Comprensión de los tipos de certificado y de punto de confianza en el WLC 9800

Contenido

Introducción

Este documento describe los diferentes tipos de certificados y puntos de confianza que se pueden utilizar en el WLC 9800.

Prerequisites

Requirements

Cisco recomienda tener conocimientos básicos sobre:

- Cisco Wireless LAN Controller (WLC) serie 9800
- Certificados digitales, autoridades de certificación (CA) y la infraestructura de clave pública (PKI)

Componentes Utilizados

Este documento no se limita a versiones específicas de hardware o software.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Certificados

¿Qué es un certificado?

Un certificado es un documento único que identifica un dispositivo, por ejemplo, para garantizar que es legítimo. Una CA debe verificar un certificado para validar dicha identidad.

Tipos de certificados en el 9800

Los puntos de acceso (AP) y el WLC necesitan algún tipo de forma de validar la identidad de cada uno. Cada vez que un nuevo AP se une al WLC, el AP valida el certificado del WLC para asegurarse de que no es solamente legítimo sino que sigue siendo válido. De esta manera, los AP pueden confiar en el dispositivo al que se están uniendo por primera vez.

Certificado instalado por el fabricante (MIC)

Este certificado se instala de forma predeterminada en los dispositivos físicos, como el 9800-80, 9800-40 y el 9800-L. Como su nombre indica, está instalado de fábrica y no se puede modificar. Este certificado se utiliza para cuando el AP se une por primera vez al WLC.

Para verificar si un certificado MIC está instalado en el 9800, puede ingresar el comando 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
```

Certificado de firma automática (SSC)

Para la instancia virtual del controlador, la 9800-CL, no hay ningún certificado instalado de fábrica. En su lugar, utiliza un certificado autofirmado que se puede generar automáticamente mediante el asistente de día 0 o mediante una secuencia de comandos en la que el certificado se crea manualmente. En las instancias virtuales del 9800, el SSC se utiliza principalmente para la unión de AP, pero también para todos los servicios HTTP(s), SSH y NETCONF. Los appliances físicos también contienen un SSC, pero, como se indicó anteriormente, no se utiliza para la unión de AP, sino para los servicios.

De nuevo, para verificar el certificado de SSC en el 9800, ingrese el comando 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
```

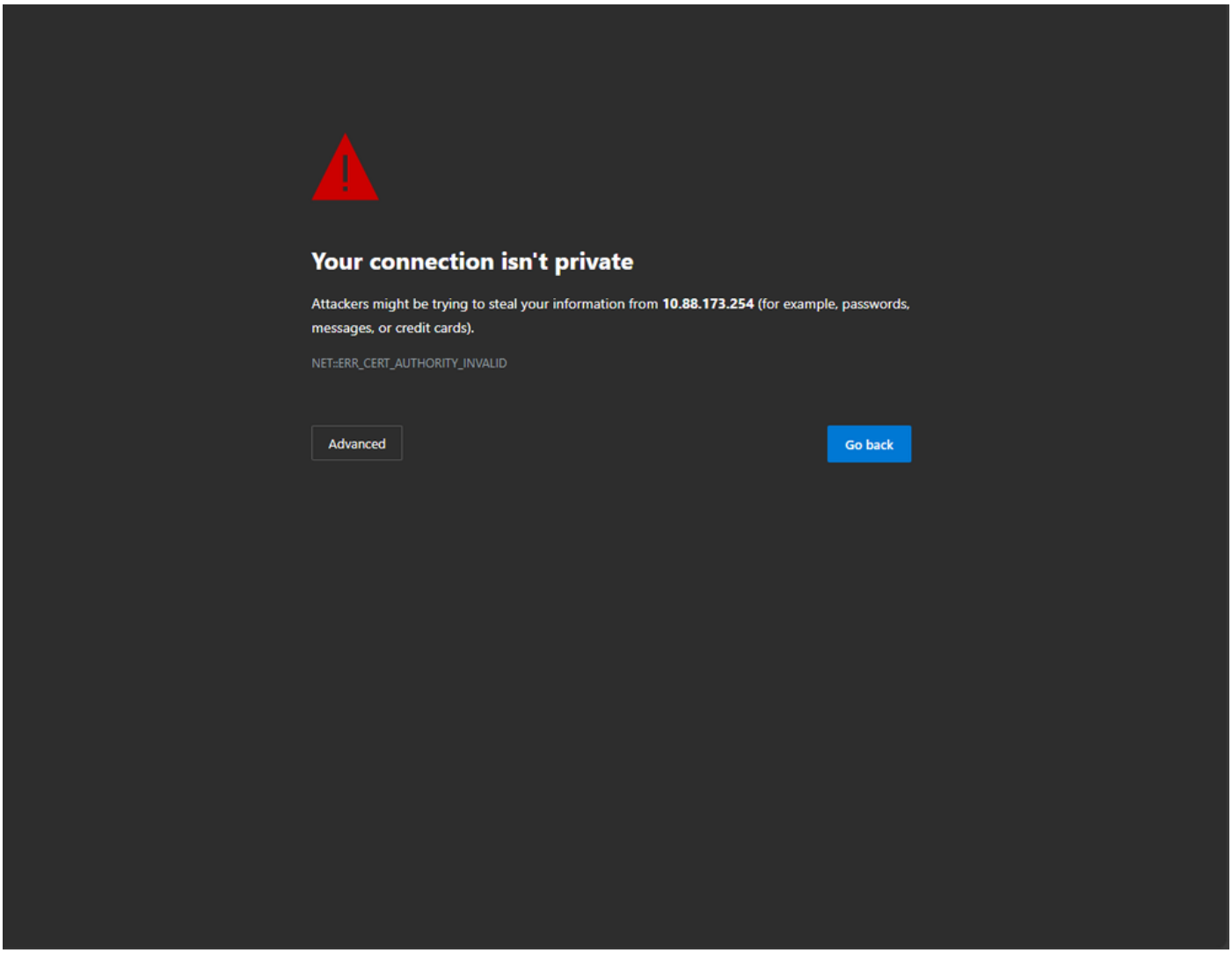
Certificado de importancia local (LSC)

Estos certificados son utilizados solamente por los AP que necesitan probar su identidad al WLC. No existen de forma predeterminada ni en el WLC ni en los AP. Los certificados LSC deben estar firmados por una CA y luego instalados en el WLC y los AP para que se validen mutuamente. Para obtener más información sobre cómo configurar los LSC en el 9800, consulte Certificados Significativos Localmente.

Puntos de confianza

¿Qué es un punto de confianza?

Un punto de confianza es lo que vincula un certificado a un servicio específico. Existen dos tipos principales de puntos de confianza: administración web y autenticación web. De forma predeterminada, el WLC utiliza el certificado autofirmado para ambos servicios, pero esto hace que aparezca un mensaje de advertencia que indica que el sitio no es seguro. Esto se debe a que el certificado autofirmado no ha sido validado por ninguna CA.



Mensaje de advertencia de CA no válida en la página web

Para evitar esto, se puede utilizar un certificado de terceros asegurándose de que ya ha sido validado por una CA. Para obtener más información sobre cómo generar y cargar en el WLC un certificado, consulte Generar y descargar el certificado CSR en los WLC Catalyst 9800.

Administración web

El punto de confianza para la administración web vincula el certificado a la interfaz gráfica de usuario (GUI) del usuario. El controlador selecciona uno de sus certificados disponibles y, si no hay ningún certificado personalizado cargado en el WLC, se utiliza el certificado autofirmado. Si el certificado predeterminado no es algo que desee utilizar, puede utilizar un certificado personalizado para el punto de confianza.

Una vez que el certificado se ha cargado en el 9800, según el documento anterior, el siguiente paso es vincular el punto de confianza a la administración web, se deben ingresar los siguientes comandos:

```
configure terminal
ip http secure-trustpoint <custom-cert>.pfx
!Restart HTTP services
```

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

Una forma de validar el certificado recién instalado se utiliza ahora como punto de confianza para los servicios HTTP; por ejemplo, introduzca el comando show ip http server status | incluir punto de confianza

<#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:

Autenticación Web

De forma similar a la administración web, la autenticación de capa 3 también se puede utilizar en el 9800. Este punto de confianza vincula un certificado a un portal web que se muestra a un usuario cuando intenta autenticarse en una WLAN a través de un portal de invitados que se presenta automáticamente al usuario. El uso de un punto de confianza para la autenticación Web ayuda a proteger las credenciales del usuario entre el WLC y el cliente que se está conectando a.

De forma predeterminada, el WLC utiliza el certificado autofirmado. De nuevo, esto hace que aparezca un mensaje de advertencia para el cliente que indica que la página web no es de confianza. Para evitar esto, se puede utilizar un certificado de terceros, al igual que con la administración web.

De manera similar a la administración web, una vez que el certificado personalizado se ha cargado en el WLC, se debe vincular al mapa de parámetro web como punto de confianza.

```
configure terminal
parameter-map type webauth global
```

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

Para validar el punto de confianza utilizado para la autenticación Web, introduzca el siguiente comando

<#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

Información Relacionada

- Certificados de significación local
- Generar y descargar certificado CSR en WLC Catalyst 9800

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).