vManage용 웹 인증서 이해

목차

소개

이 문서에서는 Cisco SD-WAN 솔루션에서 웹 인증서와 컨트롤러 인증서의 차이점을 설명합니다. 또한 이 문서에서는 웹 인증서에 대해 자세히 설명하고 이러한 두 인증서 유형 간의 사용을 명확히 설명합니다.

사전 요구 사항

요구 사항

PKI(Public Key Infrastructure)에 대한 기본 지식

사용되는 구성 요소

- Cisco vManage NMS(network management system) 버전 20.4.1
- Google Chrome 버전 94.0

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

Cisco SD-WAN에서 사용되는 인증서

Cisco SD-WAN 솔루션에는 컨트롤러 인증서 및 웹 인증서 두 가지 유형의 인증서가 사용됩니다.

웹 인증서

vManage에 대한 웹 액세스에 사용됩니다. Cisco는 기본적으로 자체 서명 인증서를 설치합니다. 자체 서명 인증서는 자체 작성자가 서명한 SSL(Secure Sockets Layer) 인증서입니다.

그러나 Cisco는 자체 웹 서버 인증서를 권장합니다. 이는 특히 네트워크 기업이 웹 액세스 제한이 있는 방화벽을 가질 수 있는 경우에 유용합니다.
Cisco는 CA(Certificate Authority)에서 발급한 공용 웹 인증서를 제공하지 않습니다.

> vManage 웹 인증서를 생성하는 방법에 대한 자세한 내용은 Generate Web Server Certificate and How To Generate Self-Signed Web Certificate For vManage 설명서를 참조하십시오.

컨트롤러 인증서

컨트롤러 간 제어 연결(예: vManage, vBonds, vSmarts)을 구축하는 데 사용됩니다.

이러한 인증서는 전체 SDWAN 패브릭 컨트롤 플레인에 매우 중요하며 항상 유효하게 유지해야 합니다.

> 자세한 컨트롤러 인증서 정보는 설명서: Cisco Systems를 통한 자동 인증서 서명

vManage용 웹 인증서 이해

HTTPS(Hypertext Transfer Protocol Secure)는 사용자의 컴퓨터와 웹 사이트 간의 데이터 무결성과 기밀성을 보호하는 인터넷 통신 프로토콜입니다. 이 경우 vManage GUI입니다. 사용자는 vManage에 액세스할 때 보안 및 사설 연결을 기대합니다.

