Secure Web Appliance에서 암호 해독 인증서 구성

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[HTTPS 암호 해독](#)

[SWA에서 암호 해독 인증서 구성](#)

- [루트 인증서 및 키 업로드](#)
- [HTTPS 프록시에 대한 인증서 및 키 생성](#)

[인증서 가져오기](#)

- [업스트림 프록시 인증서를 SWA로 가져오기](#)
- [SWA 인증서를 다른 SWA로 가져오기](#)
- [Windows 클라이언트에서 SWA 인증서 가져오기](#)
- [Mac 클라이언트에서 SWA 인증서 가져오기](#)
- [Ubuntu/Debian에서 SWA 인증서 가져오기](#)
- [CentOS 6에서 SWA 인증서 가져오기](#)
- [CentOS에서 SWA 인증서 가져오기 5](#)
- [Mozilla Firefox에서 SWA 인증서 가져오기](#)
- [Google Chrome에서 SWA 인증서 가져오기](#)
- [Microsoft Edge/Internet Explorer에서 SWA 인증서 가져오기](#)
- [Safari에서 SWA 인증서 가져오기](#)
- [그룹 정책에서 클라이언트로 SWA 인증서 가져오기](#)

[관련 콘텐츠](#)

소개

이 문서에서는 SWA(Secure Web Appliance) 및 프록시 클라이언트에서 HTTPS 암호화 인증서를 구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA에 대한 관리 액세스
- SWA의 그래픽 사용자 인터페이스(GUI) 액세스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

HTTPS 암호 해독

SWA HTTPS(Hypertext Transfer Protocol Secure) 암호 해독은 어플라이언스에 업로드하는 루트 인증서 및 개인 키 파일을 사용하여 트래픽을 암호화합니다. 어플라이언스에 업로드하는 루트 인증서 및 개인 키 파일은 PEM 형식이어야 합니다.



참고: DER 형식은 지원되지 않습니다.

루트 인증 기관이 서명한 중간 인증서를 업로드할 수도 있습니다. SWA가 서버 인증서를 나타내는 인증서를 생성하면, SWA는 업로드된 인증서와 모방된 인증서를 클라이언트 애플리케이션으로 전송합니다. 이렇게 하면 클라이언트 애플리케이션이 신뢰하는 루트 CA(Certificate Authority)에서 중간 인증서를 서명한 경우 애플리케이션은 모방된 서버 인증서를 신뢰합니다.

SWA에서 암호 해독 인증서 구성

SWA는 HTTPS 암호 해독에 기존 인증서 및 개인 키를 사용할 수 있습니다. 그러나 일부 x.509 인증서가 작동하지 않으므로 사용해야 하는 인증서 유형에 혼란이 있을 수 있습니다.

인증서에는 서버 인증서와 루트 인증서의 두 가지 주요 유형이 있습니다. 모든 x.509 인증서에는 인증서의 유형을 식별하는 기본 제약 조건 필드가 포함되어 있습니다.

- Subject Type=End Entity - 서버 인증서
- Subject Type=CA - 루트 인증서

루트 인증서 및 키 업로드

1단계. GUI에서 Security Services(보안 서비스)로 이동하고 HTTPS Proxy(HTTPS 프록시)를 선택합니다.
2단계. 설정 편집을 클릭합니다.
3단계. Use Uploaded Certificate and Key(업로드된 인증서 및 키 사용)를 클릭합니다.
4단계. Browse the Certificate(인증서 찾아보기) 필드를 클릭하여 로컬 시스템에 저장된 인증서 파일을 탐색합니다.



참고: 업로드하는 파일에 여러 인증서 또는 키가 포함되어 있으면 웹 프록시가 파일의 첫 번째 인증서 또는 키를 사용합니다.

5단계. Key 필드에서 Browse를 클릭하여 개인 키 파일을 찾습니다.



참고: 키 길이는 512, 1024 또는 2048비트여야 합니다.

6단계. 키가 암호화된 경우 Key is Encrypted를 선택합니다.
7단계. Upload Files(파일 업로드)를 클릭하여 인증서 및 키 파일을 Secure Web Appliance에 전송합니다. 업로드된 인증서 정보가 Edit HTTPS Proxy Settings(HTTPS 프록시 설정 수정) 페이지에 표시됩니다.
8단계(선택 사항) Download Certificate(인증서 다운로드)를 클릭하여 네트워크의 클라이언트 애플리케이션으로 전송합니다.

9단계. 변경 사항을 제출하고 커밋합니다.

HTTPS 프록시에 대한 인증서 및 키 생성

1단계. GUI에서 Security Services(보안 서비스)로 이동하고 HTTPS Proxy(HTTPS 프록시)를 선택합니다.
2단계. 설정 편집을 클릭합니다.

