Resolviendo problemas la autenticación Web en un regulador del Wireless LAN (WLC)

Contenido

Introducción

Este documento proporciona las extremidades para resolver problemas los problemas de la autenticación Web en un entorno del regulador del Wireless LAN (WLC).

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del protocolo del Lightweight Access Point (LWAPP) /Control y aprovisionamiento de los untos de acceso de red inalámbrica (CAPWAP)
- Conocimiento de configurar el Lightweight Access Point (REVESTIMIENTO) y el WLC para la operación básica.
- Conocimiento básico de la autenticación Web y de la autenticación Web el configurar en el WLCs. Para la información sobre configurar la autenticación Web en el WLCs, refiera al ejemplo de configuración de la autenticación Web del regulador del Wireless LAN.

Componentes Utilizados

La información en este documento se basa en un WLC 5500 que funciona con la versión de firmware 7.0.98.0.

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.

Productos Relacionados

Este documento se puede también utilizar con estos hardwares:

- Cisco Wireless Controllers de la serie 5500
- Controladores LAN inalámbricos Cisco de la serie 4400
- Controladores LAN inalámbricos Cisco de la serie 4100
- Cisco Wireless Controllers de la serie 2500
- Cisco 2100 Series Wireless LAN Controllers
- Controladores LAN inalámbricos Cisco de la serie 2000
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Wireless LAN Controller Module
- Módulo de Servicios inalámbricos de las Cisco Catalyst 6500 Series (WiSM)
- Cisco Flex Wireless Controllers de la serie 7500
- Cisco Wireless Services Module 2 (WiSM2)
- Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Autenticación Web en el WLCs

La autenticación Web es una función de seguridad de la capa 3 que hace al regulador no permitir el tráfico IP, excepto los paquetes DNS-relacionados de los paquetes DHCP-relacionados, de un cliente particular hasta que ese cliente haya suministrado correctamente un nombre de usuario válido y una contraseña una excepción del tráfico permitida con el PRE-auth ACL. La autenticación Web es la única política de seguridad que permite que el cliente consiga una dirección IP antes de la autenticación. Es un método de autenticación simple sin la necesidad de un supplicant o de una utilidad de cliente. La autenticación Web se puede hacer localmente en un WLC o sobre un servidor RADIUS. La autenticación Web es utilizada típicamente por los clientes que quieren implementar una red de acceso de invitados.