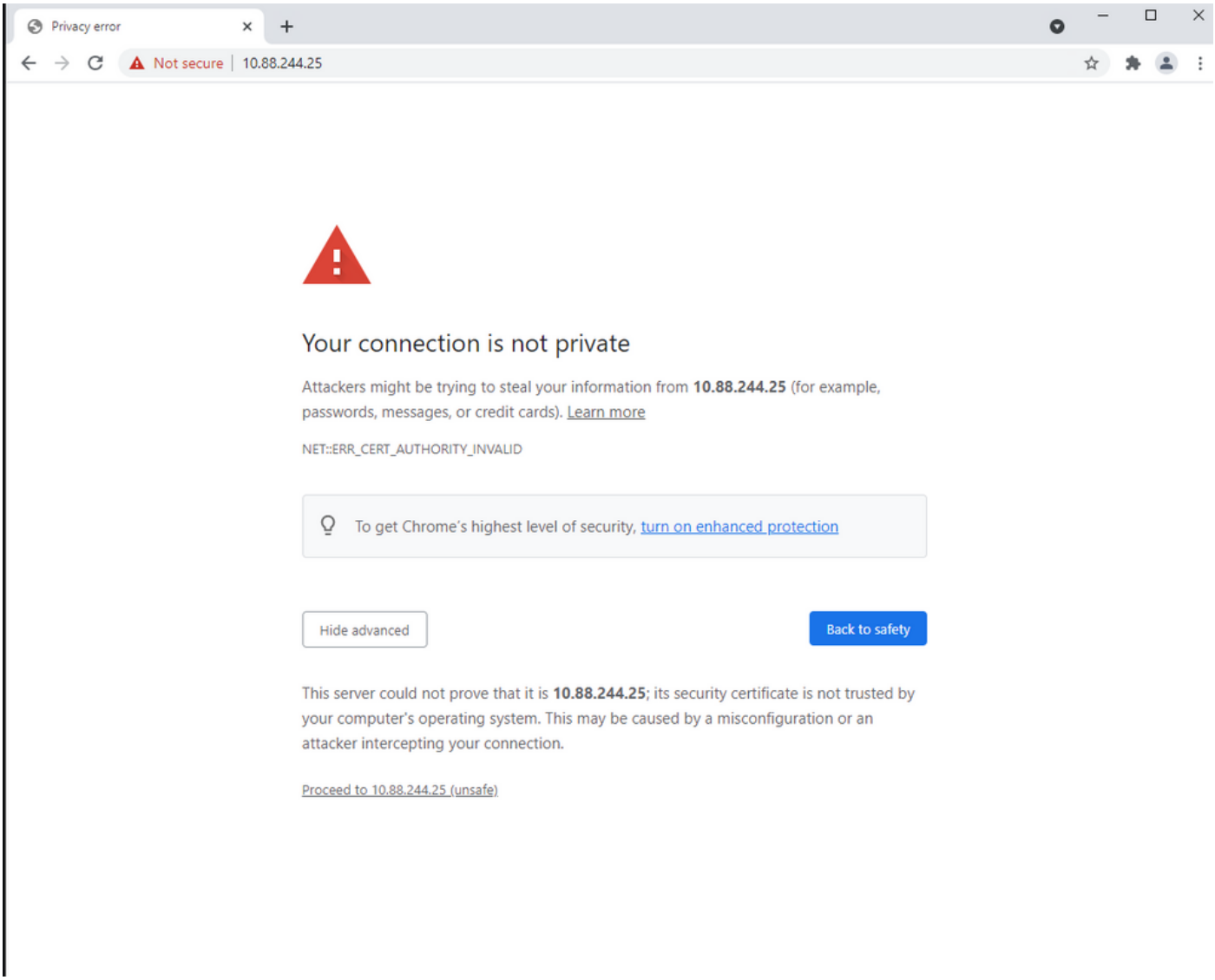
보안 및 개인 연결을 수행하려면 보안 인증서를 받아야 합니다. 인증서는 CA(Certificate Authority)에서 발급하며, 이는 vManage 도메인이 실제로 조직에 속하는지 확인하는 단계를 수행합니다.

사용자가 vManage에 액세스하면 사용자 PC는 HTTPS 연결을 수행하고 vManage 서버와 인증을 위해 설치된 SSL 인증서를 사용하여 컴퓨터 간에 보안 터널이 설정됩니다. SSL 인증서의 인증은 디바이스에 설치된 유효한 루트 CA의 데이터베이스에 대해 사용자 컴퓨터에서 수행됩니다. 일반적으로 이 컴퓨터에는 Google, GoDaddy, Enterprise CA(이 경우) 및 더 많은 공용 엔티티와 같은 여러 CA가 이미 설치되어 있습니다. 따라서 CSR(Certificate Signing Request)이 Goddady(예)에 의해 서명된 경우 신뢰할 수 있습니다.

