Begrijp Certificaat en Trustpoint Types op de 9800 WLC

Inhoud

Inleiding

Dit document beschrijft de verschillende typen certificaten en trustpoints die op de 9800 WLC kunnen worden gebruikt.

Voorwaarden

Vereisten

Cisco raadt u aan een basiskennis te hebben van:

- Cisco draadloze LAN-controller (WLC) 9800 Series
- Digitale certificaten, certificeringsinstanties (CA's) en de openbare sleutelinfrastructuur (PKI)

Gebruikte componenten

Dit document is niet beperkt tot specifieke hardware- of softwareversies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Certificaten

Wat is een certificaat?

Een certificaat is een uniek document dat een apparaat identificeert, bijvoorbeeld om ervoor te zorgen dat het legitiem is. Een certificaat moet worden geverifieerd door een CA om de identiteit te valideren.

Typen certificaten op de 9800

Access points (AP's) en WLC hebben een manier nodig om elkaars identiteit te valideren. Wanneer een nieuwe AP zich aansluit bij de WLC, valideert de AP het WLC-certificaat om ervoor te zorgen dat het niet alleen legitiem is, maar dat het nog steeds geldig is. Op deze manier kunnen AP's vertrouwen op het apparaat waar ze zich voor het eerst bij aansluiten.

Geïnstalleerd certificaat van de fabrikant (MIC)

Dit certificaat is standaard geïnstalleerd op de fysieke apparaten, zoals de 9800-80, 9800-40 en de 9800-L. Zoals de naam aangeeft, is het in de fabriek geïnstalleerd en kan het niet worden aangepast. Dit certificaat wordt gebruikt wanneer de AP voor het eerst toetreedt tot de WLC.

Om te controleren of een MIC-certificaat inderdaad op de 9800 is geïnstalleerd, kunt u de opdracht tonen draadloos 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
```

Zelfondertekend certificaat (SSC)

Voor het virtuele geval van de controller, de 9800-CL, is er geen fabrieksgeïnstalleerd certificaat. Maar eerder, gebruikt het een zelf-ondertekend certificaat dat automatisch door de tovenaar van Dag 0, of door een manuscript kan worden geproduceerd waarin het certificaat manueel wordt gecreëerd. In virtuele gevallen van de 9800 wordt de SSC voornamelijk gebruikt voor AP-deelname, maar ook voor alle HTTP(s), SSH en NETCONF-services. Fysieke apparaten bevatten ook een SSC, maar zoals eerder vermeld, wordt het niet gebruikt voor AP-toetredingen, maar voor de diensten in plaats daarvan.

Opnieuw, om het SSC certificaat op 9800 te controleren, ga het bevel in tonen draadloos beheer 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

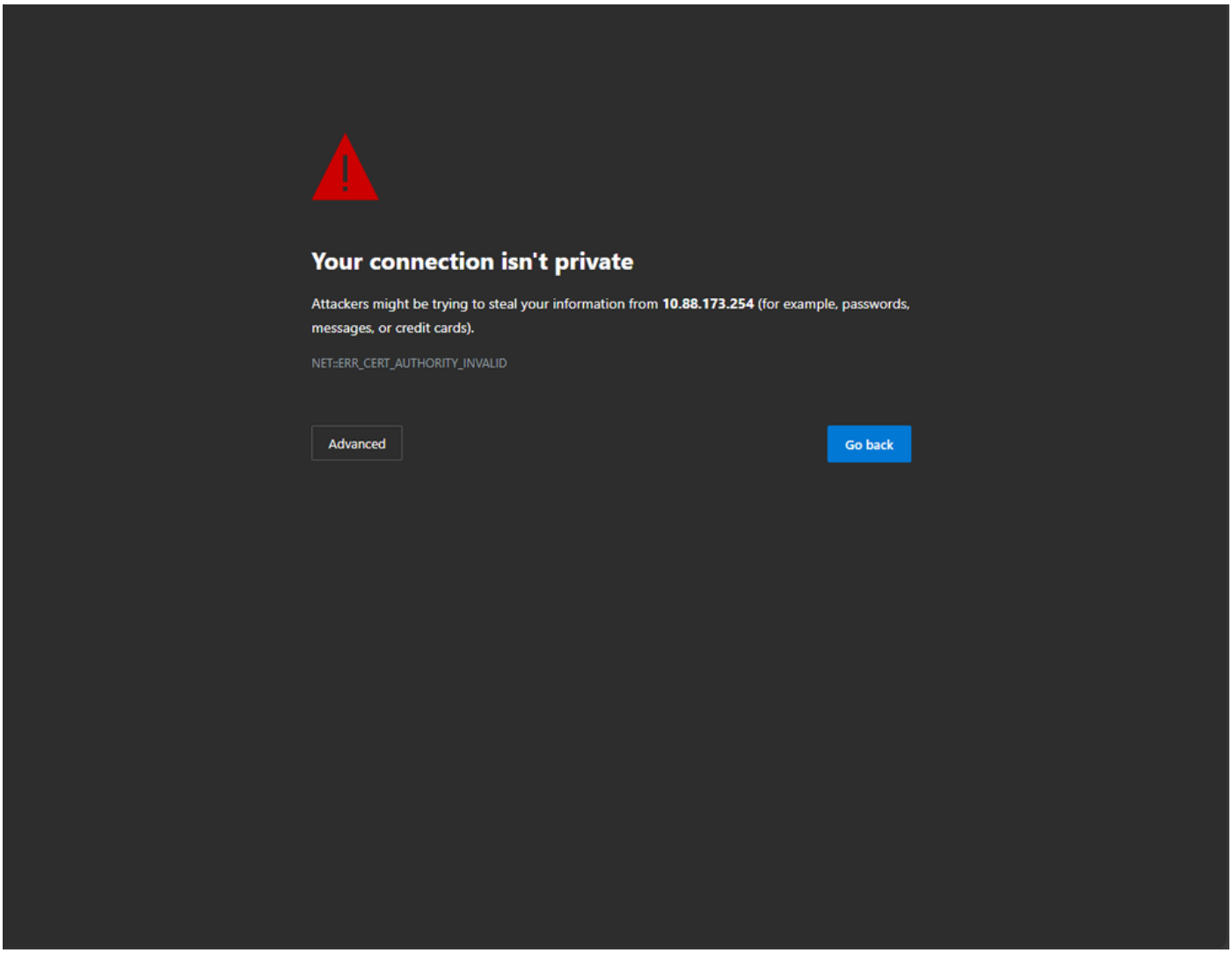
Lokaal belangrijk certificaat (LSC)

Deze certificaten worden uitsluitend gebruikt door AP's die hun identiteit moeten bewijzen aan de WLC. Ze bestaan standaard niet op de WLC noch op de AP's. De LSC-certificaten moeten worden ondertekend door een CA en later worden geïnstalleerd op zowel de WLC als de AP's om elkaar wederzijds te valideren. Raadpleeg Lokaal belangrijke certificaten voor meer informatie over het configureren van LSC's op de 9800.

Trustpoints

Wat is een Trustpoint?

Een trustpoint is wat een certificaat koppelt aan een specifieke dienst. Er zijn twee hoofdtypen van trustpoints: webbeheer en webverificatie. Standaard gebruikt de WLC het zelfondertekende certificaat voor beide diensten, maar dit zorgt ervoor dat een waarschuwingsbericht naar pop-up geeft dat de site niet veilig is. Dit komt doordat het zelfondertekende certificaat niet door een CA is gevalideerd.



Ongeldig waarschuwingsbericht op webpagina

Om dit te voorkomen, kan een certificaat van een derde worden gebruikt om ervoor te zorgen dat het al is gevalideerd door een CA. Voor meer informatie over het genereren en uploaden naar de WLC van een certificaat, raadpleegt u Generate and Download CSR-certificaat op Catalyst 9800 WLC's.

Webbeheer

Het trustpoint voor het webbeheer koppelt het certificaat aan de grafische gebruikersinterface (GUI). De controller selecteert een van de beschikbare certificaten en als er geen aangepast certificaat is geüpload naar de WLC, wordt het zelfondertekende certificaat gebruikt. Als het standaardcertificaat niet iets is dat u wilt gebruiken, kunt u een aangepast certificaat gebruiken voor het trustpoint.

Nadat het certificaat is geüpload naar de 9800, zoals in het document hierboven, de volgende stap is om het trustpoint te koppelen aan de web-administratie, moeten de volgende opdrachten worden ingevoerd:

```
configure terminal
```

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

Een manier om het nieuw geïnstalleerde certificaat te valideren wordt nu gebruikt als een trustpoint voor HTTP-services, bijvoorbeeld, voer de opdracht in status van ip http server tonen | omvat 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:
```

Web verificatie

Net als bij webbeheer kan ook Layer 3-verificatie worden gebruikt op de 9800. Dit trustpoint koppelt een certificaat aan een webportaal dat aan een gebruiker wordt getoond aangezien het probeert te verifiëren aan een WLAN door een gastportaal dat automatisch aan de gebruiker wordt voorgesteld. Het gebruik van een trustpoint voor webverificatie helpt de gebruikersreferenties te beschermen tussen de WLC en de client waarmee verbinding wordt gemaakt.

Door gebrek, gebruikt WLC het zelf-ondertekende certificaat. Opnieuw, veroorzaakt dit een waarschuwingsbericht aan pop-up voor de cliënt die dat de Web-pagina niet wordt vertrouwd op verklaart. Om dit te voorkomen, kan een 3rd party certificaat worden gebruikt net als met de web administratie.

Vergelijkbaar met webbeheer, zodra het aangepaste certificaat is geüpload naar de WLC, moet het worden gekoppeld aan de web paramater map als 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
```

Om het trustpoint te valideren dat voor webverificatie wordt gebruikt, voert u de volgende opdracht in

<#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

Gerelateerde informatie

- Lokaal belangrijke certificaten
- CSR-certificaat genereren en downloaden op Catalyst 9800 WLC's

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.