Comprendre le certificat Web pour vManage

Contenu

Introduction

Ce document décrit la différence entre le certificat Web et les certificats de contrôleur sur la solution Cisco SD-WAN. Ce document explique également en détail le certificat Web et clarifie l'utilisation de ces deux types de certificats.

Conditions préalables

Conditions requises

Connaissance de base de l'infrastructure à clé publique (ICP).

Components Used

- Cisco vManage Network Management System (NMS) version 20.4.1
- Google Chrome version 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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Certificats utilisés sur Cisco SD-WAN

Il existe deux types de certificats utilisés dans les solutions Cisco SD-WAN : les certificats de contrôleur et les certificats Web.

Certificat Web

Utilisé pour l'accès Web à vManage. Par défaut, Cisco installe un certificat auto-signé. Un certificat auto-signé est un certificat SSL (Secure Sockets Layer) signé par son propre créateur.

Cependant, Cisco recommande leur propre certificat de serveur Web. Ceci est particulièrement vrai dans les cas où les entreprises réseau peuvent avoir des pare-feu avec des restrictions d'accès au Web.
Cisco ne fournit pas de certificats Web publics émis par l'autorité de certification (AC).

> Pour plus d'informations sur la génération du certificat Web vManage, reportez-vous aux guides Generate Web Server Certificate et How To Generate Self-Signed Web Certificate For vManage.

Certificat de contrôleur

Utilisé pour établir des connexions de contrôle entre les contrôleurs, c'est-à-dire vManage, vBonds et vSmarts.

Notez que ces certificats sont essentiels pour l'ensemble du plan de contrôle de fabric SDWAN et doivent être conservés en permanence.

> Pour plus d'informations sur les certificats de contrôleur, reportez-vous au guide : Signature automatique des certificats via Cisco Systems

Comprendre le certificat Web pour vManage

Le protocole HTTPS (Hypertext Transfer Protocol Secure) est un protocole de communication Internet qui protège l'intégrité et la confidentialité des données entre l'ordinateur de l'utilisateur et le site Web, dans ce cas l'interface utilisateur graphique vManage. Les utilisateurs attendent une connexion sécurisée et privée lorsqu'ils accèdent à vManage.

Pour établir une connexion sécurisée et privée, vous devez obtenir un certificat de sécurité. Le certificat est émis par une autorité de certification (CA), qui prend les mesures nécessaires pour vérifier que votre domaine vManage appartient réellement à votre organisation.

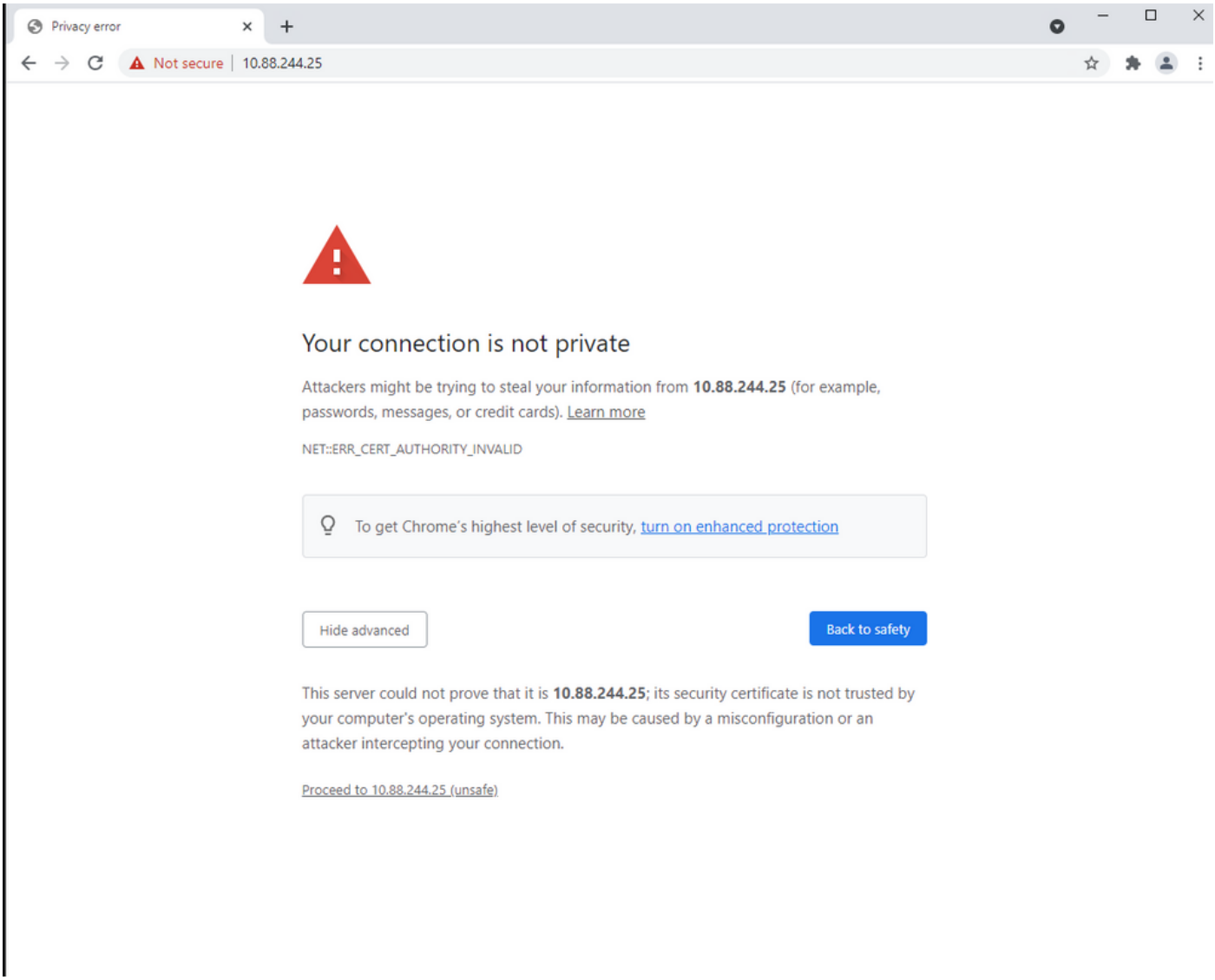
Lorsqu'un utilisateur accède à vManage, le PC de l'utilisateur effectue une connexion HTTPS et un tunnel sécurisé est établi entre le serveur vManage et l'ordinateur avec les certificats SSL installés pour l'authentification. L'authentification du certificat SSL est effectuée sur l'ordinateur de l'utilisateur par rapport à la base de données des autorités de certification racine valides installées sur le périphérique. Habituellement, l'ordinateur a déjà installé plusieurs CA comme Google, GoDaddy, Enterprise CA (si c'est le cas), et plus d'entités publiques. Par conséquent, si la demande de signature de certificat (CSR) est signée par Goddady (juste un exemple), elle est approuvée.

