Troubleshooting de autenticación Web en controlador LAN inalámbrico

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 control y aprovisionamiento de los untos de acceso de red inalámbrica (CAPWAP).
- Conocimiento de cómo configurar el Lightweight Access Point (REVESTIMIENTO) y el WLC para la operación básica.
- Conocimiento básico de la autenticación Web y cómo configurar la autenticación Web en el WLCs. Para la información sobre cómo 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 8.3.121.

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 este hardware:

- Cisco Wireless Controllers de la serie 5500
- Reguladores de la Tecnología inalámbrica de las Cisco 8500 Series
- Cisco Wireless Controllers de la serie 2500
- Cisco Airespace 3500 Series WLAN Controller
- Cisco Airespace 4000 Series Wireless LAN Controller
- Cisco Flex Wireless Controllers de la serie 7500
- Cisco Wireless Services Module 2 (WiSM2)

Autenticación Web en el WLCs

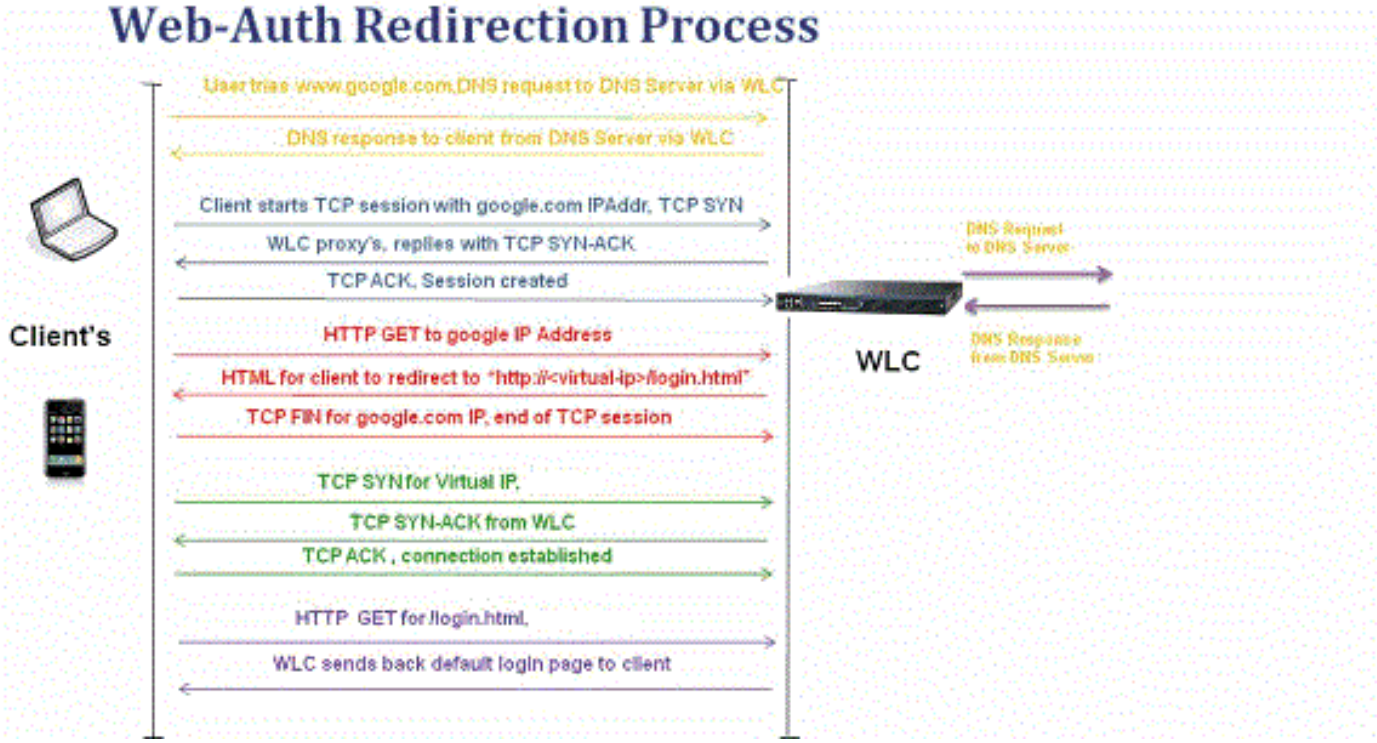
La autenticación Web es una función de seguridad de la capa 3 que hace al regulador no permitir el tráfico IP, excepto el Domain Name System (DNS) DHCP-relacionado de los paquetes - los paquetes relacionados, de un cliente particular hasta que ese cliente haya suministrado correctamente un nombre de usuario válido y una contraseña una excepción del tráfico permitida con un Access Control List del 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://192.0.2.1/login.html (si el es IP virtual se configura que) para procesar. Este proceso saca a colación eventual la página web del login.

