Informazioni sui tipi di certificato e di trust sul WLC 9800

Sommario

Introduzione

Questo documento descrive i diversi tipi di certificati e trust point che possono essere utilizzati sul WLC 9800.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza base di:

- Cisco Wireless LAN Controller (WLC) serie 9800
- Certificati digitali, Autorità di certificazione (CA) e Infrastruttura a chiave pubblica (PKI)

Componenti usati

Il documento può essere consultato per tutte le versioni hardware o software.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Certificati

Che cos'è un certificato?

Un certificato è un documento univoco che identifica un dispositivo, ad esempio per garantirne la legittimità. Un certificato deve essere verificato da una CA per convalidare tale identità.

Tipi di certificati sul modello 9800

I punti di accesso (AP) e il WLC hanno bisogno di un modo per convalidare l'identità degli altri. Ogni volta che un nuovo access point si unisce al WLC, l'access point convalida il certificato del WLC per assicurarsi che non sia solo legittimo, ma sia ancora valido. In questo modo, i punti di accesso possono avere fiducia nell'accessorio a cui sono collegati per la prima volta in assoluto.

Certificato di installazione produttore (MIC)

Per impostazione predefinita, questo certificato viene installato sugli accessori fisici, ad esempio 9800-80, 9800-40 e 9800-L. Come indica il nome, è preinstallato e non può essere modificato. Questo certificato viene usato quando l'access point viene aggiunto per la prima volta al WLC.

Per verificare se un certificato MIC è installato sul modello 9800, immettere il 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
```

Certificato autofirmato (SSC)

Per l'istanza virtuale del controller, la 9800-CL, non è presente alcun certificato preinstallato. ma utilizza un certificato autofirmato che può essere generato automaticamente tramite la procedura guidata per il giorno 0 o tramite uno script in cui il certificato viene creato manualmente. Nelle istanze virtuali dello switch 9800, il protocollo SSC viene utilizzato principalmente per il join degli access point, ma anche per tutti i servizi HTTP(s), SSH e NETCONF. Anche le appliance fisiche contengono un SSC, ma come accennato in precedenza, non viene utilizzato per il join AP, bensì per i servizi.

Di nuovo, per controllare il certificato SSC sullo switch 9800, immettere il 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
```

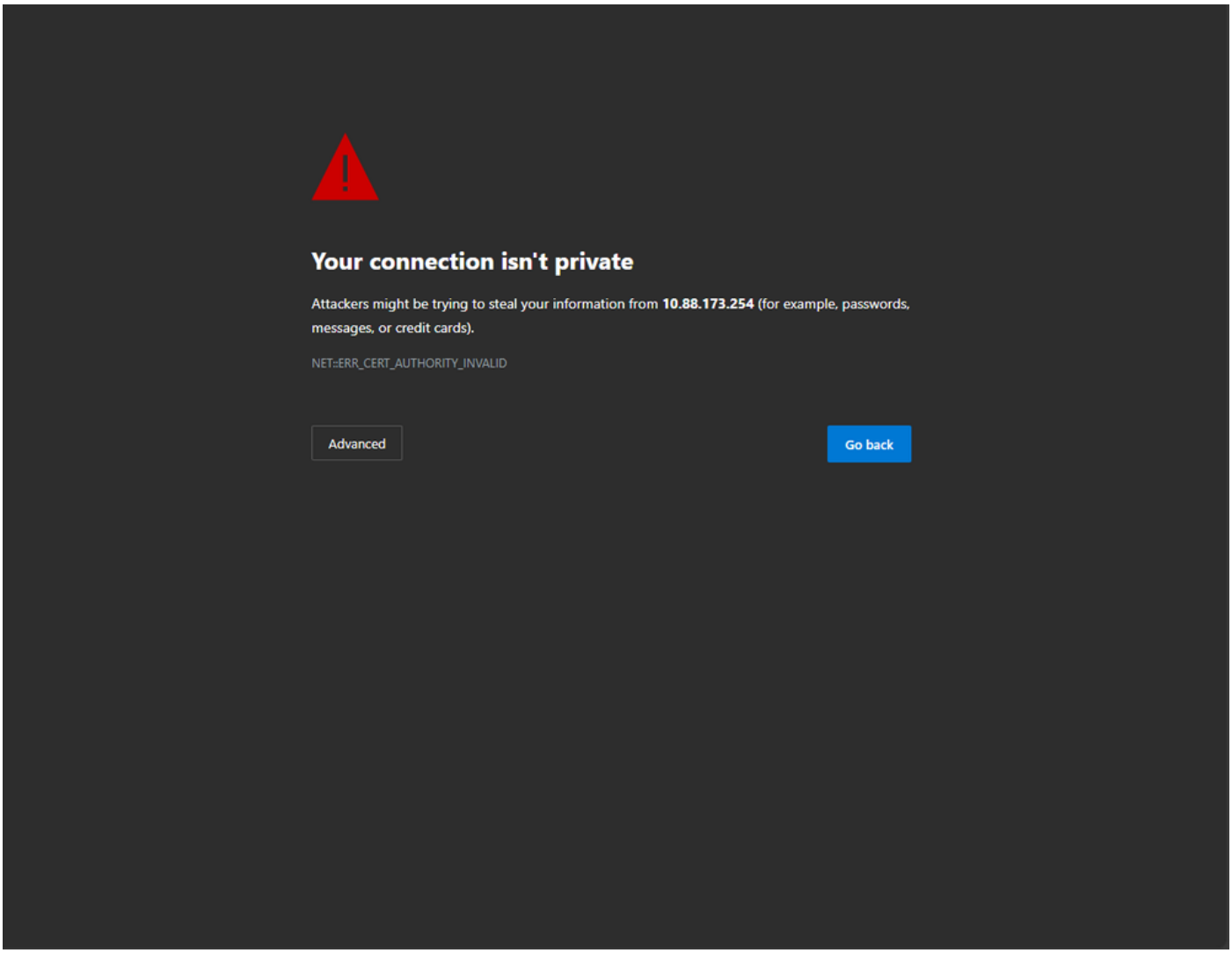
LSC (Locally Significant Certificate)

Questi certificati vengono utilizzati esclusivamente dagli access point che devono dimostrare la loro identità al WLC. Per impostazione predefinita, non esistono né sul WLC né sugli AP. I certificati LSC devono essere firmati da una CA e successivamente installati sia sul WLC che sugli AP per poter essere convalidati reciprocamente. Per ulteriori informazioni su come configurare le liste LCS sul modello 9800, fare riferimento alla sezione Certificati importanti a livello locale.

Trustpoint

Che cos'è un trust point?

Un trust point è il collegamento di un certificato a un servizio specifico. Esistono due tipi principali di trust: amministrazione Web e autenticazione Web. Per impostazione predefinita, il WLC utilizza il certificato autofirmato per entrambi i servizi, ma viene visualizzato un messaggio di avviso che indica che il sito non è sicuro. Il certificato autofirmato non è stato convalidato da alcuna CA.



Messaggio di avviso non valido CA nella pagina Web

Per evitare questo problema, è possibile utilizzare un certificato di terze parti verificando che sia già stato convalidato da una CA. Per ulteriori informazioni su come generare e caricare un certificato WLC, consultare il documento sulla generazione e il download del certificato CSR sui WLC di Catalyst 9800.

Amministrazione Web

Il trust point per l'amministrazione Web collega il certificato all'interfaccia utente grafica (GUI). Il controller seleziona uno dei certificati disponibili e, se non è stato caricato alcun certificato personalizzato nel WLC, viene utilizzato il certificato autofirmato. Se il certificato predefinito non è quello che si desidera utilizzare, è possibile utilizzare un certificato personalizzato per il trust point.

Una volta caricato il certificato sulla stampante 9800, come indicato nel documento precedente, il passaggio successivo consiste nel collegare il trust point all'amministrazione Web. Immettere i comandi successivi:

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

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

Un modo per convalidare il certificato appena installato è ora utilizzato come punto di fiducia per i servizi HTTP, ad esempio immettere il comando show ip http server status | includere un trust point

<#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:

Autenticazione Web

Analogamente all'amministrazione Web, l'autenticazione di livello 3 può essere utilizzata anche sul modello 9800. Questo trust point collega un certificato a un portale Web visualizzato a un utente durante il tentativo di autenticazione a una WLAN tramite un portale guest che viene automaticamente presentato all'utente. L'utilizzo di un trust point per l'autenticazione Web consente di proteggere le credenziali dell'utente tra il WLC e il client a cui ci si connette.

Per impostazione predefinita, il WLC utilizza il certificato autofirmato. Anche in questo caso, viene visualizzato un messaggio di avviso per il client che indica che la pagina Web non è attendibile. Per evitare ciò, è possibile utilizzare un certificato di terze parti come per l'amministrazione Web.

Analogamente all'amministrazione Web, una volta caricato nel WLC, il certificato personalizzato deve essere collegato alla mappa dei parametri Web come trustpoint.

```
configure terminal
parameter-map type webauth global
trustpoint <custom-cert>
!Restart HTTP services
```

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

Per convalidare il trust point utilizzato per l'autenticazione Web, immettere il comando successivo

<#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

Informazioni correlate

- Certificati importanti a livello locale
- Generazione e download del certificato CSR sui WLC di Catalyst 9800

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).