瞭解9800 WLC上的憑證和信任點型別

目錄

簡介

本檔案介紹可在9800 WLC上使用的不同型別的憑證和信任點。

必要條件

需求

思科建議您瞭解以下基本知識：

- 思科無線LAN控制器(WLC)9800系列
- 數位憑證、憑證授權單位(CA)以及公開金鑰基礎架構(PKI)

採用元件

本檔案所述內容不限於特定硬體或軟體版本。

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。

憑證

什麼是證書？

證書是標識裝置的唯一文檔，例如，用於確保裝置是合法的。證書必須由CA驗證才能驗證所述身份。

9800上的憑證型別

存取點(AP)和WLC需要某種方式驗證彼此的身分。每當新AP加入WLC時，AP都會驗證WLC的證書，以確保其不僅合法而且仍然有效。這樣，AP可以信任其首次加入的裝置。

製造商安裝證書(MIC)

預設情況下，此證書安裝在物理裝置（例如9800-80、9800-40和9800-L）上。顧名思義，它是出廠安裝的，不能修改。此憑證用於AP首次加入WLC時。

要檢查9800上是否確實安裝了MIC證書，可以輸入命令show wireless management trustpoint。

<#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

自簽名證書(SSC)

對於控制器9800-CL的虛擬例項，沒有出廠安裝的證書。而是使用自簽名證書，該證書可以通過Day 0嚮導自動生成，也可以通過手動建立證書的指令碼生成。在9800的虛擬例項中，SSC主要用於AP加入，也用於所有HTTP(s)、SSH和NETCONF服務。物理裝置也包含SSC，但如前所述，它不用於AP加入，而是用於服務。

要再次檢查9800上的SSC證書，請輸入命令show wireless management trustpoint。

<#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

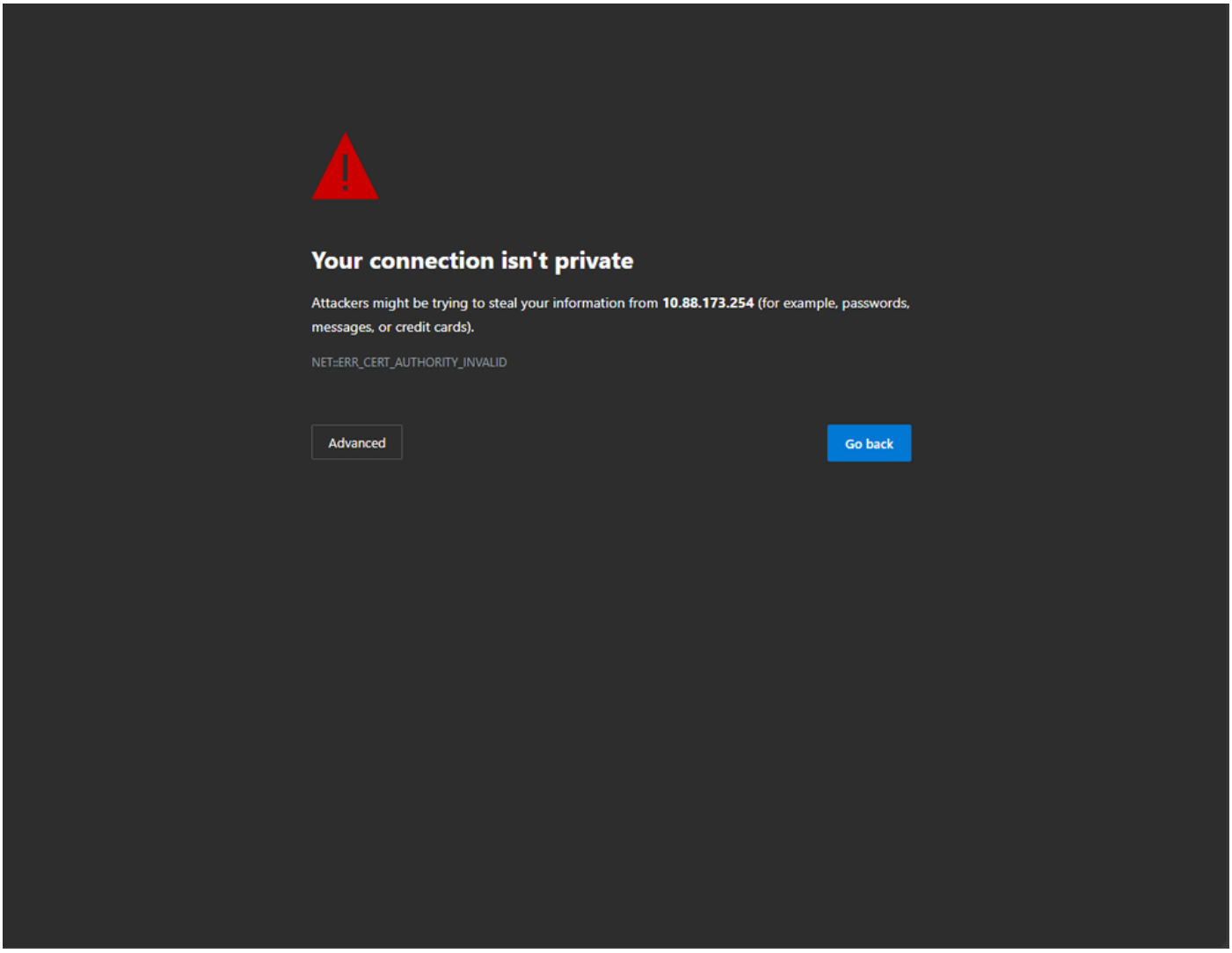
本地重要證書(LSC)

這些憑證僅由需要向WLC證明其身分的AP使用。預設情況下，WLC和AP上都不存在。LSC憑證需要由CA簽署，並於稍後安裝在WLC和AP上，才能互相驗證。有關如何在9800上配置LSC的詳細資訊，請參閱本地重要證書。

信任點

什麼是信任點？

信任點將證書連結到特定服務。信任點主要有兩種型別：Web管理和Web身份驗證。預設情況下，WLC對兩項服務都使用自簽名證書，但這會導致彈出一條警告消息，說明該站點不安全。這是因為自簽名證書尚未由任何CA驗證。



網頁上的CA無效警告消息

為了避免此問題，可以使用第三方憑證，確保該憑證已由CA驗證。有關如何產生憑證並將其上傳到WLC的詳細資訊，請參閱在Catalyst 9800 WLC上產生和下載CSR憑證。

Web管理

Web管理的信任點將證書連結到使用者圖形使用者介面(graphical user interface， GUI)。控制器會選擇其中一個可用憑證，如果沒有將自訂憑證上傳到WLC，則會使用自簽名的憑證。如果預設證書不是您要使用的證書，則可以為信任點使用自定義證書。

根據上面的文檔，證書上傳到9800後，下一步是將信任點連結到Web管理，需要輸入以下命令：

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

驗證新安裝的證書的一種方法現在正被用作HTTP服務的信任點，例如，輸入命令 show ip http server status | 包括信任點

<#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驗證

與Web管理類似，9800上也可使用第3層驗證。此信任點將證書連結到Web門戶，當使用者嘗試通過自動呈現給使用者的訪客門戶向WLAN進行身份驗證時，該Web門戶向使用者顯示。使用信任點進行Web驗證有助於保護WLC和所連線的客戶端之間的使用者憑證。

預設情況下，WLC使用自簽名的憑證。同樣，這會導致客戶端彈出一條警告消息，說明該網頁不受信任。為了避免此問題，第三方證書可與Web管理一起使用。

與Web管理類似，自訂憑證上傳到WLC後，必須將其作為trustpoint連結到Web引數映像。

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

```
end
write
```

要驗證用於Web驗證的信任點，請輸入下一個命令

<#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

相關資訊

- 具有本地意義的證書
- 在Catalyst 9800 WLC上產生和下載CSR憑證

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）。