9800 WLCでの証明書およびトラストポイントのタイプの理解

内容

概要

このドキュメントでは、9800 WLCで使用できるさまざまな種類の証明書とトラストポイントについて説明します。

前提条件

要件

次の項目に関する基本的な知識があることが推奨されます。

- Cisco Wireless LAN Controller(WLC)9800シリーズ
- デジタル証明書、認証局(CA)、および公開キーインフラストラクチャ(PKI)

使用するコンポーネント

このドキュメントは、特定のハードウェアまたはソフトウェア バージョンに限定されるものではありません。

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、クリアな（デフォルト）設定で作業を開始しています。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。

証明書

証明書とは

証明書は、デバイスを識別する一意のドキュメントです。たとえば、デバイスが正規のデバイスであることを確認するために使用されます。IDを検証するには、証明書をCAが検証する必要があります。

9800での証明書のタイプ

アクセスポイント(AP)とWLCは、互いのIDを検証する何らかの方法を必要とします。新しいAPがWLCに加入するたびに、APはWLCの証明書を検証して、それが正当なものであるだけでなく、有効であることを確認します。これにより、APは初めて参加するアプライアンスを信頼できます。

製造元でインストールされた証明書(MIC)

この証明書は、9800-80、9800-40、9800-Lなどの物理アプライアンスにデフォルトでインストールされます。その名前が示すように、出荷時にインストールされており、変更できません。この証明書は、APがWLCに初めて加入するときに使用されます。

MIC証明書が実際に9800にインストールされているかどうかを確認するには、show wireless management trustpointコマンドを入力します。

```
<#root>

9800#show wireless management trustpoint
Trustpoint Name  : CISCO_IDEVID_SUDI
Certificate Info : Available

Certificate Type : MIC <--

Private key Info : Available
FIPS suitability : Not Applicable
```

自己署名証明書（SSC）

コントローラの仮想インスタンスである9800-CLには、工場出荷時にインストールされた証明書はありません。むしろ、Day 0ウィザードまたは証明書を手動で作成するスクリプトを使用して自動的に生成できる自己署名証明書を使用します。9800の仮想インスタンスでは、SSCは主にAPへの加入に使用されますが、すべてのHTTP(s)、SSH、およびNETCONFサービスにも使用されます。物理アプライアンスにもSSCが含まれていますが、前述のように、APの加入には使用されず、代わりにサービスに使用されます。

9800のSSC証明書を確認するには、show wireless management trustpointコマンドを入力します。

```
<#root>
```

```
9800#show wireless management trustpoint
Trustpoint Name  : 9800-CL-TRUSTPOINT
Certificate Info : Available

Certificate Type : SSC <--

Certificate Hash : e55e61b683181ff0999ef317bb5ec7950ab86c9e
Private key Info : Available
FIPS suitability : Not Applicable
```

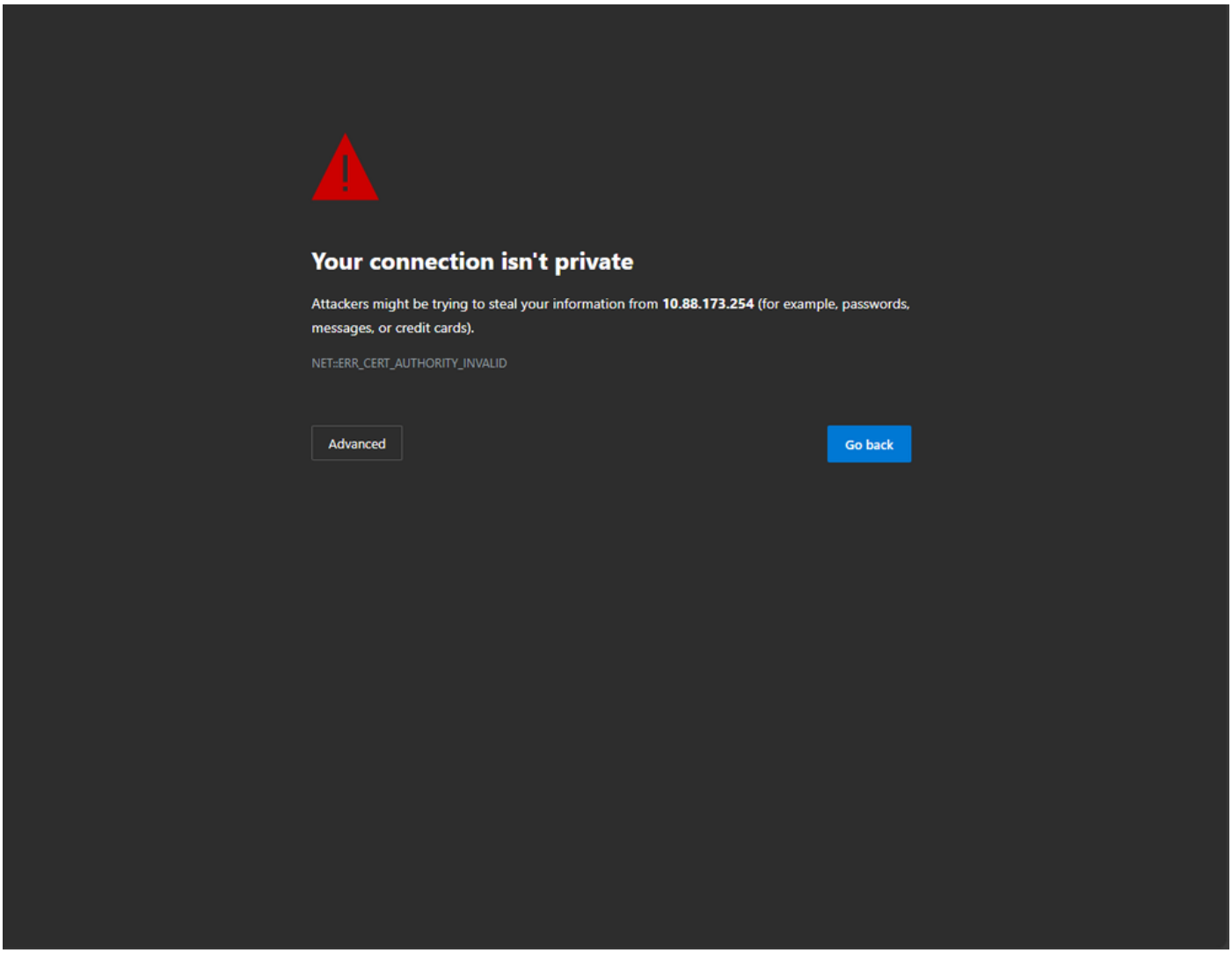
ローカルで有効な証明書(LSC)