> **Note**: Cuando usted utiliza a un servidor Web externo para la autenticación Web, las Plataformas del WLC necesitan una PRE-autenticación ACL para el servidor Web externo.

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 solicitud DNS para que dicha URL obtenga la IP para el destino. El WLC pasa 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 con el la dirección IP 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 y lo envía para el manejo de redireccionamiento. El aplicación HTTP gateway prepara a un cuerpo HTML y lo envía de vuelta como respuesta al HTTP GET solicitado por el cliente. Este HTML hace que el cliente vaya a la URL de la página Web predeterminada, por ejemplo, http:// /login.html.
- El cliente cierra la conexión TCP con la dirección IP, por ejemplo www.google.com.
- Ahora el cliente quiere ir a http:// <virtualip>/login.html y así que intenta abrir una conexión TCP con la dirección IP virtual del WLC. Envía a paquete TCP Syn para 192.0.2.1 (que sea nuestra IP virtual aquí) al WLC.
- El responde con un TCP SYN-ACK y el cliente devuelve un TCP ACK al WLC para completar la aceptación de contacto.
- El cliente envía un HTTP GET para /login.html destinó a 192.0.2.1 para pedir 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 login en la ventana del navegador donde el usuario puede continuar el inicio de sesión.

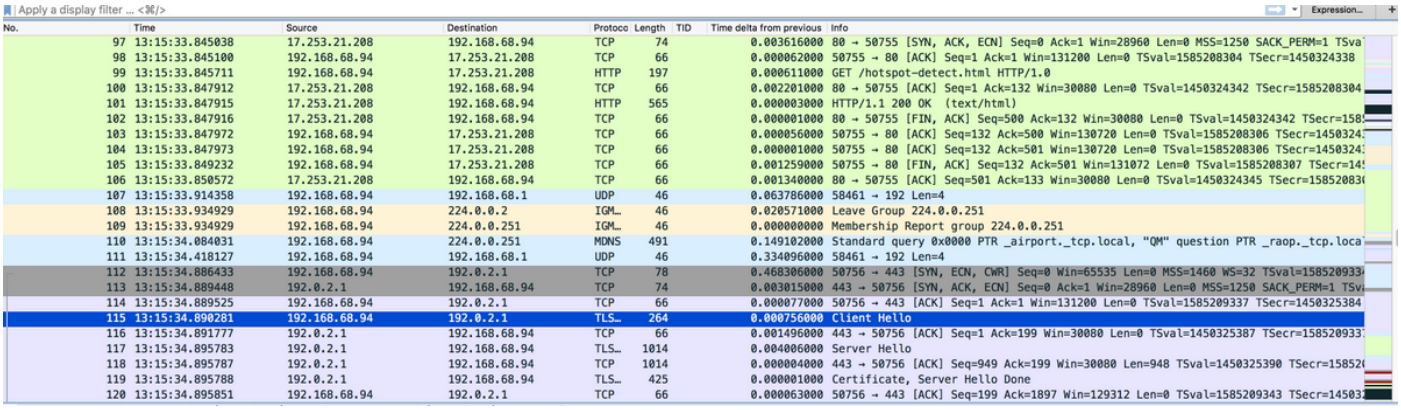
En este ejemplo, la dirección IP del cliente es 192.168.68.94. El cliente resolvió el URL al servidor Web que accedía, 10.1.0.13. Como usted puede ver, el cliente hizo la entrada en contacto de tres

