Autenticación Web en el controlador de WLAN

Contenido

Introducción

Este documento explica los procesos para la autenticación Web en un regulador del Wireless LAN (WLC).

Prerequisites

Requisitos

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

Componentes Utilizados

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

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.

Procesos internos de la autenticación Web

Posición de la autenticación Web como función de seguridad

La autenticación Web (WebAuth) es Seguridad de la capa 3. Permite la Seguridad convivial que trabaja en cualquier estación que funcione con a un navegador. Puede también ser combinada con cualquier Seguridad de la clave previamente compartida (PSK) (política de seguridad de la capa 2). Aunque la combinación de WebAuth y de PSK reduzca la porción convivial perceptiblemente y no se utilice a menudo, todavía tiene la ventaja para cifrar el tráfico del cliente. WebAuth es un método de autentificación sin el cifrado.

WebAuth no se puede configurar con 802.1x/RADIUS (Remote Authentication Dial-In User Service) hasta que la versión de software WLC 7.4 esté instalada donde puede ser configurada al mismo tiempo. Sin embargo, sea consciente que los clientes deben pasar con el dot1x y la autenticación Web. No se significa para el invitado, sino para la adición de un portal web para los empleados (quién 802.1x del uso). No hay un Service Set Identifier (SSID) todo junto para el dot1x para los empleados o el portal web para los invitados.

Cómo WebAuth trabaja

El proceso de autenticación del 802.11 está abierto, así que usted puede autenticar y asociarse sin ningún tipo de problema. Después de eso, usted es asociado, pero no en el estado de **FUNCIONAMIENTO del** WLC. Con la autenticación Web habilitada, le mantienen **WEBAUTH_REQD** donde usted no puede acceder a ningún recurso de red (ningún ping, y así sucesivamente). Usted debe recibir una dirección IP del DHCP con el direccionamiento del servidor DNS en las opciones.

Usted debe teclear un URL válido en su navegador. El cliente resuelve el URL con el protocolo DNS. El cliente entonces envía su pedido de HTTP a la dirección IP del sitio web. Las interceptaciones del WLC que petición y devuelven la página de registro del **webauth**, que las parodias la dirección IP del sitio web. En el caso de un WebAuth externo, el WLC contesta con un HTTP de respuesta que incluya su dirección IP y estados del sitio web que la página ha movido. La página fue movida al servidor Web externo usado por el WLC. Cuando le autentican, usted accede a todos los recursos de red y se reorienta al URL pedido originalmente, por abandono (a menos que un forzado reorienta fue configurado en el WLC). En resumen, el WLC permite que el cliente resuelva el DNS y consiga una dirección IP automáticamente en el estado **WEBAUTH_REQD**.

Consejo: Si usted quisiera que el WLC mirara otro puerto en vez del puerto 80, usted puede utilizar el **number> del <port del red-auth-puerto de la red de los config** para crear una

reorientación en este puerto también. Un ejemplo es la interfaz Web del Access Control Server (ACS), que está en las aplicaciones similares del puerto 2002 u otro.

> **Observe sobre el redireccionamiento HTTPS**: Por abandono y en las versiones 7.x y anterior, el WLC no reorientó el tráfico HTTPS. Esto significa que si usted abre a su navegador y teclea un direccionamiento HTTPS, sucede nada. Usted debe teclear dirección HTTP para conseguir reorientado a la página de registro que fue servida en el HTTPS.
>
> En la versión 8.0 y posterior, usted puede habilitar el cambio de dirección del tráfico HTTPS con el comando CLI que el red-**auth de la red de los config https-reorienta el permiso.**
>
> Sea consciente que éste es recurso que consume para el WLC en caso de que se envíen muchas peticiones HTTPS. Se aconseja para no utilizar esta característica antes de la versión 8.7 del WLC donde el scalability de esta característica fue aumentado. También observe que una advertencia del certificado es inevitable en este caso. De hecho, si sus pedidos de cliente cualquier URL (tal como https://www.cisco.com), el WLC todavía presenta su propio certificado publicado para la dirección IP de la interfaz virtual. Esto obviamente nunca hará juego la dirección IP URL pedida por el cliente y el certificado no será confiado en a menos que el cliente fuerce la excepción en su navegador.

Indicativo rendimiento cae de la versión de software WLC antes de 8.7 medidos:

Webauth	**Tarifa alcanzada**
3 URL - HTTP	140/en segundo lugar
1r URL - HTTP 2dos y 3ro URL - HTTPS	20/en segundo lugar
3 URL - HTTPS (despliegue grande)	<1/en segundo lugar
3 URL - HTTPS (máximo de 100 clientes)	10/en segundo lugar

En esta tabla del funcionamiento, los 3 URL se refieren como:

- El URL original ingresó por el usuario final (el Web site que el usuario quiere hojear a)
- El URL el WLC reorienta al navegador a
- La presentación final de las credenciales

La tabla del funcionamiento da el funcionamiento del WLC en caso de que los 3 URL sean HTTP, en caso de que los 3 URL sean HTTPS, o si el cliente se traslada desde el HTTP A HTTPS (más el escenario típico).