これらの証明書は、WLCにアイデンティティを証明する必要があるAPでのみ使用されます。デフォルトでは、WLCにもAPにも存在しません。LSC証明書はCAによって署名され、後でWLCとAPの両方にインストールして、相互に検証する必要があります。9800でLSCを設定する方法の詳細については、『ローカルで有効な証明書』を参照してください。

トラストポイント

トラストポイントとは

トラストポイントは、証明書を特定のサービスにリンクするものです。トラストポイントには、Web管理とWeb認証の2つの主なタイプがあります。デフォルトでは、WLCは両方のサービスに自己署名証明書を使用しますが、これにより、サイトがセキュアでないことを示す警告メッセージがポップアップ表示されます。これは、自己署名証明書がどのCAによっても検証されていないためです。



WebページのCAの無効な警告メッセージ

これを回避するために、サードパーティ証明書を使用して、CAによってすでに検証されていることを確認できます。証明書を生成してWLCにアップロードする方法の詳細については、「Catalyst 9800 WLCでのCSR証明書の生成とダウンロード」を参照してください。

Web管理

Web管理のトラストポイントは、証明書をユーザグラフィカルユーザインターフェイス(GUI)にリンクします。コントローラは使用可能な証明書の1つを選択し、WLCにアップロードされたカスタム証明書がない場合は、自己署名証明書が使用されます。デフォルトの証明書を使用しない場合は、トラストポイントにカスタム証明書を使用できます。

上記のドキュメントに従って証明書が9800にアップロードされたら、次の手順はトラストポイントをWeb管理にリンクすることです。次のコマンドを入力する必要があります。

```
configure terminal
ip http secure-trustpoint <custom-cert>.pfx
!Restart HTTP services
no ip http secure services
ip http secure services
```

```
end
write
```

新しくインストールした証明書を検証する1つの方法が、HTTPサービスのトラストポイントとして使用されています。たとえば、次のコマンドを入力します。 show ip http server status | トラストポイントを含む

<#root>

```
9800#show ip http server status | include trustpoint
```

HTTP secure server trustpoint:

.pfx <-- trustpoint configured for HTTP services

```
HTTP secure server peer validation trustpoint:
```

Web 認証

Web管理と同様に、9800でもレイヤ3認証を使用できます。このトラストポイントは、ユーザに自動的に表示されるゲストポータルを介してWLANへの認証を試みるときに、ユーザに表示されるWebポータルに証明書をリンクします。Web認証にトラストポイントを使用すると、WLCと接続先のクライアント間のユーザクレデンシャルを保護するのに役立ちます。

デフォルトでは、WLCは自己署名証明書を使用します。ここでも、Webページが信頼できないことを示す警告メッセージがクライアントにポップアップ表示されます。これを回避するために、Web管理と同様にサードパーティの証明書を使用できます。

Web管理と同様に、カスタム証明書がWLCにアップロードされたら、トラストポイントとしてWebパラメータマップにリンクする必要があります。

```
configure terminal
parameter-map type webauth global
trustpoint <custom-cert>
!Restart HTTP services
no ip http secure services
ip http secure services
end
```

```
write
```

Web認証に使用されるトラストポイントを検証するには、次のコマンドを入力します

<#root>

```
show run | section parameter-map type webauth global
parameter-map type webauth global
type webauth
virtual-ip ipv4 192.0.2.1
```

trustpoint

<-- trustpoint configured for web authentication

関連情報

- ローカルで有効な証明書
- Catalyst 9800 WLCでのCSR証明書の生成とダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。