Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN

Contenido

Introducción

Este documento explica cómo utilizar un servidor Web externo para configurar un controlador de LAN inalámbrico (WLC) para la autenticación Web.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento básico de la configuración de los Puntos de acceso ligeros (revestimientos) y del WLCs de Cisco

- Conocimiento básico del protocolo del Lightweight Access Point (LWAPP) y control y aprovisionamiento de los untos de acceso de red inalámbrica (CAPWAP)
- Conocimiento en cómo configurar y configurar a un servidor Web externo
- Conocimiento en cómo configurar y configurar el DHCP y a los servidores DNS

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC de Cisco 4400 que funciona con la versión de firmware 7.0.116.0
- REVESTIMIENTO de las Cisco 1131AG Series
- Adaptador de red inalámbrica de cliente de Cisco 802.11a/b/g que funciona con la versión de firmware 3.6
- Servidor Web externo que recibe la página de registro de la autenticación Web
- DNS y servidores DHCP para el address resolution y la asignación de IP Address a los clientes de red inalámbrica

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.

Convenciones

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

Antecedentes

La autenticación Web es una función de seguridad de la capa 3 que hace al regulador no permitir el tráfico IP (excepto el DHCP y el DNS - los paquetes relacionados) de un cliente particular hasta que ese cliente haya suministrado correctamente un nombre de usuario válido y una contraseña. La autenticación Web es un método de autenticación simple sin la necesidad de un supplicant o de una utilidad de cliente.

La autenticación Web se puede realizar usando:

- Ventana predeterminada del login en el WLC
- Versión modificada de la ventana predeterminada del login en el WLC
- Una ventana personalizada del login que usted configura en un servidor Web externo (autenticación del Web externa)
- Una ventana personalizada del login que usted descarga al regulador

Este documento proporciona un ejemplo de configuración para explicar cómo configurar el WLC para utilizar un script del login de un servidor Web externo.

Proceso de autenticación del Web externa

Con la autenticación del Web externa, la página de registro usada para la autenticación Web se

salva en un servidor Web externo. Ésta es la Secuencia de eventos cuando un cliente de red inalámbrica intenta acceder una red WLAN que tenga autenticación del Web externa habilitada:

1. El cliente (usuario final) conecta con el WLAN y abre a un buscador Web y ingresa un URL, tal como www.cisco.com.
2. El cliente envía una petición DNS a un servidor DNS para resolver www.cisco.com a la dirección IP.
3. El WLC adelante la petición al servidor DNS que, a su vez, resuelve www.cisco.com a la dirección IP y envía una contestación DNS. El regulador adelante la contestación al cliente.
4. El cliente intenta iniciar una conexión TCP con la dirección IP de www.cisco.com enviando paquete TCP Syn a la dirección IP de www.cisco.com.
5. El WLC tiene reglas configuradas para el cliente y por lo tanto puede actuar como proxy para www.cisco.com. Devuelve un paquete TCP SYN-ACK al cliente con la fuente como la dirección IP de www.cisco.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.
6. 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 que el cliente va a la página web predeterminada URL del WLC, por ejemplo, http:// <Virtual-Server-IP>/login.html.
7. El cliente entonces enciende la conexión HTTPS a la reorientación URL que la envía a 1.1.1.1. Ésta 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.
8. Porque se habilita la autenticación del Web externa, el WLC reorienta al cliente al servidor Web externo.
9. El login URL del auth del Web externa se añade al final del fichero con los parámetros tales como el AP_Mac_Address, el client_url (www.cisco.com) y el action_URL que el cliente necesita para entrar en contacto al servidor Web del regulador.**Note**: El action_URL dice a servidor Web que el nombre de usuario y contraseña está salvado en el regulador. Las credenciales se deben devolver al regulador para conseguir autenticadas.
10. El servidor Web URL del externo lleva al usuario a una página de registro.
11. La página de registro toma la entrada de los credenciales de usuario, y envía la petición de nuevo al action_URL, ejemplo http://1.1.1.1/login.html, del servidor Web del WLC.
12. El servidor Web del WLC somete el nombre de usuario y contraseña para la autenticación.
13. El WLC inicia la petición del servidor de RADIUS o utiliza la base de datos local en el WLC y autentica al usuario.
14. Si la autenticación es acertada, el servidor Web del WLC cualquiera adelante el usuario al configurado reorienta el URL o al URL el cliente comenzó con, por ejemplo www.cisco.com.
15. Si la autenticación falla, después el servidor Web del WLC reorienta al usuario de nuevo al login URL del cliente.

