ESA에서 CSR(Certificate Signing Request) 생성

목차

[소개](#)
[ESA에서 CSR 생성](#)
[GUI의 구성 단계](#)
[관련 정보](#)

소개

이 문서에서는 ESA(Email Security Appliance)에서 CSR(Certificate Signing Request)을 생성하는 방법에 대해 설명합니다.

ESA에서 CSR 생성

AsyncOS 7.1.1부터 ESA는 자체 사용을 위해 자체 서명 인증서를 생성하고 CSR을 생성하여 인증 기관에 제출하고 공용 인증서를 얻을 수 있습니다.인증 기관은 개인 키로 서명된 신뢰할 수 있는 공용 인증서를 반환합니다.GUI의 **Network > Certificates** 페이지 또는 CLI의 **certconfig** 명령을 사용하여 자체 서명 인증서를 생성하고 CSR을 생성하며 신뢰할 수 있는 공용 인증서를 설치합니다.

인증서를 처음 취득 또는 생성하는 경우 인터넷에서 "인증 기관 서비스 SSL 서버 인증서"를 검색하고 조직의 요구에 가장 적합한 서비스를 선택합니다.인증서를 얻으려면 서비스 지침을 따릅니다.

GUI의 구성 단계

1. 자체 서명 인증서를 생성하려면 GUI의 Network(네트워크) > Certificates(인증서) 페이지(또는 CLI의 **certconfig** 명령)에서 Add Certificate(인증서 추가)를 클릭합니다. Add Certificate 페이지에서 Create **Self-Signed Certificate**를 선택합니다.
2. 자체 서명 인증서에 대해 다음 정보를 입력합니다. Common Name(일반 이름) - 정규화된 도메인 이름입니다.조직 - 조직의 정확한 법적 이름입니다.조직 단위 - 조직의 섹션.구/군/시(구/군/시) - 조직이 합법적으로 위치한 시.시/도 - 조직이 법적으로 위치한 주/군 또는 지역.Country(국가) - 조직이 법적으로 위치한 국가의 두 글자 International Organization for Standardization (ISO) 약어입니다.만료 전 기간 - 인증서가 만료되기 전 일 수입니다.Private Key Size(개인 키 크기) - CSR에 대해 생성할 개인 키의 크기입니다.2048비트 및 1024비트만 지원됩니다.
3. 인증서 및 서명 정보를 보려면 **Next**를 클릭합니다.
4. 인증서의 이름을 입력합니다.AsyncOS는 기본적으로 공용 이름을 할당합니다.
5. 자체 서명 인증서에 대한 CSR을 인증 기관에 제출하려면 PEM(Privacy Enhanced Mail) 형식으로 CSR을 로컬 또는 네트워크 시스템에 저장하려면 **Download Certificate Signing Request(인증서 서명 요청 다운로드**)를 클릭합니다.

6. 인증서를 저장하고 변경 사항을 커밋하려면 Submit(제출)을 클릭합니다.변경 사항을 커밋하지 않은 상태로 두면 개인 키가 손실되고 서명된 인증서를 설치할 수 없습니다.

인증 기관이 개인 키로 서명된 신뢰할 수 있는 공개 인증서를 반환하면 Certificates(인증서) 페이지에서 인증서 이름을 클릭하고 인증서를 업로드하기 위해 로컬 시스템 또는 네트워크에 있는 파일의 경로를 입력합니다.받는 신뢰할 수 있는 공용 인증서가 PEM 형식인지 또는 어플라이언스에 업로드되기 전에 PEM으로 변환할 수 있는 형식인지 확인합니다.이를 완료하는 툴은 OpenSSL에 포함되어 있으며, 무료 소프트웨어는 http://www.openssl.org에서 제공됩니다.

인증 기관에서 인증서를 업로드하면 기존 인증서를 덮어씁니다.자체 서명 인증서와 관련된 중간 인증서를 업로드할 수도 있습니다.퍼블릭 또는 프라이빗 리스너, IP 인터페이스의 HTTPS 서비스, LDAP(Lightweight Directory Access Protocol) 인터페이스 또는 대상 도메인에 대한 모든 발신 TLS(Transport Layer Security) 연결과 함께 인증서를 사용할 수 있습니다.

관련 정보

- ESA에서 TLS를 위한 포괄적인 설정 가이드
- 기술 지원 및 문서 – Cisco Systems