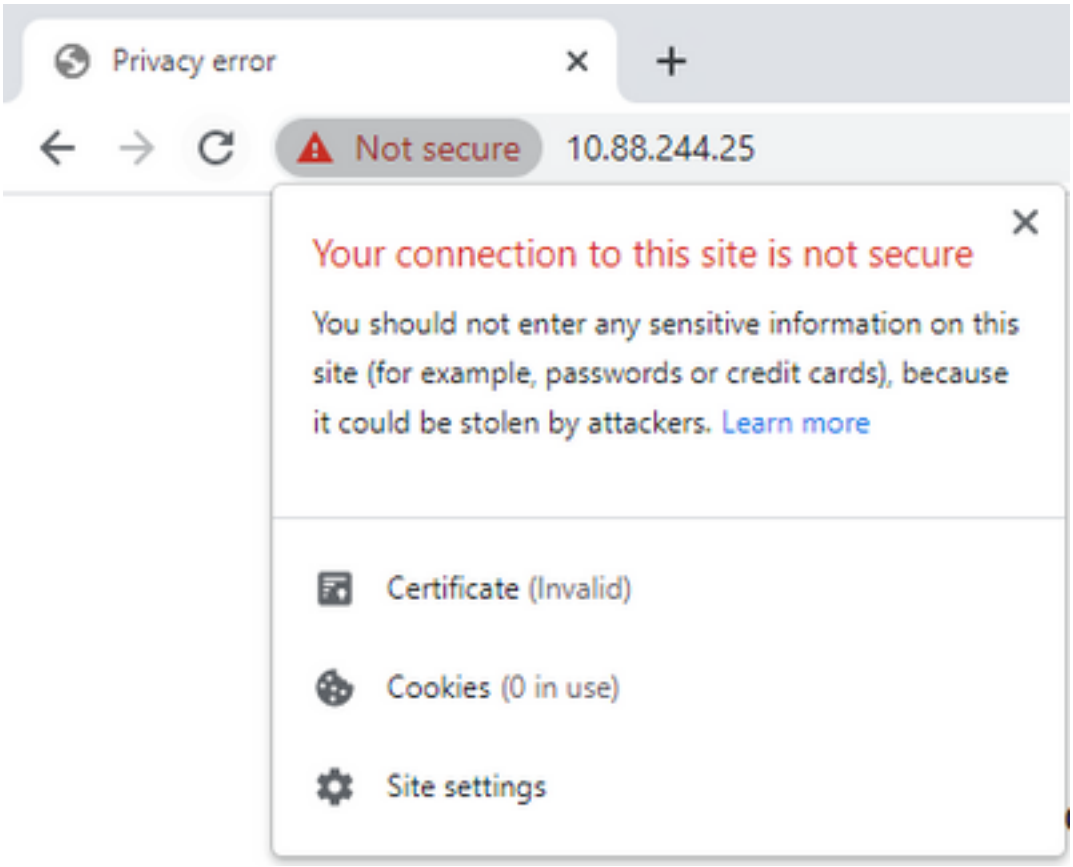
vManage의 "Connection is Not Private" 메시지

vManage 자체 서명 인증서는 CA에서 서명하지 않습니다. 이는 동일한 vManage에 의해 서명되었으며 퍼블릭 또는 프라이빗 CA에 의해 서명되지 않았으므로 PC 클라이언트에 대해 신뢰되지 않습니다. 따라서 vManage URL에 대한 비보안/프라이버시 오류 연결이 브라우저에 표시됩니다.

이미지에 표시된 대로 Google Chrome 브라우저에서 기본 자체 서명 인증서를 사용하는 vManage 오류의 예.



참고: 사이트 정보 보기 옵션을 클릭하면 인증서가 유효하지 않은 것으로 표시됩니다.



사전 대응적 정보

잘못된 웹 사이트 이름에 등록된 인증서

웹 인증서가 사이트에서 제공하는 모든 호스트 이름에 대해 가져왔는지 확인합니다. 예를 들어, 인증서가 가상의 도메인 www만 포함할 경우vManage-example-test입니다.com - vManage example-test를 사용하여 사이트를 로드하는 방문자입니다.com(www 없음) 접두사) 및 Public CA에서 서명된 인증서를 가져오면 신뢰할 수 있지만 인증서 이름 불일치 오류가 있는 또 다른 오류가 발생합니다.

> **참고:** SSL/TLS 인증서의 일반 이름이 브라우저의 도메인 또는 주소 표시줄과 일치하지 않을 때 일반 이름 불일치 오류가 발생합니다.

관련 정보

- CSR 디코더
- 인증서 서명 요청 생성
- 기술 지원 및 문서 – Cisco Systems