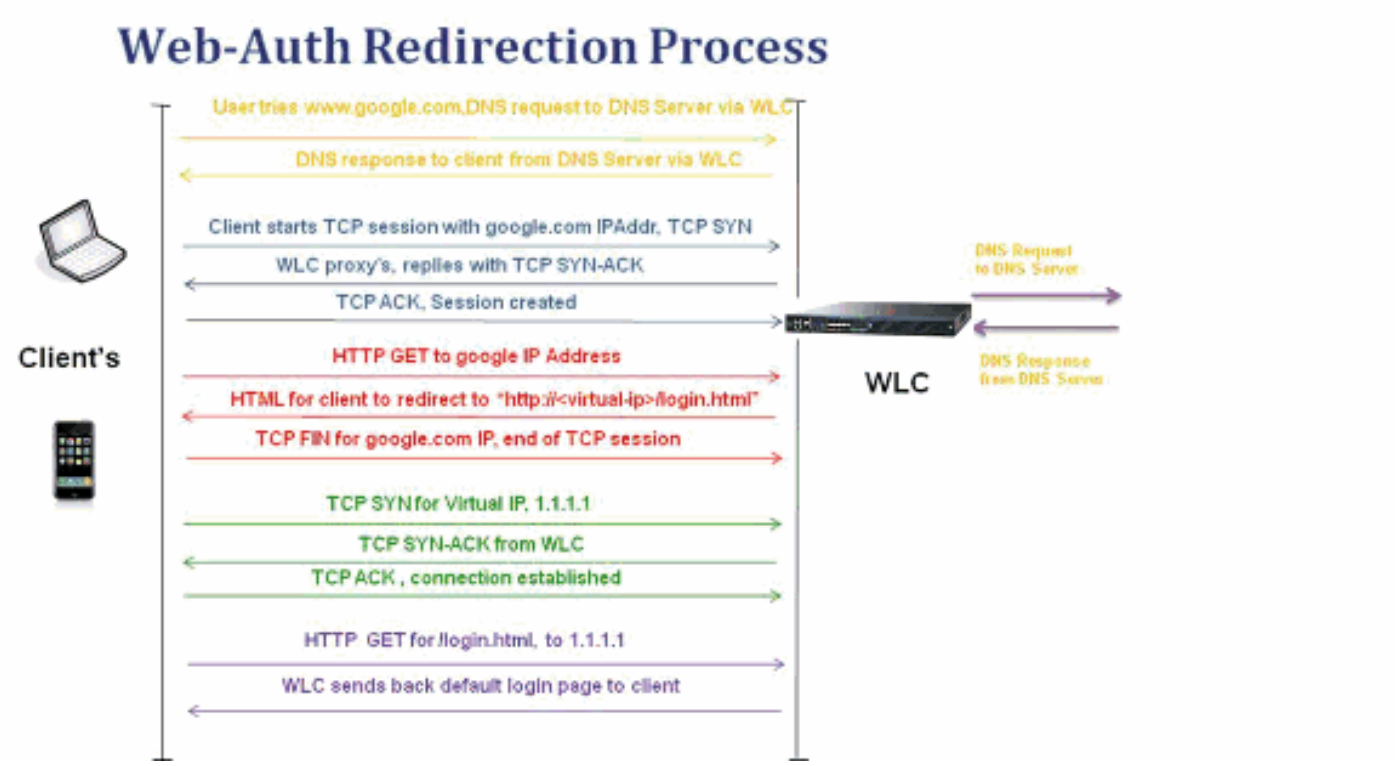
La autenticación Web comienza cuando el regulador intercepta el primer paquete TCP HTTP (puerto 80) GET del cliente. Para que el buscador Web del cliente consiga esto lejano, el cliente debe primero obtener una dirección IP, y hace una traducción del URL a la dirección IP (resolución de DNS) para el buscador Web. Esto deja al buscador Web saber qué dirección IP para enviar el HTTP GET.

Cuando la autenticación Web se configura en la red inalámbrica (WLAN), el regulador bloquea todo el tráfico (hasta que se completa el proceso de autenticación) del cliente, a excepción del tráfico del DHCP y DNS. Cuando el cliente envía el primer HTTP GET al puerto TCP 80, el regulador reorienta al cliente a https:1.1.1.1/login.html para procesar. Este proceso saca a colación eventual la página web del login.

Nota: Cuando usted utiliza a un servidor Web externo para la autenticación Web, algunas de las Plataformas del WLC necesitan una PRE-autenticación ACL para el servidor Web externo, que incluye el regulador de las Cisco 5500 Series, las Cisco 2100 Series regulador, las Cisco 2000 Series y el módulo de red del regulador. Para las otras Plataformas del WLC la PRE-autenticación ACL no es obligatoria.

Nota: Pero, es una práctica adecuada configurar una Autenticación previa ACL para el servidor Web externo cuando usted utiliza una autenticación del Web externa.

Esta sección explica el proceso de redireccionamiento de la autenticación Web detalladamente.



