HTTPS-omleiding via WebEth configureren

Inhoud

Inleiding

In dit document wordt de configuratie beschreven van de omleiding van webverificatie via HTTPS. Dit is een optie die wordt geïntroduceerd in Cisco Unified Wireless Network (CUWN) release 8.0.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben van deze onderwerpen:

- Basiskennis van WLC-webverificatie (Wireless LAN Controller)
- Hoe te om de WLC voor Web-Verificatie te configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500 Series WLC die CUWN firmware versie 8.0 draait.

> **Opmerking:** De configuratie en web-auth uitleg die in dit document wordt gegeven, zijn van toepassing op alle WLC-modellen en elk CUWN-beeld dat gelijk is aan of hoger is dan 8.0.100.0.

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Web authenticatie is een Layer 3 beveiligingsfunctie. Het blokkeert al het IP/gegevensverkeer, behalve DHCP-gerelateerde pakketten/DNS-gerelateerde pakketten, van een bepaalde client tot een draadloze client een geldige gebruikersnaam en een wachtwoord heeft geleverd.Web verificatie wordt doorgaans gebruikt door klanten die een gast-toegangsnetwerk willen implementeren.Web verificatie start wanneer de controller het eerste TCP HTTP (poort 80) Get Packet van de client onderschept.

Om ervoor te zorgen dat de webbrowser van de client dit tot ver kan brengen, moet de client eerst een IP-adres verkrijgen en een vertaling van de URL naar IP-adres (DNS-resolutie) voor de webbrowser doen. Dit laat de webbrowser weten welk IP-adres om HTTP GET te verzenden. Wanneer de client de eerste HTTP GET naar TCP poort 80 verstuurt, stuurt de controller de client naar https:<Virtual IP>/login.html voor verwerking. Dit proces vult uiteindelijk de inlogwebpagina in.

Voorafgaand aan releases eerder dan CUWN 8.0 (d.w.z. tot 7.6), als de draadloze client een HTTPS-pagina (TCP 443) indient, wordt de pagina niet opnieuw gericht naar het webauthenticatieportaal. Aangezien steeds meer websites HTTPS gaan gebruiken, wordt deze optie in releases CUWN 8.0 en later opgenomen. Als een draadloze client https://<website> probeert te maken, wordt deze optie opnieuw gericht naar de logpagina van de web-auth-client. Deze optie is ook erg nuttig voor de apparaten die https-verzoeken met een toepassing verzenden (maar niet met een browser).

certificaatfout

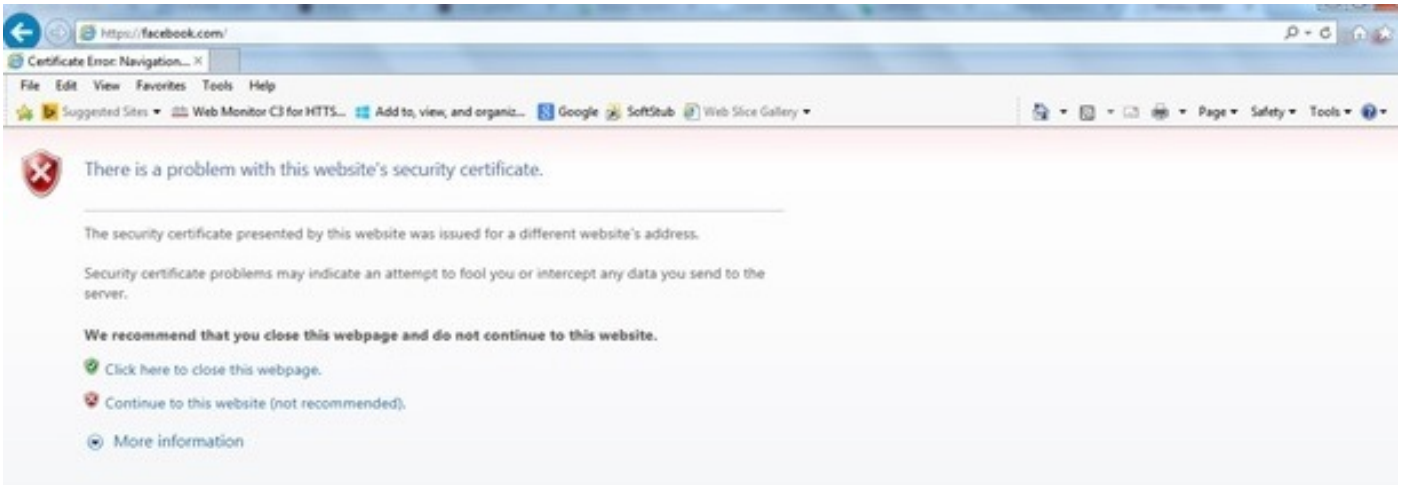
Het waarschuwingsbericht "certificaat is niet afgegeven door een vertrouwde certificeringsinstantie." verschijnt op de browser nadat u de https-redirect-functie hebt ingesteld. Dit wordt gezien zelfs als u een geldig wortel of geketend certificaat hebt op de controller zoals getoond in afbeelding 1 en afbeelding 2. De reden is dat het certificaat dat u op de controller hebt geïnstalleerd, is afgegeven aan uw virtuele IP-adres.

> **Opmerking:** Als u een HTTP-redirect probeert en dit certificaat op de WLC heeft, krijgt u deze fout in de certificaatwaarschuwing niet. In het geval van HTTPS-redirect wordt deze fout echter weergegeven.