vías para poner en marcha la conexión TCP y después envió un paquete HTTP GET que comenzaba con el paquete 96 (00 es el paquete HTTP). Esto no fue accionada por el usuario, sino era el accionar porta automatizado sistema operativo de la detección (como podemos conjeturar del URL pedido). El regulador intercepta los paquetes y las contestaciones con el código 200. El paquete del código 200 tiene una reorientación URL en él:

```
<HTML><HEAD>
<TITLE> 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://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

Entonces cierra la conexión TCP a través de la entrada en contacto de tres vías.

El cliente entonces enciende la conexión HTTPS a la reorientación URL que la envía a 192.0.2.1, 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 112 comienza las transacciones.


Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=145
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=1585208
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=15852
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=14503

Usted tiene la opción para configurar el Domain Name para la dirección IP virtual del WLC. 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. Una vez que consigue una dirección IP de la resolución de DNS, intenta abrir a una sesión TCP con esa dirección IP, que es una dirección IP configurada 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 de Secure Sockets Layer (SSL).

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

- Utilice 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.
- Utilice 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.
- Utilice 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.

Notas:
- El conjunto personalizado de la autenticación Web 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.

- 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 en el 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.

- 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, solamente también existe una regla de la NEGACIÓN para el puerto 443 o 80 de precedencia más alta.

- 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.

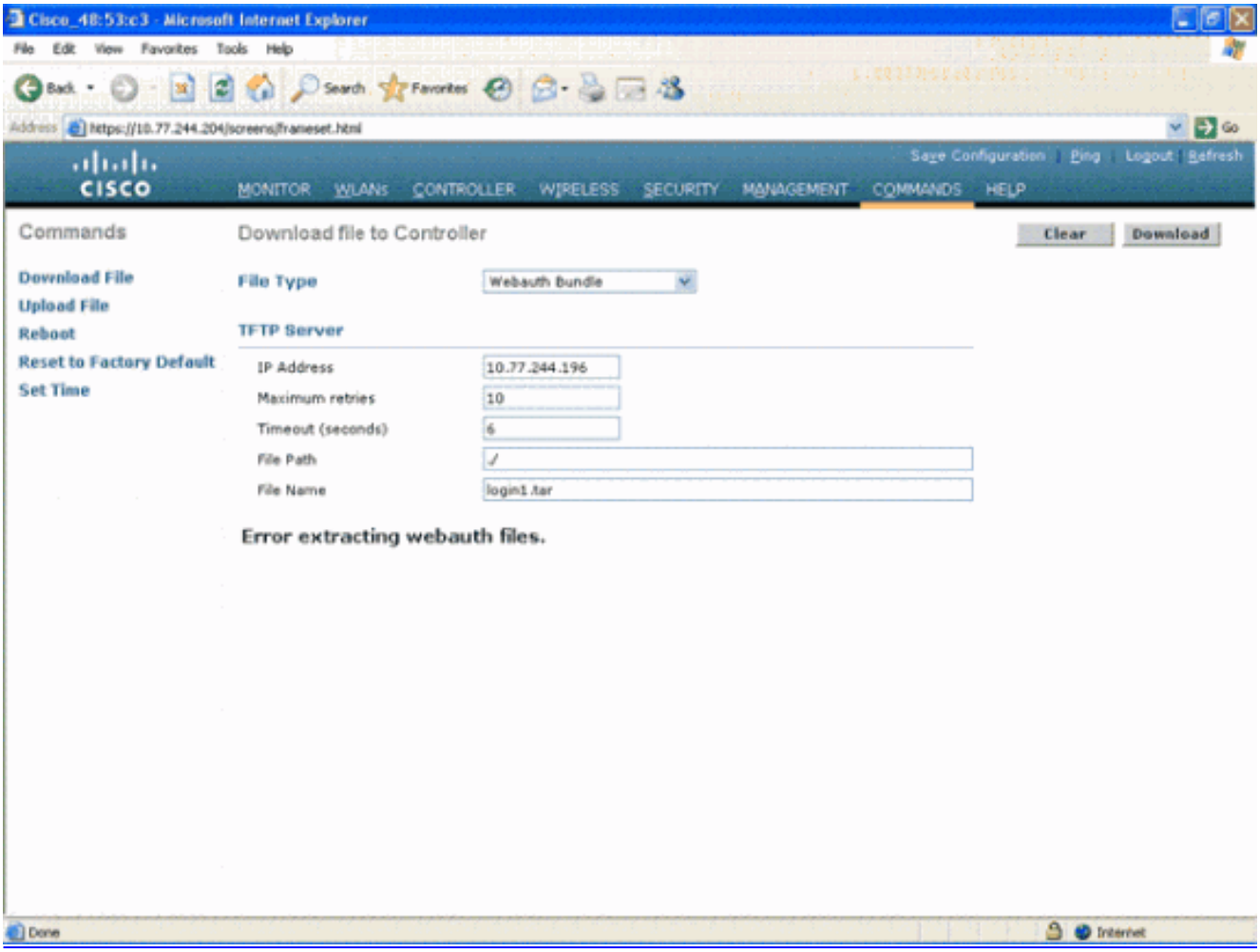
Troubleshooting de Autenticación Web

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

1. Marque si el cliente consigue una dirección IP. Si no, los usuarios pueden desmarcar el **DHCP requirieron la** casilla de verificación en la red inalámbrica (WLAN) y dan a cliente de red inalámbrica un IP Address estático. Esto asume la asociación con el Punto de acceso.
