了解9800 WLC上的证书和信任点类型

目录

简介

先决条件

- 要求
- 使用的组件

证书

- 什么是证书？
- 9800上的证书类型

信任点

- 什么是信任点？

相关信息

简介

本文档介绍可在9800 WLC上使用的不同类型的证书和信任点。

先决条件

要求

思科建议您掌握以下方面的基本知识：

- 思科无线局域网控制器(WLC)9800系列
- 数字证书、证书颁发机构(CA)以及公钥基础设施(PKI)

使用的组件

本文档不限于特定硬件或软件版本。

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。

证书

什么是证书？

证书是标识设备以确保其合法性的唯一文档。证书必须由证书颁发机构(CA)验证才能验证身份。

9800上的证书类型

接入点(AP)和WLC需要验证每个身份的方法。当新的AP加入WLC时，AP会验证WLC证书，以确保其不仅合法而且仍然有效。这样，AP可以信任它们第一次加入的设备。

制造商安装证书(MIC)

默认情况下，此证书安装在物理设备上，例如9800-80、9800-40和9800-L。顾名思义，它是出厂预装的，不能修改。当AP首次加入WLC时使用此证书。

要检查9800上是否安装了MIC证书，可以运行show wireless management trustpoint命令。

<#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
```

自签证书 (SSC)

对于控制器的虚拟实例9800-CL，没有出厂安装的证书。它使用可以通过Day 0向导自动生成的自签名证书，或者通过手动创建证书的脚本自动生成。在9800的虚拟实例中，SSC主要用于AP加入，但也用于所有HTTP(s)、SSH和NETCONF服务。

物理设备也包含SSC，但如前所述，它不用于AP加入，而是用于服务。要检查9800上的SSC证书，请运行show wireless management trustpoint命令。

<#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

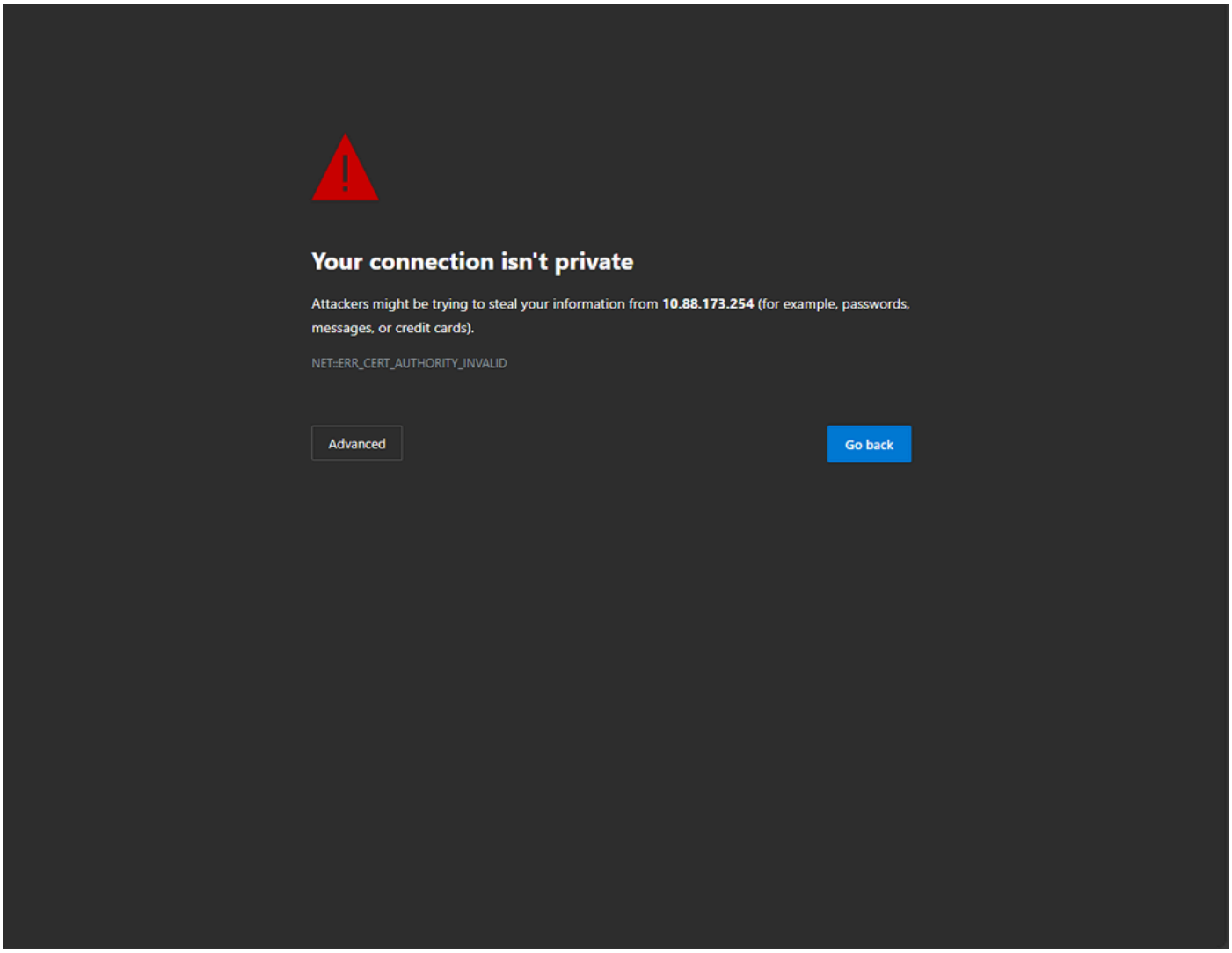
本地重要证书(LSC)

这些证书仅供AP使用，AP必须向WLC证明其身份。默认情况下，它们在WLC或AP上不存在。LSC证书必须由CA签署，之后安装在WLC和AP上，才能相互验证。有关如何在9800上配置LSC的详细信息，请参阅本地重要证书。

信任点

什么是信任点？

信任点将证书链接到特定服务。信任点主要有两种类型：web管理和web身份验证。默认情况下，WLC对两种服务使用自签名证书，但是，这会导致弹出一条警告消息，说明站点不安全。这是因为自签名证书尚未由CA验证。



网页上的CA无效警告消息

为避免这种情况，可使用第三方证书确保已由CA验证。有关如何生成证书并将其上传到WLC的详细信息，请参阅[在Catalyst 9800 WLC上生成和下载CSR证书]。

Web管理

Web管理的信任点将证书链接到用户图形用户界面(GUI)。 控制器选择其可用证书之一，如果没有上传到WLC的自定义证书，则使用自签名证书。如果不想使用默认证书，则可以将自定义证书用于信任点。

根据上面的文档，证书上传到9800后，下一步是将信任点链接到Web管理。运行下一个命令：

