Kenntnis der Zertifikat- und Vertrauenspunkttypen auf dem 9800 WLC

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Zertifikate](#)
[Was ist ein Zertifikat?](#)
[Zertifikattypen auf dem 9800](#)
[Vertrauenspunkte](#)
[Was ist ein Trustpoint?](#)
[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die verschiedenen Typen von Zertifikaten und Vertrauenspunkten beschrieben, die auf dem 9800 WLC verwendet werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Grundkenntnisse in folgenden Bereichen verfügen:

- Cisco Wireless LAN Controller (WLC) der Serie 9800
- Digitale Zertifikate, Zertifizierungsstellen (Certificate Authorities, CAs) und die Public Key Infrastructure (PKI)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Hardware- oder Softwareversionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Zertifikate

Was ist ein Zertifikat?

Ein Zertifikat ist ein eindeutiges Dokument, das ein Gerät identifiziert, um beispielsweise dessen Legitimität sicherzustellen. Ein Zertifikat muss von einer Zertifizierungsstelle überprüft werden, um die Identität zu validieren.

Zertifikattypen auf dem 9800

Access Points (APs) und der WLC müssen irgendwie die Identität des jeweils anderen validieren können. Wenn ein neuer WAP dem WLC beitritt, validiert der WAP das WLC-Zertifikat, um sicherzustellen, dass es nicht nur legitim, sondern auch noch gültig ist. Auf diese Weise können APs der Appliance vertrauen, der sie zum ersten Mal überhaupt beitreten.

MIC (Manufacturer Installed Certificate)

Dieses Zertifikat wird standardmäßig auf den physischen Appliances installiert, z. B. 9800-80, 9800-40 und 9800-L. Wie der Name schon sagt, ist es werkseitig installiert und kann nicht geändert werden. Dieses Zertifikat wird verwendet, wenn der WAP zum ersten Mal dem WLC beitritt.

Um zu überprüfen, ob auf dem 9800 tatsächlich ein MIC-Zertifikat installiert ist, können Sie den Befehl show wireless management trustpoint eingeben.

<#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
```

Selbstsigniertes Zertifikat (SSC)

Für die virtuelle Instanz des Controllers, 9800-CL, ist kein werkseitig installiertes Zertifikat vorhanden. Stattdessen wird ein selbstsigniertes Zertifikat verwendet, das automatisch über den Day-0-Assistenten oder über ein Skript generiert werden kann, in dem das Zertifikat manuell erstellt wird. In virtuellen Instanzen des 9800 wird der SSC hauptsächlich für den AP-Beitritt, aber auch für alle HTTP(s)-, SSH- und NETCONF-Dienste verwendet. Physische Appliances enthalten auch eine SSC, die jedoch, wie bereits erwähnt, nicht für den AP-Beitritt verwendet wird, sondern für die Services.

Um das SSC-Zertifikat auf dem 9800 zu überprüfen, geben Sie den Befehl show wireless management trustpoint ein.

<#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

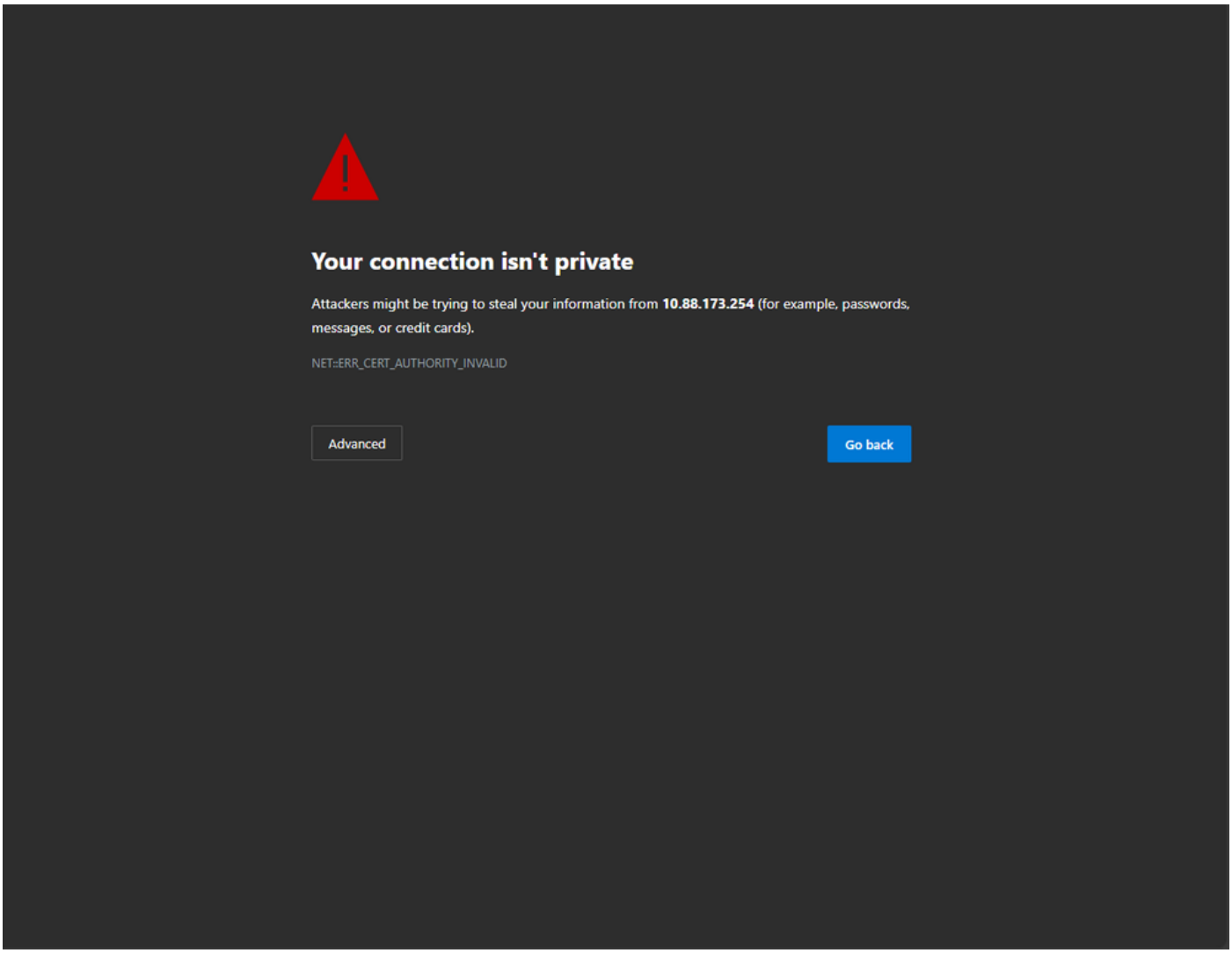
LSC (Locally Signed Certificate)

Diese Zertifikate werden ausschließlich von APs verwendet, die dem WLC ihre Identität nachweisen müssen. Sie sind standardmäßig weder auf dem WLC noch auf den APs vorhanden. Die LSC-Zertifikate müssen von einer Zertifizierungsstelle signiert und später sowohl auf dem WLC als auch auf den APs installiert werden, um sich gegenseitig zu validieren. Weitere Informationen zum Konfigurieren von LSCs auf dem 9800 finden Sie unter Lokal relevante Zertifikate.

Vertrauenspunkte

Was ist ein Trustpoint?

Ein Vertrauenspunkt ist, was ein Zertifikat mit einem bestimmten Dienst verknüpft. Es gibt zwei Haupttypen von Vertrauenspunkten: Webverwaltung und Webauthentifizierung. Standardmäßig verwendet der WLC das selbstsignierte Zertifikat für beide Dienste. Dies führt jedoch zu einer Warnmeldung, die besagt, dass die Website nicht sicher ist. Dies liegt daran, dass das selbstsignierte Zertifikat von keiner Zertifizierungsstelle validiert wurde.



Ungültige CA-Warnmeldung auf Webseite

Um dies zu vermeiden, kann ein Drittanbieterzertifikat verwendet werden, das sicherstellt, dass es bereits von einer Zertifizierungsstelle validiert wurde. Weitere Informationen zum Generieren und Hochladen eines Zertifikats auf den WLC finden Sie unter Generate and Download CSR Certificate on Catalyst 9800 WLCs.

Webverwaltung

Der Vertrauenspunkt für die Webverwaltung verknüpft das Zertifikat mit der grafischen Benutzeroberfläche (GUI). Der Controller wählt eines seiner verfügbaren Zertifikate aus, und wenn kein benutzerdefiniertes Zertifikat in den WLC hochgeladen wurde, wird das selbstsignierte Zertifikat verwendet. Wenn Sie das Standardzertifikat nicht verwenden möchten, können Sie ein benutzerdefiniertes Zertifikat für den Vertrauenspunkt verwenden.

Nach dem Hochladen des Zertifikats auf den 9800 (siehe Dokument oben) besteht der nächste Schritt darin, den Vertrauenspunkt mit der Webverwaltung zu verknüpfen. Die nächsten Befehle müssen eingegeben werden:

```
configure terminal
```

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

Eine Möglichkeit zur Validierung des neu installierten Zertifikats besteht nun darin, als Vertrauenspunkt für HTTP-Dienste zu fungieren. Geben Sie beispielsweise den Befehl show ip http server status | Vertrauenspunkt einschließen

<#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:
```

Webauthentifizierung

Ähnlich wie bei der Webverwaltung kann auch beim 9800 die Layer-3-Authentifizierung verwendet werden. Dieser Vertrauenspunkt verknüpft ein Zertifikat mit einem Webportal, das einem Benutzer angezeigt wird, wenn er versucht, sich über ein Gastportal, das dem Benutzer automatisch angezeigt wird, bei einem WLAN zu authentifizieren. Die Verwendung eines Vertrauenspunkts für die Webauthentifizierung trägt zum Schutz der Benutzeranmeldeinformationen zwischen dem WLC und dem Client bei, der eine Verbindung herstellt.

Standardmäßig verwendet der WLC das selbstsignierte Zertifikat. Auch hier wird eine Warnmeldung für den Client angezeigt, die besagt, dass die Webseite nicht vertrauenswürdig ist. Um dies zu vermeiden, kann wie bei der Webverwaltung ein Zertifikat von einem Drittanbieter verwendet werden.

Ähnlich wie bei der Webverwaltung muss das benutzerdefinierte Zertifikat, nachdem es in den WLC hochgeladen wurde, als Vertrauenspunkt mit der Webparamater-Map verknüpft werden.

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

Um den für die Webauthentifizierung verwendeten Vertrauenspunkt zu validieren, geben Sie den nächsten Befehl ein.

<#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

Zugehörige Informationen

- Lokal relevante Zertifikate
- Erstellen und Herunterladen eines CSR-Zertifikats auf Catalyst 9800 WLCs

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.