Comprensión del certificado web para vManage

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Certificados utilizados en Cisco SD-WAN](#)
[Certificado web](#)
[Certificado del controlador](#)
[Comprensión del certificado web para vManage](#)
[Mensaje "La conexión no es privada" en vManage](#)
[Información proactiva](#)
[Certificado registrado en el nombre incorrecto del sitio web](#)
[Información Relacionada](#)

Introducción

Este documento describe la diferencia entre el certificado web y los certificados de controlador en la solución Cisco SD-WAN. Este documento también explica en detalle el certificado Web y aclara el uso entre estos dos tipos de certificados.

Prerequisites

Requirements

Conocimiento básico de la infraestructura de clave pública (PKI).

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Certificados utilizados en Cisco SD-WAN

Existen dos tipos de certificados que se utilizan en las soluciones de Cisco SD-WAN, certificados de controlador y certificados web.

Certificado web

Se utiliza para el acceso web a vManage. Cisco instala un certificado autofirmado de forma predeterminada. Un certificado autofirmado es un certificado de capa de sockets seguros (SSL) firmado por su propio creador.

Sin embargo, Cisco recomienda su propio certificado de servidor web. Esto se aplica especialmente a los casos en los que las empresas de red pueden tener firewalls con restricciones de acceso a la Web.
Cisco no proporciona certificados web públicos emitidos por la Autoridad de Certificación (CA).

> Para obtener más información sobre cómo generar el certificado Web vManage, consulte las guías: Generar certificado de servidor Web y Cómo generar certificado Web firmado automáticamente para vManage

Certificado del controlador

Se utiliza para generar conexiones de control entre los controladores, vManage, vBonds y vSmarts.

Tenga en cuenta que estos certificados son fundamentales para todo el plano de control de fabric de SDWAN y deben mantenerse válidos en todo momento.

> Para obtener más información sobre certificados de controlador, consulte la guía: Firma automática de certificados a través de Cisco Systems

Comprensión del certificado web para vManage

Hypertext Transfer Protocol Secure (HTTPS) es un protocolo de comunicación por Internet que protege la integridad y confidencialidad de los datos entre el equipo del usuario y el sitio web en este caso la GUI de vManage. Los usuarios esperan una conexión segura y privada cuando acceden a vManage.

Para lograr una conexión segura y privada, debe obtener un certificado de seguridad. El certificado lo emite una autoridad de certificación (CA), que realiza los pasos necesarios para comprobar que su dominio vManage pertenece realmente a su organización.

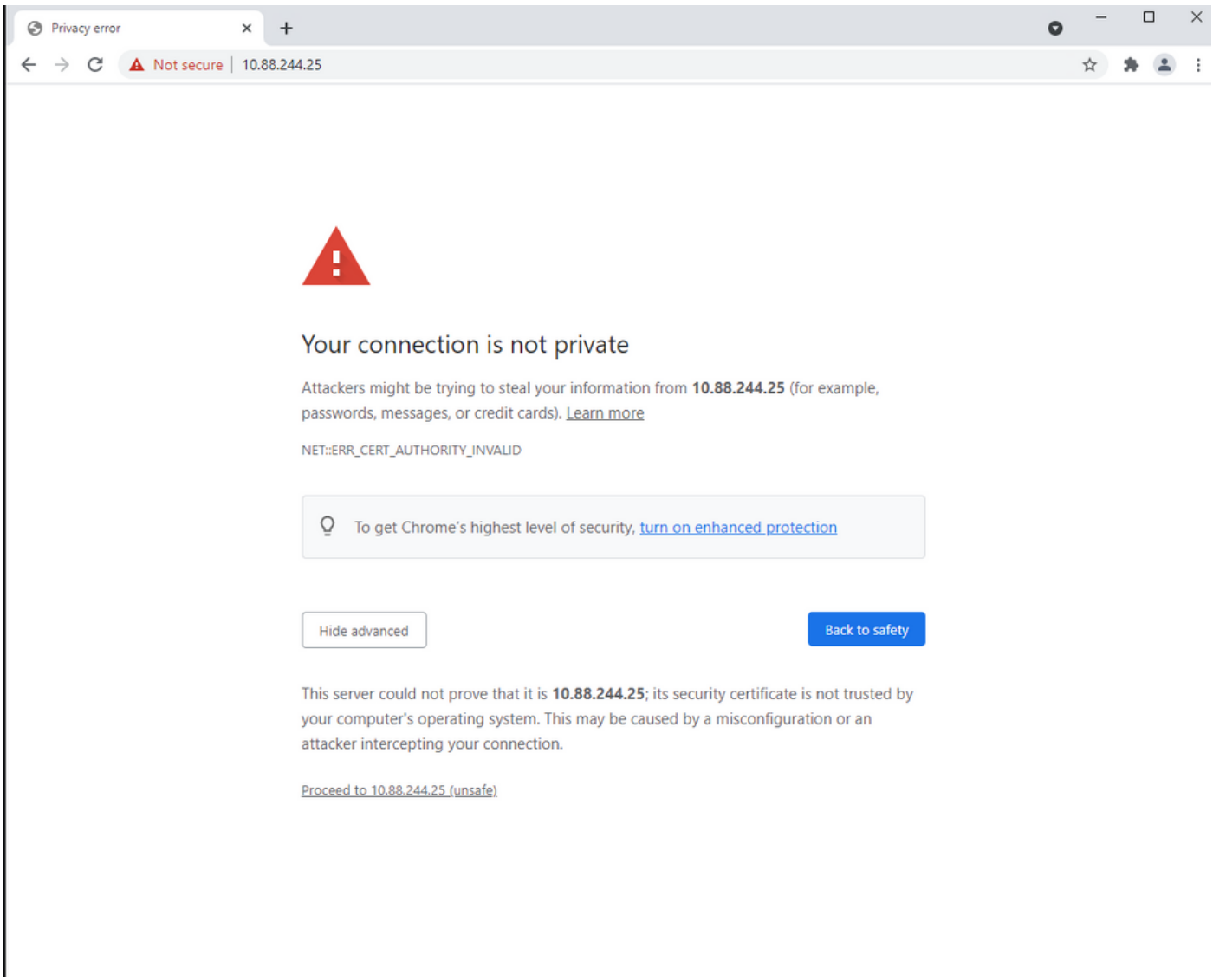
Cuando un usuario accede a vManage, el equipo del usuario realiza una conexión HTTPS y se establece un túnel seguro entre el servidor vManage y el equipo con los certificados SSL instalados para la autenticación. La autenticación del certificado SSL se realiza en el equipo del usuario en la base de datos de CA raíz válidas instaladas en el dispositivo. Por lo general, el equipo ya ha instalado varias CA como Google, GoDaddy, Enterprise CA (si es así) y más entidades públicas. Por lo tanto, si la solicitud de firma de certificados (CSR) está firmada por Goddady (sólo un ejemplo), es de confianza.

