Begrijp het Webcertificaat voor vManager

Inhoud

Inleiding

Dit document beschrijft het verschil tussen het Webcertificaat en de controllercertificaten in Cisco SD-WAN oplossing. Dit document verklaart ook in detail het Webcertificaat en verduidelijkt het gebruik tussen deze twee soorten certificaten.

Voorwaarden

Vereisten

Basiskennis van de openbare sleutelinfrastructuur (PKI).

Gebruikte componenten

- Cisco vManager Network Management System (NMS) versie 20.4.1
- Google Chrome versie 9.4.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Certificaten gebruikt op Cisco SD-WAN

Er zijn twee soorten certificaten gebruikt in Cisco SD-WAN oplossingen, controllercertificaten en webcertificaten.

Webcertificaat

Gebruikt voor webtoegang tot de vManager. Cisco installeert standaard een zelf-ondertekend certificaat. Een zelfondertekend certificaat is een Secure Socket Layer (SSL) certificaat dat door zijn eigen schepper wordt ondertekend.

Maar Cisco raadt hun eigen webservercertificaat aan. Dit is in het bijzonder in gevallen waar netwerkbedrijven firewalls kunnen hebben met beperkingen op webtoegang.
Cisco biedt geen openbare webcertificaten die zijn afgegeven door de certificeringsinstantie (CA).

> Raadpleeg de gidsen voor meer informatie over het genereren van het vManager-webcertificaat: genereer webservercertificaat en hoe u een zelf-ondertekend webcertificaat voor vManager kunt genereren

Controller-certificaat

Gebruikt om besturingsverbindingen te maken tussen de controllers, d.w.z. vManager, vBonds, vSmarts.

Let op dat deze certificaten cruciaal zijn voor het gehele SDWAN-fabric-besturingsplane en te allen tijde geldig blijven.

> Raadpleeg de handleiding voor meer informatie over controllers: Geautomatiseerde certificering via Cisco Systems

Begrijpen met webcertificaat voor vManager

Hypertext Transfer Protocol Secure (HTTPS) is een protocol voor internetcommunicatie dat de integriteit en vertrouwelijkheid van gegevens tussen de computer van de gebruiker en de website in dit geval de vManager GUI beschermt. Gebruikers verwachten een veilige en privéverbinding als ze toegang krijgen tot de vManager.

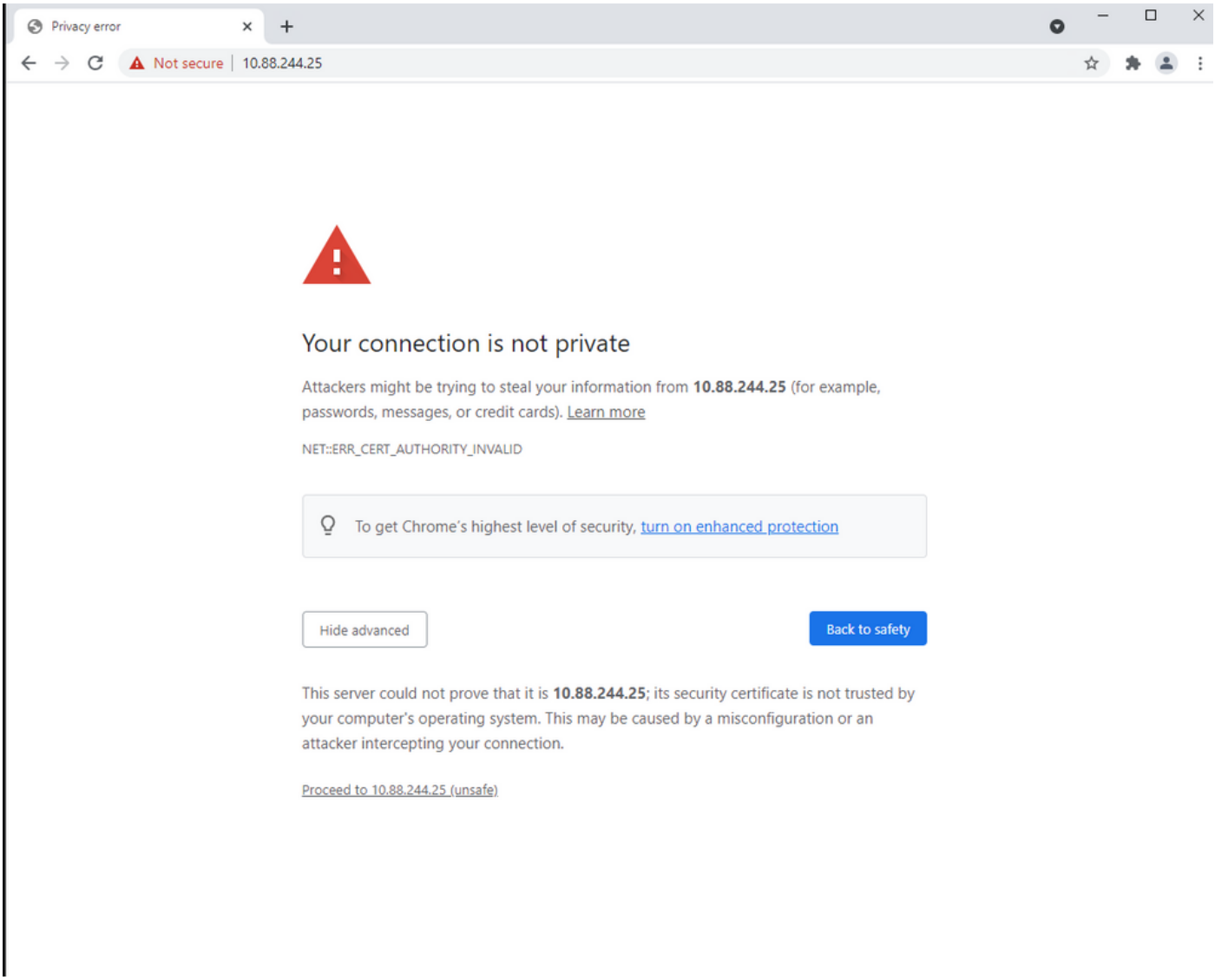
Om een veilige en privé verbinding te bereiken, moet u een veiligheidscertificaat verkrijgen. Het certificaat wordt afgegeven door een certificeringsinstantie (CA), die stappen neemt om te controleren of uw vManager-domein feitelijk aan uw organisatie toebehoort.

Wanneer een gebruiker toegang heeft tot de vManager, voert de gebruiker-PC een HTTPS-verbinding uit en er wordt een beveiligde tunnel tot stand gebracht tussen de vManager-server en de computer met de SSL-certificaten die voor verificatie zijn geïnstalleerd. De authenticatie van het SSL certificaat wordt op de gebruikerscomputer uitgevoerd tegen de databank van geldige wortel CAs die op het apparaat geïnstalleerd zijn. Normaal gesproken heeft de computer al meerdere apparaten geïnstalleerd, zoals Google, GoDaddy, Enterprise CA (als dit het geval is) en meer publieke entiteiten. Daarom, als het certificaatverzoek (CSR) door Goddady (slechts een voorbeeld) wordt ondertekend, wordt het vertrouwd.