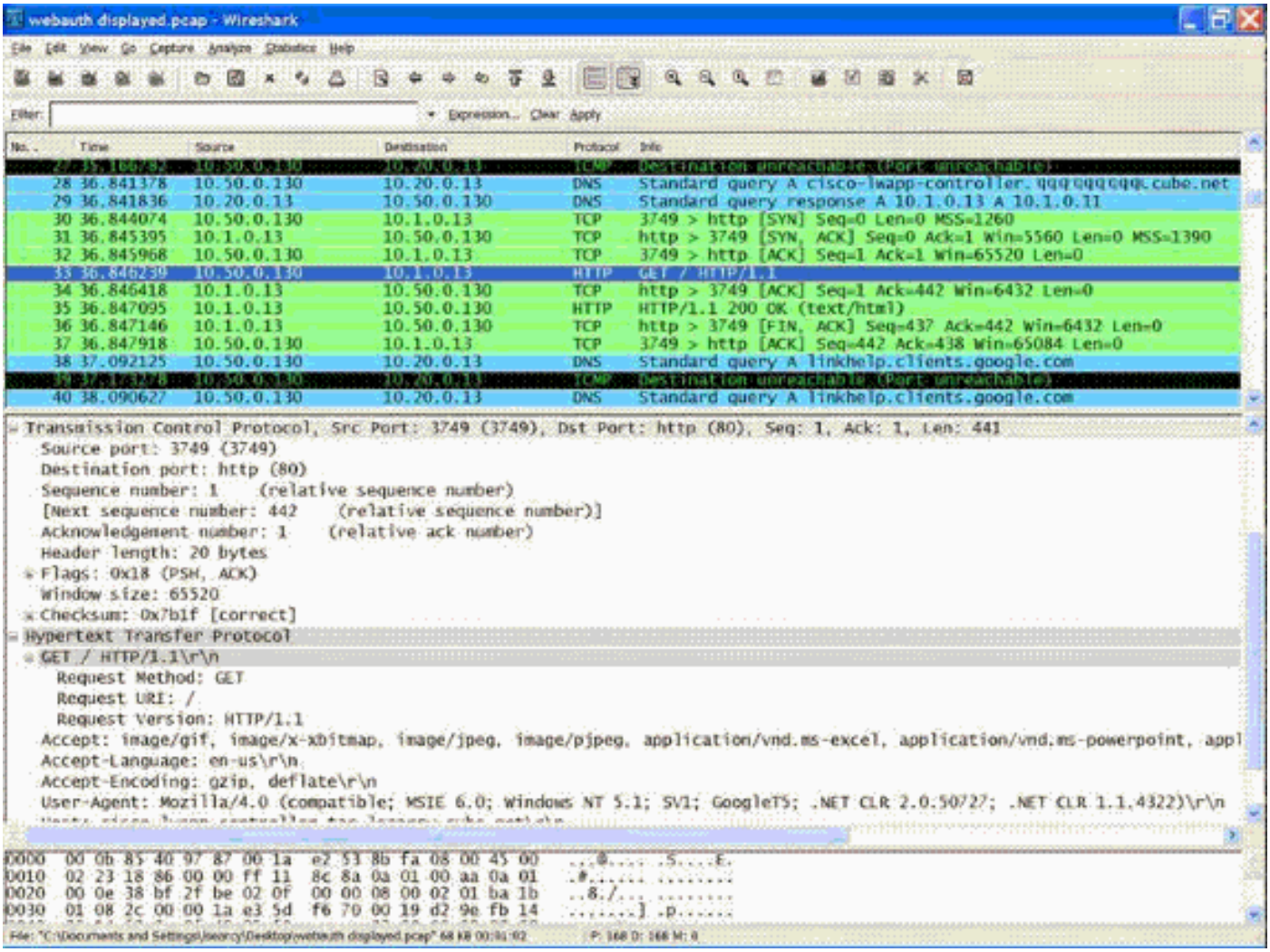
- Usted abre al buscador Web y teclea adentro un URL, por ejemplo, `http://www.google.com`. El cliente envía una petición DNS para que este URL consiga el IP para el destino. El WLC desvía la petición DNS al servidor DNS y el servidor DNS responde detrás con una contestación DNS, que contiene la dirección IP del destino `www.google.com`, que a su vez se remite a los clientes de red inalámbrica
- El cliente entonces intenta abrir una conexión TCP con el IP Address de destino. Envía paquete TCP Syn un destinado a la dirección IP de `www.google.com`.
- El WLC tiene reglas configuradas para el cliente y por lo tanto puede actuar como proxy para `www.google.com`. Devuelve un paquete TCP SYN-ACK al cliente con la fuente como la dirección IP de `www.google.com`. El cliente devuelve un paquete ACK TCP para completar la aceptación decontacto con TCP de tres vías y la conexión TCP se establece completamente.
- El cliente envía un paquete HTTP GET destinado a `www.google.com`. El WLC intercepta este paquete, lo envía para la dirección del cambio de dirección. El gateway de aplicación HTTP prepara a un cuerpo del HTML y lo envía detrás como la contestación al HTTP GET pedido por el cliente. Este HTML hace al cliente para ir a la página web predeterminada URL del WLC, por ejemplo, `http:// <Virtual-Server-IP>/login.html`.
- El cliente cierra la conexión TCP con la dirección IP, por ejemplo `www.google.com`.
- Ahora el cliente quiere ir a `http://1.1.1.1/login.html` y así que intenta abrir una conexión TCP con la dirección IP virtual del WLC. Envía a paquete TCP Syn para 1.1.1.1 al WLC.