Cómo hacer un trabajo (local) interno de WebAuth con una página interna

Si usted necesita configurar una red inalámbrica (WLAN) con una interfaz dinámica operativa, los clientes deben también recibir una dirección IP del servidor DNS con el DHCP. Antes de que usted fije cualquier **webauth**, usted debe probar que su red inalámbrica (WLAN) trabaja correctamente, que usted puede resolver las solicitudes DNS (**nslookup**), y que usted puede hojear las páginas web. Entonces, usted puede fijar la autenticación Web como funciones de seguridad de la capa 3. Usted puede crear a sus usuarios en la base de datos local o en un servidor RADIUS externo, por ejemplo. Refiera al documento del ejemplo de configuración de la autenticación Web del regulador del Wireless LAN.

Cómo configurar un WebAuth local de encargo con la página de encargo

El webauth de encargo se puede configurar con el **redirectUrl de la ficha de seguridad**. Esto fuerza una reorientación a un Web page específico que usted ingresa. Cuando autentican al usuario, reemplaza el URL original el cliente pedido y visualiza la página para la cual la reorientación fue asignada.

La función personalizada permite que usted utilice una página HTML de encargo en vez de la página de registro predeterminada. Cargue su HTML y archivos de imagen lían al regulador. En la página de la carga, busque al **conjunto del webauth** en un formato del alquitrán. Generalmente, PicoZip crea los alquitranes que trabajan compatible con el WLC. Por un ejemplo de un conjunto de WebAuth, refiera a la página del software de la descarga para los conjuntos inalámbricos de WebAuth del regulador. Esté seguro de seleccionar la versión apropiada para su WLC. Una buena recomendación es personalizar a un conjunto que exista; no cree a un conjunto desde el principio.

Hay algunas limitaciones con el **webauth de encargo** que varían con las versiones y los bug. Las cosas a mirar para incluyen:

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

Si su paquete del cliente no trabaja, intentar con un paquete de encargo simple. Entonces agregue los archivos y la complejidad uno a la vez para alcanzar el paquete el cliente intentado para utilizar. Esto debe ayudarle a identificar el problema. Por un ejemplo en cómo configurar una página de encargo, refiera a crear una página de registro personalizada de la autenticación Web, una sección dentro de la guía de configuración del controlador LAN de la tecnología inalámbrica de Cisco, la versión 7.0.

Reemplace la técnica de la configuración global

Para cada red inalámbrica (WLAN), usted configura con el **comando global config de la invalidación** y fija un tipo de WebAuth para cada red inalámbrica (WLAN). Esto significa que usted puede tener un interno/un valor por defecto WebAuth con un interno/un valor por defecto de encargo WebAuth para otra red inalámbrica (WLAN). Esto también permite que usted configure diversas páginas de encargo para cada red inalámbrica (WLAN). Usted debe combinar todas sus páginas en el mismo conjunto y cargarlas al WLC. Entonces, usted puede fijar su página de encargo con el **comando global config de la invalidación** en cada red inalámbrica (WLAN) y seleccionarla que el archivo sea la página de registro de todos los archivos dentro del conjunto. Usted puede elegir una diversa página de registro dentro del conjunto para cada red inalámbrica (WLAN).

Problema del cambio de dirección

Hay una variable dentro del conjunto HTML que permite el cambio de dirección. No ponga su cambio de dirección forzado URL allí. Para cualquier cambio de dirección publica en WebAuth de encargo, Cisco recomienda marcar al conjunto. Si usted ingresa una reorientación URL con **+=** en el WLC GUI, éste podría sobregrabar *o* agregar al URL definido dentro del conjunto. Por ejemplo,

en el WLC GUI, el campo del **redirectURL** se fija a www.cisco.com; sin embargo, en el conjunto muestra: **redirectURL+=** "www.google.com". **El +=** reorienta a los usuarios a www.cisco.comwww.google.com, que es un URL inválido.

Cómo hacer un trabajo (local) externo de la autenticación Web con una página externa

Según lo explicado ya abreviadamente, la utilización de un servidor de WebAuth del externo es apenas un repositorio externo para la página de registro. Los credenciales de usuario todavía son autenticados por el WLC. El servidor Web externo permite solamente que usted utilice una página de registro especial o diversa. Aquí están los pasos realizados para un WebAuth externo:

1. El cliente (usuario final) abre a un buscador Web y ingresa un URL.

2. Si no autentican al cliente y autenticación se utiliza del Web externa, el WLC reorienta al usuario al servidor Web externo URL. Es decir el WLC envía un HTTP reorienta al cliente con la dirección IP del spoofed del sitio web y a las puntas a la dirección IP del servidor externo. La conexión con el sistema de autenticación URL del Web externa se añade al final del fichero con los parámetros tales como el **AP_Mac_Address**, el **client_url** (www.website.com), y el **action_URL** ese las clientes necesitas de entrar en contacto al servidor Web del Switch.

3. El servidor Web externo URL envía al usuario a una página de registro. Entonces el usuario puede utilizar un Access Control List de la PRE-autenticación (ACL) para acceder el servidor. El ACL es necesario para todos los modelos del WLC excepto las 4400 Series y Wism1.

4. La página de registro toma los credenciales de usuario entrados y envía la petición de nuevo al **action_URL**, tal como http://192.0.2.1/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 192.0.2.1 de la interfaz virtual en el Switch.

5. El servidor Web del WLC somete el nombre de usuario y contraseña para la autenticación.

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

7. Si la autenticación es acertada, el servidor Web del WLC cualquiera adelante el usuario al configurado reorienta el URL o al URL el cliente ingresó.

8. Si la autenticación falla, después el servidor Web del WLC reorienta al usuario de nuevo al login URL del cliente.

   Note: Utilizamos 192.0.2.1 como ejemplo IP virtual adentro de este documento. El rango 192.0.2.x se aconseja para el uso para IP virtual pues es no routable. Una más vieja documentación puede referir al "1.1.1.x" o eso puede todavía ser qué se configura en su WLC como éste era la configuración predeterminada. Sin embargo, observe que este IP ahora un IP Address ruteable válido y por lo tanto la subred 192.0.2.x está aconsejado en

lugar de otro.

Note: Si el (APS) de los Puntos de acceso está en el modo de FlexConnect, un **preauth** ACL es inútil. La flexión ACL se puede utilizar para permitir el acceso al servidor Web para los clientes que no se han autenticado. Refiera a la autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN.

Passthrough de la red

Ésta es una variación de la autenticación del Web interna. Visualiza una página con una advertencia o una declaración alerta, pero no indica para las credenciales. El usuario debe hacer clic la **autorización**. Usted puede habilitar la entrada de información del email, y el usuario puede ingresar su dirección email, que se convierte en su nombre de usuario. Cuando el usuario está conectado, marque su lista de los clientes activos; que enumeran al usuario con la dirección email ellos ingresó como el nombre de usuario. Para más información, refiera al ejemplo de configuración del passthrough de la red del regulador del Wireless LAN.

La red condicional reorienta

Si usted habilita una red condicional reoriente, el usuario se reorienta condicional a una página web determinada después de que la autenticación del 802.1x haya completado con éxito. 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 de usuario cuando alcanza la fecha de vencimiento o cuando el usuario necesita pagar una cuenta el uso/el acceso continuos. Si el servidor de RADIUS vuelve el cisco av-pair URL-**reoriente**, después reorientan al usuario al URL especificado cuando abren a un navegador. Si el servidor también vuelve el cisco av-pair URL-reorientar-**ACL**, después el ACL especificado está instalado como PRE-autenticación ACL para este cliente. No consideran autorizado completamente en este momento y puede pasar solamente al cliente el tráfico permitido por la PRE-autenticación ACL. Después de que el cliente complete una operación determinada en el URL especificado (por ejemplo, un cambio de la contraseña o un pago de la cuenta), después el cliente debe reautentificar. Cuando el servidor de RADIUS no vuelve una URL-**reorientación**, consideran al cliente autorizado completamente y permitido pasar el tráfico.

Note: La red condicional reorienta la característica está disponible solamente para los WLAN que se configuran para el 802.1x o WPA+WPA2 la Seguridad de la capa 2.

Después de que usted configure al servidor de RADIUS, usted puede entonces configurar la red condicional reorienta en el regulador con el regulador GUI o CLI. Refiera a estos guías pasos a paso: Usando el GUI para configurar la red reoriente y con el CLI para configurar la red reoriente.

La red de la página del chapoteo reorienta

Si usted habilita la red de la página del chapoteo reoriente, el usuario se reorienta a una página web determinada después de que la autenticación del 802.1x haya completado con éxito. Después de que la reorientación, el usuario tenga acceso total a la red. Usted puede especificar la página de la reorientación en su servidor de RADIUS. Si el servidor de RADIUS vuelve el cisco av-pair URL-**reoriente**, después reorientan al usuario al URL especificado cuando abren a un navegador. Consideran autorizado completamente en este momento y se permiten al cliente

pasar el tráfico, incluso si el servidor de RADIUS no vuelve una URL-**reorientación**.

Note: La red de la página del chapoteo reorienta la característica está disponible solamente para los WLAN que se configuran para el 802.1x o WPA+WPA2 la Seguridad de la capa 2.

Después de que usted configure al servidor de RADIUS, usted puede entonces configurar la red de la página del chapoteo reorienta en el regulador con el regulador GUI o CLI.

WebAuth en el error del filtro MAC

Esto le requiere configurar los filtros MAC en el menú de seguridad de la capa 2. Si validan a los usuarios con éxito con sus direcciones MAC, después van directamente al estado de **funcionamiento**. Si no son, después van al estado **WEBAUTH_REQD** y la autenticación Web normal ocurre.

Note: Esto no se soporta con el passthrough de la red. Para más información, siga la actividad en el pedido de mejora CSCtw73512 .

Autenticación Web central

La autenticación Web central refiere a un escenario donde el WLC recibe no más cualquier servicios. La diferencia reside en el hecho de que envían al portal web ISE y no pasa el cliente directamente con 192.0.2.1 en el WLC. Se exteriorizan la página de registro y el portal entero.

La autenticación Web central ocurre cuando usted hace el Network Admission Control (NAC) RADIUS habilitar en las configuraciones avanzadas de la red inalámbrica (WLAN) y el MAC filtra habilitado.

El concepto global es que el WLC envía una autenticación de RADIUS (generalmente para el filtro MAC) al ISE, que contesta con los pares del valor de atributo reorientar-**URL** (AV). Entonces ponen al usuario en el estado **POSTURE_REQD** hasta que el ISE dé la autorización con un cambio de la petición de la autorización (CoA). El mismo escenario sucede en la postura o la central WebAuth. WebAuth central no es compatible con WPA-Enterprise/802.1x porque el portal del invitado no puede devolver las claves de la sesión para el cifrado como hace con el Protocolo de Autenticación Extensible (EAP).

Autenticación de usuario externo (RADIUS)

Esto es solamente válido para WebAuth local cuando el WLC maneja las credenciales, o cuando se habilita una directiva de la red de la capa 3. Usted puede entonces autenticar a los usuarios localmente en el WLC o externamente vía el RADIUS.

Hay una orden en la cual el WLC marca para saber si hay las credenciales del usuario.

1. En todo caso, primero mira en su propia base de datos.
2. Si no encuentra a los usuarios allí, va al servidor de RADIUS configurado en la red inalámbrica (WLAN) del invitado (si hay una configurada).
3. Él entonces incorporares la lista global del servidor de RADIUS contra los servidores de RADIUS donde marcan al **usuario de la red**.

Esta tercera punta es muy importante y contesta a la cuestión de muchos que no configuren el RADIUS para esa red inalámbrica (WLAN), pero nota que todavía marca contra el RADIUS cuando no encuentran al usuario en el regulador. Esto es porque marcan al **usuario de la red** contra sus servidores de RADIUS en la lista global.

El WLC puede autenticar a los usuarios al servidor de RADIUS con el protocolo password authentication (PAP), el Challenge Handshake Authentication Protocol (CHAP) o el EAP-MD5 (mensaje Digest5). Esto es un Parámetro global y es configurable del GUI o del CLI:

Del GUI: navegue al **regulador >** a la **autenticación de RADIUS de la red**

Del CLI: ingrese la aduana-**red RADIUSauth <pap|chap|md5chap> de los config**

Note: El servidor del invitado del NAC utiliza solamente el PAP.

Cómo fijar una red inalámbrica (WLAN) atada con alambre del invitado

Es fácil configurar y muy cercano a la configuración inalámbrica del invitado. Usted puede configurarlo con uno o dos reguladores (solamente si uno es auto-ancla).

Elija un VLA N como el VLA N en el cual usted coloca a los Usuarios invitados atados con alambre, por ejemplo, en el VLA N 50. Cuando un invitado atado con alambre quiere el acceso a Internet, conecte la laptop a un puerto en un Switch configurado para el VLA N 50. Este VLA N 50 debe estar permitido y presente en la trayectoria a través del puerto troncal del WLC. En un caso de dos WLCs (un ancla y una no nativas), este VLA N atado con alambre del invitado debe llevar al WLC no nativo (WLC1 Nombrado) y no al ancla. WLC1 entonces lleva el cuidado de hacer un túnel el tráfico el WLC DMZ (el ancla, WLC2 Nombrado), que libera el tráfico en la red ruteada.

Aquí están los cinco pasos para configurar el acceso de invitado atado con alambre:

1. **Configure una interfaz dinámica (VLA N) para el acceso de Usuario invitado atado con alambre.**

   En WLC1, cree una interfaz dinámica VLAN50. En la página de la **configuración de la interfaz**, marque el cuadro del **invitado LAN**. Entonces, los campos tales como **dirección IP** y el **gateway** desaparecen. La única cosa sus necesidades del WLC de saber sobre esta interfaz es que el tráfico está ruteado del VLA N 50. Estos clientes son invitados atados con alambre.

2. **Cree un LAN cableado para el acceso de Usuario invitado.**

   En un regulador, se utiliza una interfaz cuando está asociada a una red inalámbrica (WLAN). El segundo paso es crear una red inalámbrica (WLAN) en sus reguladores de la oficina principal. Navegue a los **WLAN** y haga clic **nuevo**. En el **tipo de la red inalámbrica (WLAN)**, elija al **invitado LAN**.

   En el **nombre del perfil** y **WLAN SSID**, ingrese un nombre que identifique este WLAN. Estos nombres pueden ser diferentes, pero no pueden contener los espacios. Se utiliza La red

inalámbrica (WLAN) del término, pero este perfil de la red no se relaciona con el perfil de la red inalámbrica.

La ficha general ofrece dos listas desplegables: **Ingreso** y **salida**. El ingreso es el VLA N del cual los usuarios vienen (VLA N 50); La salida es el VLA N al cual usted quiere enviarlo.

Para el **ingreso**, elija **VLAN50**.

Para la **salida**, es diferente. Si usted tiene solamente un regulador, usted necesita crear otra interfaz dinámica, **estándar** este vez (no invitado LAN), y usted envía a sus usuarios atados con alambre a esta interfaz. En este caso, envíelos al regulador DMZ. Por lo tanto, para la **interfaz de egreso**, elija la **interfaz de administración**.

El modo seguro para este invitado LAN “red inalámbrica (WLAN)” es WebAuth, que es aceptable. **Autorización del** tecleo para validar.

3. **Configure el regulador no nativo (oficina principal).**

   De la lista de la red inalámbrica (WLAN), haga clic el **ancla de la movilidad** en el extremo de la línea del **invitado LAN**, y elija su regulador DMZ. Se asume aquí que ambos reguladores se conocen. Si no se conocen todavía, vaya al **grupo de la Administración del regulador >** de **movilidad >** de la **movilidad**, y agregue **DMZWLC** en WLC1. Entonces agregue **WLC1** en el DMZ. Ambos reguladores no deben estar en el mismo grupo de la movilidad. Si no, las reglas de seguridad básica están quebradas.

4. **Configure al regulador del ancla (el regulador DMZ).**

   Su regulador de la oficina principal está listo. Usted ahora necesita preparar su regulador DMZ. Abra una sesión del buscador Web en su regulador DMZ y navegue a los **WLAN**. Cree una nueva red inalámbrica (WLAN). En el **tipo de la red inalámbrica (WLAN)**, elija al **invitado LAN**.

   En el **nombre del perfil** y **WLAN SSID**, ingrese un nombre que identifique este WLAN. Utilice los mismos valores según lo ingresado en el regulador de la oficina principal.

   La interfaz de ingreso aquí no es **ninguna**. No importa realmente, porque el tráfico se recibe con los Ethernetes sobre el túnel IP (EoIP). Esta es la razón por la cual usted no necesita especificar ninguna interfaz de ingreso.

   La interfaz de egreso es la en el cual suponen a los clientes ser enviados. Por ejemplo, el **VLA N DMZ** es el VLA N 9. crea una interfaz dinámica estándar para el VLA N 9 en su DMZWLC, después elige el **VLA N 9** como la interfaz de egreso.

   Usted necesita configurar el extremo del túnel del ancla de la movilidad. **De la lista de la red inalámbrica (WLAN)**, elija el **ancla de la movilidad para el invitado LAN**. Envíe el tráfico al regulador local, **DMZWLC**. Los ambos extremos están listos ahora.

5. **Ajuste al invitado LAN.**

Usted puede también ajustar las configuraciones de la red inalámbrica (WLAN) en los ambos extremos. Tenga cuidado, las configuraciones debe ser idéntico en los ambos extremos. Por ejemplo, si usted elige hacer clic en la **ficha Avanzadas de la red inalámbrica (WLAN)**, **permita la invalidación AAA** en WLC1, usted necesitan marcar el mismo cuadro en DMZWLC. Si hay algunas diferencias en las selecciones en la red inalámbrica (WLAN) por ambas partes, el túnel se rompe. DMZWLC rechaza el tráfico; usted puede ver cuando usted **funcionar con la movilidad del debug**.

Tenga presente que todos los valores están obtenidos realmente de DMZWLC: IP Addresses, valores del VLA N, y así sucesivamente. Configure el lado WLC1 idénticamente, de modo que retransmita la petición al WLCDMZ.

Certificados para la página de registro

Esta sección proporciona los procesos que usted necesita seguir si usted quiere poner su propio certificado en la página de WebAuth, o si usted quiere ocultar 192.0.2.1 WebAuth URL y visualizar un URL Nombrado.

Cargue un certificado para la autenticación Web del regulador

Con el GUI (**WebAuth > certificado**) o CLI (**webauthcert del** tipo de la transferencia) usted puede cargar un certificado en el regulador. Si es un certificado que usted creó con su Certificate Authority (CA) o un certificado oficial de tercera persona, debe estar en el formato del .pem. Antes de que usted envíe, usted debe también ingresar la clave del certificado.

Después de que la carga, una reinicialización se requiera para que el certificado exista. Una vez que está reiniciado, vaya a la página del certificado de WebAuth en el GUI y le muestra los detalles del certificado que usted cargó (validez y así sucesivamente). El campo importante es el Common Name (CN), que es el nombre publicado al certificado. Este campo se discute en este documento bajo sección “Certificate Authority y otros Certificados en el regulador”.

Después de que usted haya reiniciado y haya verificado los detalles del certificado, le presentan con el nuevo certificado del regulador en la página de registro de WebAuth. Sin embargo, puede haber dos situaciones.

1. Si su certificado ha sido publicado por uno de los pocos la raíz principal CA que cada ordenador confía en, después es aceptable. Un ejemplo es Verisign, pero Verisign sub-CA raíz CA le firma generalmente y no. Usted puede incorporar su almacén de certificados del navegador si usted ve CA mencionado allí según lo confiado en.

2. Si usted consiguió su certificado de un company/CA más pequeño, todos los ordenadores no lo confían en. Usted debe proporcionar el certificado company/CA al cliente también, y esperanzadamente uno de la raíz CA publicará ese certificado. Eventual, usted termina para arriba con un encadenamiento tal como “certificado ha sido publicado por CA x > certificado de CA x ha sido publicado por CA y > certificado de CA y ha sido publicado por esta Raíz confiable CA”. El objetivo final es alcanzar CA que el cliente confíe en.

Certificate Authority y otros Certificados en el regulador

Para ser librado de la advertencia que “este certificado no se confía en”, usted debe también ingresar el certificado del CA que publicó el certificado del regulador en el regulador. Entonces el regulador presenta ambos Certificados (el certificado y su certificado de CA del regulador). El certificado de CA debe ser CA de confianza o tiene los recursos para verificar CA. Usted puede construir realmente un encadenamiento de los Certificados de CA que llevan a CA de confianza en el top.

Usted debe colocar el encadenamiento entero en el mismo archivo. Esto significa que su archivo contiene el contenido tal 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 el certificado hacer juego el URL

El WebAuth URL se fija a 192.0.2.1 para autenticarse y se publica el certificado (éste es el campo CN del certificado del WLC). Si usted quiere cambiar el WebAuth URL a “myWLC.com”, por ejemplo, entre la **configuración del** virtualinterface **(la** interfaz de 192.0.2.1) y allí usted puede ingresar un **nombre de host del** virtualDNS**, tal como** myWLC.com. Esto substituye 192.0.2.1 en su barra URL. Este nombre debe también ser resolvable. La traza de sniffer muestra cómo toda trabaja, pero cuando el WLC envía la página de registro, el WLC muestra el direccionamiento de myWLC.com, y el cliente resuelve este nombre con su DNS. Este nombre debe resolver como 192.0.2.1. Esto significa que si usted también utiliza un nombre para la Administración del WLC, usted debe utilizar un nombre diferente para WebAuth. Es decir si usted utiliza myWLC.com asociado al IP Address de administración del WLC, usted debe utilizar un nombre diferente para el WebAuth, tal como myWLCwebauth.com.

Problemas del certificado del Troubleshooting

Esta sección explica cómo y lo que a marcar para resolver problemas los problemas del certificado.

Cómo marcar

Usted puede descargar el OpenSSL (para Windows, buscar para el OpenSSL Win32) y instalarlo. Sin ninguna configuración, usted puede entrar en el **openssl del** directorio BIN y del intento **s_client – conecte** www.mywebauthpage.com:443, si este URL es el URL donde su página de WebAuth se enlaza en su DNS. Refiera “qué para marcar” la sección de este documento por un ejemplo.

Si sus Certificados utilizan CA privado, usted necesita colocar certificado raíz CA en un directorio en una máquina local y utilizar la opción del openssl **- CApath**. Si usted tiene CA intermedio, usted debe ponerlo en el mismo directorio también.

Para obtener la información general sobre el certificado y marcarla, utilice:

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

Puede ser que sea también útil convertir los Certificados con el uso del openssl:

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

Qué se debe verificar

Usted puede ver qué Certificados se envían al cliente cuando conecta. Lea el certificado del dispositivo — el CN debe ser el URL donde está accesible la página web. Lea “publicado por” la línea del certificado del dispositivo. Esto debe hacer juego el CN del segundo certificado. Entonces este segundo certificado “publicado por” debe hacer juego el CN del certificado siguiente, y así sucesivamente. Si no, no hace un encadenamiento real. En el OpenSSL hecho salir mostrado aquí, usted puede ver que el **openssl** no puede verificar el certificado del dispositivo porque su “publicado por” no hace juego el nombre del certificado de CA proporcionado.

Salida SSL

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

Otro posible problema es el certificado no se puede cargar al regulador. En esta situación no hay cuestión de la validez, CA, y así sucesivamente. Para verificar esto, le pueden en primer lugar controle la Conectividad del Trivial File Transfer Protocol (TFTP) e intentar transferir un archivo de configuración. Entonces, si usted ingresa la **transferencia del debug todo el comando enable**, usted ve que el problema es la instalación del certificado. Esto podía ser debido a la clave incorrecta usada con el certificado. Podría también ser que el certificado está en un formato incorrecto o está corrompido.

Cisco recomienda que usted compara el contenido del certificado a una haber sabido, certificado válido. Esto permite que usted vea si un atributo de **LocalkeyID** muestra todo el 0s (sucedido ya). Si es así entonces el certificado debe ser reconvertido. Hay dos comandos con el OpenSSL que permiten que usted vuelva del .pem a .p12, y después reedita un .pem con la clave de su opción.

PRE-paso: Si usted recibió un .pem que contiene un certificado seguido por una clave, copie/goma la parte clave: **----COMIENCE LA CLAVE ---- hasta ------- CLAVE DE FINAL ------** del .pem en “key.pem”.

1. **¿pkcs12 del openssl - exportación - en certificate.pem - inkey key.pem - hacia fuera newcert.p12? Le** indican con una clave; ingrese check123**.**

2. **el pkcs12 del openssl - en newcert.p12 - hacia fuera workingnewcert.pem - el passin pass:check123 - el passout pass:check123 esto** da lugar a un .pem operativo con la contraseña check123**.**

Otras situaciones a resolver problemas

Aunque el **ancla de la movilidad** no se haya discutido en este documento, si usted está en una situación **asegurada del invitado**, aseegurese el intercambio de la movilidad ocurre correctamente y eso que usted ve que el cliente llega en el ancla. Cualquier problemas más otra de WebAuth necesitan el Troubleshooting en el ancla.

Aquí están algunos problemas frecuentes que usted puede resolver problemas:

- **Los usuarios no pueden asociarse a la red inalámbrica (WLAN) del invitado**.

  Esto no se relaciona con WebAuth. Marque la configuración del cliente, los ajustes de seguridad en la red inalámbrica (WLAN), si se habilita, y si las radios están activas y operativas, y así sucesivamente.

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

  En una situación del ancla del invitado, esto está lo más a menudo posible porque el no nativo y el ancla no fueron configurados exactamente la misma manera. Si no, marque la configuración DHCP, Conectividad, y así sucesivamente. Confirme independientemente de si otros WLAN pueden utilizar al mismo servidor DHCP sin un problema. Esto todavía no se relaciona con WebAuth.

- **No reorientan al usuario a la página de registro**.

  Éste es la mayoría del síntoma común, pero es más exacto. Hay dos escenarios posibles.

  No reorientan al usuario (el usuario ingresa un URL y nunca alcanza la página de WebAuth). Para esta situación, control:

  que un servidor de los DN válidos se ha asignado al cliente vía el DHCP (**ipconfig /all**),

  que el DNS es accesible del cliente (**nslookup** www.website.com),

  que el usuario ingresó un URL válido para ser reorientado,

  que el usuario fue en HTTP URL encendido un puerto 80 (por ejemplo, alcanzar un ACS con http://localhost:2002 no le reorienta puesto que usted envió encendido el puerto 2002 en vez de 80).

  Reorientan al usuario a 192.0.2.1 correctamente, pero la página sí mismo no visualiza.

  Esta situación es más probable un problema del WLC (bug) o un problema del client cara. Podría ser que el cliente tiene algún Firewall o software o directiva del bloqueo. También podría ser que han configurado un proxy en su buscador Web.

  Recomendación: Tome una traza de sniffer en PC del cliente. No hay necesidad del software inalámbrico especial, sólo Wireshark, que se ejecuta en el adaptador de red inalámbrica y le muestra si el WLC contesta e intenta reorientar. Usted tiene dos posibilidades: o no hay respuesta del WLC, o algo es incorrecto con el contacto SSL para la página de WebAuth. Para el problema del contacto SSL, usted puede marcar si el navegador del usuario tiene en cuenta SSLv3 (algo permite solamente SSLv2), y si es demasiado agresivo en la verificación del certificado.

  Es un paso común para ingresar manualmente http:// 192.0.2.1 para marcar si el Web page aparece sin el DNS. Realmente, usted puede teclear http://6.6.6.6 y conseguir el mismo efecto. El WLC reorienta cualquier IP Address que usted ingrese. Por lo tanto, si usted

ingresa http:// 192.0.2.1, no hace que usted trabaja alrededor del cambio de dirección de la red. Si usted ingresa https:// 192.0.2.1(secure), esto no trabaja porque el WLC no reorienta el tráfico HTTPS (por abandono, esto es realmente posible en la versión 8.0 y posterior). La mejor manera de cargar la página directamente sin una reorientación es ingresar https://192.0.2.1/login.html.

- **Los usuarios no pueden autenticar**.

  Vea la sección de este documento que discuta la autenticación. Compruebe las credenciales localmente el RADIUS.

- **Los usuarios pueden autenticar con éxito con WebAuth, pero no tienen acceso a internet luego**.

  Usted puede quitar WebAuth de la Seguridad de la red inalámbrica (WLAN), y entonces usted debe tener una red inalámbrica (WLAN) abierta. Usted puede entonces intentar acceder la red, el DNS y así sucesivamente. Si usted experimenta los problemas allí también, quite las configuraciones de WebAuth en conjunto y marque su configuración de las interfaces.

Para obtener más información, consulte: Resolver problemas la autenticación Web en un regulador del Wireless LAN (WLC).

Servidor proxy HTTP y cómo trabaja

Usted puede utilizar un servidor proxy HTTP. Si usted necesita al cliente agregar una excepción en su navegador que 192.0.2.1 no es pasar a través del servidor proxy, usted puede hacer que el WLC está atento el tráfico HTTP en el puerto del servidor proxy (generalmente 8080).

Para entender este escenario, usted necesita conocer lo que lo hace un proxy de HTTP. Es algo que usted configura en el lado del cliente (dirección IP y puerto) en el navegador.

El escenario usual cuando un usuario visita un sitio web es resolver el nombre al IP con el DNS, y entonces lo pide la página web al servidor Web. El proceso debe enviar siempre el pedido de HTTP para la página al proxy. El proxy procesa el DNS, si procede, y adelante al servidor Web (si la página no se oculta ya en el proxy). La discusión es cliente-a-proxy solamente. Independientemente de si el proxy obtiene la página web real es inútil al cliente.

Aquí está el proceso de autenticación Web:

- El usuario teclea adentro un URL.
- PC del cliente envía al servidor proxy.
- IP del servidor proxy de las interceptaciones y de las parodias del WLC; contesta al PC con una reorientación a 192.0.2.1

En esta etapa, si el PC no se configura para él, pide la página de 192.0.2.1 WebAuth al proxy así que no trabaja. El PC debe hacer una excepción para 192.0.2.1; después envía un pedido de HTTP a 192.0.2.1 y procede con WebAuth. Cuando están autenticadas, todas las comunicaciones pasan con el proxy otra vez. Una configuración de la excepción está generalmente en el navegador cerca de la configuración del servidor proxy. Usted debe ver el mensaje: “No utilice el proxy para esos IP Addresses”.

Con la versión 7.0 del WLC y posterior, el **proxy del webauth de la** característica **reorienta** se puede habilitar en las opciones de configuración globales del WLC. Cuando está habilitado, el WLC marca si configuran a los clientes para utilizar manualmente un proxy. En ese caso, reorientan al cliente a una página que les muestre cómo modificar sus configuraciones de representación para hacer que todo trabaja. El proxy de WebAuth reorienta se puede configurar para trabajar en una variedad de puertos y es compatible con la autenticación Web central.

Por un ejemplo en el cambio de dirección del proxy de WebAuth, refiera al proxy de la autenticación Web en un ejemplo de la configuración de controlador del Wireless LAN.

Autenticación Web en el HTTP en vez del HTTPS

Usted puede iniciar sesión en la autenticación Web en el HTTP en vez del HTTPS. Si usted inicia sesión en el HTTP, usted no recibe las alertas del certificado.

Para anterior que el código de la versión 7.2 del WLC, usted debe inhabilitar la administración de HTTPS del WLC y dejar la Administración HTTP. Sin embargo, esto permite solamente administración de la Web del WLC sobre el HTTP.

Para el código de la versión 7.2 del WLC, utilice el **comando disable del secureweb del red-auth de la red de los config** de inhabilitar. Esto inhabilita solamente el HTTPS para la autenticación Web y no la Administración. ¡Observe que esto requiere una reinicialización del regulador!

En el código, usted de la versión 7.3 del WLC y posterior puede habilitar/neutralización HTTPS para WebAuth solamente vía el GUI y el CLI.

Información Relacionada

- Ejemplo de configuración de la autenticación Web del regulador del Wireless LAN
- Software de la descarga para los conjuntos inalámbricos de WebAuth del regulador
- Crear una página de registro personalizada de la autenticación Web
- Autenticación del Web externa con el ejemplo de configuración de los reguladores del Wireless LAN
- Ejemplo de configuración del passthrough de la red del regulador del Wireless LAN
- Usando el GUI para configurar la red reoriente
- Usando el CLI para configurar la red reoriente
- Resolviendo problemas la autenticación Web en un regulador del Wireless LAN (WLC)
- Proxy de la autenticación Web en un ejemplo de la configuración de controlador del Wireless LAN
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems