Entender la autenticación Web en controladores LAN inalámbricos (WLC)

Contenido

Introducción

Este documento describe los procesos para la autenticación Web en controladores de LAN inalámbrica (WLC).

Prerequisites

Requirements

Cisco recomienda que usted tenga conocimiento básico de la configuración del WLC.

Componentes Utilizados

La información en este documento se basa en todos los modelos de hardware WLC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Procesos internos de autenticación Web

Posición de la autenticación Web como función de seguridad

La autenticación Web (WebAuth) es seguridad de capa 3. Permite una seguridad fácil de usar que funciona en cualquier estación que ejecute un navegador.

Se puede combinar con cualquier seguridad de clave precompartida (PSK) (política de seguridad de capa 2).

Aunque la combinación de WebAuth y PSK reduce la parte fácil de usar, tiene la ventaja de cifrar el tráfico del cliente.

WebAuth es un método de autenticación sin cifrado.

WebAuth no se puede configurar con 802.1x/RADIUS (servicio de usuario de acceso telefónico de autenticación remota) hasta que se instale y configure simultáneamente la versión 7.4 del software WLC.

Los clientes deben pasar por la autenticación dot1x y web. Está pensado para la adición de un portal web para empleados (que utilizan 802.1x), no para invitados.

No existe un identificador de conjunto de servicios (SSID) "todo en uno" para dot1x para empleados o portal web para invitados.

Cómo funciona WebAuth

El proceso de autenticación 802.11 está abierto, por lo que puede autenticarse y asociarse sin ningún problema. Después de eso, usted está asociado, pero no en el WLC **RUN** estado.

Con la autenticación web habilitada, se le mantiene en **WEBAUTH_REQD** donde no puede acceder a ningún recurso de red.

Debe recibir una dirección IP DHCP con la dirección del servidor DNS en las opciones.

Escriba una dirección URL válida en el explorador. El cliente resuelve la URL a través del protocolo DNS. A continuación, el cliente envía su solicitud HTTP a la dirección IP del sitio web.

El WLC intercepta esa solicitud y devuelve el **webauth** , que imita la dirección IP del sitio web. Con una WebAuth externa, el WLC responde con una respuesta HTTP que incluye su dirección IP del Web site y declara que la página se ha movido.

La página fue trasladada al servidor Web externo utilizado por el WLC. Cuando se autentica, obtiene acceso a todos los recursos de red y se le redirige a la URL solicitada originalmente de forma predeterminada (a menos que se haya configurado un redireccionamiento forzado en el WLC).

En resumen, el WLC permite al cliente resolver el DNS y obtener una dirección IP automáticamente en **WEBAUTH_REQD** estado.

Para controlar otro puerto en lugar del puerto 80, utilice **config network web-auth-port** para crear también un redireccionamiento en este puerto.

Un ejemplo es la interfaz web de Access Control Server (ACS), que se encuentra en el puerto 2002 u otras aplicaciones similares.

> Nota sobre la redirección de HTTPS: De forma predeterminada, el WLC no redirigió el tráfico HTTPS. Esto significa que si escribe una dirección HTTPS en su navegador, no sucede nada. Debe escribir una dirección HTTP para que se le redirija a la página de inicio de sesión que se suministró en HTTPS.
>
> En la versión 8.0 y posteriores, puede habilitar la redirección del tráfico HTTPS con el comando CLI **config network web-auth https-redirect enable.**
>
> Esto utiliza una gran cantidad de recursos para el WLC en los casos en que se envían muchas solicitudes HTTPS. No es recomendable utilizar esta función antes de la versión 8.7 del WLC donde se mejoró la escalabilidad de esta función. Tenga en cuenta también que una advertencia de certificado es inevitable en este caso. Si el cliente solicita cualquier URL (tal como https://www.cisco.com), el WLC todavía presenta su propio certificado emitido para la dirección IP de la interfaz virtual. Esto nunca coincide con la dirección URL/IP solicitada por el cliente y el certificado no es de confianza a menos que el cliente fuerce la excepción en su navegador.

Caída indicativa del rendimiento de la versión del software WLC antes de 8.7 medida :

Webauth	Tasa alcanzada
3 URL: HTTP	140/segundo
1ª URL: HTTP 2ª y 3ª URL: HTTPS	20/segundo
3 URL: HTTPS (gran implementación)	<1/segundo
3 URL: HTTPS (máximo de 100 clientes)	10/segundo

En esta tabla de rendimiento, las 3 URL se denominan:

- La URL original introducida por el usuario final
- La URL a la cual el WLC redirige el navegador
- El envío de credenciales final

La tabla de rendimiento proporciona el rendimiento del WLC en caso de que las 3 URL sean HTTP, en caso de que las 3 URL sean HTTPS o si el cliente pasa de HTTP a HTTPS (típico).