2. 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 la sesión HTTP GET 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 Microsoft 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 consigue 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 teclear cualquier dirección IP (incluso no existente) que deba resolver a través del adaptador de red inalámbrica.¿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 su uso.

4. Para la autenticación Web con una 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 5508 reguladores, elija los **Productos > la Tecnología inalámbrica > el regulador del Wireless LAN > los reguladores del Wireless LAN de los Controladores autónomos > de las Cisco 5500 Series > el regulador > el software del Wireless LAN de Cisco 5508 en el chasis > el conjunto de la autenticación Web 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 que esté cargado al WLC. Asegúrese de que uno de los archivos incluidos en el conjunto de .tar 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.**Note**: 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. 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.
7. 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. **Note**: Navegue al menú del **regulador > de las interfaces del** WLC GUI para asignar un **nombre del host de DNS a la** interfaz virtual.
8. 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.
9. 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.

10. 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.

11. Inhabilite las configuraciones de representación en el buscador del cliente hasta que se complete la autenticación Web.
12. El método de autentificación del Web predeterminada es el protocolo password authentication (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 para ver los debugs del servidor de RADIUS.
13. Ponga al día el driver del hardware en el ordenador al último código del sitio web del fabricante.
14. Verifique las configuraciones en el supplicant (programa sobre la laptop).
15. 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.
16. En el cliente, gire los registros EAPOL (WPA+WPA2) y RASTLS de una ventana de comando. Elija el **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.
17. 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
    ```
18. Si el problema no se resuelve después de que usted complete estos pasos, recoja estos debugs y utilice al administrador del caso de soporte 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 Controlador LAN Inalámbrico
- Ejemplo de configuración de autenticación Web externa con controladores inalámbricos
- Soporte Técnico y Documentación - Cisco Systems