Comprendre les types de certificat et de point de confiance sur le WLC 9800

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Certificats

- Qu'est-ce qu'un certificat ?
- Types de certificats sur le 9800

Points de confiance

- Qu'est-ce qu'un Trustpoint ?

Informations connexes

Introduction

Ce document décrit les différents types de certificats et de points de confiance qui peuvent être utilisés sur le WLC 9800.

Conditions préalables

Exigences

Cisco vous recommande d'avoir des connaissances de base sur :

- Contrôleur LAN sans fil Cisco (WLC) série 9800
- Certificats numériques, autorités de certification (CA) et infrastructure à clé publique (PKI)

Composants utilisés

Ce document n'est pas limité à des versions matérielles ou logicielles spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Certificats

Qu'est-ce qu'un certificat ?

Un certificat est un document unique qui identifie un périphérique pour s'assurer qu'il est légitime. Un certificat doit être vérifié par une autorité de certification (CA) pour valider l'identité.

Types de certificats sur le 9800

Les points d'accès (AP) et le WLC nécessitent un moyen de valider chaque identité. Lorsqu'un nouvel AP rejoint le WLC, l'AP valide le certificat des WLC pour s'assurer qu'il est non seulement légitime, mais qu'il est toujours valide. De cette façon, les AP peuvent faire confiance à l'appliance qu'ils rejoignent pour la première fois.

Certificat installé par le fabricant (MIC)

Ce certificat est installé par défaut sur les appareils physiques, tels que les modèles 9800-80, 9800-40 et 9800-L. Comme son nom l'indique, il est installé en usine et ne peut pas être modifié. Ce certificat est utilisé lorsque l'AP se connecte pour la première fois au WLC.

Pour vérifier si un certificat MIC est installé sur le 9800, vous pouvez exécuter la commande 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
```

Certificat auto-signé (SSC)

Pour l'instance virtuelle du contrôleur, le 9800-CL, il n'y a aucun certificat installé en usine. Il utilise un certificat auto-signé qui peut être généré automatiquement via l'assistant Jour 0 ou via un script dans lequel le certificat est créé manuellement. Dans l'instance virtuelle du 9800, le SSC est utilisé principalement pour la jonction AP, mais aussi pour tous les services HTTP(s), SSH et NETCONF.

Les appareils physiques contiennent également un SSC, cependant, comme indiqué précédemment, il n'est pas utilisé pour la jonction AP, mais pour les services à la place. Pour vérifier le certificat SSC sur le 9800, exécutez la commande 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
```

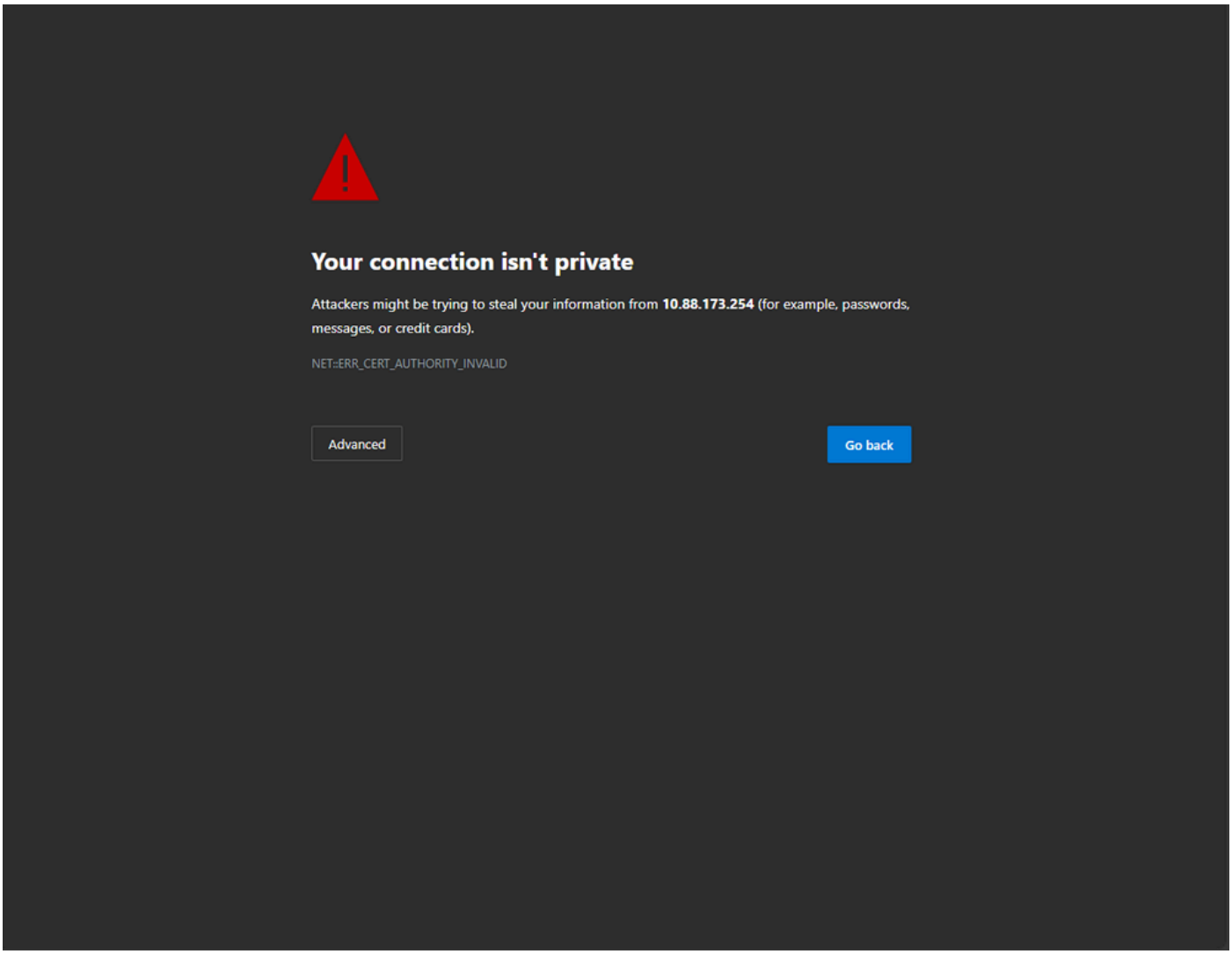
Certificat significatif localement (LSC)