- El WLC responde detrás con un TCP SYN-ACK y el cliente devuelve un TCP ACK al WLC para completar el apretón de manos.
- El cliente envía un HTTP GET para /login.html destinó a 1.1.1.1 para petición la página de registro.
- Esta petición se permite hasta el servidor Web del WLC, y el servidor responde detrás con la página de registro predeterminada. El cliente recibe la página de registro en la ventana del buscador donde el usuario puede continuar y iniciar sesión.

Aquí está un ejemplo. En este ejemplo, la dirección IP del cliente es 10.50.0.130. El cliente resolvió el URL al servidor Web que accedía 10.1.0.13. Como usted puede ver, el cliente hizo el apretón de manos de tres vías para poner en marcha la conexión TCP y después envió un paquete HTTP GET que comenzaba con el paquete 30. El regulador está interceptando los paquetes y está contestando con el código 200. El paquete del código 200 tiene una reorientación URL en él:

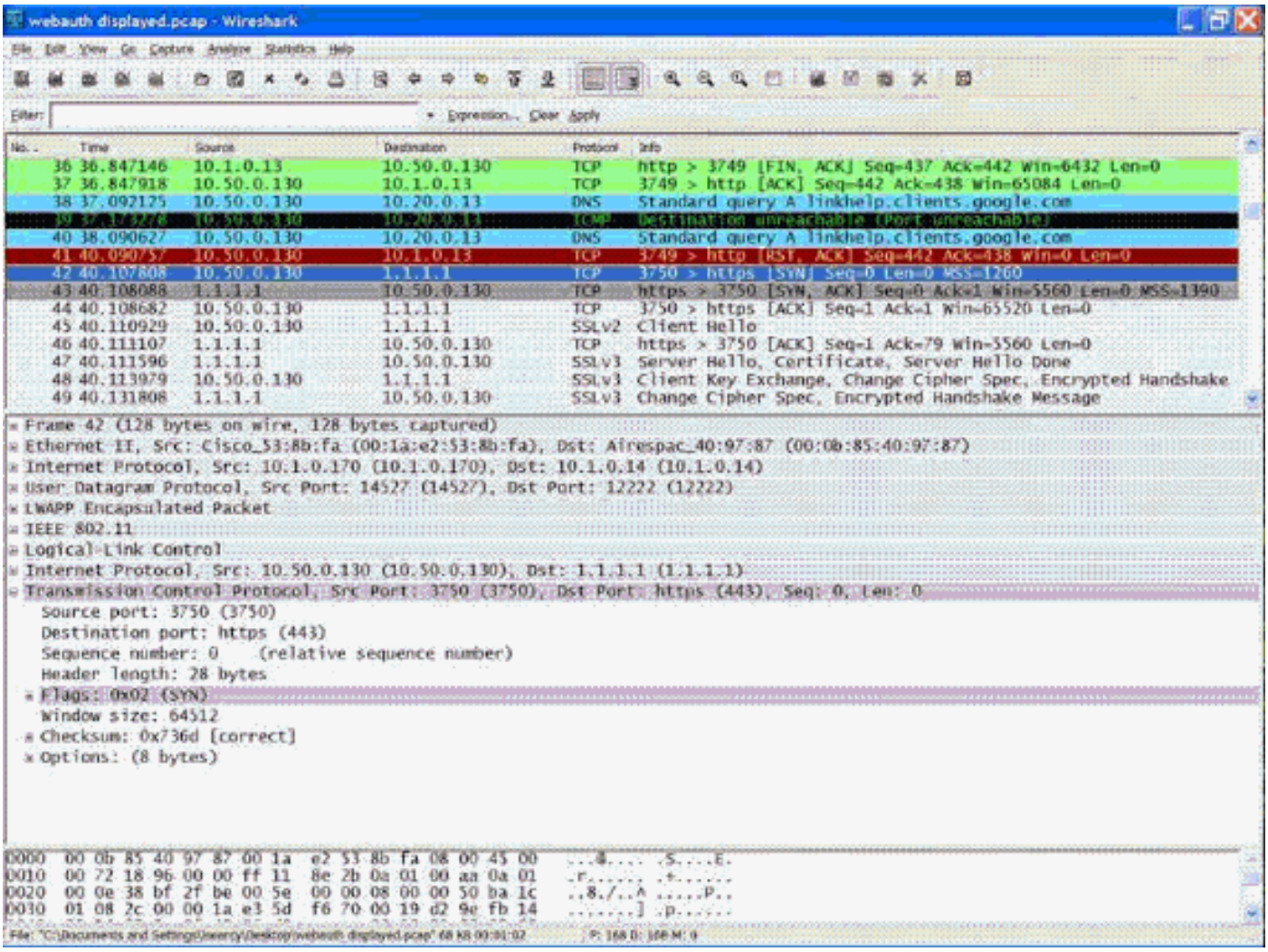
```
<HTML><HEAD><TITLE>Cisco Systems Inc. Web Authentication Redirect</TITLE><META
http-equiv="Cache-control" content="no-cache"><META http-equiv="Pragma"
content="no-cache"><META http-equiv="Expires" content="-1"><META http-equiv="refresh"
content="1; URL=https://1.1.1.1/login.html?redirect=cisco-lwapp-controller.qqq.qqqqq.
cube.net/"></HEAD></HTML>
```

