Comprendre le certificat Web pour vManage

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Certificats utilisés sur Cisco SD-WAN

- Certificat Web
- Certificat du contrôleur

Comprendre le certificat Web pour vManage

- La connexion n'est pas un message privé sur vManage

Informations proactives

- Certificat enregistré sur le nom incorrect du site Web

Informations connexes

Introduction

Ce document décrit la différence entre le certificat Web et les certificats de contrôleur sur la solution Cisco SD-WAN.

Conditions préalables

Exigences

Cisco recommande que vous ayez une connaissance de ce sujet :

- Connaissances de base de l'infrastructure à clé publique (PKI).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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 ; Certificats de contrôleur et 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. Toutefois, Cisco recommande son propre certificat de serveur Web. Ceci est particulièrement vrai dans les cas où les entreprises de réseau peuvent avoir des pare-feu avec des restrictions d'accès Web. Cisco ne fournit pas de certificats Web publics émis par l'autorité de certification (CA).

Pour plus d'informations sur la façon de générer le certificat Web vManage, consultez les guides : Generate Web Server Certificate et How To Generate Self-Signed Web Certificate For vManage

---

Certificat du contrôleur

Utilisé pour établir des connexions de contrôle entre les contrôleurs, par exemple, vManage, vBonds, vSmarts. Ces certificats sont essentiels pour l'ensemble du plan de contrôle du fabric SD-WAN et doivent être maintenus valides à tout moment.

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

---

Comprendre le certificat Web pour vManage

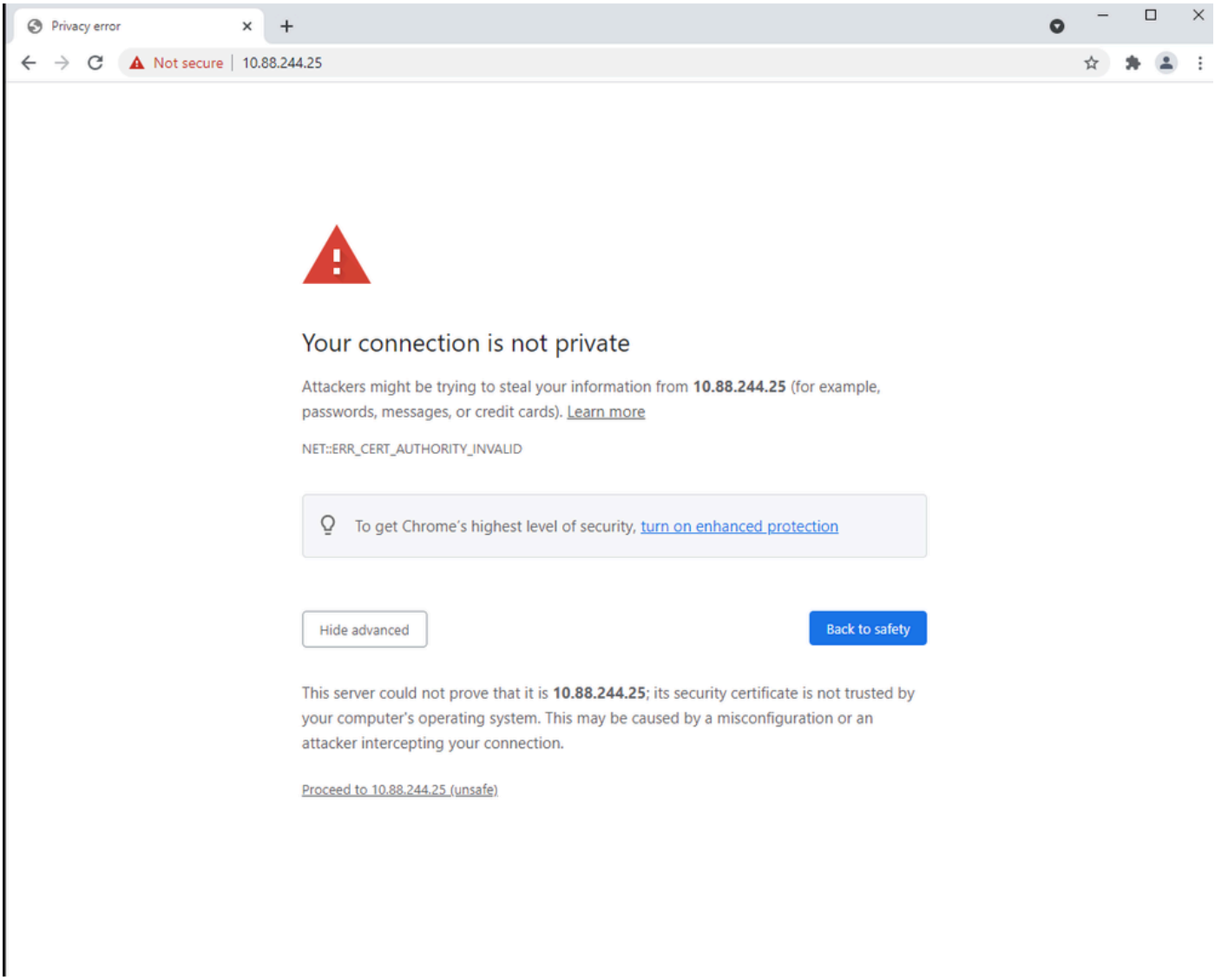
Le protocole HTTPS (Hypertext Transfer Protocol Secure) est un protocole de communication Internet qui protège l'intégrité et la confidentialité des données entre l'ordinateur de l'utilisateur et le site Web, en l'occurrence l'interface utilisateur graphique vManage. Les utilisateurs attendent une connexion sécurisée et privée lorsqu'ils accèdent à vManage. Pour obtenir 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, l'ordinateur de l'utilisateur établit une connexion HTTPS et un tunnel sécurisé est établi entre le serveur vManage et l'ordinateur sur lequel les certificats SSL sont 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. Généralement, 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 GoDaddy (juste un exemple), elle est approuvée.

