Entender os tipos de certificado e pontos confiáveis na WLC 9800

Contents

Introdução

Este documento descreve os diferentes tipos de certificados e pontos confiáveis que podem ser usados no 9800 WLC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento básico de:

- Controladora de LAN sem fio (WLC) 9800 Series da Cisco
- Certificados Digitais, Autoridades de Certificação (CAs), bem como a Infraestrutura de Chave Pública (PKI)

Componentes Utilizados

Este documento não está restrito a versões específicas de hardware ou software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Certificados

O que é um certificado?

Um certificado é um documento exclusivo que identifica um dispositivo, por exemplo, para garantir sua legitimidade. Um certificado deve ser verificado por uma CA para validar essa identidade.

Tipos de certificados no 9800

Os pontos de acesso (APs) e a WLC precisam de algum tipo de maneira de validar a identidade um do outro. Sempre que um novo AP se une à WLC, o AP valida o certificado da WLC para garantir que ele não seja apenas legítimo, mas que ainda seja válido. Dessa forma, os APs podem confiar no dispositivo ao qual estão se juntando pela primeira vez.

Certificado instalado pelo fabricante (MIC)

Esse certificado é instalado por padrão nos dispositivos físicos, como o 9800-80, 9800-40 e o 9800-L. Como os nomes sugerem, ele é instalado na fábrica e não pode ser modificado. Esse certificado é usado para quando o AP ingressa pela primeira vez na WLC.

Para verificar se um certificado MIC está realmente instalado no 9800, você pode inserir o 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 autoassinado (SSC)

Para a instância virtual do controlador, o 9800-CL, não há certificado instalado de fábrica. Em vez disso, ele usa um certificado autoassinado que pode ser gerado automaticamente através do assistente Dia 0 ou através de um script no qual o certificado é criado manualmente. Em instâncias virtuais do 9800, o SSC é usado principalmente para junção de AP, mas também para todos os serviços HTTP(s), SSH e NETCONF. Os dispositivos físicos também contêm um SSC, mas, como dito antes, ele não é usado para junção de AP, mas para os serviços.

Novamente, para verificar o certificado SSC no 9800, insira o 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
```

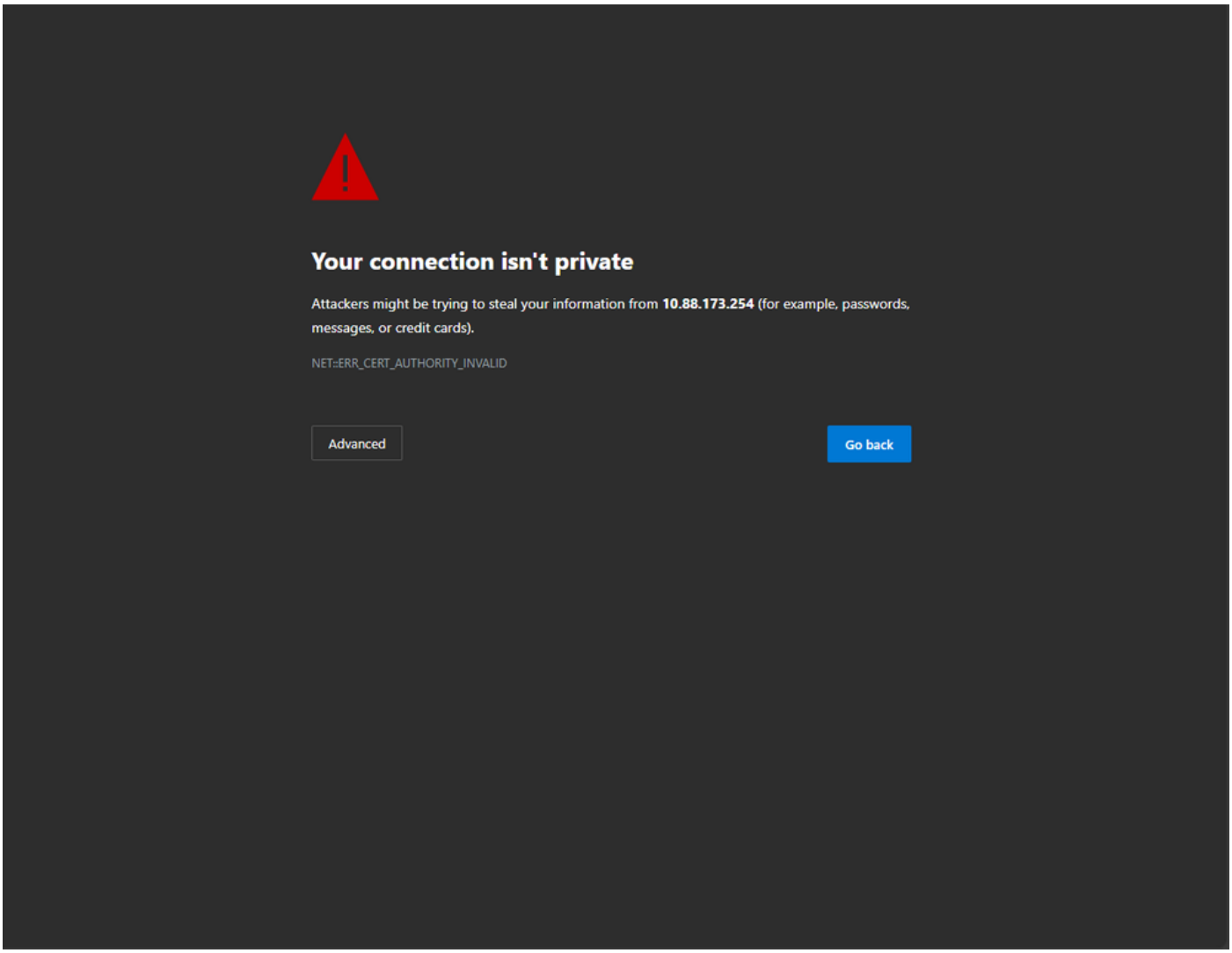
Certificado localmente significativo (LSC)

Esses certificados são usados somente por APs que precisam provar sua identidade para a WLC. Eles não existem por padrão nem na WLC nem nos APs. Os certificados LSC precisam ser assinados por uma CA e, posteriormente, instalados na WLC e nos APs para validar mutuamente um ao outro. Para obter mais informações sobre como configurar LSCs no 9800, consulte Locally Significant Certificates.

Pontos de confiança

O que é um ponto de confiança?

Um ponto confiável é o que vincula um certificado a um serviço específico. Há dois tipos principais de pontos de confiança: administração da Web e autenticação da Web. Por padrão, a WLC usa o certificado autoassinado para ambos os serviços, mas isso faz com que uma mensagem de aviso seja exibida, informando que o site não é seguro. Isso ocorre porque o certificado autoassinado não foi validado por nenhuma CA.



Mensagem de aviso inválida de autoridade de certificação na página da Web

Para evitar isso, um certificado de terceiros pode ser usado, certificando-se de que já foi validado por uma CA. Para obter mais informações sobre como gerar e fazer upload de um certificado para a WLC, consulte Gerar e fazer download do certificado CSR nas WLCs do Catalyst 9800.

Administração da Web

O ponto confiável para a administração da Web vincula o certificado à interface gráfica do usuário (GUI). O controlador seleciona um de seus certificados disponíveis e, se não houver nenhum certificado personalizado carregado para o WLC, o certificado autoassinado será usado. Se o certificado padrão não for algo que você deseja usar, você poderá usar um certificado personalizado para o ponto confiável.

Após o upload do certificado para o 9800, conforme o documento acima, a próxima etapa é vincular o ponto confiável à administração da Web. Os próximos comandos precisam ser inseridos:

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

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

Uma forma de validar o certificado recém-instalado está sendo usada como um ponto confiável para serviços HTTP, por exemplo, insira o comando show ip http server status | incluir trustpoint

<#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:
```

Autenticação da Web

Semelhante à administração da Web, a autenticação da camada 3 também pode ser usada no 9800. Esse ponto confiável vincula um certificado a um portal da Web que é mostrado a um usuário quando ele tenta se autenticar em uma WLAN por meio de um portal convidado que é apresentado automaticamente ao usuário. Usar um ponto confiável para autenticação da Web ajuda a proteger as credenciais do usuário entre a WLC e o cliente ao qual está se conectando.

Por padrão, a WLC usa o certificado autoassinado. Novamente, isso faz com que uma mensagem de aviso seja exibida para o cliente informando que a página da Web não é confiável. Para evitar isso, um certificado de terceiros pode ser usado como na administração da Web.

Semelhante à administração da Web, uma vez que o certificado personalizado tenha sido carregado para o WLC, ele deve ser vinculado ao mapa de parâmetros da Web como ponto confiável.

```
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 o ponto confiável usado para a autenticação da Web, digite o comando seguinte

<#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

Informações Relacionadas

- Certificados localmente significativos
- Gerar e fazer download do certificado CSR nas WLCs do Catalyst 9800

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.