Grundlegendes zum Webzertifikat für vManage

Inhalt

Einleitung

In diesem Dokument wird der Unterschied zwischen dem Webzertifikat und den Controller-Zertifikaten in der Cisco SD-WAN-Lösung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in diesem Thema verfügen:

- Grundkenntnisse der Public Key Infrastructure (PKI).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco vManage Network Management System (NMS) Version 20.4.1
- Google Chrome, Version 94.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Auf dem Cisco SD-WAN verwendete Zertifikate

In Cisco SD-WAN-Lösungen werden zwei Arten von Zertifikaten verwendet: Controller-Zertifikate und Webzertifikate.

Webzertifikat

Wird für den Webzugriff auf vManage verwendet. Cisco installiert standardmäßig ein selbstsigniertes Zertifikat. Ein selbstsigniertes Zertifikat ist ein SSL-Zertifikat (Secure Sockets Layer), das von seinem eigenen Ersteller signiert wird. Cisco empfiehlt jedoch ein eigenes Webserverzertifikat. Dies gilt insbesondere für Fälle, in denen Netzwerkunternehmen Firewalls mit Webzugriffsbeschränkungen verwenden können. Cisco stellt keine von der Zertifizierungsstelle (Certificate Authority, CA) ausgestellten öffentlichen Webzertifikate zur Verfügung.

Weitere Informationen zum Generieren des vManage-Webzertifikats finden Sie in den Leitfäden: Webserverzertifikat generieren und So generieren Sie selbstsigniertes Webzertifikat für vManage

---

Controller-Zertifikat

Wird zum Herstellen von Steuerverbindungen zwischen den Controllern verwendet, z. B. vManage, vBonds, vSmarts. Diese Zertifikate sind für die gesamte SD-WAN-Fabric-Steuerungsebene von kritischer Bedeutung und müssen jederzeit gültig sein.

Weitere Informationen zu Controller-Zertifikaten finden Sie im Leitfaden: Automatische Zertifikatssignatur über Cisco Systems

---

Webzertifikat für vManage verstehen

Hypertext Transfer Protocol Secure (HTTPS) ist ein Internetkommunikationsprotokoll, das die Integrität und Vertraulichkeit von Daten zwischen dem Computer des Benutzers und der Website, in diesem Fall der vManage-Benutzeroberfläche, schützt. Benutzer erwarten eine sichere und private Verbindung, wenn sie auf vManage zugreifen. Um eine sichere und private Verbindung zu erreichen, müssen Sie ein Sicherheitszertifikat erhalten. Das Zertifikat wird von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt, die überprüft, ob Ihre vManage-Domäne tatsächlich zu Ihrer Organisation gehört.