Note: Para configurar el webauthentication externo para utilizar los puertos con excepción del HTTP y del HTTPS, publique este comando:

```
(Cisco Controller) >config network web-auth-port

<port>          Configures an additional port to be redirected for web authentication.
```

Configuración de la red

El ejemplo de configuración utiliza esta configuración. UN REVESTIMIENTO se registra al WLC. Usted necesita configurar a un **invitado de la** red inalámbrica (WLAN) para los Usuarios invitados y tuvo que habilitar la autenticación Web para los usuarios. Usted también necesita asegurarse de que el regulador reoriente al usuario al servidor Web externo URL (para la autenticación del Web externa). El servidor Web del externo recibe la página de registro de la red que se utiliza para la autenticación.

Los credenciales de usuario se deben validar contra la base de datos local mantenida en el regulador. Después de la autenticación satisfactoria, los usuarios deben no ser prohibidos el acceso al invitado de la red inalámbrica (WLAN). El regulador y los otros dispositivos necesitan ser configurados para esta configuración.

Note: Usted puede utilizar una versión personalizada del script del login, que serán utilizados para la autenticación Web. Usted puede descargar un script de la autenticación Web de la muestra de la página de las descargas de software de Cisco. Por ejemplo, para los 4400 reguladores, navegue a los **Productos > a la Tecnología inalámbrica > al regulador del Wireless LAN > a los Controladores autónomos > al Cisco Wireless LAN Controllers de la serie 4400 > al regulador > al 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**.

Note: 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.

Note: Este documento asume que configuran el DHCP, el DNS y a los servidores Web externos. Refiera a la documentación para información apropiada del otro vendedor en cómo configurar el DHCP, el DNS y al servidor Web externo.

Configurar

Antes de que usted configure el WLC para la autenticación del Web externa, usted debe configurar el WLC para la operación básica y registrar los revestimientos al WLC. Este documento asume que el WLC está configurado para la operación básica y que los revestimientos están registrados al WLC. Refiera al registro ligero AP (REVESTIMIENTO) a un regulador del Wireless LAN (WLC) si usted es usuario nuevo que intenta configurar el WLC para la operación básica con los revestimientos.

Complete estos pasos para configurar los revestimientos y el WLC para esta configuración:

1. Cree una interfaz dinámica para los Usuarios invitados
2. Cree una Autenticación previa ACL
3. Cree una base de datos local en el WLC para los Usuarios invitados
4. Configure el WLC para la autenticación del Web externa
5. Configure la red inalámbrica (WLAN) para los Usuarios invitados

Cree una interfaz dinámica para los Usuarios invitados

Complete estos pasos para crear una interfaz dinámica para los Usuarios invitados:

1. Del WLC GUI, elija los **reguladores > las interfaces**.La ventana de las interfaces aparece. Esta ventana enumera las interfaces que se configuran en el regulador. Esto incluye las interfaces predeterminadas, que son la interfaz de administración, interfaz del ap-administrador, la interfaz virtual y la interfaz de puerto del servicio, y las interfaces dinámicas definidas por el usario.
2. Tecleo **nuevo** para crear una nueva interfaz dinámica.
3. En las **interfaces > la nueva ventana**, ingrese el nombre de la interfaz y la identificación de VLAN. Entonces, el tecleo **se aplica**.En este ejemplo, la interfaz dinámica se nombra **invitado** y la identificación de VLAN se asigna **10.**
4. En las **interfaces > edite la** ventana, para la interfaz dinámica, ingrese el IP Address, la máscara de subred, y el default gateway. Asígnela a un puerto físico en el WLC, y ingrese el IP Address del servidor DHCP. Entonces, el tecleo **se aplica**.

Cree una Autenticación previa ACL

Al usar 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 (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.

Sin embargo, es una práctica adecuada configurar una Autenticación previa ACL para el servidor Web externo al usar la autenticación del Web externa.

Complete estos pasos para configurar la Autenticación previa ACL para la red inalámbrica (WLAN):

1. Del WLC GUI, elija la **Seguridad > las listas de control de acceso**.Esta ventana permite que usted vea los ACL actuales que son similares al Firewall estándar ACL.
2. Tecleo **nuevo** para crear un nuevo ACL.
3. Ingrese el nombre del ACL y del tecleo **se aplican**.En este ejemplo, el ACL se nombra PRE-Auth-para-Externo-Red-**Servidor**.
4. Para el nuevo ACL creado, el tecleo **edita**.El ACL > edita la ventana aparece. Esta ventana deja al usuario definir las nuevas reglas o modificar las reglas del ACL que existen.
5. El tecleo **agrega la nueva regla**.
6. Defina una regla ACL que permita el acceso para los clientes al servidor Web externo.En este ejemplo, 172.16.1.92 es la dirección IP externa del servidor Web.
7. El tecleo **se aplica** para confiar los cambios.

Cree una base de datos local en el WLC para los Usuarios invitados

La base de datos de usuarios para los Usuarios invitados se puede salvar en la base de datos local del regulador del Wireless LAN, o pudo ser externo salvado del regulador.

En este documento la base de datos local en el regulador se utiliza para autenticar a los usuarios. Usted debe crear a un usuario de red local y definir una contraseña para la conexión con el sistema cliente de la autenticación Web. Complete estos pasos para crear la base de datos de usuarios en el WLC:

1. Del WLC GUI, elija la **Seguridad**.

2. Haga clic a los **usuarios de red local del** menú AAA a la izquierda.
3. Haga clic **nuevo** para crear a un usuario nuevo.Visualizaciones de una nueva ventana que pide la información del nombre de usuario y contraseña.
4. Ingrese un Nombre de usuario y una contraseña para crear a un usuario nuevo, después confirme la contraseña que usted quiere utilizar.Este ejemplo crea al usuario nombrado **User1**.
5. Agregue una descripción, si lo desea.Este ejemplo utiliza el **user1 del invitado**.
6. Haga clic en **Aplicar** para guardar la configuración del usuario nuevo.
7. Relance los pasos 3-6 para agregar a más usuarios a la base de datos.

Configure el WLC para la autenticación del Web externa

El siguiente paso es configurar el WLC para la autenticación del Web externa. Complete estos pasos:

1. Del regulador GUI, elija el **auth de la Seguridad > de la red > la página de registro de la red** para acceder la página de registro de la red.
2. De la casilla desplegable del tipo de la autenticación Web, elija el **externo (reoriente al servidor externo)**.
3. En la sección **externa del servidor Web**, agregue al nuevo servidor Web externo.
4. En la **reorientación URL después del** campo del **login**, ingrese el URL de la página a la cual reorientarán al usuario final sobre a la autenticación satisfactoria. En el campo **URL del auth del Web externa**, ingrese el URL donde la página de registro se salva en el servidor Web externo.**Note**: En las versiones 5.0 del WLC y posterior, la página del logout para la autenticación Web puede también ser personalizada. Refiera a las páginas del login, de la falla de registro y del logout de la asignación por la sección de la red inalámbrica (WLAN) de la *configuración de controlador Guide,5.2 del Wireless LAN* para más información sobre cómo configurarla.

Configure la red inalámbrica (WLAN) para los Usuarios invitados

El último paso es crear los WLAN para los Usuarios invitados. Complete estos pasos:

1. Haga clic los **WLAN del** regulador GUI para crear una red inalámbrica (WLAN).La ventana del WLAN aparece. Esta ventana enumera los WLAN configurados en el regulador.
2. Tecleo **nuevo** para configurar una nueva red inalámbrica (WLAN).En este ejemplo, la red inalámbrica (WLAN) se nombra **Guest** y el ID DE WLAN es **1.**
3. Haga clic en Apply (Aplicar).
4. En la red inalámbrica (WLAN) > edite la ventana, definen los parámetros específicos a la red inalámbrica (WLAN).Para la red inalámbrica (WLAN) del invitado, en la ficha general, elija la interfaz apropiada del campo de nombre de la interfaz.Este ejemplo asocia al **invitado de la** interfaz dinámica que fue creado previamente al invitado de la red inalámbrica (WLAN).Vaya a la **pestaña Seguridad**. Bajo Seguridad de la capa 2, no se selecciona **ninguno** en este ejemplo.**Note**: La autenticación Web no se soporta con la autenticación del 802.1x. Esto significa que usted no puede elegir el 802.1x o a WPA/WPA2 con el 802.1x como la Seguridad de la capa 2 cuando usted utiliza la autenticación Web. La autenticación Web se soporta con el resto de los parámetros de seguridad de la capa 2.En el campo de Seguridad de la capa 3, marque la **casilla de verificación Web Policy** y elija la **opción de**

autenticación.Se elige esta opción porque la autenticación Web se utiliza para autenticar a los clientes inalámbricos del invitado.Elija la Autenticación previa apropiada ACL del menú desplegable.En este ejemplo, se utiliza la Autenticación previa ACL que fue creada previamente.Haga clic en Apply (Aplicar).

Verificación

El cliente de red inalámbrica sube y el usuario ingresa el URL, tal como www.cisco.com, en el buscador Web. Porque no han autenticado al usuario, el WLC reorienta al usuario al login URL del Web externa.

Indican al usuario para los credenciales de usuario. Una vez que el usuario somete el nombre de usuario y contraseña, la página de registro toma la entrada de los credenciales de usuario y encendido somete envía la petición de nuevo al ejemplo del action_URL, http://1.1.1.1/login.html, del servidor Web del WLC. Se proporciona esto mientras que un parámetro de entrada al cliente reorienta el URL, donde está el direccionamiento 1.1.1.1 de la interfaz virtual en el Switch.

El WLC autentica al usuario contra la base de datos local configurada en el WLC. Después de la autenticación satisfactoria, el servidor Web del WLC cualquiera adelante el usuario al configurado reorienta el URL o al URL el cliente comenzó con, por ejemplo www.cisco.com.

Troubleshooting

Utilice estos comandos debug para resolver problemas su configuración.

- haga el debug del <client-MAC-direccionamiento xx de las direcciones MAC: xx: xx: xx: xx: xx>
- debug aaa all enable
- permiso del estado PEM del debug
- permiso de los eventos PEM del debug
- permiso del mensaje DHCP del debug
- permiso del paquete DHCP del debug
- permiso del debug P.M. SSH-appgw
- permiso del debug P.M. SSH-TCP

Use esta sección para resolver problemas de configuración.

Los clientes reorientados al servidor de autenticación del Web externa reciben una advertencia del certificado

Problema: Cuando reorientan a los clientes al servidor de autenticación del Web externa de Cisco, reciben una advertencia del certificado. Hay un certificado válido en el servidor, y si usted conecta con el servidor de autenticación del Web externa directamente la advertencia del certificado no se recibe. ¿Es esto porque presentan la dirección IP virtual (1.1.1.1) del WLC al cliente en vez de la dirección IP real del servidor de autenticación del Web externa que se asocia al certificado?

Solución: Yes. Independientemente de si usted realiza la autenticación del local o del Web externa, usted todavía golpea al servidor Web interno en el regulador. Cuando usted reorienta a un servidor Web externo, usted todavía recibe la advertencia del certificado del regulador a

menos que usted tenga un certificado válido en el regulador sí mismo. Si la reorientación se envía al https, usted recibe la advertencia del certificado del regulador y del servidor Web externo, a menos que ambos tengan un certificado válido.

Para librarse de las advertencias todas del certificado juntas, usted necesita tener un certificado del nivel de la raíz publicado y descargado sobre su regulador. El certificado se publica para un nombre del host y usted pone que nombre del host en el cuadro del nombre del host DNS bajo interfaz virtual en el regulador. Usted también necesita agregar el nombre del host a su servidor DNS local y señalarlo a la dirección IP virtual (1.1.1.1) del WLC.

Refiera a la generación del pedido de firma de certificado (CSR) para un certificado de tercera persona en un controlador de WLAN (WLC) para más información.

Error: la “página no puede ser visualizada”

Problema: Después de que el regulador se actualice a 4.2.61.0, la “página no puede ser” mensaje de error visualizado aparece cuando usted utiliza una página web descargada para la autenticación Web. Esto trabajada bien antes de la actualización. La página web interna predeterminada carga sin ningún problema.

Solución: De la versión 4.2 y posterior del WLC se introduce una nueva función en donde usted puede tener páginas de registro cutomized múltiplo para la autenticación Web.

Para tener la carga de la página web correctamente, no es suficiente fijar el tipo de la autenticación Web según lo **personalizado** global en la **página de registro del auth de la Seguridad > de la red > de la red**. Debe también ser configurado en una red inalámbrica (WLAN) determinada. A tal efecto, complete estos pasos:

1. Registro en el GUI del WLC.
2. Haga clic en la lengueta **WLAN**, y acceda el perfil del WLAN configurado para la autenticación Web.
3. En la red inalámbrica (WLAN) > edite la página, hacen clic la **ficha de seguridad**. Entonces, elija la **capa 3.**
4. En esta página, no elija **ninguno** como la Seguridad de la capa 3.
5. Marque el cuadro de la **directiva de la red**, y elija la **opción de autenticación**.
6. Marque el cuadro del **permiso de la** configuración global de la invalidación, elija **personalizado (descargado)** como el tipo del auth de la red, y seleccione la página de registro deseada del menú de **Pagepull del login** abajo. Haga clic en Apply (Aplicar).

Información Relacionada

- Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN
- Vídeo: Autenticación Web en los controladores LAN de la tecnología inalámbrica de Cisco (WLCs)
- Ejemplo de Configuración de VLANs en Controladores de LAN Inalámbrica
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems