vManageのWeb証明書について

内容

概要

このドキュメントでは、Web証明書とCisco SD-WANソリューションのコントローラ証明書の違いについて説明します。このドキュメントでは、Web証明書について詳しく説明し、これら2種類の証明書の使用について説明します。

前提条件

要件

公開キーインフラストラクチャ(PKI)に関する基礎知識。

使用するコンポーネント

- Cisco vManageネットワーク管理システム(NMS)バージョン20.4.1
- Google Chromeバージョン94.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

Cisco SD-WANで使用される証明書

Cisco SD-WANソリューションで使用される証明書には、コントローラ証明書とWeb証明書の2種類があります。

Web証明書

vManageへのWebアクセスに使用されます。シスコはデフォルトで自己署名証明書をインストールします。自己署名証明書は、独自の作成者によって署名されたセキュアソケットレイヤ(SSL)証明書です。

ただし、シスコでは独自のWebサーバ証明書を推奨しています。これは、ネットワーク企業がWebアクセス制限を持つファイアウォールを使用できる場合に特に当てはまります。
シスコは、認証局(CA)によって発行されたパブリックWeb証明書を提供しません。

> vManage Web証明書の生成方法の詳細については、ガイド「Webサーバ証明書の生成」および「vManage用の自己署名Web証明書の生成方法」を参照してください

コントローラ証明書

vManage、vBonds、vSmartsなどのコントローラ間の制御接続を構築するために使用されます。

これらの証明書はSDWANファブリックコントロールプレーン全体にとって重要であり、常に有効である必要があります。

> コントローラ証明書の詳細については、『Automated certificate signing through Cisco Systems』を参照してください

vManageのWeb証明書について

Hypertext Transfer Protocol Secure(HTTPS)は、ユーザのコンピュータとWebサイト（この場合はvManage GUI）間のデータの整合性と機密性を保護するインターネット通信プロトコルです。ユーザは、vManageにアクセスするときに、セキュアなプライベート接続を期待します。

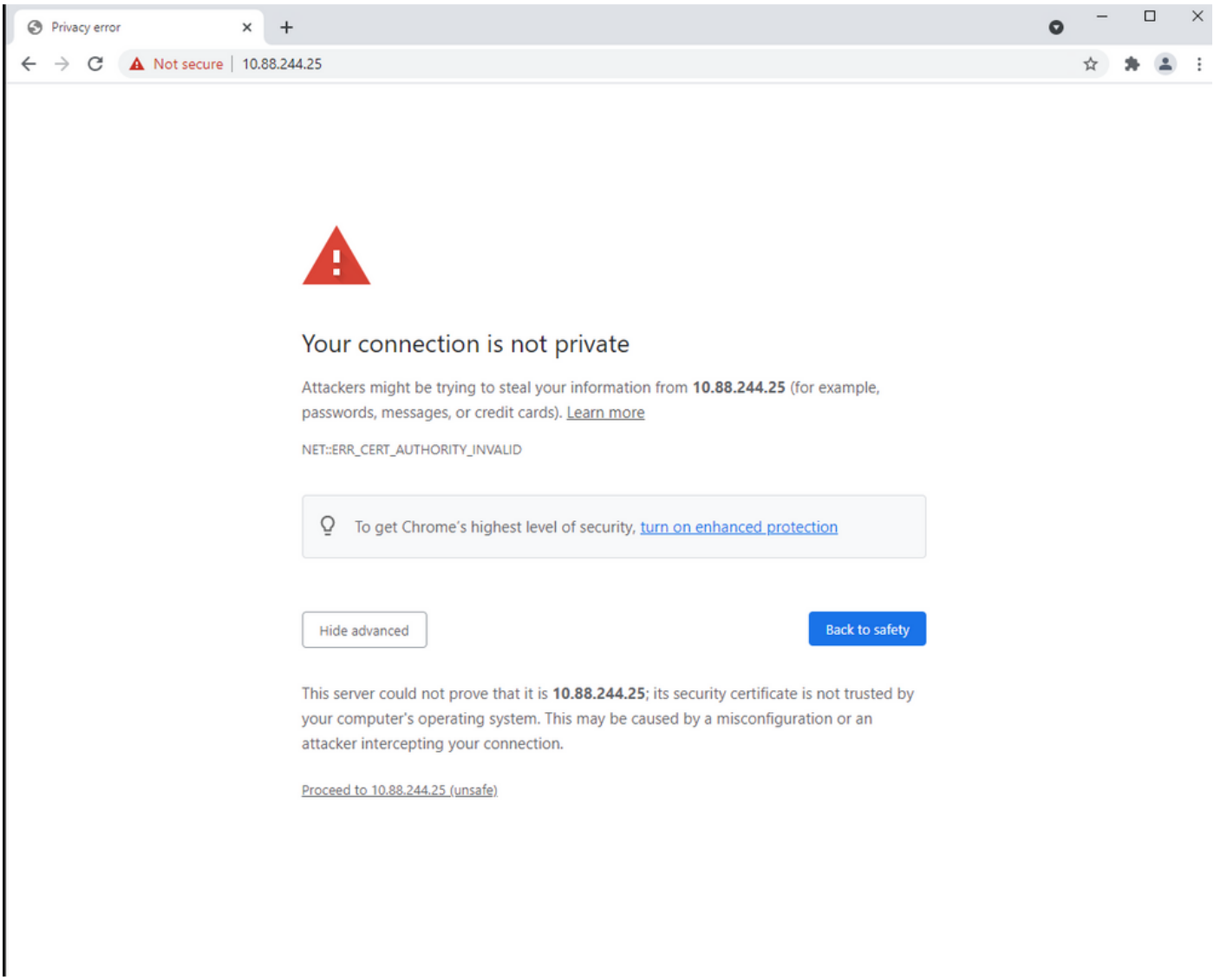
セキュアなプライベート接続を実現するには、セキュリティ証明書を取得する必要があります。証明書は認証局(CA)によって発行されます。これにより、vManageドメインが実際に組織に属していることを確認する手順が実行されます。

ユーザがvManageにアクセスすると、ユーザPCはHTTPS接続を実行し、SSL証明書がインストールされたvManageサーバとコンピュータの間に安全なトンネルが確立されて認証が行われます。SSL証明書の認証は、デバイスにインストールされている有効なルートCAのデータベースに対してユーザコンピュータで実行されます。通常、コンピュータには、Google、GoDaddy、エンタープライズCA（この場合）、およびより多くのパブリックエンティティのような複数のCAがすでにインストールされています。したがって、証明書署名要求(CSR)がGoddady（単なる例）によって署名されている場合は、信頼されます。

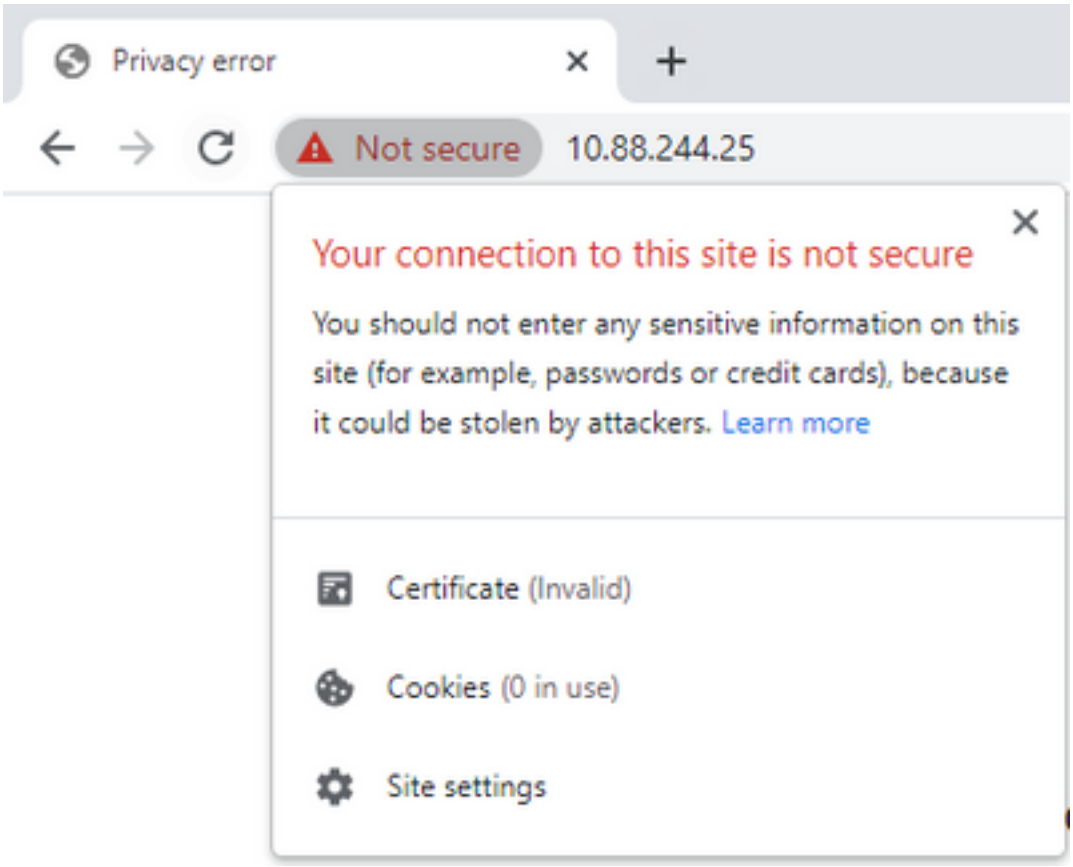
vManageの「Connection Is Not private」メッセージ

vManage自己署名証明書がCAによって署名されていない。これは同じvManageによって署名されており、パブリックCAでもプライベートCAでも署名されていないため、PCクライアントに対して信頼されません。このため、ブラウザにvManage URLの非セキュア/プライバシーエラー接続が表示されます。

図に示すように、Google Chromeブラウザによるデフォルトの自己署名証明書を使用したvManageエラーの例。



注：サイト情報の表示オプションをクリックすると、証明書が無効として表示されます。



プロアクティブな情報

不正なWebサイト名に登録された証明書

サイトがサービスするすべてのホスト名に対してWeb証明書が取得されていることを確認します。たとえば、証明書が架空のドメインwwwのみをカバーしている場合です。vManage-example-testcom。vManage-example-testを使用してサイトをロードするビジター。com（wwwなし）プレフィクスを使用してIPアドレスを設定し、パブリックCAによって署名付き証明書を取得します。信頼できますが、証明書名の不一致エラーを含む別のエラーが発生します。

> **注**：SSL/TLS証明書の共通名がブラウザのドメインまたはアドレスバーと一致しない場合、共通名の不一致エラーが発生します。

関連情報

- CSRデコーダ
- 証明書署名要求の生成
- テクニカル サポートとドキュメント – Cisco Systems