Entonces cierra la conexión TCP a través del apretón de manos de tres vías.



El cliente entonces enciende la conexión HTTPS a la reorientación URL que la envía a 1.1.1.1, que es la dirección IP virtual del regulador. El cliente tiene que validar el certificado de servidor o ignorarlo para traer para arriba el túnel SSL. En este caso, es un certificado autofirmado así que el cliente lo ignoró. La página web del login se envía a través de este túnel SSL. El paquete 42

comienza las transacciones.



Usted tiene una opción para configurar el Domain Name para la dirección IP virtual del regulador del Wireless LAN. Si usted configura el Domain Name para la dirección IP virtual, este Domain Name se vuelve en el paquete de la AUTORIZACIÓN HTTP del regulador en respuesta al paquete HTTP GET del cliente. Usted entonces tiene que realizar una resolución de DNS para este Domain Name y una vez que consigue una dirección IP de la resolución de DNS, intenta abrir a una sesión TCP con esa dirección IP, que es un IP configurado en una interfaz virtual del regulador.

Eventual, la página web se pasa a través del túnel al cliente y el usuario devuelve el nombre de usuario/la contraseña a través del túnel SSL.

La autenticación Web es realizada por uno de estos tres métodos:

- Autenticación Web usando una página web interna (valor por defecto). Refiera a elegir la página de la conexión con el sistema de autenticación del Web predeterminada para más información sobre el uso de la página web predeterminada.
- Autenticación Web usando una página de registro personalizada. Refiera a crear una página de registro personalizada de la autenticación Web para más información sobre cómo utilizar la página de registro personalizada.
- Autenticación Web usando una página de registro de un servidor Web externo. Refiérase usando una página de registro personalizada de la autenticación Web de un servidor Web externo para más información sobre cómo utilizar una página de registro de un servidor Web

externo.

Nota: El conjunto personalizado del auth de la red tiene un límite de hasta 30 caracteres para los nombres de fichero. Asegúrese de que no hay nombres de fichero dentro del conjunto mayores de 30 caracteres.

Nota: De la versión 7.0 del WLC hacia adelante, si la autenticación Web se habilita en la red inalámbrica (WLAN) y usted también tiene reglas ACL CPU, las reglas basadas cliente de la autenticación Web toman siempre la precedencia más alta mientras el cliente sea unauthenticated en el estado de `WebAuth_Reqd`. Una vez que el cliente va al estado de `FUNCIONAMIENTO`, las reglas ACL CPU consiguen aplicadas.

Nota: Por lo tanto si el CPU ACL se habilita en el WLC, una regla de la permit para el IP de la interfaz virtual se requiere (en CUALQUIER dirección) en estas condiciones:

- Cuando el CPU ACL no tiene una permit TODA LA regla para las ambas direcciones.
- Cuando existe una permit TODA LA regla, pero allí también existe una regla de la NEGACIÓN para el puerto 443 o 80 de precedencia más alta.