3단계. Use Generated Certificate and Key를 선택합니다.
4단계. Generate New Certificate and Key(새 인증서 및 키 생성)를 클릭합니다.
5단계. Generate Certificate and Key(인증서 및 키 생성) 대화 상자에서 정보를 입력하여 루트 인증서에 표시합니다. Common Name(공통 이름) 필드에 슬래시(/)를 제외한 모든 ASCII 문자를 입력할 수 있습니다.
6단계. Generate(생성)를 클릭합니다.
7단계. 생성된 인증서 정보가 Edit HTTPS Proxy Settings(HTTPS 프록시 설정 수정) 페이지에 표시됩니다.
8단계. (선택 사항) Download Certificate(인증서 다운로드)를 클릭하여 네트워크의 클라이언트 애플리케이션에 전송할 수 있습니다.
9단계(선택 사항) CSR(Certificate Signing Request)을 CA에 제출할 수 있도록 Download Certificate Signing Request(인증서 서명 요청 다운로드) 링크를 클릭합니다.
10단계(선택 사항) 서명된 인증서를 CA에서 수신한 후 Secure Web Appliance에 업로드합니다. 어플라이언스에서 인증서를 생성한 후 언제라도 이 작업을 수행할 수 있습니다.
11단계. 변경 사항을 제출하고 커밋합니다.

인증서 가져오기

업스트림 프록시 인증서를 SWA로 가져오기

SWA가 업스트림 프록시를 사용하도록 구성되고 업스트림 프록시가 HTTPS 암호 해독용으로 구성된 경우 업스트림 프록시 암호화 인증서를 SWA로 가져와야 합니다. 신뢰할 수 있는 인증서 목록을 관리하고 인증서를 추가한 다음 기능적으로 인증서를 제거할 수 있습니다.

1단계. GUI에서 Network(네트워크)를 선택하고 Certificate Management(인증서 관리)를 선택합니다.
2단계. Certificate Management(인증서 관리) 페이지에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭합니다.
3단계. Cisco에서 인정하는 목록 대신 서명 권한이 있는 신뢰할 수 있는 사용자 지정 루트 인증서를 추가하려면 Import(가져오기)를 클릭한 다음 인증서 파일을 제출합니다.

4단계. 변경 사항을 제출하고 커밋합니다.

SWA 인증서를 다른 SWA로 가져오기

HTTPS 프록시에 대한 하나의 SWA에 HTTPS 인증서 및 키를 업로드하고 원본 파일에 액세스할 수 있는 경우 구성 파일에서 다른 SWA로 가져올 수 있습니다.

1단계. 두 SWA의 GUI에서 System Administration(시스템 관리)을 선택하고 Configuration File(컨

피그레이션 파일)을 클릭합니다.

2단계. 보거나 저장하려면 로컬 컴퓨터에서 Download file을 클릭합니다.

3단계. Encrypt passwords in the Configuration Files(컨피그레이션 파일에서 비밀번호 암호화)를 선택합니다.

4단계. (선택 사항) Use a user-defined file name(사용자 정의 파일 이름 사용)을 선택하고 원하는 이름을 Configuration File(컨피그레이션 파일)에 추가합니다.

5단계. Current Configuration(현재 컨피그레이션) 아래에서 Submit(제출)을 클릭하여 configuration.xml 파일을 다운로드합니다.

6단계. 다운로드한 파일을 텍스트 편집기 또는 XML 편집기로 엽니다.

7단계. 이러한 태그를 인증서와 함께 SWA에서 복사하고 태그 내의 모든 데이터를 복사한 다음 다른 SWA의 컨피그레이션 파일에서 교체합니다.

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

8단계. 대상 SWA의 .xml 파일에 변경 사항을 저장합니다.

9단계. 편집된 .xml 구성 파일을 대상 SWA로 다시 가져오려면 GUI에서 System Administration(시스템 관리)을 선택하고 Configuration File(구성 파일)을 클릭합니다.

10단계. [구성 로드] 섹션에서 [로컬 컴퓨터에서 구성 파일 로드]를 클릭합니다.

11단계. Choose file(파일 선택)을 클릭하고 편집한 .xml 구성 파일을 선택합니다.

12단계. Load(로드)를 클릭하여 인증서 및 키와 함께 새 컨피그레이션 파일을 가져옵니다.

13단계. 시스템 프롬프트가 표시되면 변경 사항을 커밋합니다.

Windows 클라이언트에서 SWA 인증서 가져오기

Microsoft Windows 운영 체제가 설치된 클라이언트 컴퓨터에서 SWA HTTPS 프록시 인증서를 신뢰할 수 있는 인증서로 가져오려면 다음 단계를 검토하십시오.

1단계. 작업 표시줄에서 시작을 클릭하고 컴퓨터 인증서 관리를 입력합니다.
2단계. Certificates-Local Computer(인증서-로컬 컴퓨터) 페이지에서 Trusted Root Certification(신뢰할 수 있는 루트 인증)을 확장하고 Certificates(인증서) 폴더를 마우스 오른쪽 단추로 클릭합니다.
3단계. All Tasks(모든 작업)를 클릭하고 Import(가져오기)를 선택합니다.
4단계. Certificate Import Wizard(인증서 가져오기 마법사) 페이지에서 Next(다음)를 클릭합니다.
5단계. SWA 인증서 파일을 가져오려면 Browse(찾아보기)를 클릭하고 SWA에서 다운로드한 인증서를 선택합니다.



팁: SWA 인증서를 다운로드하려면 Upload a Root Certificate and Key(루트 인증서와 키 업로드) 또는 Generating a Certificate and Key for the HTTPS Proxy(HTTPS 프록시에 대한 인증서 및 키 생성) 섹션의 8단계를 참조하십시오.

6단계. 다음 확인란에 모든 인증서 넣기를 클릭합니다.
7단계. Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)를 선택하고 Next(다음)를 클릭합니다.
8단계. Finish(마침)를 클릭합니다.

또는 이 명령을 실행하여 신뢰할 수 있는 루트 인증 기관에 인증서를 가져올 수도 있습니다.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



참고: <SWA Certificate/CertificateName.crt에 대한 경로>를 현재 다운로드한 인증서 경로 및 파일 이름으로 바꿔야 합니다.

Mac 클라이언트에서 SWA 인증서 가져오기

1단계. SWA에서 Mac OS 클라이언트로 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 파일 확장명을 .crt로 바꿉니다.
3단계. 이 명령을 실행하여 인증서를 신뢰할 수 있는 인증서로 가져옵니다.

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```



참고: 현재 다운로드한 인증서 경로 및 파일 이름으로 교체해야 합니다.

Ubuntu/Debian에서 SWA 인증서 가져오기

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 텍스트 편집기에서 인증서 파일을 열고 모든 내용을 복사합니다.
3단계. .crt를 확장자로 /usr/local/share/ca-certificates/에 새 파일을 생성합니다.
4단계. 원하는 텍스트 편집기로 파일을 편집하고 복사한 텍스트를 새 파일에 붙여 넣은 다음 저장합니다.
5단계. 이 명령을 실행하여 운영 체제의 인증서를 새로 고칩니다.

```
sudo update-ca-certificates
```



팁: 인증서가 클라이언트에 로컬로 저장된 경우 인증서를 /usr/local/share/ca-certificates/로 복사하고 sudo update-ca-certificates를 실행할 수 있습니다.



참고: 일부 버전에서는 다음 명령을 사용하여 ca-certificates 패키지를 설치해야 합니다. sudo apt-get install -y ca-certificates를 선택합니다.

CentOS 6에서 SWA 인증서 가져오기

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 텍스트 편집기에서 인증서 파일을 열고 파일 내의 모든 내용을 복사합니다.
3단계. .crt 확장자를 사용하여 /etc/pki/ca-trust/source/anchors/에서 새 파일을 생성합니다.
4단계. 원하는 텍스트 편집기로 파일을 편집하고 이전에 복사한 텍스트를 새 파일로 복사한 다음 저장합니다.
5단계. ca-certificates 패키지를 설치합니다.

```
yum install ca-certificates
```

6단계. 이 명령을 실행하여 운영 체제의 인증서를 새로 고칩니다.

```
update-ca-trust extract
```



팁: 인증서가 클라이언트에 로컬로 저장된 경우, ca-certificates를 설치한 후 /etc/pki/ca-trust/source/anchors/and run update-ca-trust extract를 실행하여 인증서를 복사할 수 있습니다.

CentOS에서 SWA 인증서 가져오기 5

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 텍스트 편집기에서 인증서 파일을 열고 파일 내의 모든 내용을 복사합니다.
3단계. 현재 폴더에 확장명이 .crt인 새 파일(예: SWA.crt)을 만듭니다.
4단계. 원하는 텍스트 편집기로 /etc/pki/tls/certs/ca-bundle.crt을 편집하고, 복사한 텍스트를 파일 끝에 붙여 넣은 다음 저장합니다.



팁: 클라이언트에 인증서가 로컬로 저장되어 있는 경우(이 예에서는 파일 이름이 SWA.crt임) 다음 명령을 사용하여 인증서를 추가할 수 있습니다. cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

Mozilla Firefox에서 SWA 인증서 가져오기

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 파일 확장명을 .crt로 바꿉니다.
3단계. Firefox를 열고 메뉴(오른쪽 상단 모서리의 막대 3개)를 클릭합니다.
4단계. Settings(설정)를 선택합니다(일부 버전에서는 Options(옵션)).
5단계. 왼쪽 메뉴에서 Privacy & Security(개인 정보 및 보안)를 클릭하고 Certificates(인증서)로 스크롤합니다.
6단계. View Certificates(인증서 보기)를 클릭합니다.
7단계. Authorities(권한) 탭을 클릭한 다음 Import(가져오기)를 클릭합니다.
8단계. 인증서 파일을 선택하고 Open(열기)을 클릭합니다.
9단계. OK(확인)를 클릭합니다.

Google Chrome에서 SWA 인증서 가져오기

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 파일 확장명을 .crt로 바꿉니다.
3단계. Google Chrome을 열고 Google Chrome 사용자 지정 및 제어(오른쪽 상단 모서리에 3 개의 점)를 클릭합니다.
4단계. Settings(설정)를 선택합니다.
5단계. 왼쪽 메뉴에서 Privacy and Security를 클릭합니다.
6단계. Security를 선택합니다.
7단계. Manage certificates(인증서 관리)로 스크롤하여 오른쪽의 버튼을 클릭합니다.
8단계. Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 탭을 선택하고 Import(가져오기)를 클릭합니다.
9단계. 인증서 파일을 선택하고 Open(열기)을 클릭합니다.
10단계. OK(확인)를 클릭합니다.



참고: 운영 체제에 SWA 인증서를 설치 하는 경우, Google Chrome는 해당 인증서를 신뢰하므로 브라우저로 인증서를 별도로 가져올 필요가 없습니다.

Microsoft Edge/Internet Explorer에서 SWA 인증서 가져오기

Microsoft Edge 및 Internet Explorer(IE)에서는 운영 체제 인증서를 사용합니다. 운영 체제에 SWA 인증서를 설치 하는 경우 인증서를 브라우저로 별도로 가져올 필요가 없습니다.

Safari에서 SWA 인증서 가져오기

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 파일 확장명을 .crt로 바꿉니다.
3단계. 실행 패드에서 Keychain Access를 선택합니다.
4단계. 파일 메뉴에서 키 체인 추가를 클릭합니다.
5단계. SWA 인증서 파일을 선택하고 Add를 클릭합니다.
6단계. Security를 선택합니다.
7단계. Manage certificates(인증서 관리)로 스크롤하여 오른쪽의 버튼을 클릭합니다.
8단계. Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관) 탭을 선택하고 Import(가져오기)를 클릭합니다.
9단계. 인증서 파일을 선택하고 Open(열기)을 클릭합니다.
10단계. OK(확인)를 클릭합니다.

그룹 정책에서 클라이언트로 SWA 인증서 가져오기

Active Directory의 그룹 정책을 사용하여 클라이언트 컴퓨터에 인증서를 배포하려면 다음 단계를

수행합니다.

1단계. SWA에서 HTTPS 프록시 인증서를 다운로드합니다.
2단계. 파일 확장명을 .crt로 바꿉니다.
3단계. 인증서 파일을 도메인 컨트롤러에 복사합니다.
4단계. 도메인 컨트롤러에서 Start(시작)를 클릭하고 Group Policy Management(그룹 정책 관리) 스냅인을 엽니다.
5단계. 원하는 GPO(그룹 정책 개체)를 찾거나 클라이언트로 가져올 SWA 인증서를 포함하는 새 GPO를 만듭니다.
6단계. GPO를 마우스 오른쪽 단추로 클릭하고 Edit를 클릭합니다.
7단계. 왼쪽 메뉴에서 Computer Configuration(컴퓨터 구성) > Policies(정책) > Windows Settings(Windows 설정) > Security Settings(보안 설정) > Public Key Policies(공용 키 정책)로 이동합니다.
8단계. 신뢰할 수 있는 루트 인증 기관을 마우스 오른쪽 단추로 클릭하고 가져오기를 클릭합니다.
9단계. Welcome to the Certificate Import Wizard(인증서 가져오기 마법사 시작) 페이지에서 Next(다음)를 클릭합니다.
10단계. 가져올 SWA 인증서 파일을 선택하고 Next(다음)를 클릭합니다.
11단계. Place all certificates in the following store(다음 저장소에 모든 인증서 저장)를 클릭한 다음 Next(다음)를 클릭합니다.
12단계. 제공된 정보가 정확한지 확인하고 Finish(마침)를 클릭합니다.

참고: 일부 상황에서는 클라이언트를 다시 시작하거나 gpupdate /force를 실행하여 Active Directory 클라이언트 시스템에 변경 사항을 적용해야 합니다.

관련 콘텐츠

- AsyncOS 14.5 for Cisco Secure Web Appliance - GD 사용 설명서(일반 배포)
- 그룹 정책을 사용하여 클라이언트 컴퓨터에 인증서 배포 | Microsoft Learn
- 기술 지원 및 문서 − Cisco Systems

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.