Wanneer de client HTTPS://<web-site> probeert, verwacht de browser het certificaat dat is afgegeven aan het IP-adres van de site en dat is opgelost door de DNS. Wat ze echter ontvangen is het certificaat dat is afgegeven aan de interne webserver van de WLC (virtueel IP-adres) waardoor de browser de waarschuwing geeft. Dit is puur vanwege de manier waarop HTTPS werkt en gebeurt altijd als je probeert de HTTPS-sessie te onderscheppen zodat web-auth-omleiding kan werken.

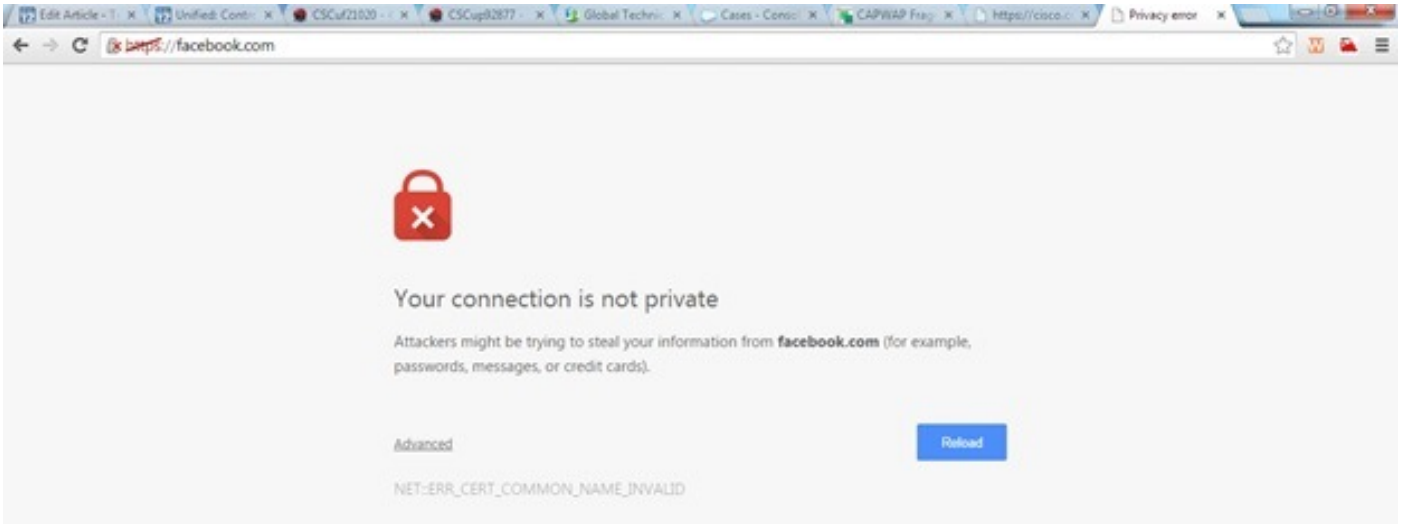
U kunt in verschillende webbrowsers verschillende certificaatfoutmeldingen zien, maar deze hebben allemaal betrekking op hetzelfde probleem als de vorige melding.

Figuur 1



Dit is een voorbeeld van de manier waarop de fout in Chrome kan worden weergegeven:

Figuur 2



Configureren

Configuratie van WLC voor HTTPS-omleiding

Deze configuratie gaat ervan uit dat het Wireless LAN (WLAN) al is geconfigureerd voor de Layer 3 Web autorisatie-beveiliging. Zo schakelt u HTTPS in of uit op dit Web-auth WLAN:

```
(WLC)>config wlan security web-auth enable 10
(WLC)>config network web-auth https-redirect enable
WARNING! - You have chosen to enable https-redirect.
This might impact performance significantly
```

Zoals de voorbeeldconfiguratie laat zien, kan dit invloed hebben op doorvoersnelheid voor een HTTPS-omleiding maar niet op HTTP-omleiding

Zie Webverificatie op WLAN-controller voor meer informatie en een configuratie van de WLAN-verificatie.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met **show.** Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

```
(WLC)>show network summary

Web Auth Secure Web ..................... Enable
Web Auth Secure Redirection ............... Enable
```

1. Schakel deze apparaten in:
   ```
   (WLC) debug client
   ```

   ```
   (WLC)> debug web-auth redirect enable
   ```
2. Controleer de uitwerpselen:
   ```
   (WLC) >show debug

   MAC Addr 1.............................. 24:77:03:52:56:80

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Associeer de client aan de web-auth enabled SSID's.
4. Zoek deze uitwerpselen:
   ```
   *webauthRedirect: Jan 16 03:35:35.678: 24:77:3:52:56:80- received connection.
   client socket = 9
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- trying to read on socket 95
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- calling parser with bytes = 204
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- bytes parsed = 204
   *webauthRedirect: Jan 16 03:35:35.679: captive-bypass detection enabled,
   checking for wispr in HTTP GET, client mac=24:77:3:52:56:80
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Preparing redirect
   URL according to configured Web-Auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- got the hostName
   for virtual IP(wirelessguest.test.com)
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Checking custom-web
   config for WLAN ID:10
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Global status is
   enabled, checking on web-auth type
   *webauthRedirect: Jan 16 03:35:35.679: 24:77:3:52:56:80- Web-auth type Customized,
   using URL:https://wirelessguest.test.com/fs/customwebauth/login.html
   ```
   Opmerking: Verzeker dat of Secure web (web-web van het netwerk veilig te stellen/uit te schakelen) of web-auth beveiligde (web-auth security web-auth-web (configuratie netwerk web-auth security) geactiveerd is om de HTTPS-omleiding te maken. Merk ook op dat de doorvoersnelheid enigszins kan worden verminderd wanneer er een omleiding over HTTPS wordt gebruikt.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.