```
configure terminal
ip http secure-trustpoint <custom-cert>.pfx
```

```
!Restart HTTP services
no ip http secure services
ip http secure services
end
write
```

验证新安装的证书的一种方法现在正被用作HTTP服务的信任点。例如，运行show ip http server status | include trustpoint命令：

<#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 身份验证

与Web管理类似，9800上也可以使用第3层身份验证。此信任点将证书链接到Web门户，当用户尝试通过自动呈现给用户的访客门户向WLAN进行身份验证时，该Web门户向用户显示。使用信任点进行Web身份验证可保护WLC和客户端连接到的客户端之间的用户凭证。

默认情况下，WLC使用自签名证书。同样，这会导致客户端弹出警告消息，说明该网页不受信任。为避免这种情况，可以像Web管理一样使用第三方证书。

与Web管理类似，一旦自定义证书上传到WLC，它必须作为信任点链接到Web参数映射。

```
configure terminal
parameter-map type webauth global
trustpoint <custom-cert>
!Restart HTTP services
```

```
no ip http secure services
ip http secure services
end
write
```

要验证用于Web身份验证的信任点，请运行以下命令：

<#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
```

自动证书续订

出于安全原因，趋势是证书的生存期始终较短。这可能会导致定期更新证书时需要额外维护。可以使用SCEP或EST自动续订AP和WLC证书（请参阅参考部分中的相关指南）。

相关信息

- 本地重要证书
- 在Catalyst 9800 WLC上生成和下载CSR证书
- 在9800上配置信任点
- 9800上使用EST自动证书续订
- 为AP上的802.1X配置LSC

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。