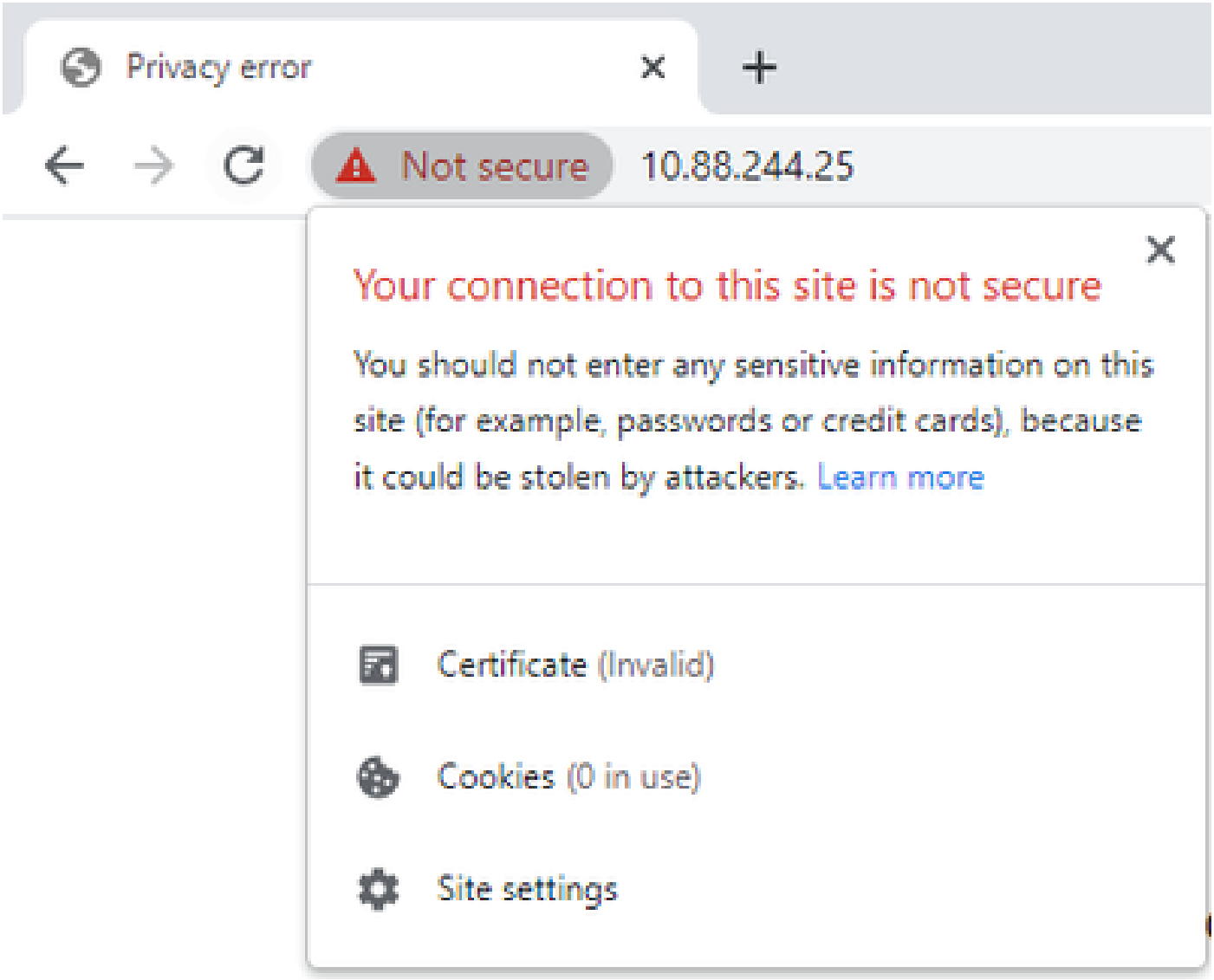
La connexion n'est pas un message privé sur vManage

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 d'erreur vManage avec le certificat auto-signé par défaut par le navigateur Google Chrome, comme illustré dans l'image.



Remarque : Cliquez sur l'option Afficher les informations du site. Le certificat est affiché comme non valide.



Informations proactives

Certificat enregistré sur le nom incorrect du site Web

Assurez-vous que le certificat Web a été obtenu pour tous les noms d'hôte que votre site dessert. Par exemple, si votre certificat ne couvre que 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, elle est approuvée, mais elle obtient une autre erreur avec une erreur d'incompatibilité 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'adresse du navigateur.

Informations connexes

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.