Generación de CSR para Certificados de Terceros y Descarga de Certificados No Encadenados en el WLC

Contenido

Introducción

Este documento explica cómo generar un pedido de firma de certificado (CSR) para obtener un certificado de tercera persona y cómo descargar un certificado soltado a un regulador del Wireless LAN (red inalámbrica (WLAN)) (WLC).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el WLC, el Lightweight Access Point (REVESTIMIENTO), y el indicador luminoso LED amarillo de la placa muestra gravedad menor del cliente de red inalámbrica para la operación básica
- Conocimiento de cómo utilizar la aplicación del OpenSSL para el Secure Socket Layer (SSL)

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 4.2.61.0
- Aplicación del OpenSSL para Microsoft Windows**Nota:** Se requiere el OpenSSL 0.9.8 pues el WLC no soporta actualmente el OpenSSL 1.0.
- Herramienta de la inscripción que es específica al Certification Authority (CA) de tercera persona

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

Por abandono, el uso del WLCs un accesorio uno mismo-firmó el certificado SSL. El uso del WLCs este certificado SSL en una de estas situaciones:

- Cuando los clientes intentan conectar con la red WLAN con el uso de la autenticación Web basada en SSL
- Cuando un usuario intenta iniciar sesión al WLC con el uso de HTTP seguro (HTTPS) (autenticación de WebAdmin)

En ambos casos, en la primera tentativa de acceder el WLC, usted puede recibir una alerta de seguridad del web browser que parezca esto:

A le indican que valide el certificado del WLC porque los clientes no tienen un certificado de la

Raíz confiable para el certificado que está instalado en el WLC. El certificado SSL en el WLC no está en la lista de Certificados que el sistema del cliente confíe en. Hay dos maneras de parar la generación de esta ventana emergente de la alerta de seguridad del web browser:

- Utilice el certificado uno mismo-firmado SSL en el WLC y configure las estaciones del cliente para validar el certificado.Incluya el certificado autofirmado en el WLC en la lista de Certificados que se confíen en la estación del cliente.
- Genere un CSR y instale un certificado que sea firmado por una fuente (CA de tercera persona) para que los clientes hacen ya los Certificados de la Raíz confiable instalar, por ejemplo Verisign.Usted puede hacer esto off-line del WLC con el uso de un programa como el OpenSSL. Refiera al proyecto OpenSSL para más información en el OpenSSL.

Este documento explica cómo generar un CSR para un certificado del otro vendedor y cómo descargar un certificado soltado de la autenticación Web al WLC.

Soporte para el certificado encadenado

Las versiones del software WLC que 5.1.151.0 no soportan anterior los Certificados encadenados. Utilice uno de la solución alternativa de estas opciones para este problema:

- Adquiera un certificado soltado de CA, así que significa que la raíz de firma está confiada en.
- Tenga todos los certificados raíz válidos del intermedio CA, confiados en o untrusted, instalados en el cliente.

Con la versión 5.1.151.0 y posterior, el soporte del WLCs encadenó los Certificados para la autenticación Web. Los Certificados de la autenticación Web pueden ser ninguno de estos:

- Encadenado
- Soltado
- Autogenerado

Refiérase generan el CSR para los Certificados de tercera persona y descargan los Certificados encadenados al WLC para la información sobre cómo utilizar los Certificados encadenados en el WLC.

CSR

Un certificado es un documento electrónico que usted utiliza para identificar un servidor, una compañía, o alguna otra entidad y asociar esa identidad a una clave pública.

Los CA son las entidades que validan las identidades y publican los Certificados. El certificado que CA publica los lazos una clave pública determinada al nombre de la entidad que el certificado identifica (por ejemplo el nombre de un servidor o de un dispositivo). Solamente la clave pública que el certificado certifica los trabajos con la clave privada correspondiente que es poseída por la entidad que el certificado identifica. Los Certificados ayudan a prevenir el uso de las claves públicas falsas para la personificación.

Un CSR es un mensaje que un candidato envía a CA para solicitar un certificado de identidad digital. En general, una compañía de tercera persona de CA, como confía o Verisign, requiere un CSR antes de que la compañía pueda crear un certificado digital.

La generación CSR es independiente del dispositivo en el cual usted planea instalar un certificado

externo. Tan un CSR y un archivo de clave privado se pueden generar en cualquier Windows o máquina UNIX individual. La generación CSR no es Switch-dependiente o dispositivo-dependiente en este caso.

Porque el WLC no genera un CSR, usted debe utilizar una aplicación de terceros tal como OpenSSL para generar un CSR para el WLC.

La sección genera un CSR discute los comandos que usted debe publicar en la aplicación del OpenSSL para generar una clave privada y el CSR.

Complete estos pasos para conseguir un certificado de tercera persona de CA:

1. Genere un privado/un par clave público.
2. Con el uso de la clave pública, genere un CSR.
3. Someta el CSR a CA.
4. Extraiga el certificado que CA presenta.
5. Combine el certificado y la clave privada en un archivo del pkcs12.
6. Convierta el archivo del pkcs12 a un archivo de codificación del Privacy Enhanced Mail (PEM).
7. Descargue el nuevo certificado de tercera persona (archivo del .pem) sobre el WLC.

Genere un CSR

Complete estos pasos para generar un CSR y someter el CSR a CA de tercera persona:

1. Instale y abra la aplicación del OpenSSL.**Nota:** Se requiere el OpenSSL 0.9.8 pues el WLC no soporta actualmente el OpenSSL 1.0.En Windows, por abandono, openssl.exe está situado en c:\openssl\bin.
2. Ejecutar este comando:`OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem` **Nota:** Soporte del WLCs un tamaño de clave máximo de **2048** bits.Después de que usted publique el comando, hay un prompt para una cierta información: Nombre del país, estado, ciudad, y así sucesivamente.
3. Proporcione la información requerida.La mayoría de la información importante que usted necesita proporcionar correctamente es el Common Name. Asegúrese de que el nombre del host que se utiliza para crear el certificado (Common Name) haga juego la entrada de nombre del host del Domain Name System (DNS) para el IP de la interfaz virtual en el WLC y de que el nombre existe realmente en el DNS también. También, después de que usted realice el cambio a la interfaz VIP, usted debe reiniciar el sistema para que este cambio tome el efecto.**Nota:** El nombre del host DNS se debe ingresar en el WLC bajo **interfaces > edita** para la interfaz virtual. Esto se utiliza para verificar la fuente de Certificados cuando se habilita el auth de la red. Reinicie el regulador para hacer que este cambio tome el efecto.Después de que usted proporcione todos los detalles requeridos, usted termina para arriba con dos archivos:una nueva clave privada que tiene el nombre mykey.pemun CSR que tiene el nombre myreq.pemEstos archivos se salvan en el directorio predeterminado donde el OpenSSL está instalado (c:\openssl\bin, en este caso). El archivo myreq.pem es el archivo que contiene la información CSR. Esta información se debe presentar a CA de tercera persona de modo que CA de tercera persona pueda generar un certificado digital. Aquí está la salida del comando de ejemplo cuando usted publica este comando con el uso de la aplicación del OpenSSL:`OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -`

```
out myreq.pem Loading 'screen' into random state - done Generating a 1024 bit RSA private
key ..........................................................++++++
.....................................................++++++ writing new private key to
'mykey.pem' ----- You are about to be asked to enter information that will be incorporated
into your certificate request. What you are about to enter is what is called a
Distinguished Name or a DN. There are quite a few fields but you can leave some blank For
some fields there will be a default value, If you enter '.', the field will be left blank.
----- Country Name (2 letter code) [AU]:US State or Province Name (full name) [Some-
State]:CA Locality Name (eg, city) []:San Jose Organization Name (eg, company) [Internet
Widgits Pty Ltd]:ABC Organizational Unit Name (eg, section) []:CDE Common Name (eg, YOUR
name) []:XYZ.ABC Email Address []:Test@abc.com Please enter the following 'extra'
attributes to be sent with your certificate request A challenge password []:Test123 An
optional company name []: OpenSSL>
```
Nota: Recuerde la contraseña de impugnación y preserve el archivo clave. Muy probablemente, usted necesitará la contraseña cuando usted importa el certificado firmado digitalmente que CA de tercera persona envía (a menos que CA de tercera persona envía una nueva contraseña junto con el certificado digital que genera para usted o su organización).

4. Ahora que su CSR está listo, la copia y pega la información CSR en cualquier herramienta de la inscripción de CA.Para copiar y pegar la información en la forma de la inscripción, abra el archivo en un editor de textos que no agregue los caracteres adicionales. Cisco recomienda que usted utiliza el Bloc de notas de Microsoft o UNIX vi. refiere al sitio web de CA de tercera persona para más información sobre cómo someter el CSR a través de la herramienta de la inscripción.Después de que usted someta el CSR a CA de tercera persona, CA de tercera persona firma digitalmente el certificado y devuelve el certificado firmado vía el email.
5. Copie la información del certificado firmado que usted recibe detrás de CA en un archivo.Este ejemplo nombra el archivo CA.pem.
6. Combine el certificado CA.pem con la clave privada, y después convierta el archivo a un archivo del .pem.Publique este comando en la aplicación del OpenSSL:`openssl>pkcs12 -export -in CA.pem -inkey mykey.pem -out CA.p12 -clcerts -passin pass:check123 -passout pass:check123 !--- This command should be on one line. openssl>pkcs12 -in CA.p12 -out final.pem -passin pass:check123 -passout pass:check123`
Nota: En este comando, usted debe ingresar una contraseña para los parámetros **- passin** y **- passout**. La contraseña que se configura para **-** parámetro del **passout** debe hacer juego el parámetro del **certpassword** que se configura en el WLC. En este ejemplo, la contraseña que se configura para **- passin** y **- los** parámetros del **passout** son **check123**. El paso 4 del procedimiento en la descarga el certificado de tercera persona a la sección del WLC de este documento discute la configuración del parámetro del **certpassword.El final.pem es el** archivo que se transfiere vía el TFTP al WLC de Cisco.Ahora que usted tiene el certificado de CA de tercera persona, usted necesita descargar el certificado al WLC.

Descargue el certificado de tercera persona al WLC

Utilice a un servidor TFTP para cargar el nuevo certificado. Siga estas guías de consulta para el uso del TFTP:

- Si usted carga el certificado a través del puerto del servicio, el servidor TFTP debe estar en la misma subred como el WLC porque el puerto del servicio no es routable. Sin embargo, si usted carga el certificado a través del puerto de red del sistema de distribución (DS), el servidor TFTP puede estar en cualquier subred.
- El servidor TFTP no puede ejecutarse en el mismo ordenador que el Cisco Wireless Control

System (WCS) porque el WCS y el servidor TFTP utilizan el mismo puerto de comunicación. Complete estos pasos para cargar un certificado externamente generado HTTPS:

1. Mueva el archivo final.pem al directorio predeterminado en su servidor TFTP.
2. En el comando line interface(cli), publique el **comando transfer download start** para ver las configuraciones actuales de la descarga, y ingrese **n** en el prompt.Aquí tiene un ejemplo:`>transfer download start Mode..... TFTP Data Type..... Admin Cert TFTP Server IP..... xxx.xxx.xxx.xxx TFTP Path..... <directory path> TFTP Filename..... Are you sure you want to start? (y/n) n Transfer Canceled`
3. Publique estos comandos para cambiar las configuraciones de la descarga:**>transfer download mode tftp >transfer download datatype webauthcert >transfer download serverip** *<TFTP server IP address>* **>transfer download path** *<absolute TFTP server path to the update file>* **>transfer download filename** *final.pem*
4. Ingrese la contraseña para el archivo del .pem de modo que el sistema operativo pueda desencriptar la clave y el certificado SSL.**>transfer download certpassword** *password* `>Setting password to password` **Nota:** Sea que el **certpassword** es lo mismo que **- la** contraseña segura del parámetro del **passout** que el paso 6 de la generación una sección CSR discute. En este ejemplo, el **certpassword** debe ser **check123**.
5. Publique el **comando transfer download start** para ver las configuraciones actualizadas. Entonces ingrese **y** en el pronto para confirmar las configuraciones actuales de la descarga y comenzar la descarga del certificado y de la clave.Aquí tiene un ejemplo:`(Cisco Controller) >transfer download start Mode..... TFTP Data Type..... Admin Cert TFTP Server IP..... 172.16.1.1 TFTP Packet Timeout..... 6 TFTP Max Retries..... 10 TFTP Path..... c:\OpenSSL\bin/ TFTP Filename..... final.pem This may take some time. **Are you sure you want to start? (y/N) y TFTP Webadmin cert transfer starting. Certificate installed. Reboot the switch to use new certificate.** **Nota:** Para instalar un certificado de tercera persona para la autenticación administrativa (admin) (para un usuario que intenta iniciar sesión al WLC con el uso del HTTPS), cambie el tipo de datos al **webadmincert** en el comando del **datatype de la descarga de la transferencia**, y relance los pasos 3 a 5 de este procedimiento.
6. Publique este comando para habilitar el HTTPS:**>config network secureweb enable**
7. Salve el certificado SSL, clave, y asegure la contraseña de la red al NVRAM para conservar sus cambios a través de las reinicializaciones.**>save config** `Are you sure you want to save? (y/n) y Configuration Saved!`
8. Reinicie el regulador.**>reset system** `Are you sure you would like to reset the system? (y/n) y System will now restart! The controller reboots.` **Nota:** Si un certificado está instalado ya, el procedimiento para descargar un nuevo borra el viejo.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Usted puede utilizar el **comando summary del certificado de la demostración** en el WLC para

marcar si el WLC utiliza el certificado de tercera persona como se esperaba. Aquí tiene un ejemplo:

```
(Cisco Controller) >show certificate summary Web Administration Certificate.................
3rd Party Web Authentication Certificate.................. 3rd Party Certificate compatibility
mode:.................. off
```

La salida confirma que un certificado de tercera persona está utilizado como el certificado de la administración Web y certificado de la autenticación Web.

La próxima vez que eso que un usuario intenta iniciar sesión a la red WLAN con el uso de la autenticación Web basada en SSL, no se indica al usuario que valide una alerta de seguridad de la red, a condición de que el certificado de tercera persona que está instalado en el WLC está en la lista de CA de confianza que el buscador del cliente soporte.

Troubleshooting

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Usted puede utilizar el **comando debug pm pki enable** en el WLC. Funcione con el comando cuando usted instala el certificado en el WLC.

Siempre que ocurra cualquier transferencia a o desde el regulador, es útil girar la **transferencia del debug todo el comando enable** y volver a efectuar la transferencia para ver los detalles de qué ha ocurrido. Las transferencias pueden fallar adentro transitan (el número apropiado de bits o los bytes no se mueve desde el servidor al regulador), o una vez que el archivo consigue allí, el contenido es cualquier ilegible al regulador o no se encuentra para ser apropiado para la función deseada.

Información Relacionada

- Actualización del Software del Controlador de la LAN Inalámbrica (WLC)
- Genere el CSR para los Certificados de tercera persona y descargue los Certificados encadenados al WLC
- Preguntas Frecuentes sobre el Troubleshooting de los Controladores de WAN Inalámbricos (WLC)
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- Soporte de Productos de Red Inalámbrica
- Proyecto OpenSSL
- Soporte Técnico y Documentación - Cisco Systems