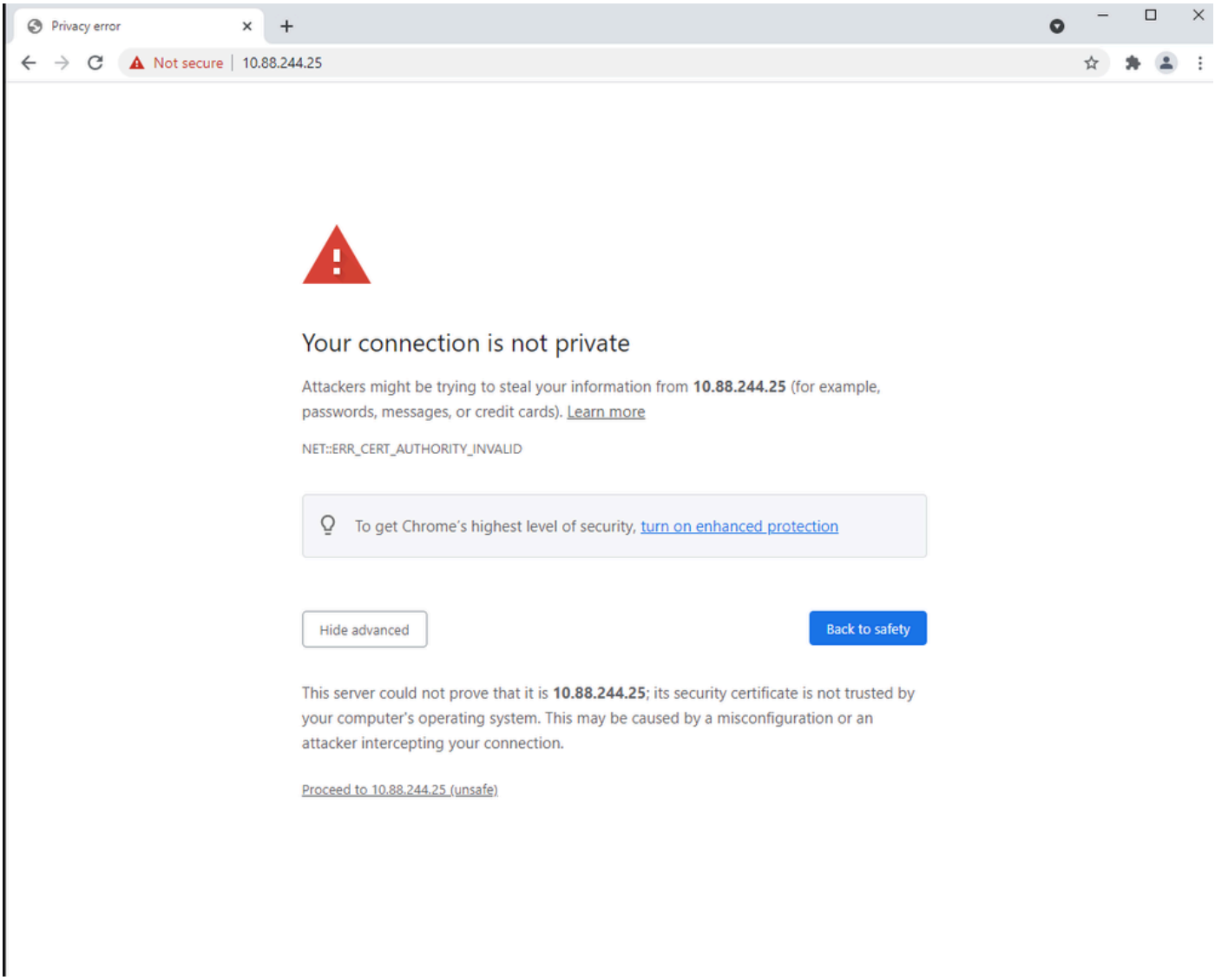
Wenn ein Benutzer auf vManage zugreift, führt der Benutzer-PC eine HTTPS-Verbindung durch, und es wird ein sicherer Tunnel zwischen dem vManage-Server und dem Computer mit den zur Authentifizierung installierten SSL-Zertifikaten eingerichtet. Die Authentifizierung des SSL-Zertifikats wird auf dem Benutzercomputer anhand der Datenbank gültiger, auf dem Gerät installierter Root-Zertifizierungsstellen durchgeführt. In der Regel hat der Computer bereits mehrere CA wie installiert, Google, GoDaddy, Enterprise CA (wenn dies der Fall ist), und mehr

öffentliche Einrichtungen. Wenn also die CSR (Certificate Signing Request) von GoDaddy signiert wird (nur ein Beispiel), ist sie vertrauenswürdig.

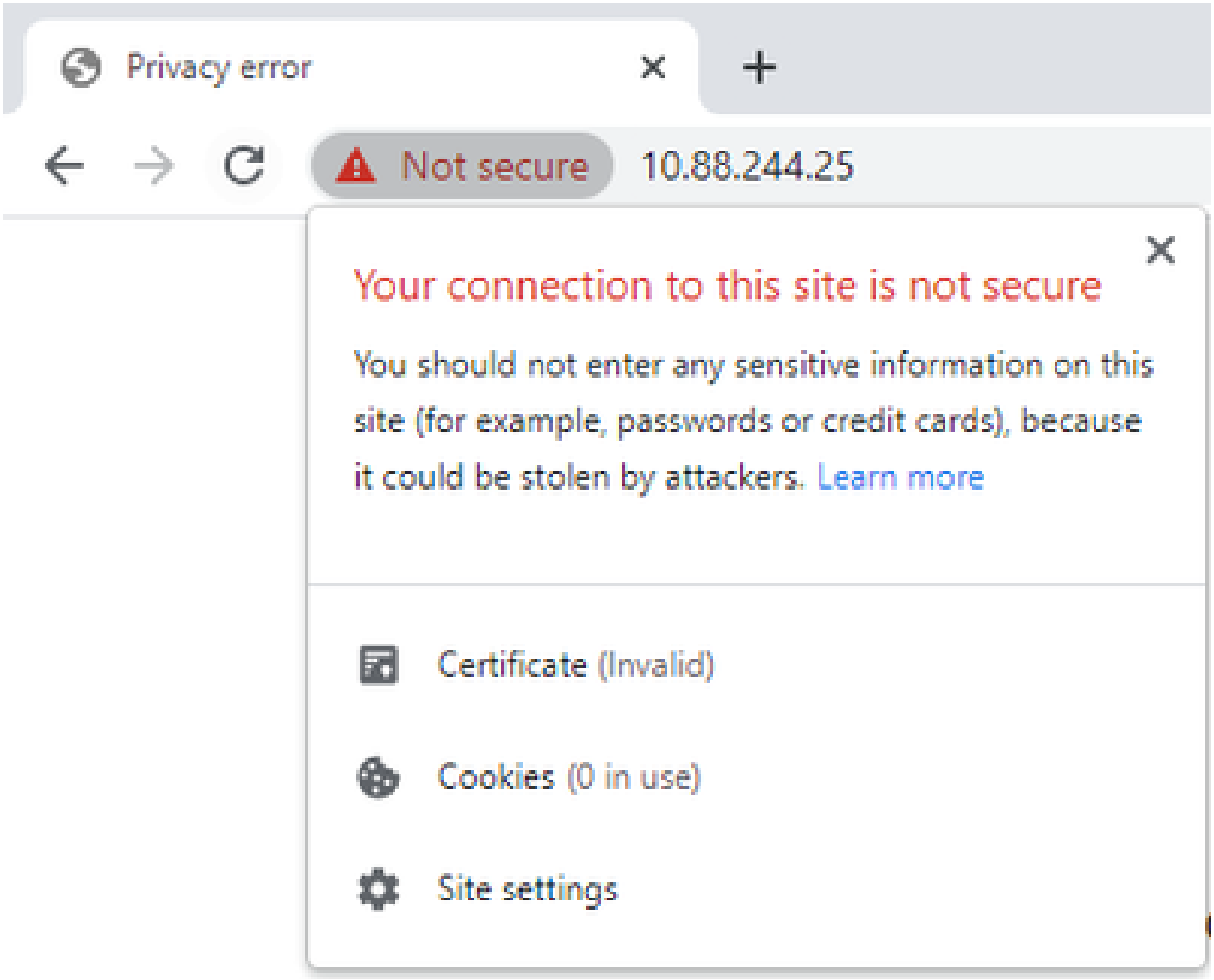
Verbindung ist keine private Nachricht auf vManage

Das selbstsignierte vManage-Zertifikat wird nicht von einer Zertifizierungsstelle signiert. Es wurde vom gleichen vManager und weder von der öffentlichen noch von der privaten Zertifizierungsstelle signiert, daher ist es für einen PC-Client nicht vertrauenswürdig. Aus diesem Grund zeigt der Browser eine nicht sichere/Datenschutzfehlerverbindung für die vManage-URL an.

Beispiel für den vMange-Fehler mit dem selbstsignierten Standardzertifikat des Google Chrome-Browsers, wie im Bild gezeigt.



Anmerkung: Klicken Sie auf die Option Site-Informationen anzeigen. Das Zertifikat wird als ungültig angezeigt.



Proaktive Informationen

Das Zertifikat wurde unter dem falschen Websitenamen registriert.

Stellen Sie sicher, dass das Webzertifikat für alle Hostnamen abgerufen wurde, die von Ihrer Website bedient werden. Wenn Ihr Zertifikat beispielsweise nur die fiktive Domäne www abdeckt.vManage-example-test:com, ein Besucher, der die Website mit vManage-example-test lädt.com (ohne das www. Präfix), und wenn es empfängt ein signiertes Zertifikat von einer öffentlichen Zertifizierungsstelle. Es ist vertrauenswürdig, aber es wird ein weiterer Fehler mit einem Zertifikatnamenskonfliktfehler ausgegeben.

Hinweis: Wenn der allgemeine Name des SSL/TLS-Zertifikats nicht mit der Domäne oder Adressleiste im Browser übereinstimmt, tritt ein Fehler auf.

Zugehörige Informationen

- CSR-Decoder
- Generieren einer Zertifikatsignierungsanforderung
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.