Cómo hacer que WebAuth interno (local) funcione con una página interna

Para configurar una WLAN con una interfaz dinámica operativa, los clientes también reciben una dirección IP de servidor DNS a través de DHCP.

Antes de cualquier **webauth** , está configurado, compruebe que WLAN funciona correctamente, las solicitudes DNS se pueden resolver (**nslookup**), y las páginas web se pueden navegar.

Establezca la autenticación Web como funciones de seguridad de capa 3. Cree usuarios en la base de datos local o en un servidor RADIUS externo.

Consulte el documento Ejemplo de Configuración de Autenticación Web del Controlador de LAN Inalámbrica.

Cómo Configurar un WebAuth Local Personalizado con una Página Personalizada

Local' **webauth** se puede configurar con **redirectUrl** desde **Security** ficha. Esto fuerza una redirección a una página web específica que usted ingresa.

Cuando el usuario es autenticado, invalida la URL original que el cliente solicitó y muestra la página para la cual fue asignada la redirección.

La función personalizada permite utilizar una página HTML personalizada en lugar de la página de inicio de sesión predeterminada. Cargue el paquete de archivos html e image en el controlador.

En la página de carga, busque **webauth bundle** en formato tar. PicoZip crea tars que funcionan de manera compatible con el WLC.

Para ver un ejemplo de un paquete WebAuth, consulte la página Download Software for Wireless Controller WebAuth Bundles. Seleccione la versión apropiada para su WLC.

Se recomienda personalizar un paquete que existe; no cree un nuevo paquete.

Existen algunas limitaciones con **custom webauth** que varían según las versiones y los errores.

- el tamaño del archivo .tar (no más de 5 MB)
- el número de archivos en el .tar
- la longitud del nombre de archivo de los archivos (no más de 30 caracteres)

Si el paquete no funciona, intente un paquete personalizado simple. Añada individualmente archivos y complejidad para llegar al paquete que el usuario intentó utilizar. Esto ayuda a identificar el problema.

Para configurar una página personalizada, refiérase a Creación de una Página de Login de Autenticación Web Personalizada, una sección dentro de la Guía de Configuración de Cisco Wireless LAN Controller, Versión 7.6.

Invalidar técnica de configuración global

Configure con el comando **override global config** y establezca un tipo de WebAuth para cada WLAN. Esto permite una WebAuth interna/predeterminada con una WebAuth interna/predeterminada personalizada para otra WLAN.

Esto permite la configuración de diferentes páginas personalizadas para cada WLAN.

Combine todas las páginas en el mismo paquete y cárguelas en el WLC.

Establezca su página personalizada con el comando **override global config** en cada WLAN y seleccione qué archivo es la página de inicio de sesión de todos los archivos dentro del paquete.

Elija una página de inicio de sesión diferente dentro del paquete para cada WLAN.

Problema de redirección

Hay una variable dentro del conjunto HTML que permite la redirección. No coloque la URL de redirección forzada allí.

Para problemas de redirección en WebAuth personalizado, Cisco recomienda verificar el paquete.

Si ingresa una URL de redireccionamiento con **+=** en la GUI del WLC, esto podría sobrescribir *o* agregar a la URL definida dentro del paquete.

Por ejemplo, en la GUI del WLC, el **redirectURL** se establece en www.cisco.com; sin embargo, en el paquete se muestra: **redirectURL+=** '(URL del sitio web)'. **+=** redirige a los usuarios a una URL no válida.

Cómo hacer que una autenticación Web externa (local) funcione con una página externa

La utilización de un servidor WebAuth externo es sólo un repositorio externo para la página de inicio de sesión. Las credenciales del usuario todavía son autenticadas por el WLC. El servidor web externo permite sólo una página de inicio de sesión especial o diferente.

Pasos realizados para una WebAuth externa:

1. El cliente (usuario final) abre un navegador web e introduce una URL.

2. Si el cliente no está autenticado y se utiliza la autenticación Web externa, el WLC redirige al usuario a la URL del servidor Web externo. El WLC envía un redireccionamiento HTTP al cliente con la dirección IP imitada y señala a la dirección IP del servidor externo. La URL de inicio de sesión de autenticación Web externa se anexa con parámetros como **AP_Mac_Address**,el **client_url** (dirección URL del cliente) y el **action_URL** necesario para ponerse en contacto con el servidor web del switch.

3. La URL del servidor Web externo envía al usuario a una página de inicio de sesión. El usuario puede utilizar una lista de control de acceso (ACL) previa a la autenticación para acceder al servidor.

4. La página de inicio de sesión devuelve la solicitud de credenciales de usuario al **action_URL**, como http://192.0.2.1/login.html, del servidor web WLC. Esto se proporciona como un parámetro de entrada a la URL de redirección, donde 192.0.2.1 es la dirección de la interfaz virtual en el switch.

5. El servidor web del WLC envía el nombre de usuario y la contraseña para la autenticación.

6. El WLC inicia la solicitud del servidor RADIUS o utiliza la base de datos local en el WLC, y luego autentica al usuario.

7. Si la autenticación es exitosa, el servidor web del WLC reenvía al usuario a la URL de redirección configurada o a la URL que el cliente ingresó.

8. Si la autenticación falla, entonces el servidor Web del WLC redirige al usuario de nuevo a la URL de login del usuario.

   Nota : En este documento, utilizamos 192.0.2.1 como ejemplo de ip virtual. Se recomienda utilizar el rango 192.0.2.x para ip virtual ya que no es enrutable. La documentación anterior posiblemente se refiere a "1.1.1.x" o es todavía lo que está configurado en su WLC como este solía ser el ajuste predeterminado. Sin embargo, tenga en cuenta que esta IP es ahora una dirección IP enrutable válida y, por lo tanto, se recomienda la subred 192.0.2.x en su lugar.

Si los puntos de acceso (AP) están en modo FlexConnect, se **preauth** ACL no es relevante. Las ACL flexibles se pueden utilizar para permitir el acceso al servidor web a los clientes que no se han autenticado.

Consulte el Ejemplo de Configuración de Autenticación Web Externa con Controladores de LAN Inalámbrica.

Paso a través de Web

Web Passthrough (Paso a través de Web) es una variación de la autenticación Web interna. Muestra una página con una advertencia o una sentencia de alerta, pero no solicita credenciales.

El usuario hace clic en **aceptar**. Active la entrada de correo electrónico y el usuario podrá introducir su dirección de correo electrónico, que se convertirá en su nombre de usuario.

Cuando el usuario esté conectado, compruebe su lista de clientes activos y verifique que el usuario aparezca en la lista con la dirección de correo electrónico que introdujo como nombre de usuario.

Para obtener más información, consulte el Ejemplo de Configuración del Paso a Través de Web del Controlador de LAN Inalámbrica 5760/3850.

Redirección web condicional

Si habilita una redirección web condicional, el usuario se redirige condicionalmente a una página web determinada después de que la autenticación 802.1x se haya completado correctamente.

Usted puede especificar la paginación de la reorientación y las condiciones bajo las cuales la reorientación ocurre en tu servidor de RADIUS.

Las condiciones pueden incluir la contraseña cuando llegue a la fecha de vencimiento o cuando el usuario necesite pagar una factura por uso/acceso continuo.

Si el servidor RADIUS devuelve el par AV de Cisco **url-redirect**, el usuario será redirigido a la URL especificada cuando abra un navegador.

Si el servidor también devuelve el par AV de Cisco **url-redirect-acl**, la ACL especificada se instala como una ACL de autenticación previa para este cliente.

El cliente no se considera totalmente autorizado en este punto y solo puede pasar el tráfico permitido por la ACL de autenticación previa. Una vez que el cliente completa una operación determinada en la URL especificada (por ejemplo, un cambio de contraseña o pago de factura), el cliente debe volver a autenticarse.

Cuando el servidor RADIUS no devuelve un **url-redirect**, el cliente se considera totalmente autorizado y con permiso para pasar tráfico.

> **Nota:** La función de redirección web condicional solo está disponible para las WLAN configuradas para la seguridad 802.1x o WPA+WPA2 de capa 2.

Después de la configuración del servidor RADIUS, configure la redirección web condicional en el controlador con la GUI o CLI del controlador. Consulte estas guías paso a paso: Configuración de Web Redirect (GUI) y Configuración de Web Redirect (CLI).

Redirección web de página de bienvenida

Si activa la redirección web de la página de bienvenida, el usuario será redirigido a una página web concreta después de que la autenticación 802.1x se haya completado correctamente. Después de la redirección, el usuario tiene acceso completo a la red.

Puede especificar la página de redirección en el servidor RADIUS. Si el servidor RADIUS devuelve el par AV de Cisco **url-redirect**, el usuario será redirigido a la URL especificada cuando abra un navegador.

El cliente se considera totalmente autorizado en este punto y se le permite pasar tráfico, incluso si el servidor RADIUS no devuelve un **url-redirect**.

> **Nota:** La función de redireccionamiento de la página de bienvenida solo está disponible para las WLAN configuradas para la seguridad 802.1x o WPA+WPA2 de capa 2.

Después de la configuración del servidor RADIUS, configure la redirección web de la página de inicio en el controlador con la GUI o CLI del controlador.

Error de WebAuth en filtro MAC

Una WebAuth en Falla de Filtro MAC requiere que configure filtros MAC en el menú de seguridad

de Capa 2.

Si los usuarios se validan correctamente con sus direcciones MAC, accederán directamente a la **run** estado.

Si no lo están, entonces van al **WEBAUTH_REQD** y se produce la autenticación web normal.

> **Nota:** No se admite con paso a través de la Web.Para obtener más información, siga la actividad de la solicitud de mejora ID de error de Cisco CSCtw73512

Autenticación web central

La autenticación Web central se refiere a un escenario donde el WLC ya no aloja ningún servicio. El cliente se envía directamente al portal web de ISE y no pasa por 192.0.2.1 en el WLC. La página de inicio de sesión y todo el portal se externalizan.

La autenticación Web central tiene lugar cuando se ha activado el control de admisión a la red (NAC) RADIUS en la configuración avanzada de los filtros WLAN y MAC.

El WLC envía una autenticación RADIUS (generalmente para el filtro MAC) a ISE, que responde con el **redirect-url** valor de atributo (AV).

A continuación, se coloca al usuario **POSTURE_REQD** hasta que ISE conceda la autorización con una solicitud de cambio de autorización (CoA). El mismo escenario ocurre en Posture o Central WebAuth.

Central WebAuth no es compatible con WPA-Enterprise/802.1x porque el portal de invitados no puede devolver claves de sesión para el cifrado como lo hace con el protocolo de autenticación extensible (EAP).

Autenticación de usuario externo (RADIUS)

La autenticación de usuario externo (RADIUS) es solamente válida para WebAuth local cuando el WLC maneja las credenciales, o cuando una política web de la capa 3 está habilitada. Autentique a los usuarios localmente o en el WLC o externamente a través de RADIUS.

Hay un orden en el que el WLC verifica las credenciales del usuario.

1. En cualquier caso, primero busca en su propia base de datos.
2. Si no encuentra a los usuarios allí, va al servidor RADIUS configurado en el WLAN invitado (si hay uno configurado).
3. A continuación, comprueba la lista global de servidores RADIUS con los servidores RADIUS donde **network user** está activado.

Este tercer punto responde a la pregunta de aquellos que no configuran RADIUS para esa WLAN, pero observan que aún verifica el RADIUS cuando el usuario no se encuentra en el controlador.

Esto se debe a **network user** se compara con los servidores RADIUS de la lista global.

El WLC puede autenticar a los usuarios al servidor RADIUS con el protocolo de autenticación de

contraseña (PAP), el protocolo de autenticación por desafío mutuo (CHAP) o EAP-MD5 (Message Digest5).

Este es un parámetro global y se puede configurar desde la GUI o la CLI:

Desde la GUI: desplácese hasta **Controller > Web RADIUS Authentication**

Desde CLI: escriba **config custom-web RADIUSauth**

> **Nota**: El servidor invitado NAC sólo utiliza PAP.

Cómo configurar una WLAN de invitado por cable

Una configuración de WLAN de invitado por cable es similar a la configuración de invitado inalámbrico. Se puede configurar con uno o dos controladores (solo si uno es de anclaje automático).

Elija una VLAN como VLAN para usuarios invitados por cable, por ejemplo, en la VLAN 50. Cuando un invitado por cable desee acceder a Internet, conecte el portátil a un puerto de un switch configurado para la VLAN 50.

Esta VLAN 50 debe estar permitida y presente en la trayectoria a través del puerto trunk del WLC.

En un caso de dos WLC (un ancla y un extranjero), esta VLAN de invitado por cable debe conducir al WLC extranjero (llamado WLC1) y no al ancla.

El WLC1 entonces se ocupa del túnel de tráfico al WLC DMZ (el ancla, llamado WLC2), que libera el tráfico en la red ruteada.