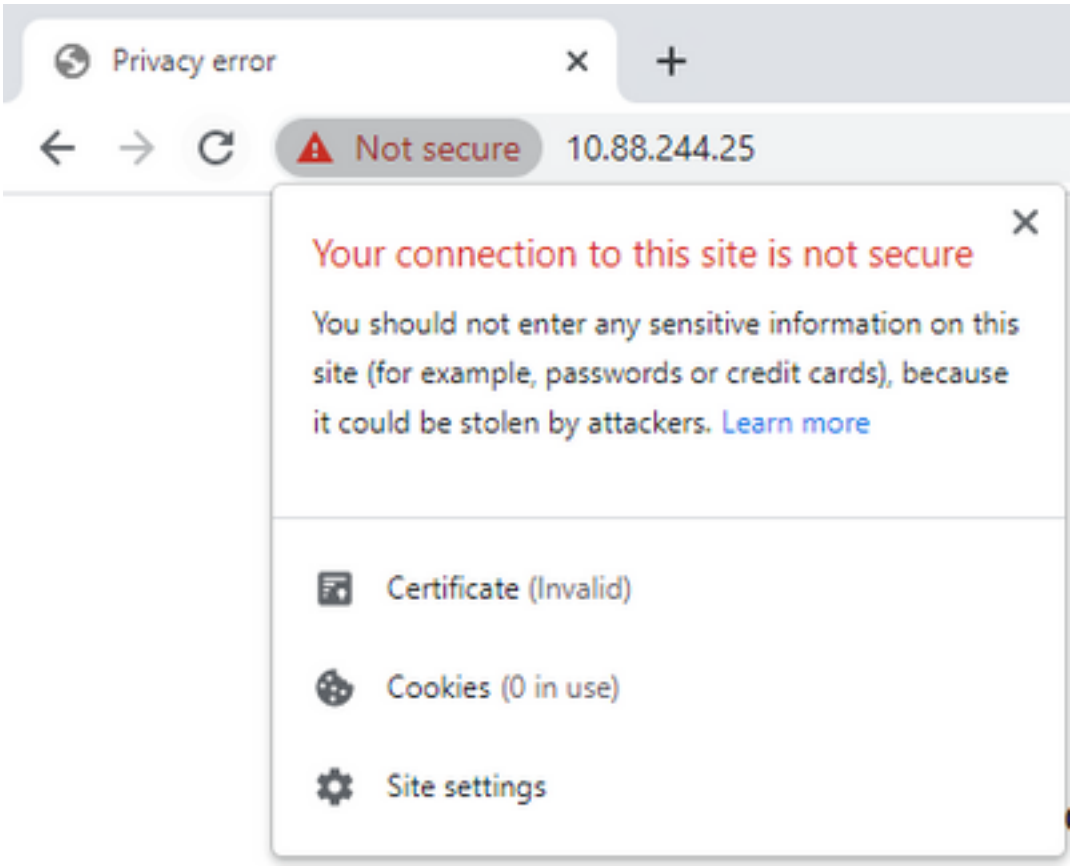
"Verbinding is niet privé"-bericht op vManager

Het vManager zelfgetekende certificaat is niet ondertekend door een CA. Het is ondertekend door dezelfde vManager en noch door de openbare noch door particuliere CA, zodat het niet vertrouwd is voor een pc-client. Dat is de reden dat browser een niet beveiligde/privacy-foutverbinding voor de vManager URL weergeeft.

Voorbeeld van de fout in het beheer met het standaard zelfgetekende certificaat van de browser Google Chrome zoals getoond in de afbeelding.



Opmerking: Klik op de optie Site-informatie, het certificaat wordt ongeldig weergegeven.



Proactieve informatie

Certificaat geregistreerd onder de onjuiste webnaam

Zorg ervoor dat het webcertificaat is verkregen voor alle hostnamen die uw website dient. Als uw certificaat bijvoorbeeld alleen fictieve domein www bestrijkt.vBijvoorbeeld-test beheren.com, een bezoeker die de site laadt met de vManager-voorbeeld-test.com (zonder www). prefix), en als dit krijgt een ondertekend certificaat van een openbare CA, het wordt vertrouwd maar het krijgt een andere fout met een fout van de certificaaternaam mismatch.

> **Opmerking:** Er is een fout die vaak voorkomt bij de naamfout wanneer de algemene naam van het SSL/TLS-certificaat niet overeenkomt met het domein of de adresbalk in de browser.

Gerelateerde informatie

- CSR-decoder
- Een certificaataanvraag genereren
- Technische ondersteuning en documentatie – Cisco Systems