Ces certificats sont uniquement utilisés par les AP qui doivent prouver leur identité au WLC. Ils n'existent pas par défaut sur le WLC ou les AP. Les certificats LSC doivent être signés par une autorité de certification, puis installés sur le WLC et les points d'accès pour s'assurer mutuellement une validation mutuelle. Pour plus d'informations sur la façon de configurer des LSC sur le 9800, référez-vous à Certificats significatifs localement.

Points de confiance

Qu'est-ce qu'un Trustpoint ?

Un point de confiance lie un certificat à un service spécifique. Il existe deux principaux types de points de confiance : administration web et authentification web. Par défaut, le WLC utilise le certificat auto-signé pour les deux services, cependant, cela entraîne un message d'avertissement indiquant que le site n'est pas sécurisé. Cela est dû au fait que le certificat auto-signé n'a pas été validé par une autorité de certification.



Message d'avertissement CA non valide sur la page Web

Pour éviter cela, un certificat tiers peut être utilisé pour s'assurer qu'il a été validé par une autorité de certification. Pour plus d'informations sur la façon de générer et télécharger un certificat sur le WLC, référez-vous à Générer et télécharger un certificat CSR sur les WLC Catalyst 9800.

Administration Web

Le point de confiance pour l'administration Web lie le certificat à l'interface utilisateur graphique (GUI). Le contrôleur sélectionne l'un de ses certificats disponibles et, s'il n'y a aucun certificat personnalisé téléchargé sur le WLC, le certificat auto-signé est utilisé. Si vous ne souhaitez pas utiliser le certificat par défaut, vous pouvez utiliser un certificat personnalisé pour le point de confiance.

Une fois le certificat téléchargé sur le 9800, conformément au document ci-dessus, l'étape suivante consiste à lier le point de confiance à l'administration Web. Exécuter la commande suivante :

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

Un moyen de valider le certificat nouvellement installé est maintenant utilisé comme point de confiance pour les services HTTP. Par exemple, exécutez show ip http server status | include trustpoint, commande :

<#root>

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

HTTP secure server trustpoint: <trustpoint>.pfx <-- trustpoint configured for HTTP services


HTTP secure server peer validation trustpoint:
```

Authentification Web

Comme pour l'administration Web, l'authentification de couche 3 peut également être utilisée sur le 9800. Ce point de confiance lie un certificat à un portail Web qui est affiché à un utilisateur lorsqu'il tente de s'authentifier auprès d'un WLAN via un portail invité qui est automatiquement présenté à l'utilisateur. L'utilisation d'un point de confiance pour l'authentification Web protège les

informations d'identification utilisateur entre le WLC et le client auquel se connecte.

Par défaut, le WLC utilise le certificat auto-signé. Là encore, un message d'avertissement s'affiche sur le client pour indiquer que la page Web n'est pas approuvée. Pour éviter cela, un certificat tiers peut être utilisé comme l'administration Web.

Comme pour l'administration Web, une fois que le certificat personnalisé est téléchargé sur le WLC, il doit être lié à la carte de paramètre Web en tant que point de confiance.

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

Pour valider le point de confiance utilisé pour l'authentification Web, exécutez la commande suivante :

<#root>

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

trustpoint <custom-trustpoint> <-- trustpoint configured for web authentication
```

Renouvellement automatique des certificats

La tendance est de toujours avoir des durées de vie plus courtes dans les certificats pour des raisons de sécurité. Cela peut entraîner une maintenance supplémentaire lors du renouvellement régulier des certificats. Les certificats AP et WLC peuvent être renouvelés automatiquement à l'aide de SCEP ou EST (voir les guides pertinents dans la section de référence).

Informations connexes

- Certificats valables localement
- Générer et télécharger un certificat CSR sur les WLC Catalyst 9800
- Configuration des points de confiance sur le 9800
- Renouvellement automatique des certificats avec EST sur le 9800
- Configurer LSC pour 802.1X sur les points d'accès

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.