구성할 준비가 되었습니다. 이 문서의 "인증서 설치" 섹션을 진행하십시오.

OpenSSL을 사용하여 인증서 생성

PC/워크스테이션에서 openssl을 실행할 로컬 액세스 권한이 있는 경우 다음 명령을 실행하여 인증서를 생성하고 필요한 .pem 파일 및 개인 키를 별도의 두 파일에 저장할 수 있습니다.

```
openssl req -newkey rsa:2048 -new -nodes -x509 -days 3650 -keyout sma_key.pem -out sma_cert.pem
```

이제 SMA에서 인증서를 구성할 준비가 되었습니다. 이 문서의 "인증서 설치" 섹션을 진행하십시오.

추가 옵션, ESA에서 인증서 내보내기

위에서 설명한 것처럼 인증서를 .pfx에서 .pem으로 변환하는 대신 ESA에서 비밀번호를 마스킹하지 않고 구성 파일을 저장할 수 있습니다.저장된 ESA .xml 구성 파일을 열고 <certificate> 태그를 검색합니다.인증서 및 개인 키는 이미 .pem 형식입니다.아래의 "Install the Certificate(인증서 설치)" 섹션에 설명된 대로 SMA에 가져올 인증서 및 개인 키를 복사합니다.

참고:이 옵션은 AsyncOS 11.1 이상을 실행하는 어플라이언스에 대해서만 유효하며, 여기서

'plain passphrase' 옵션을 사용하여 구성 파일을 저장할 수 있습니다. 최신 버전의 AsyncOS는 패스프레이즈를 마스크 처리하거나 암호를 암호화하는 옵션만 제공합니다. 두 옵션 모두 인증서 가져오기 또는 붙여넣기 옵션에 필요한 개인 키를 암호화합니다.

참고:위에서 #2, "Download Certificate Signing Request(인증서 서명 요청 다운로드)"를 선택하고 CA에서 서명한 인증서를 보유한 경우, 인증서 및 개인 키의 사본을 만들기 위해 컨피그레이션 파일을 저장하기 전에 인증서가 생성된 ESA로 서명된 인증서를 다시 가져와야 합니다.ESA GUI에서 인증서 이름을 클릭하고 "Upload Signed Certificate" 옵션을 사용하여 가져오기를 수행할 수 있습니다.

SMA에 인증서 설치

단일 인증서를 모든 서비스에 사용할 수 있으며, 개별 인증서를 4개의 서비스 각각에 사용할 수 있습니다.

- 인바운드 TLS
- 아웃바운드 TLS
- HTTPS
- LDAPS

SMA에서 CLI를 통해 로그인하고 다음 단계를 완료합니다.

1. certconfig를 **실행합니다**.
2. **설정** 옵션을 선택합니다.
3. 모든 서비스에 대해 동일한 인증서를 사용할지 아니면 각 개별 서비스에 대해 별도의 인증서를 사용할지를 선택해야 합니다. "Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and LDAPS?"라는 메시지가 표시되면 "Y"를 선택하면 인증서와 키를 한 번만 입력하면 모든 서비스에 해당 인증서를 할당합니다."N"을 입력하도록 선택한 경우 다음 메시지가 표시되면 각 서비스에 대해 인증서, 키 및 중간 인증서(해당하는 경우)를 입력해야 합니다.인바운드, 아웃바운드, HTTPS 및 관리
4. 메시지가 표시되면 인증서 또는 키를 붙여넣습니다.
5. '.'로 끝남 현재 항목을 붙여 넣었음을 나타내기 위해 각 항목에 대한 고유한 행에 있습니다. 자세한 내용은 "예제" 섹션을 참조하십시오.
6. 중간 인증서가 있는 경우 확인 메시지가 표시되면 해당 인증서를 입력해야 합니다.
7. 완료되면 **Enter**를 눌러 SMA의 기본 CLI 프롬프트로 돌아갑니다.
8. commit를 실행하여 컨피그레이션을 저장합니다.

