La configuración HTTPS reorienta sobre el Red-auth

Contenido

Introducción

Este documento describe la configuración sobre el cambio de dirección de la autenticación Web sobre el HTTPS. Esto es una característica introducida en la versión 8.0 de la red del Cisco Unified Wireless (CUWN).

Prerrequisitos

Requisitos

Cisco recomienda tener conocimientos de estos temas:

- Conocimiento básico de la autenticación Web del regulador del Wireless LAN (WLC)
- Cómo configurar el WLC para la autenticación Web.

Componentes Utilizados

La información en este documento se basa en el WLC de las Cisco 5500 Series que funciona con la versión de firmware 8.0 CUWN.

> Nota: La configuración y la explicación del red-auth proporcionada en este documento es aplicables a todos los modelos del WLC y a cualquier imagen CUWN iguales a o más adelante que 8.0.100.0.

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 la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

La autenticación Web es una función de seguridad de la capa 3. Bloquea todo el tráfico IP/data, excepto los paquetes DNS-relacionados de los paquetes DHCP-relacionados, de un cliente particular hasta que un cliente de red inalámbrica haya suministrado un nombre de usuario válido y una contraseña. La autenticación Web es utilizada típicamente por los clientes que quieren implementar una red de acceso de invitados. La autenticación Web comienza cuando el regulador intercepta el primer paquete TCP HTTP (puerto 80) GET del cliente.

Para que el buscador Web del cliente consiga esto lejano, el cliente debe primero obtener una dirección IP, y hace una traducción del URL a la dirección IP (resolución de DNS) para el buscador Web. Esto deja al buscador Web saber qué dirección IP para enviar el HTTP GET. Cuando el cliente envía el primer HTTP GET al puerto TCP 80, el regulador reorienta al cliente al https: IP>/login.html <virtual para procesar. Este proceso saca a colación eventual la página web del login.

Antes de las versiones anterior que CUWN 8.0 (es decir hasta 7.6), si el cliente de red inalámbrica presenta una página HTTPS (TCP 443), la página no se reorienta al portal de la autenticación Web. Mientras que los sitios web comienzan cada vez más a utilizar el HTTPS, esta característica se incluye en las versiones CUWN 8.0 y posterior. Con esta característica en el lugar, si un cliente de red inalámbrica intenta el <website> de https://, se reorienta a la página de registro del red-auth. También esta característica es muy útil para los dispositivos que envían las peticiones del https con una aplicación (pero no con un navegador).

Error del certificado

El mensaje de advertencia “certificado no es publicado por un Certificate Authority de confianza.” aparece en el navegador después de que usted configure la característica de la https-reorientación. Se ve esto incluso si usted tiene una raíz válida o un certificado encadenado en el regulador tal y como se muestra en del cuadro 1 y del cuadro 2. La razón es que el certficiate que usted instaló en el regulador está publicado a su dirección IP virtual.

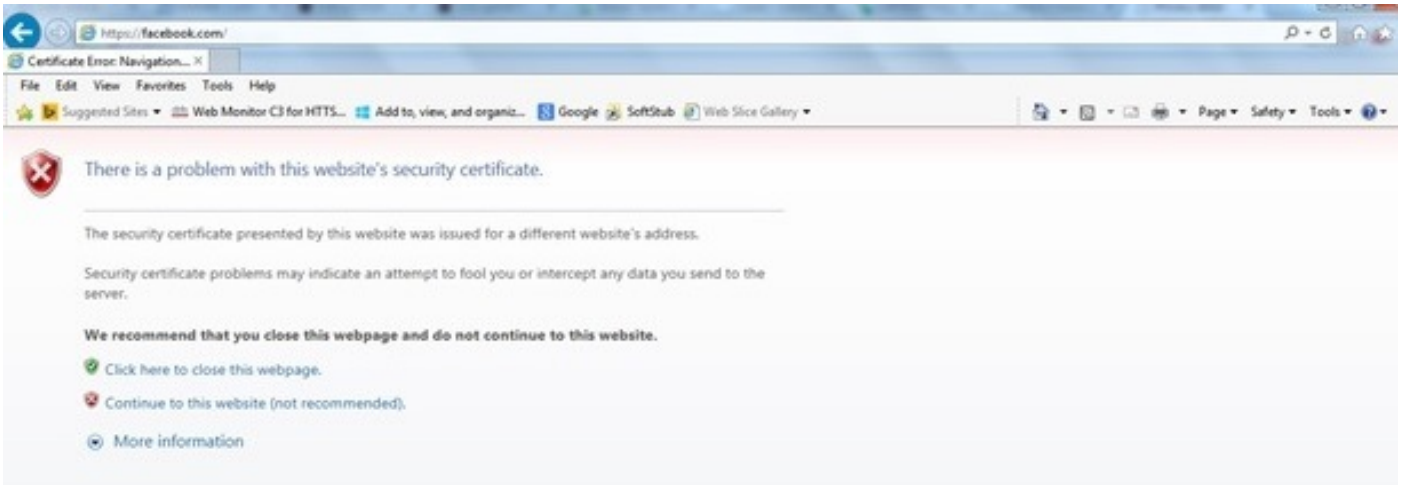
> Nota: Si usted intenta un El HTTP vuelve a dirigir y tiene este certifcate en el WLC, usted no consigue a este certificado el error amonestador. No obstante en el caso de HTTPS-reoriente, este error aparece.

Cuando el cliente intenta el <website> de HTTPS://, el navegador cuenta con el certificado publicado a la dirección IP del sitio resuelta por el DNS. Sin embargo, qué reciben es el certificado que fue publicado al servidor Web interno del WLC (dirección IP virtual) que hace al navegador publicar la advertencia. Esto está puramente debido a la manera que el HTTPS trabaja y que sucede siempre si usted intenta interceptar a las sesiones HTTP para que el cambio de dirección del red-auth trabaje.

Usted puede ser que vea diversos mensajes de error del certificado en diversos navegadores

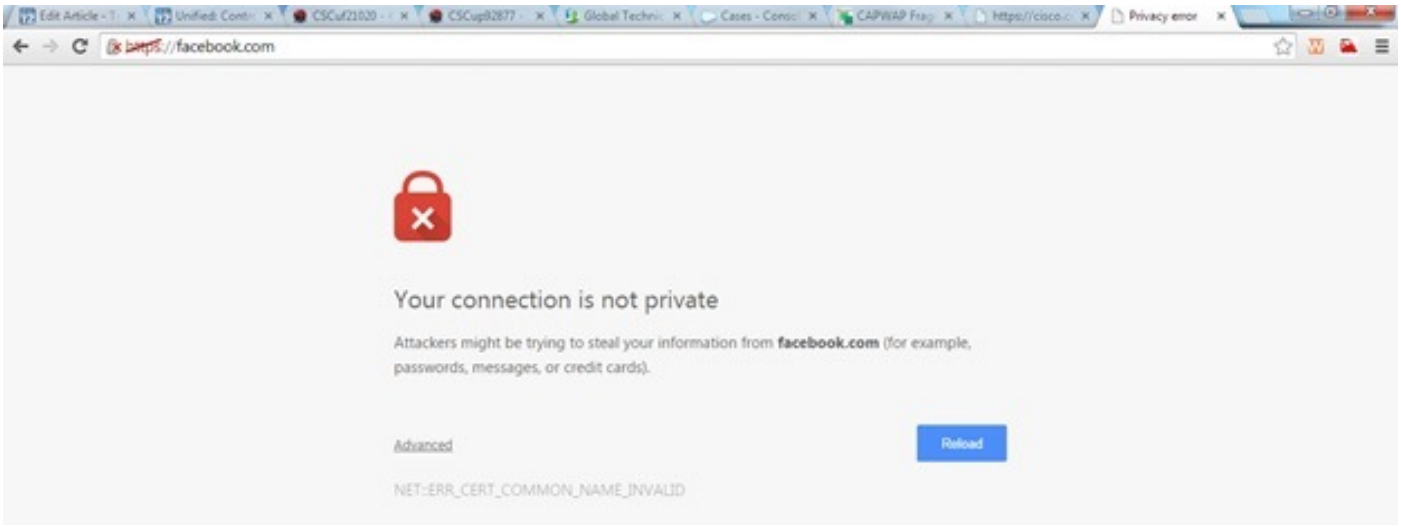
pero todos relacionarse con el mismo problema según lo descrito previamente.

Figura 1



Éste es un ejemplo de cómo el error puede aparecer en Chrome:

Figura 2



Configurar

Configure el WLC para el redireccionamiento HTTPS

Esta configuración asume que el Wireless LAN (red inalámbrica (WLAN)) está configurado ya para la Seguridad del authentciation de la red de la capa 3. Para habilitar o la neutralización HTTPS reorienta en esta red inalámbrica (WLAN) del Red-auth:

```
(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
```

Pues el ejemplo de configuración muestra, éste pudo afectar la producción para un redireccionamiento HTTPS pero no la redirección de HTTP

Para más información y una configuración de la autenticación Web WLAN, vea la autenticación Web en el controlador de WLAN.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

```
(WLC)>show network summary

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

1. Habilite estos debugs:`(WLC) debug client <MAC address>`

   `(WLC)> debug web-auth redirect enable`
2. Verifique los debugs:`(WLC) >show debug`

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

   Debug Flags Enabled:
   webauth redirect enabled.
   ```
3. Asocie al cliente al SSID habilitado red-auth.
4. Busque estos debugs:`*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`Nota: Asegúrese de que la red segura (permiso/neutralización del secureweb de la red de los config) o el red-auth seguro (permiso/neutralización del secureweb del red-auth de la red de los config) esté habilitada para hacer que el HTTPS reoriente el trabajo. También observe que pudo haber una reducción leve en la producción cuando el cambio de dirección sobre el HTTPS se utiliza.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.