Nota: La regla de la permit para IP virtual debe estar para el protocolo TCP y el puerto 80, si se inhabilita el secureweb, o el puerto 443, si se habilita el secureweb. Esto es necesario para permitir el acceso del cliente a la autenticación satisfactoria del poste de la dirección IP de la interfaz virtual cuando el CPU ACL existe.

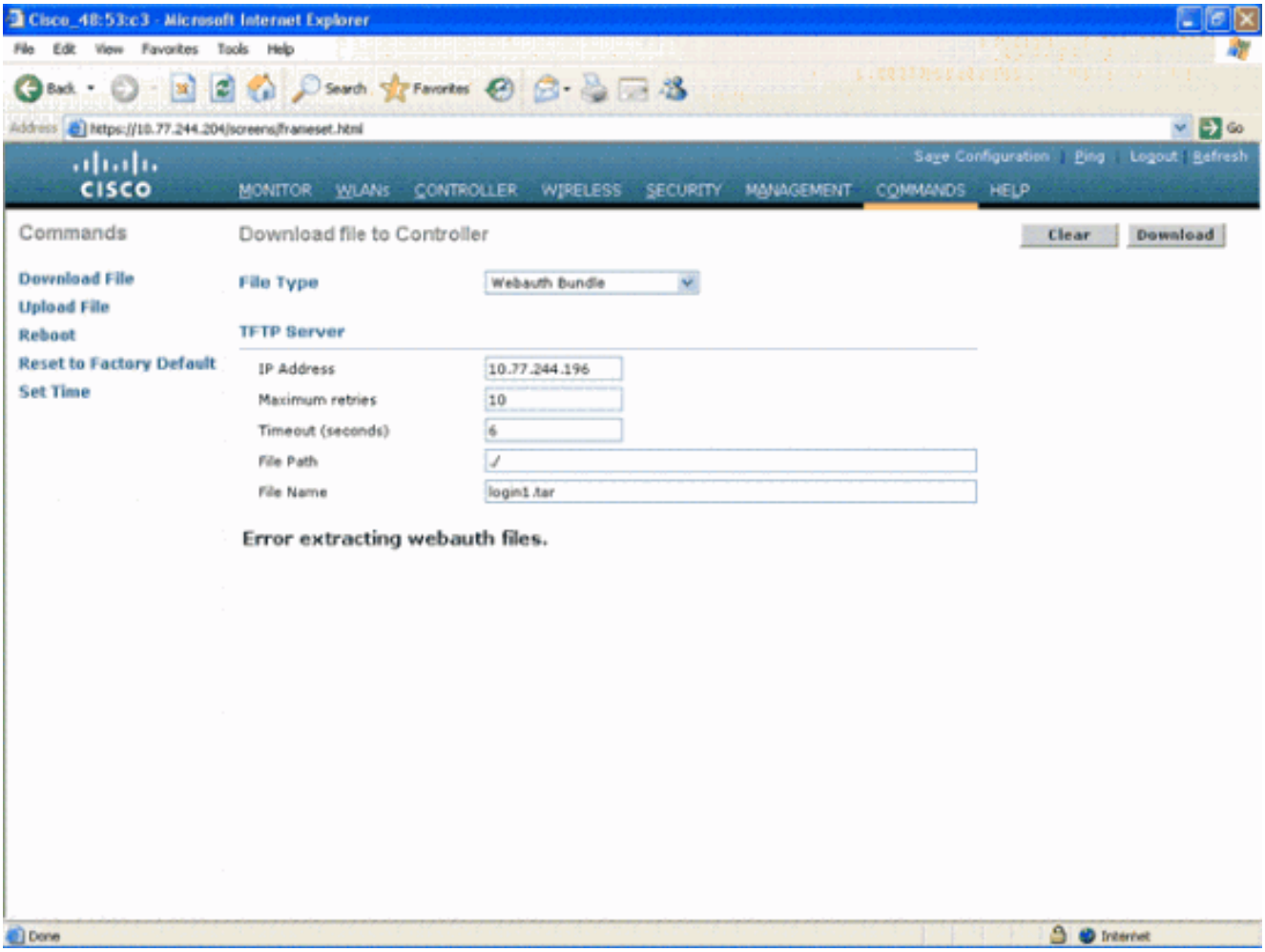
Resolver problemas la autenticación Web

Después de que usted configure la autenticación Web, si la característica no trabaja como se esperaba, complete estos pasos de Troubleshooting:

1. Marque si el cliente consigue una dirección IP. Si no, los usuarios pueden desmarcar el **DHCP requerido** en la red inalámbrica (WLAN) y dar al cliente de red inalámbrica un IP Address estático. Esto asume la asociación con el Punto de acceso. Refiera a la sección de los *problemas del IP Addressing de resolver problemas del cliente en la red del Cisco Unified Wireless para resolver problemas los asuntos relacionados del DHCP*.
2. En las versiones del WLC anterior que 3.2.150.10, usted debe ingresar manualmente **https://1.1.1.1/login.html** para navegar a la ventana de la autenticación Web.El siguiente paso en el proceso es resolución de DNS del URL en el buscador Web. Cuando un cliente WLAN conecta con una red inalámbrica (WLAN) configurada para la autenticación Web, el cliente obtiene una dirección IP del servidor DHCP. El usuario abre a un buscador Web y ingresa un direccionamiento de Web site. El cliente entonces realiza la resolución de DNS de obtener la dirección IP del sitio web. Ahora, cuando el cliente intenta alcanzar el sitio web, el WLC intercepta el HTTP consigue la sesión del cliente y reorienta al usuario a la página de registro de la autenticación Web.
3. Por lo tanto, asegúrese de que el cliente pueda realizar la resolución de DNS para que el cambio de dirección trabaje. En Windows, elija el **Start (Inicio) > Run (Ejecutar)**, ingrese el **CMD** para abrir una ventana de comando, y haga un “nslookup www.cisco.com” y vea si se vuelve el IP Address.En los mac/Linux: abra una ventana de terminal y haga un “nslookup www.cisco.com” y vea si se vuelve la dirección IP.Si usted cree el cliente no está consiguiendo la resolución de DNS, usted puede cualquiera:Ingrese o el IP Address del URL (por ejemplo, http://www.cisco.com es http://198.133.219.25)Intente alcanzar directamente la página del webauth del regulador con https:// <Virtual_interface_IP_Address>/login.html.

Éste es típicamente http://1.1.1.1/login.html.¿Ingresando este URL saca a colación el Web page? Si sí, es más probable un Problema de DNS. Puede ser que también sea un problema del certificado. El regulador, por abandono, utiliza un certificado autofirmado y la mayoría de los buscadores Web advierten contra usarlos.

4. Para la autenticación Web usando la página web personalizada, asegúrese de que el código HTML para la página web personalizada es apropiado.Usted puede descargar un script de la autenticación Web de la muestra de las descargas de software de Cisco. Por ejemplo, para los 4400 reguladores, elija los **Productos > la Tecnología inalámbrica > el regulador del Wireless LAN > los Controladores autónomos > el Cisco Wireless LAN Controllers de la serie 4400 > el regulador > el software del Wireless LAN de Cisco 4404 en el chasis > la autenticación Web Bundle-1.0.1 del regulador del Wireless LAN** y descargue el **archivo webauth_bundle.zip**.Estos parámetros se agregan al URL cuando reorientan al buscador de Internet del usuario a la página de registro personalizada:ap_mac — La dirección MAC del Punto de acceso al cual el usuario de red inalámbrica es asociado.switch_url — El URL del regulador al cual los credenciales de usuario deben ser fijados.reoriente — El URL al cual reorientan al usuario después de que la autenticación sea acertada.código de estado — El código de estado volvió del servidor de la autenticación Web del regulador.wlan — La red inalámbrica (WLAN) SSID a la cual el usuario de red inalámbrica es asociado.Éstos son los códigos de estado disponibles:Código de estado 1: “Le abren una sesión ya. No se requiere ninguna otra acción en su partición”Código de estado 2: “Le no configuran para autenticar contra el portal web. No se requiere ninguna otra acción en su partición”Código de estado 3: “El nombre de usuario especificado no se puede utilizar ahora. Quizás el nombre de usuario se registra ya en el sistema?”Código de estado 4: “Le han excluido.”Código de estado 5: “El Nombre de usuario y la combinación de la contraseña que usted ha ingresado es inválidos. Intente por favor otra vez.”
5. Todos los archivos y imágenes que necesitan aparecer en la página web personalizada se deben liar en un archivo de .tar antes de cargar al WLC. Asegúrese de que uno de los archivos incluidos en el conjunto del alquitrán sea login.html. Usted recibe este mensaje de error si usted no incluye el archivo de
login.html:



Refiera a las guías de consulta para la sección de la autenticación Web Customized del ejemplo de configuración de la autenticación Web del regulador del Wireless LAN para más información sobre cómo crear una ventana personalizada de la autenticación Web.**Nota:** Los archivos que son grandes y los archivos que tienen nombres largos darán lugar a un error de la extracción. Se recomienda que las imágenes están en el formato de .jpg.