Estos son los cinco pasos para configurar el acceso de invitado por cable:

1. **Configure una interfaz dinámica (VLAN) para el acceso de usuarios invitados por cable.**

   En WLC1, cree una interfaz dinámica VLAN50. En el **interface configuration** , consulte la **Guest LAN** caja. A continuación, campos como **IP address** y **gateway** desaparecer. El WLC necesita reconocer que el tráfico se rutea desde la VLAN 50. Estos clientes son invitados por cable.

2. **Cree una LAN por cable para el acceso de usuarios invitados.**

   En un controlador, se utiliza una interfaz cuando se asocia a una WLAN. A continuación, cree una WLAN en los controladores de la oficina principal. Vaya a **WLANs** y haga clic en **New**. IN **WLAN Type**, elija **Guest LAN**.

   En **Profile Name** y **WLAN SSID**, ingrese un nombre que identifique esta WLAN. Estos nombres pueden ser diferentes, pero no pueden contener espacios. Se utiliza el término WLAN, pero este perfil de red no está relacionado con el perfil de red inalámbrica.

   General ofrece dos listas desplegables: **Ingress** y **Egress**. La entrada es la VLAN de la que provienen los usuarios (VLAN 50); La salida es la VLAN a la que se envían.

Para **Ingress**, elija **VLAN50**.

Para **Egress**, es diferente. Si sólo tiene un controlador, cree otra interfaz dinámica, un **standard** esta vez (no una LAN para invitados) y envíe usuarios conectados por cable a esta interfaz. En este caso, envíelos al controlador DMZ. Por lo tanto, **Egress** interfaz, seleccione la **Management Interface**.

Security para esta "WLAN" de LAN de invitado es WebAuth, que es aceptable. Haga clic **Ok** para validar.

3. Configure el controlador externo (oficina principal).

Desde **WLAN list**, haga clic en **Mobility Anchor** al final de la **Guest LAN** y seleccione el controlador DMZ. Aquí se supone que ambos controladores se reconocen entre sí. Si no es así, vaya a **Controller** > **Mobility Management** > **Mobility group**y agregue DMZWLC en WLC1. Luego agregue WLC1 en DMZ. Ambos controladores no deben estar en el mismo grupo de movilidad. De lo contrario, se rompen las reglas básicas de seguridad.

4. Configure el controlador de anclaje (el controlador DMZ).

El controlador principal de la oficina está listo. Ahora prepare el controlador DMZ. Abra una sesión del navegador web en el controlador DMZ y navegue hasta las WLAN. Cree una nueva WLAN. IN **WLAN Type**, elija **Guest LAN**.

IN **Profile Name** y **WLAN SSID**, introduzca un nombre que identifique esta WLAN. Utilice los mismos valores que los especificados en el controlador principal de la oficina.

Ingress interfaz aquí es **None**. No importa porque el tráfico se recibe a través del túnel Ethernet sobre IP (EoIP). No es necesario especificar ninguna interfaz de entrada.

Egress es donde se enviarán los clientes. Por ejemplo, el **DMZ VLAN** es VLAN 9. Cree una interfaz dinámica estándar para VLAN 9 en el DMZWLC y, a continuación, seleccione **VLAN 9** como la interfaz de salida.

Configure el final del túnel de anclaje de movilidad. En la lista WLAN, elija **Mobility Anchor for Guest LAN**. Envíe el tráfico al controlador local, DMZWLC. Ambos extremos están listos.

5. Ajuste la red LAN de invitado.

También puede ajustar los parámetros WLAN en ambos extremos. La configuración debe ser idéntica en ambos extremos. Por ejemplo, si hace clic en el botón **WLAN Advanced** ficha, **Allow AAA override** en WLC1, marque la misma casilla en DMZWLC. Si hay alguna diferencia en la WLAN en cualquier lado, el túnel se rompe. DMZWLC rechaza el tráfico; puede ver cuando **run debug mobility**.

Tenga en cuenta que todos los valores se obtienen realmente de DMZWLC: Direcciones IP, valores de VLAN, etc. Configure el lado WLC1 de manera idéntica, de modo que retransmita

la solicitud a la WLCDMZ.

Certificados de la página de inicio de sesión

Esta sección proporciona los procesos para colocar su propio certificado en la página WebAuth o para ocultar la dirección URL 192.0.2.1 de WebAuth y mostrar una dirección URL con nombre.

Cargar un certificado para la autenticación web del controlador

Mediante la GUI (**WebAuth** > **Certificate**) o CLI (tipo de transferencia **webauthcert**) puede cargar un certificado en el controlador.

Tanto si se trata de un certificado creado con su entidad emisora de certificados (CA) como de un certificado oficial de terceros, debe estar en formato .pem.

Antes de enviar, también debe introducir la clave del certificado.

Después de la carga, se requiere un reinicio para que el certificado esté en su lugar. Una vez reiniciado, vaya a la página de certificado de WebAuth en la GUI para encontrar los detalles del certificado que cargó (validez, etc.).

El campo importante es el nombre común (CN), que es el nombre asignado al certificado. Este campo se analiza en este documento en la sección "Autoridad certificadora y otros certificados del controlador".

Después de reiniciar y verificar los detalles del certificado, se le presenta el nuevo certificado del controlador en la página de inicio de sesión de WebAuth. Sin embargo, puede haber dos situaciones.

1. Si su certificado ha sido emitido por una de las pocas CA raíz principales en las que todos los equipos confían, entonces está bien. Un ejemplo es VeriSign, pero normalmente está firmado por una subCA Verisign y no por la CA raíz. Puede registrar el almacén de certificados del explorador si ve la CA mencionada como de confianza.

2. Si obtuvo el certificado de una compañía o CA más pequeña, todos los equipos no confían en ellos. Proporcione también el certificado de la empresa/CA al cliente y una de las CA raíz emite ese certificado. Finalmente, tiene una cadena como "El certificado ha sido emitido por CA x > CA x el certificado ha sido emitido por CA y > CA y el certificado ha sido emitido por esta CA raíz de confianza". El objetivo final es alcanzar una CA en la que el cliente sí confía.

Autoridad de certificación y otros certificados en el controlador

Para deshacerse de la advertencia "este certificado no es de confianza", ingrese el certificado de la CA que emitió el certificado del controlador en el controlador.

A continuación, el controlador presenta ambos certificados (el certificado del controlador y su certificado de CA). El certificado de la CA debe ser una CA de confianza o tener los recursos para verificar la CA. En realidad, puede crear una cadena de certificados de CA que lleve a una CA de confianza en la parte superior.

Coloque toda la cadena en el mismo archivo. El archivo contiene contenido como este ejemplo:

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

Cómo hacer que el certificado coincida con la URL

La URL de WebAuth se establece en 192.0.2.1 para autenticarse y se emite el certificado (este es el campo CN del certificado WLC).

Para cambiar la URL de WebAuth a 'myWLC.com', por ejemplo, vaya al **virtual interface configuration** (la interfaz 192.0.2.1) y allí puede introducir un **virtual DNS hostname**, como myWLC.com.

Esto reemplaza a 192.0.2.1 en su barra de URL. Este nombre también debe poder resolverse. El rastreo del sabueso muestra cómo funciona todo, pero cuando el WLC envía la página de login, el WLC muestra la dirección myWLC.com, y el cliente resuelve este nombre con su DNS.

Este nombre debe resolverse como 192.0.2.1. Esto significa que si también utiliza un nombre para la administración del WLC, utilice un nombre diferente para WebAuth.

Si utiliza myWLC.com asignado a la dirección IP de administración del WLC, debe utilizar un nombre diferente para el WebAuth, tal como myWLCwebauth.com.

Solucionar problemas de certificados

Esta sección explica cómo y qué comprobar para resolver problemas de certificados.

Cómo realizar la comprobación

Descargue OpenSSL (para Windows, busque OpenSSL Win32) e instálelo. Sin ninguna configuración, puede ir al directorio bin e intentarlo **openssl s_client –connect** **(your web auth URL):443**,

si esta URL es la URL a la que está vinculada su página WebAuth en su DNS, consulte "Qué comprobar" en la siguiente sección de este documento.

Si los certificados utilizan una CA privada, coloque el certificado de CA raíz en un directorio de un equipo local y utilice la opción openssl **-CApath**. Si tiene una CA intermedia, colóquela también en el mismo directorio.

Para obtener información general sobre el certificado y comprobarlo, utilice:

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

También es útil convertir certificados con el uso de openssl:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

Qué se debe verificar

Puede ver qué certificados se envían al cliente cuando se conecta. Lea el certificado del dispositivo: el CN debe ser la URL donde se puede acceder a la página web.

Lea la línea "emitido por" del certificado del dispositivo. Debe coincidir con el CN del segundo certificado. Este segundo certificado, "emitido por", debe coincidir con el CN del siguiente certificado, y así sucesivamente. De lo contrario, no crea una cadena real.

En el resultado de OpenSSL que se muestra aquí, observe que **openssl** no se puede comprobar el certificado de dispositivo porque su "emitido por" no coincide con el nombre del certificado de CA proporcionado.

Salida SSL

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

Otro posible problema es que el certificado no se puede cargar en el controlador. En esta situación no hay cuestión de validez, CA, etc.

Para verificarlo, verifique la conectividad del Protocolo de transferencia de archivos trivial (TFTP) e intente transferir un archivo de configuración. Si introduce el **debug transfer all enable** , observe que

el problema es la instalación del certificado.

Esto puede deberse a que se utilizó una clave incorrecta con el certificado. También puede ser que el certificado tenga un formato incorrecto o esté dañado.

Cisco recomienda comparar el contenido del certificado con un certificado conocido y válido. Esto le permite ver si un **LocalkeyID** el atributo muestra todos los ceros (ya se han producido). Si es así, el certificado debe ser reconvertido.

Hay dos comandos con OpenSSL que le permiten volver de .pem a .p12, y luego volver a emitir un .pem con la clave de su elección.

Si recibió un archivo .pem que contiene un certificado seguido de una clave, copie y pegue la parte clave: **----BEGIN KEY ---- until ------- END KEY ------** de .pem a "key.pem".

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12** ? Se le solicitará una clave; escriba **check123**.

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123** Esto da como resultado un archivo .pem operativo con la contraseña **check123**.

Otras situaciones a resolver

Aunque el **anclaje de movilidad** no se ha tratado en este documento, si se encuentra en una situación de **invitado anclado**, asegúrese de que el intercambio de movilidad se produzca correctamente y de que vea que el cliente llega al anclaje.

Cualquier otro problema de WebAuth debe solucionarse en el anclaje.

Estos son algunos problemas comunes que puede resolver:

- **Los usuarios no pueden asociarse a la WLAN de invitado**.

  Esto no está relacionado con WebAuth. Compruebe la configuración del cliente, los parámetros de seguridad de la WLAN, si está activada y si las radios están activas y operativas, etc.

- **Los usuarios no obtienen la dirección IP**.

  En una situación de anclaje de invitado, esto se debe con mayor frecuencia a que el anclaje externo y el anclaje no se configuraron exactamente de la misma manera. De lo contrario, compruebe la configuración DHCP, la conectividad, etc.
- Confirme si otras WLAN pueden utilizar o no el mismo servidor DHCP sin ningún problema. Esto todavía no está relacionado con WebAuth.

- **El usuario no se redirige a la página de inicio de sesión**.

  Este es el síntoma más común, pero es más preciso. Hay dos escenarios posibles.

El usuario no es redirigido (el usuario ingresa una URL y nunca llega a la página WebAuth). Para esta situación, marque:

que se ha asignado un servidor DNS válido al cliente mediante DHCP (**ipconfig /all**),

que el DNS es accesible desde el cliente (**nslookup (website URL**),

que el usuario ha introducido una URL válida para ser redirigido,

que el usuario se dirigió a una URL HTTP en el puerto 80 (por ejemplo, para alcanzar un ACS con http://localhost:2002 no lo redirige ya que usted envió en el puerto 2002 en lugar de 80).

El usuario es redirigido a 192.0.2.1 correctamente, pero la página en sí no se muestra.

Esta situación es más probable que sea un problema del WLC (bug) o un problema del lado del cliente. Puede ser que el cliente tenga algún firewall o software o bloque de políticas. También puede ser que hayan configurado un proxy en su navegador web.

Recomendación: Realice un seguimiento del sabueso en el equipo cliente. No hay necesidad de software inalámbrico especial, solamente Wireshark, que se ejecuta en el adaptador inalámbrico y le muestra si el WLC responde e intenta redirigir. Tiene dos posibilidades: no hay respuesta del WLC, o algo está mal con el intercambio de señales SSL para la página WebAuth. Para el problema de intercambio de señales SSL, puede verificar si el navegador del usuario permite SSLv3 (algunos sólo permiten SSLv2) y si es demasiado agresivo en la verificación del certificado.

Es un paso común ingresar manualmente http://192.0.2.1 para verificar si la página web aparece sin DNS. En realidad, puede escribir http://10.0.0.0 y obtener el mismo efecto. El WLC redirige cualquier dirección IP que usted ingrese. Por lo tanto, si ingresa http://192.0.2.1, no le hará trabajar alrededor del redireccionamiento web. Si ingresa https://192.0.2.1(secure), esto no funciona porque el WLC no redirige el tráfico HTTPS (de forma predeterminada, esto es realmente posible en la versión 8.0 y posterior). La mejor manera de cargar la página directamente sin un redireccionamiento es ingresar https://192.0.2.1/login.html.

- **Los usuarios no pueden autenticarse**.

  Consulte la sección de este documento que trata sobre la autenticación. Verifique las credenciales localmente en el RADIUS.

- **Los usuarios pueden autenticarse correctamente a través de WebAuth, pero después no tienen acceso a Internet**.

  Puede quitar WebAuth de la seguridad de la WLAN, y después tiene una WLAN abierta. A continuación, puede intentar acceder a la Web, al DNS, etc. Si también experimenta problemas allí, quite por completo la configuración de WebAuth y verifique la configuración de sus interfaces.

Para obtener más información, consulte: Resolución de problemas de autenticación Web en un

controlador de LAN inalámbrica (WLC).

Servidor proxy HTTP y cómo funciona

Puede utilizar un servidor proxy HTTP. Si necesita que el cliente agregue una excepción en su navegador de que 192.0.2.1 no debe pasar a través del servidor proxy, puede hacer que el WLC escuche el tráfico HTTP en el puerto del servidor proxy (generalmente 8080).

Para entender este escenario, necesita saber qué hace un proxy HTTP. Es algo que se configura en el lado del cliente (dirección IP y puerto) en el navegador.

La situación habitual cuando un usuario visita un sitio web es resolver el nombre en IP con DNS y, a continuación, pedir la página web al servidor web. El proceso siempre envía la solicitud HTTP para la página al proxy.

El proxy procesa el DNS, si es necesario, y lo reenvía al servidor web (si la página no está ya almacenada en caché en el proxy). La discusión es solo de cliente a proxy. Si el proxy obtiene o no la página web real es irrelevante para el cliente.

Este es el proceso de autenticación web:

- El usuario escribe en una URL.
- El PC cliente envía al servidor proxy.
- WLC intercepta e imita la IP del servidor proxy; responde al PC con una redirección a 192.0.2.1

En esta etapa, si la PC no está configurada para ello, solicita la página 192.0.2.1 WebAuth al proxy para que no funcione. El PC debe hacer una excepción para 192.0.2.1; luego envía una solicitud HTTP a 192.0.2.1 y continúa con WebAuth.

Cuando se autentica, todas las comunicaciones pasan de nuevo a través del proxy. Una configuración de excepción suele estar en el explorador cerca de la configuración del servidor proxy. A continuación, verá el mensaje: "No utilizar proxy para esas direcciones IP".

Con WLC versión 7.0 y posterior, la función **webauth proxy redirect** se puede habilitar en las opciones globales de la configuración del WLC.

Cuando está habilitado, el WLC verifica si los clientes están configurados para utilizar manualmente un proxy. En ese caso, redirigen al cliente a una página que le muestra cómo modificar la configuración de proxy para que todo funcione.

La redirección del proxy de WebAuth se puede configurar para funcionar en una variedad de puertos y es compatible con la autenticación Web central.

Para ver un ejemplo sobre la redirección de proxy de WebAuth, consulte Ejemplo de Configuración de Web Authentication Proxy en un Controlador de LAN Inalámbrica.

Autenticación web en HTTP en lugar de HTTPS

Puede iniciar sesión en la autenticación web en HTTP en lugar de HTTPS. Si inicia sesión en HTTP, no recibirá alertas de certificados.

Para versiones anteriores al código WLC versión 7.2, debe inhabilitar la administración HTTPS del WLC y dejar la administración HTTP. Sin embargo, esto solamente permite la administración Web del WLC sobre HTTP.

Para el código de la versión 7.2 del WLC, utilice el **config network web-auth secureweb disable** comando para desactivar. Esto solo inhabilita HTTPS para la autenticación web y no para la administración. Tenga en cuenta que esto requiere un reinicio del controlador.

En WLC Release 7.3 y el código posterior, puede habilitar/inhabilitar HTTPS para WebAuth solamente vía GUI y CLI.

Información Relacionada

- Ejemplo de Configuración de la Autenticación Web del Controlador LAN Inalámbrico
- Descargue el software para los paquetes WebAuth del controlador inalámbrico
- Creación de una Página de Login de Autenticación Web Personalizada
- Ejemplo de configuración de autenticación web externa con controladores de LAN inalámbrica
- Ejemplo de Configuración del Wireless LAN Controller 5760/3850 Web Passthrough
- Configuración de Web Redirect (GUI)
- Configuración de Web Redirect (CLI)
- Troubleshooting de autenticación Web en controlador LAN inalámbrico
- Ejemplo de Configuración de Web Authentication Proxy en un Controlador de LAN Inalámbrica
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).