Mensaje "La conexión no es privada" en vManage

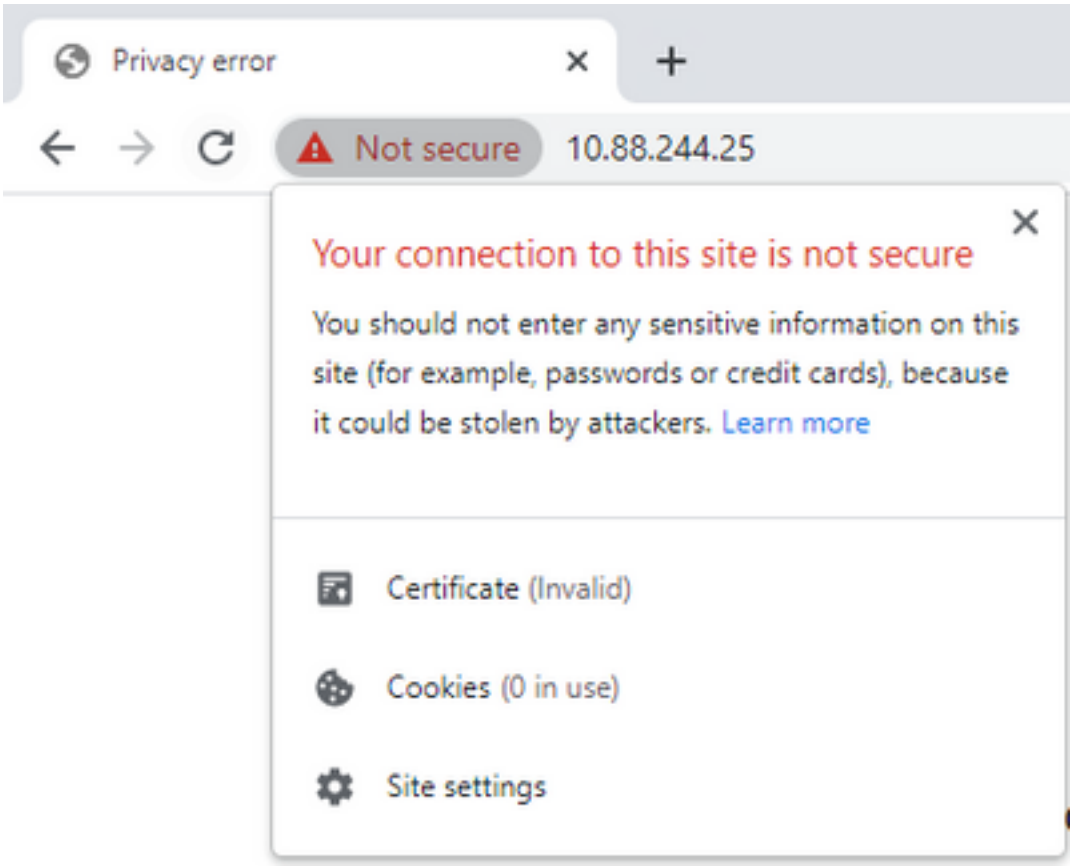
El certificado autofirmado de vManage no está firmado por una CA. Ha sido firmado por el mismo vManage y ni por la CA pública ni privada, por lo que no es de confianza para un cliente de PC. Por este motivo, el explorador muestra una conexión de error de confidencialidad/no segura para

la dirección URL de vManage.

Ejemplo para el error vManager con el certificado autofirmado predeterminado por el navegador de Google Chrome, como se muestra en la imagen.



Nota: Haga clic en la opción de ver información del sitio, el certificado se muestra como no válido.



Información proactiva

Certificado registrado en el nombre incorrecto del sitio web

Asegúrese de que se ha obtenido el certificado web para todos los nombres de host a los que atiende su sitio. Por ejemplo, si su certificado sólo cubre el dominio ficticio www.vManage-ejemplo-test.com, un visitante que carga el sitio con la prueba de ejemplo de vManage.com (sin www. prefijo), y si obtiene un certificado firmado por una CA pública, es de confianza pero recibe otro error con un error de discordancia de nombre de certificado.

> **Nota:** Se produce un error de discordancia de nombre común cuando el nombre común del certificado SSL/TLS no coincide con el dominio o la barra de dirección del navegador.

Información Relacionada

- Decodificador CSR
- Generar una solicitud de firma de certificado
- Soporte Técnico y Documentación - Cisco Systems