Message « Connection Is Not private » sur vManage

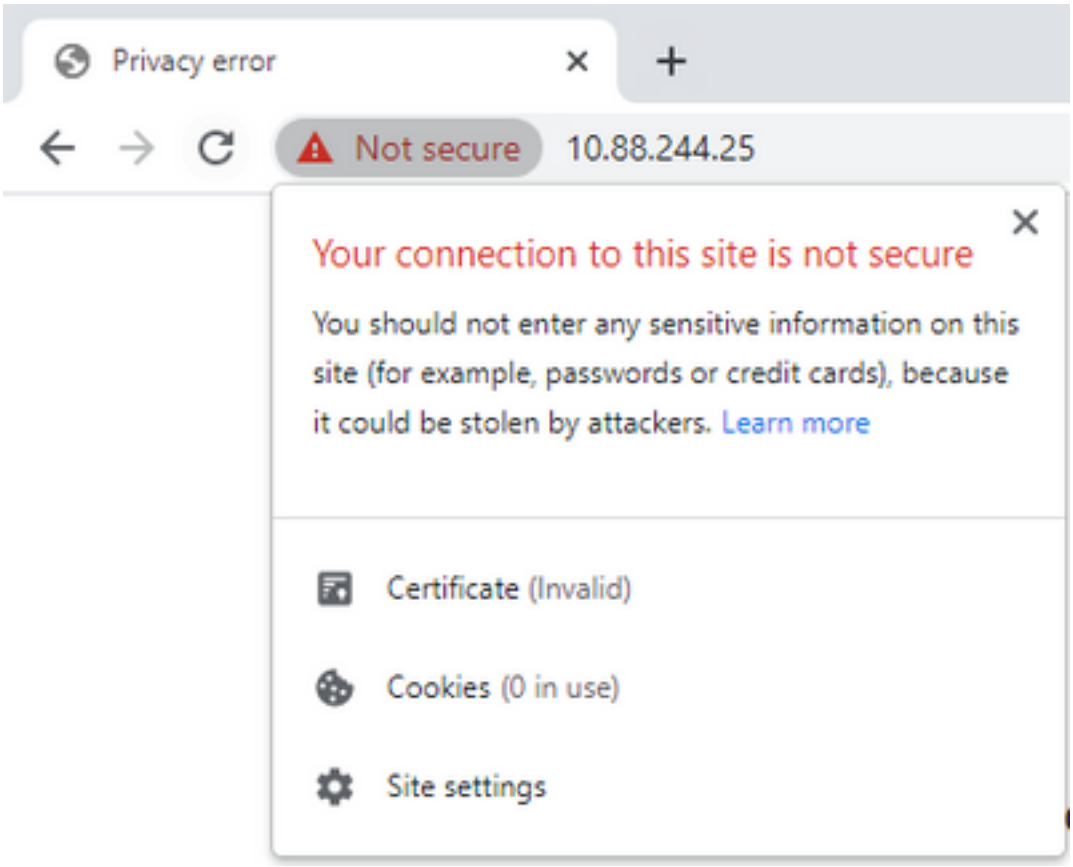
Le certificat auto-signé vManage n'est pas signé par une autorité de certification. Il a été signé par le même vManage et ni par l'autorité de certification publique ni privée, par conséquent il n'est pas approuvé pour un client PC. C'est la raison pour laquelle le navigateur affiche une connexion

d'erreur non sécurisée/de confidentialité pour l'URL vManage.

Exemple pour l'erreur vMange avec le certificat auto-signé par défaut par le navigateur Google Chrome comme indiqué dans l'image.



Note: Cliquez sur l'option Afficher les informations du site, le certificat est affiché comme non valide.



Informations proactives

Certificat enregistré sur le nom de site Web incorrect

Assurez-vous que le certificat Web a été obtenu pour tous les noms d'hôte que votre site sert. Par exemple, si votre certificat couvre uniquement le domaine fictif www.vManage-example-test.com, un visiteur qui charge le site avec vManage-example-test.com (sans le www. préfixe), et s'il obtient un certificat signé par une autorité de certification publique, il est approuvé, mais il obtient une autre erreur avec une erreur de non-correspondance de nom de certificat.

> **Remarque :** Une erreur de non-correspondance de nom commun se produit lorsque le nom commun du certificat SSL/TLS ne correspond pas au domaine ou à la barre d'adresses du navigateur.

Informations connexes

- Décodeur CSR
- Générer une demande de signature de certificat
- Support et documentation techniques - Cisco Systems