6. El Internet Explorer 6.0 es SP1 o más adelante el navegador recomendado para el uso de la autenticación Web. Otros navegadores pueden o no pueden trabajar.
7. Asegúrese de que la opción del **scripting** no esté bloqueada en el buscador del cliente pues la página web personalizada en el WLC es básicamente un script HTML. En IE 6.0, esto se inhabilita por abandono por motivos de seguridad.**Nota:** El estallido encima del molde necesita ser inhabilitado en el navegador si usted ha configurado cualquier surge los mensajes para el usuario.**Nota:** Si usted hojea a un sitio del **https**, el cambio de dirección no trabaja. Refiera al Id. de bug Cisco CSCar04580 (clientes registrados solamente) para más información.
8. Si usted tiene un **nombre del host** configurado para la **interfaz virtual del** WLC, aseegurese que la resolución de DNS está disponible para el nombre del host de la interfaz virtual.**Nota:** Navegue al menú del **regulador > de las interfaces del** WLC GUI para asignar un **nombre del host de DNS a la** interfaz virtual.
9. El Firewall instalado en la computadora cliente bloquea a veces la página de registro de la autenticación Web. Inhabilite el Firewall antes de que usted intente acceder la página de registro. El firewall puede ser habilitado otra vez una vez que se termina la autenticación web.
10. El Firewall de la topología/de la solución se puede colocar entre el cliente y el servidor del red-auth, que depende de la red. En cuanto a cada diseño de red/solución implementados,

el usuario final debe aseegurarse estos puertos se permite en el escudo de protección de la red.

11. Para que la autenticación Web ocurra, el cliente debe primero asociarse a la red inalámbrica (WLAN) apropiada en el WLC. Navegue al menú del **monitor > de los clientes** en el WLC GUI para ver si asocian al cliente al WLC. Marque si el cliente tiene un IP Address válido.
12. Inhabilite las configuraciones de representación en el buscador del cliente hasta que se complete la autenticación Web.
13. El método de autentificación del Web predeterminada es PAP. Asegúrese de que la autenticación PAP esté permitida en el servidor de RADIUS para que esto trabaje. Para marcar el estatus de la autenticación de cliente, marque los debugs y los mensajes del registro del servidor de RADIUS. Usted puede utilizar el **comando all aaa del debug** en el WLC de ver los debugs del servidor de RADIUS.
14. Ponga al día el driver del hardware en el ordenador al último código del sitio web del fabricante.
15. Verifique las configuraciones en el supplicant (programa sobre la laptop).
16. Cuando usted utiliza el supplicant de los Config de Windows cero incorporado a Windows:Verifique al usuario hace las últimas correcciones instalar.Ejecute los debugs en el supplicant.
17. En el cliente, gire los registros EAPOL (WPA+WPA2) y RASTLS de una ventana de comando, Start (Inicio) > Run (Ejecutar) > cmd:`netsh ras set tracing eapol enable`
    `netsh ras set tracing rastls enable`Para inhabilitar los registros, funcione con el mismo comando pero substituya el permiso por la neutralización. Para XP, todos los registros serán situados en C:\Windows\tracing.
18. Si usted todavía no tiene ninguna página web del login, recoja y analice esta salida de un solo cliente:`debug client <mac_address in format xx:xx:xx:xx:xx:xx>`
    ```
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
19. Si el problema no se resuelve después de que usted complete estos pasos, recoja estos debugs y utilice la herramienta de la solicitud de servicio de TAC (clientes registrados solamente) para abrir una solicitud de servicio.`debug pm ssh-appgw enable`
    ```
    debug pm ssh-tcp enable
    debug pm rules enable
    debug emweb server enable
    debug pm ssh-engine enable packet <client ip>
    ```

Información Relacionada

- Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN
- Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems