瞭解vManage的Web證書

目錄

簡介

本檔案介紹Cisco SD-WAN解決方案上的Web憑證和控制器憑證之間的差異。

必要條件

需求

思科建議您瞭解以下主題：

- 公開金鑰基礎架構(PKI)的基本知識。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco vManage網路管理系統(NMS)版本20.4.1
- Google Chrome版本94.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

Cisco SD-WAN上使用的證書

Cisco SD-WAN解決方案中使用兩種型別的證書；控制器憑證和Web憑證。

Web證書

用於vManage的Web訪問。預設情況下，思科會安裝自簽名證書。自簽名證書是安全套接字層(SSL)證書，由自己的建立者簽名。但是，思科建議使用自己的Web伺服器證書。尤其適用於網路企業可以使用具有Web存取限制的防火牆的情況。Cisco不提供由憑證授權單位(CA)發出的公共Web憑證。

有關如何生成vManage Web證書的詳細資訊，請參閱生成Web伺服器證書和如何為vManage生成自簽名Web證書指南

控制器證書

用於在控制器之間構建控制連線，例如vManage、vBonds、vSmarts。這些證書對於整個SD-WAN交換矩陣控制平面至關重要，必須始終保持有效。

有關控制器證書的詳細資訊，請參閱指南：通過Cisco Systems進行自動證書簽名

瞭解vManage的Web證書

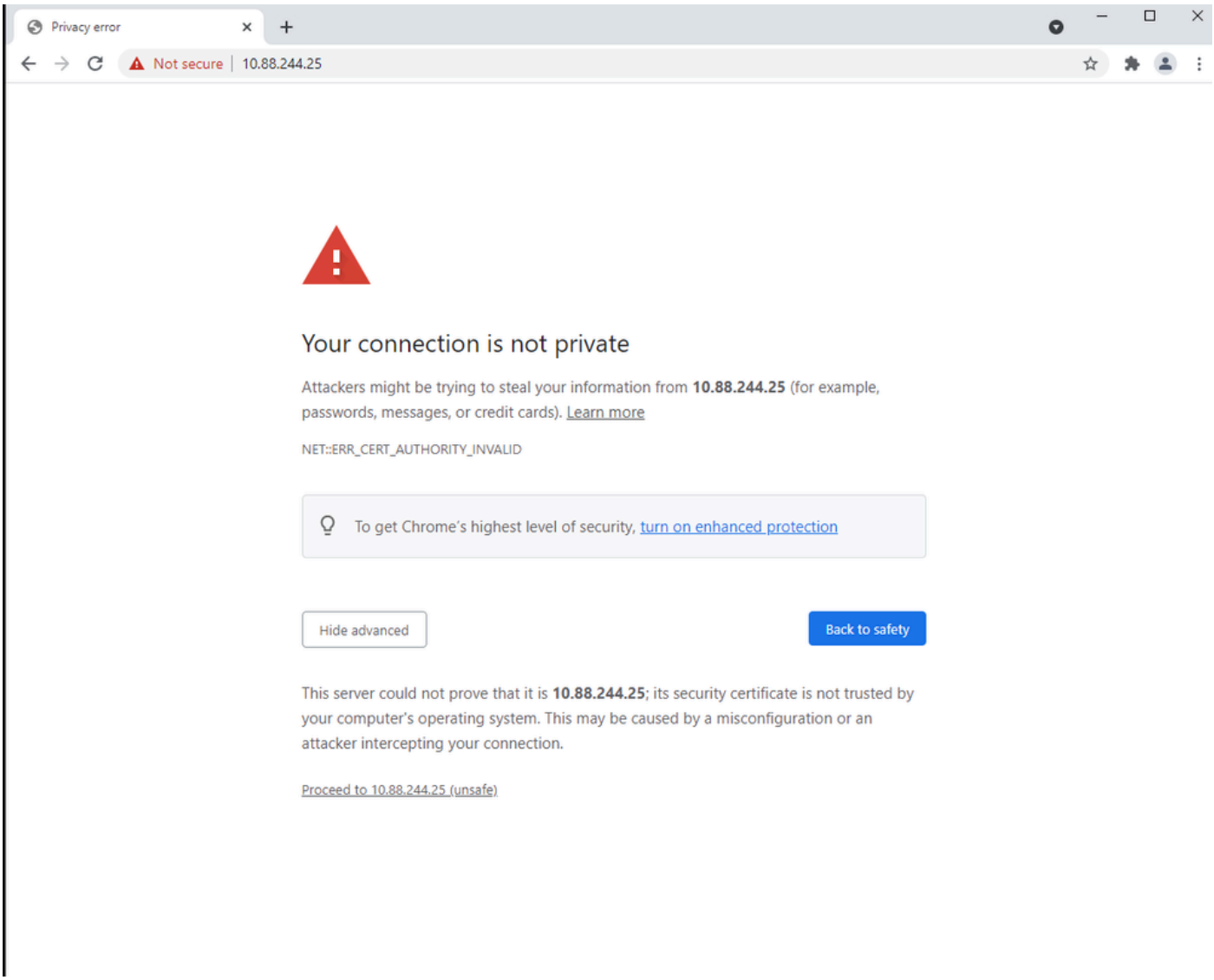
超文本傳輸協定安全(HTTPS)是一種網際網路通訊協定，在此情況下保護使用者電腦與網站之間(vManage GUI)資料的完整性和機密性。使用者訪問vManage時希望獲得安全和專用連線。要獲得安全和專用連線，您必須獲取安全證書。證書由證書頒發機構(CA)頒發，該機構採取措施驗證您的vManage域是否實際屬於您的組織。

當使用者訪問vManage時，使用者PC執行HTTPS連線，並在vManage伺服器和安裝了用於身份驗證的SSL證書的電腦之間建立安全隧道。在使用者電腦上對裝置上安裝的有效根CA的資料庫執行SSL證書的身份驗證。通常，電腦已經安裝了多個CA，如Google、GoDaddy、企業CA（如果情況如此）和更多的公共實體。因此，如果憑證簽署請求(CSR)由GoDaddy簽署（只是一個範例），則信任該請求。

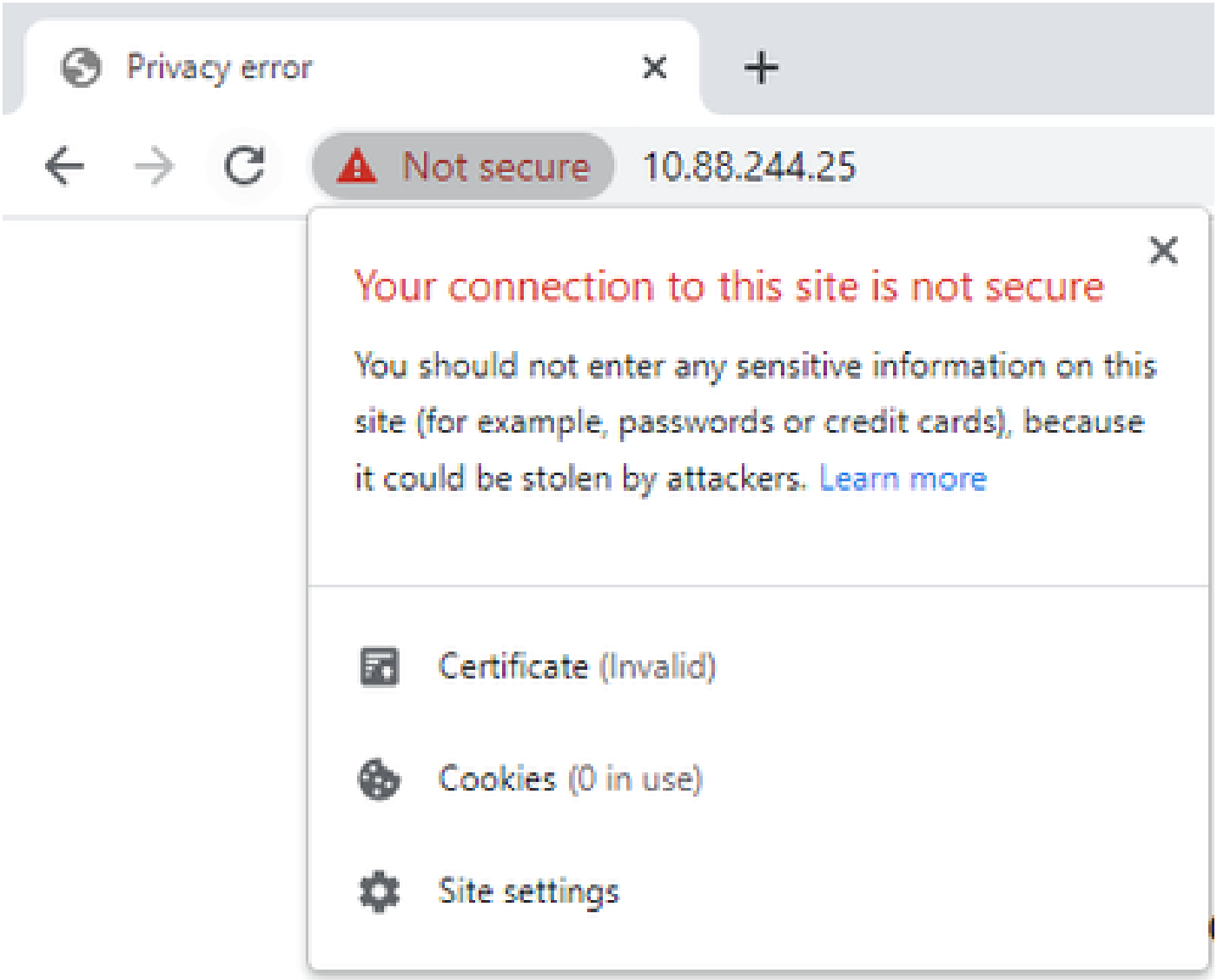
連線不是vManage上的私有消息

vManage自簽名證書不是由CA簽名的。簽名者為同一個vManage，非公有CA或私有CA，因此不受PC客戶端信任。因此，瀏覽器會顯示vManage URL的不安全/隱私錯誤連線。

Google Chrome瀏覽器的預設自簽憑證的vMange錯誤範例，如下圖所示。



附註：按一下view site information選項。證書顯示為無效。



主動資訊

註冊到錯誤網站名稱的證書

確保已為您的站點提供的所有主機名獲取Web證書。例如，如果您的憑證僅涵蓋虛構網域www.vManage-example-test。com，使用vManage-example-test載入站點的訪問者。com(不帶www. 字首)，如果是 獲取由公共CA簽名的證書，該證書受信任，但會收到另一個錯誤以及證書名稱不匹配錯誤。

注意：當SSL/TLS證書的公用名稱與瀏覽器中的域或位址列不匹配時，會發生公用名稱不匹配錯誤。

相關資訊

- CSR解碼器
- 生成證書簽名請求

- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。