了解vManage的Web证书

目录

简介

本文档介绍Cisco SD-WAN解决方案上的Web证书和控制器证书之间的区别。本文档还详细说明了Web证书，并阐明了这两种类型的证书之间的使用。

先决条件

要求

公钥基础设施(PKI)的基础知识。

使用的组件

- Cisco vManage网络管理系统(NMS)版本20.4.1
- Google Chrome版本94.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

思科SD-WAN上使用的证书

思科SD-WAN解决方案中使用两种类型的证书：控制器证书和Web证书。

Web证书

用于对vManage的Web访问。默认情况下，思科安装自签名证书。自签名证书是由其自己的创建者签名的安全套接字层(SSL)证书。

但是，思科建议自己的Web服务器证书。这尤其适用于网络企业可以拥有具有Web访问限制的防火墙的情况。
思科不提供由证书颁发机构(CA)颁发的公共Web证书。

> 有关如何生成vManage Web证书的详细信息，请参阅指南：生成Web服务器证书和如何为vManage生成自签名Web证书

控制器证书

用于在控制器（如vManage、vBonds、vSmarts）之间建立控制连接。

请注意，这些证书对于整个SDWAN交换矩阵控制平面至关重要，必须始终有效。

> 有关控制器证书的详细信息，请参阅指南：通过思科系统自动签名证书

了解vManage的Web证书

超文本传输协议安全(HTTPS)是一种互联网通信协议，在本例中为vManage GUI保护用户计算机和网站之间数据的完整性和机密性。用户在访问vManage时期望获得安全的专用连接。

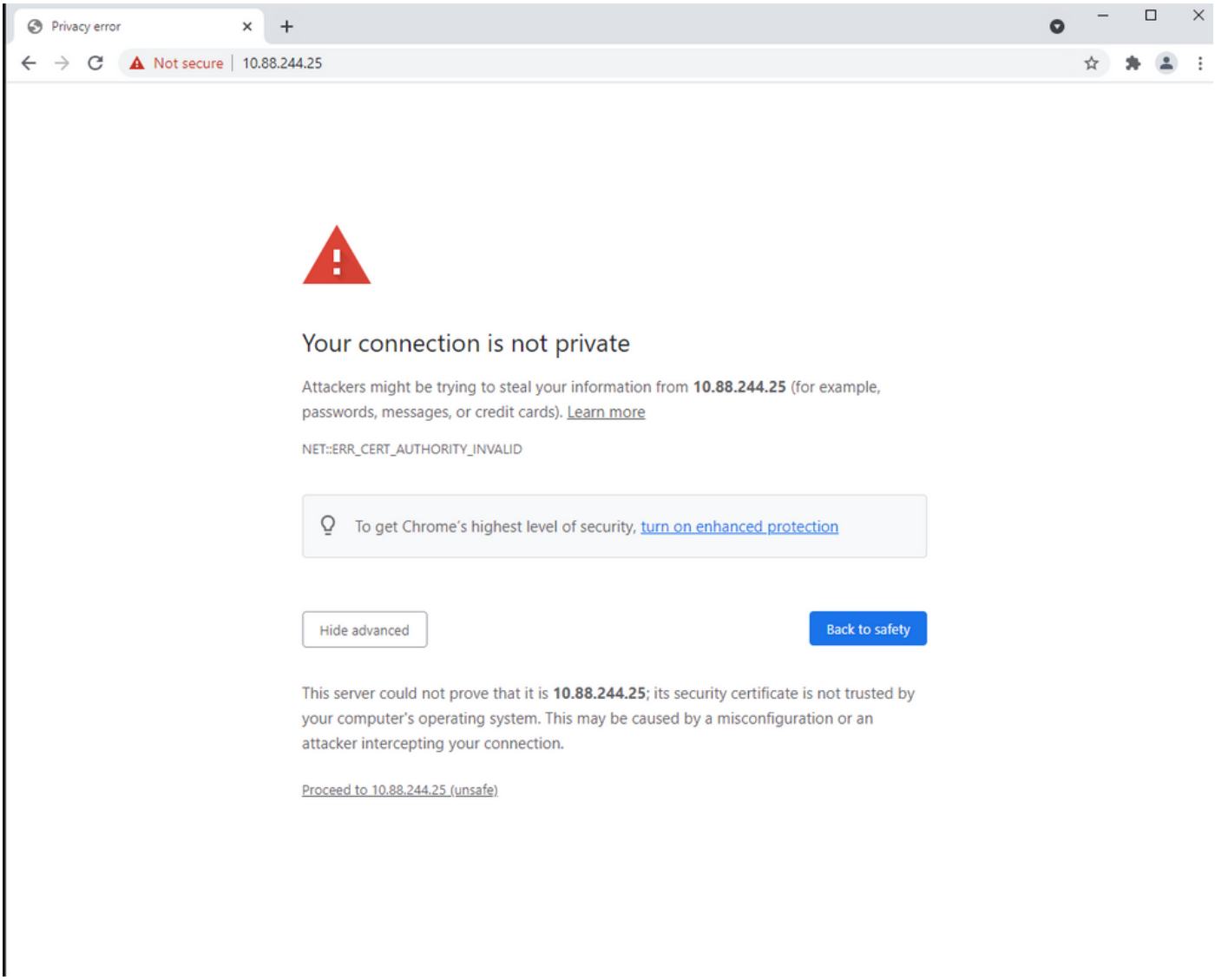
要实现安全和专用连接，必须获取安全证书。证书由证书颁发机构(CA)颁发，该机构会采取措施验证您的vManage域实际属于您的组织。

当用户访问vManage时，用户PC执行HTTPS连接，并在vManage服务器与安装了SSL证书进行身份验证的计算机之间建立安全隧道。SSL证书的身份验证是在用户计算机上根据设备上安装的有效根CA的数据库执行的。通常，计算机已安装多个CA，如Google、GoDaddy、Enterprise CA（如果情况如此）和更多公共实体。因此，如果证书签名请求(CSR)由Goddady签名（只是一个示例），则它是受信任的。

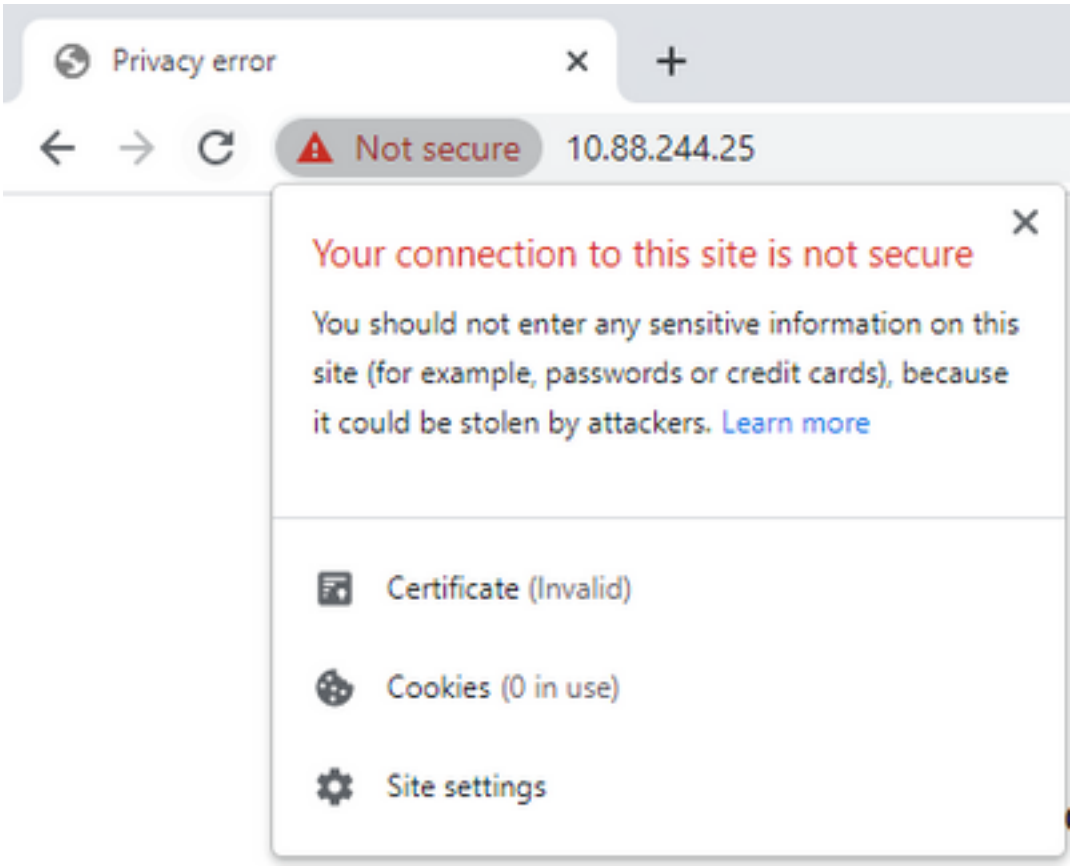
vManage上的“Connection Is Not Private”消息

vManage自签名证书未由CA签名。它已由同一vManage签署，且既不由公共CA也不由私有CA签署，因此它不受PC客户端信任。因此，浏览器显示vManage URL的不安全/隐私错误连接。

如图所示，Google Chrome浏览器默认自签名证书的vMange错误示例。



注意：点击查看站点信息选项，证书显示为无效。



主动信息

注册到不正确网站名称的证书

确保已为您的站点服务的所有主机名获取Web证书。例如，如果证书仅涵盖虚构域www。vManage-example-test。com，此访问者使用vManage-example-test加载站点。com(不含www. 前缀)，如果 通过公共CA获取签名证书，它受信任，但它会收到另一个错误，证书名称不匹配错误。

> **注意**：当SSL/TLS证书的公用名与浏览器中的域或地址栏不匹配时，会出现公用名不匹配错误。

相关信息

- CSR解码器
- 生成证书签名请求
- 技术支持和文档 - Cisco Systems