참고: Ctrl+C를 사용하여 certconfig 명령을 종료하지 마십시오. 그러면 변경 사항이 즉시 취소됩니다.

예

```
mysma.local> certconfig

Currently using the demo certificate/key for receiving, delivery, HTTPS management access, and
LDAPS.
```

```
Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
[]> setup

Do you want to use one certificate/key for receiving, delivery, HTTPS management access, and
LDAPS? [Y]> y

paste cert in PEM format (end with '.'):
-----BEGIN CERTIFICATE-----
MIIDXTCCAkWgAwIBAwIJAIXvIlkArow9MA0GCSqGSIb3DQEBBQUAMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzAeFw0xNzExMTAxNjA3MTRaFw0yNzExMDgxNjA3MTRaMG4xCzAJBgNV
BAYTAlVTMRowGAYDVQQDDBF3dS5jYWxvLmNpc2NvLmNvbTEMMAoGA1UEBwwDUlRQ
MQ4wDAYDVQQKDAVDaXNjbzEXMBUGA1UECAwOTm9ydGggQ2Fyb2xpbmExDDAKBgNV
BAsMA1RBQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKPz0perw3QA
ZH8xctOrvvjsnOPkItmSc+DUqtVKM6OOOkNHA2WY9XJ3+vESwkIdwexibj6VUQ85
K7NE6zOgRfpYdQsxmpIWhzYf9qCBOXuKsRw/9jonKk98DfHFM02J3BSmmgZ0MPp7
6EwA/sZAN+aqYB7IE1fgnqpEXek8xFlfcVnS2YTc7NXz78lNK0jvXOtCVBrWFu0z
lEmZVpAj0AKkz1nujvzfOqEzed+tjauZr7nDIaiTrzhLKte4pJUm3T61q/PhegvN
Iy/WHN1xojP+FzjRAUlmtmjMzHyM2///dmq8JivUlaLXX9vUfdK3VViIOIz4zngG
Rz85QXO7ivcCAwEAATANBgkqhkiG9w0BAQUFAAOCAQEAM10zCcOOtqV1LDBmoDqd
4G2IhVbBESsbvZ/QmB6kpikT4pe5clQucskHq4D/xg1EZyfuXu+4auMie4B9Dym8
8pjbMDDi9hJPZ7j85nWMd6SfWhQUOPankdazpCycN6gNVzRBgPdR8tLOvt90vtV4
KCPmDYbwi6kfOl8tvjWHMh/wYicfvFRy0vPMpemtbCVGyC3cpquv8nFDutB6exym
skotn5wixCqErKlnHdUa3Z+zhutIAm/Q0sVWQQlbZZ+MIxBegyJ0ucTmBqqQHhhJ
pSO7PbevxwanYVXvNR8o2feAWs5LYkrwqdGRxLJmHjFnMV3PbkwRPgFWQ6AD1g12
34==
-----END CERTIFICATE-----
.
paste key in PEM format (end with '.'):
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCj89KXq8N0AGR/
MXLTq7747Jzj5CLZknPg1KrVSjOjjjpDRwNlmPVyd/rxEsJCHcHsYm4+lVEPOSuz
ROszoEX6WHULMZqSFoc2H/aggTl7irEcP/Y6JypPfA3xxTNNidwUppoGdDD6e+hM
AP7GQDfmqmAeyBNX4J6qRF3pPMRZX3FZ0tmE3OzV8+/JTStI71zrQlQa1hbtM5RJ
mVaQI9ACpM9Z7o783zqhM3nfrY2rma+5wyGok684SyrXuKSVJt0+tavz4XoLzSMv
1hzdcaIz/hc40QFJZrZozMx8jNv//3ZqvCYr1JWi11/b1H3St1VYiDiM+M54Bkc/
OUFzu4r3AgMBAAECggEAB9EFjsaZHGwyXmAIpe/PvIVnW3QSd0YEsUjiViXh/V+4
BmIZ1tuqhAkVVS38RfOuPatZrzEmOrASlcro3b6751oVRnHYeTOKwblXZEKU739m
vz6Lai1Y1o5HCepJbl5uuCtTN5CNjzueERWRD/ma0Kv5xi3qwitK1TpKMeb8Q3h2
YABmpk0TyJQ5ixLw3ch9ru1nqiO5zQ91GvIuDckudUu/bBnao+jV7D362lIPyLG8
03GqNviNZ6c3wjD0yQWg619g+ZmjM8DTtDR16zmzBvQ4TgZi22sUWrSSILRa69jW
q8XszQVRydl+gt666iUeN/ozmEMt5J8pu3i9vf3G2QKBgQDHyfv55rjZbWyf0eAT
Ch5T1YsjjMgMOtC9ivi5mMQCunWyRiyZ6qqSBME9Tper/YdAA07PoNtTpVPYyuVX
DDmyuWGHE04baf5QEmSgvQjXOSUPN5TI9hc5/mtvD8QjDO6rebUWxV3NJoR7YNrz
OmfARMXxaF+/mEj+6blSjZuGaQKBgQDSFKvYownPL6qTFhIH7B3kOLwZHk6cJUau
Zoaj7vTw7LrVJv1B0iLPmttEXeJgxzlFYR8tzfn0kTxGQlnhQxXkQ1kdDeqaiLvm
0TtmHMDupjDNKCNH8yBPqB+BIA4cB+/vo23W1HMHpGgqYWRRX/qremL72XFZSRnM
B8nRwK4aXwKBgB+hkwtVxB5ofLIxAFEDYRnUzVqrh2CoTzQzNH3t+dqUut2mzpjv
1mGX7yBNuSW51hgEbg3hYdg0bLn+JaFKhjgNsas5Gzyr41+6CcSJKUUp/vwRyLSo
gbTk2w2SaXNDMOZlNo6MYPWCC6edBg1MSfDe8pft9nrXGXeCeZzgXqdBAoGAQ6Iq
DQ24O76h0Ma7OVe36+CkFgYe0sBheAZD9IUa0HG2WKc7w7QORv4Y93KuTe/1rTNu
YUW94hHb8Natrwr1Ak74YpU3YVcB/3Z/BAnfxzUz4ui4KxLH5T1AH0cdo8KeaW0Z
EJ/HBL/WVUaTkGsw/YHiWiiQCGmzZ29edyvsIUsCgYEAvJtx0ZBAJ443WeHajZWm
J2SLKy0KHeDxZOZ4CwF5sRGsmMofILbK0OuHjMirQ5U9HFLpcINt11VWwhOiZZ5l
k6o79mYhfrTMa4LlHOTyScvuxELqow82vdj6gqX0HVj4fUyrrZ28MiYOMcPw6Y12
34VjKaAsxgZIgN3LvoP7aXo=
-----END PRIVATE KEY-----
.
Do you want to add an intermediate certificate? [N]> n
```

```
Currently using one certificate/key for receiving, delivery, HTTPS management access, and LDAPS.


Choose the operation you want to perform:
- SETUP - Configure security certificates and keys.
- PRINT - Display configured certificates/keys.
- CLEAR - Clear configured certificates/keys.
[]>

mysma.local> commit

Please enter some comments describing your changes:
[]> Certificate installation

Changes committed: Fri Nov 10 11:46:07 2017 EST
```

SMA에서 가져온 및 구성된 인증서 확인

1. HTTPS(https://<SMA IP 또는 호스트 이름>)를 사용하여 GUI를 통해 SMA에 연결하고 로그인 자격 증명을 입력합니다.
2. 브라우저의 주소 표시줄에 있는 URL 옆에 있는 잠금 아이콘 또는 정보 아이콘을 클릭하여 인증서의 유효성, 만료 등을 확인합니다. 사용 중인 브라우저에 따라 작업 및 결과가 달라질 수 있습니다.
3. 인증서 체인을 확인하려면 Certification Path(인증 경로)를 클릭합니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems