Configurar certificado de descifrado en dispositivo web seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Descifrado HTTPS

Configurar certificado de descifrado en SWA

- Cargar un certificado raíz y una clave
- Generar un certificado y una clave para el proxy HTTPS

Importar certificado

- Importar certificado de proxy upstream a SWA
- Importar certificado SWA a otro SWA
- Importar certificado SWA en cliente de Windows
- Importar certificado SWA en cliente Mac
- Importar certificado SWA en Ubuntu/Debian
- Importar certificado SWA en CentOS 6
- Importar certificado SWA en CentOS 5
- Importar certificado SWA en Mozilla Firefox
- Importar certificado SWA en Google Chrome
- Importar certificado SWA en Microsoft Edge/Internet Explorer
- Importar certificado SWA en Safari
- Importar certificado SWA de directiva de grupo a clientes

Contenido relacionado

Introducción

Este documento describe los pasos para configurar certificados de cifrado HTTPS en dispositivos web seguros (SWA) y clientes proxy.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso administrativo a SWA
- Acceso a la interfaz gráfica de usuario (GUI) de SWA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descifrado HTTPS

El descifrado del protocolo de transferencia de hipertexto seguro (HTTPS) de SWA utiliza certificados raíz y archivos de clave privada que se cargan en el dispositivo para cifrar el tráfico. El certificado raíz y los archivos de clave privada que cargue en el dispositivo deben estar en formato PEM.



Nota: No se admite el formato DER.

También puede cargar un certificado intermedio firmado por una autoridad de certificación raíz. Cuando SWA crea un certificado que representa el certificado del servidor, envía el certificado cargado junto con el certificado imitado a la aplicación cliente. De ese modo, mientras el certificado intermedio esté firmado por una entidad emisora de certificados (CA) raíz en la que confía la aplicación cliente, la aplicación confía en el certificado de servidor imitado.

Configurar certificado de descifrado en SWA

El SWA puede utilizar un certificado y una clave privada existentes para el descifrado HTTPS. Sin embargo, puede haber confusión sobre el tipo de certificado que debe utilizarse, ya que no todos los certificados x.509 funcionan.

Hay dos tipos principales de certificados: Certificados de servidor y Certificados raíz. Todos los certificados x.509 contienen un campo Restricciones básicas, que identifica el tipo de certificado:

- Subject Type=Entidad final - Certificado de servidor
- Subject Type=CA - Certificado raíz

Cargar un certificado raíz y una clave

Paso 1. Desde la GUI, navegue hasta Servicios de seguridad y elija Proxy HTTPS.
Paso 2. Haga clic en Editar configuración.
Paso 3. Haga clic en Usar certificado y clave cargados.
Paso 4. Haga clic en Examinar el campo Certificado para navegar al archivo de certificado almacenado en el equipo local.



Nota: Si el archivo que carga contiene varios certificados o claves, el proxy web utiliza el primer certificado o clave del archivo.

Paso 5. Haga clic en Browse en el campo Key para navegar al archivo de clave privada.



Nota: La longitud de la clave debe ser de 512, 1024 o 2048 bits.

Paso 6. Seleccione Key is Encrypted (La clave está cifrada) si la clave está cifrada.
Paso 7. Haga clic en Cargar archivos para transferir el certificado y los archivos de clave al Dispositivo web seguro. La información del certificado cargado se muestra en la página Edit HTTPS Proxy Settings.
Paso 8. (Opcional) Haga clic en Descargar certificado para transferir a las aplicaciones cliente en la red.

Paso 9. Envíe y confirme los cambios.

Generar un certificado y una clave para el proxy HTTPS

Paso 1. Desde la GUI, navegue hasta Servicios de seguridad y elija Proxy HTTPS.
Paso 2. Haga clic en Editar configuración.
Paso 3. Elija Use Generated Certificate and Key.
Paso 4. Haga clic en Generar nuevo certificado y clave.
Paso 5. En el cuadro de diálogo Generar certificado y clave, ingrese la información para mostrarla en el certificado raíz. Puede introducir cualquier carácter ASCII excepto la barra diagonal (/) en el campo Nombre común.
Paso 6. Haga clic en Generar.
Paso 7. La información del certificado generado se muestra en la página Editar configuración de proxy HTTPS.
Paso 8. (Opcional) Haga clic en Descargar certificado para transferirlo a las aplicaciones cliente de la red.
Paso 9. (Opcional) Haga clic en el enlace Descargar solicitud de firma de certificado para poder enviar la solicitud de firma de certificado (CSR) a una CA.
Paso 10. (Opcional) Cargue el certificado firmado en el dispositivo web seguro después de recibirlo de la CA. Puede hacerlo en cualquier momento después de generar el certificado en el dispositivo.
Paso 11. Enviar y Registrar cambios.

Importar certificado

Importar certificado de proxy upstream a SWA

Si SWA está configurado para utilizar un proxy upstream y el proxy upstream está configurado para el descifrado HTTPS, debe importar el certificado de cifrado del proxy upstream a SWA. Puede administrar la lista de certificados de confianza, agregarle certificados y quitarle certificados funcionalmente.

Paso 1. En la GUI, elija Red y elija Administración de certificados.
Paso 2. Haga clic en Administrar certificados raíz de confianza en la página Administración de certificados.
Paso 3. Para agregar un certificado raíz de confianza personalizado con autoridad de firma, no en la lista de certificados reconocidos de Cisco, haga clic en Importar y, a continuación, envíe el archivo del certificado.

Paso 4. Enviar y Registrar cambios.

Importar certificado SWA a otro SWA

Si ha cargado el certificado y la clave HTTPS en un SWA para el proxy HTTPS y se puede acceder a los archivos originales, puede importarlos a otro SWA desde el archivo de configuración.

Paso 1. En la GUI de ambos SWA, elija Administración del sistema y haga clic en Archivo de configuración.

Paso 2. Haga clic en Descargar archivo en el equipo local para ver o guardar.

Paso 3. Elija Cifrar contraseñas en los Archivos de configuración.

Paso 4. (Opcional) Elija Use a user-defined file name (Utilizar un nombre de archivo definido por el usuario) y agregue el nombre deseado al archivo de configuración.

Paso 5. Haga clic en Enviar en Configuración actual para descargar el archivo configuration .xml.

Paso 6. Abra los archivos descargados con editores de texto o editores XML.

Paso 7. Copie estas etiquetas de SWA con el certificado, copie todos los datos dentro de las etiquetas y reemplácelos en el archivo de configuración del otro SWA:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

Paso 8. Guarde los cambios en el archivo .xml del SWA de destino.

Paso 9. Para volver a importar el archivo de configuración .xml editado al SWA de destino, en la interfaz gráfica de usuario, elija Administración del sistema y haga clic en Archivo de configuración.

Paso 10. En la sección Cargar configuración, haga clic en Cargar un archivo de configuración desde el equipo local.

Paso 11. Haga clic en Elegir archivo y elija el archivo de configuración .xml editado.

Paso 12. Haga clic en Cargar para importar el nuevo archivo de configuración con el certificado y

la clave.

Paso 13. Realice los cambios si el sistema se lo solicita.

Importar certificado SWA en cliente de Windows

Para importar el certificado de proxy HTTPS SWA como de confianza en los equipos cliente con el sistema operativo Microsoft Windows, revise estos pasos:

Paso 1. Haga clic en Inicio en la barra de tareas y escriba Administrar certificados de equipo.
Paso 2. En la página Certificados: Equipo local, expanda Certificación de raíz de confianza y haga clic con el botón secundario en la carpeta Certificados.
Paso 3. Haga clic en Todas las tareas y elija Importar.
Paso 4. En la página Asistente para importación de certificados, haga clic en Siguiente.
Paso 5. Para importar el archivo de certificado SWA, haga clic en Examinar y seleccione el certificado que descargó de SWA.



Consejo: Para descargar el certificado SWA, consulte el Paso 8 de la sección Carga de un Certificado y una Clave Raíz o Generación de un Certificado y una Clave para el Proxy HTTPS.

Paso 6. Haga clic en Colocar todos los certificados en la siguiente casilla de verificación.
Paso 7. Elija Trusted Root Certification Authorities y haga clic en Next.
Paso 8. Haga clic en Finalizar.

Como alternativa, puede ejecutar este comando para importar el certificado a las autoridades de certificación raíz de confianza.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



Nota: Debe reemplazar **<**Path to SWA Certificate/CertificateName.crt**>** por la ruta de acceso y el nombre de archivo del certificado descargado actualmente.

Importar certificado SWA en cliente Mac

Paso 1. Descargue el certificado de proxy HTTPS de SWA al cliente Mac OS.
Paso 2. Cambie el nombre de la extensión de archivo a .crt.
Paso 3. Ejecute este comando para importar el certificado como certificado de confianza:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```

Nota: Debe reemplazarlo por la ruta de acceso y el nombre de archivo del certificado descargado actualmente.

Importar certificado SWA en Ubuntu/Debian

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Abra el archivo de certificado en el editor de texto y copie todo el contenido.
Paso 3. Cree un nuevo archivo en /usr/local/share/ca-certificates/ con una extensión .crt.
Paso 4. Edite el archivo con el editor de texto deseado y pegue el texto copiado en el nuevo archivo, y guarde.
Paso 5. Ejecute este comando para actualizar los certificados del sistema operativo.

```
sudo update-ca-certificates
```

Consejo: Si tiene el certificado almacenado localmente en el cliente, puede copiar el certificado en /usr/local/share/ca-certificates/y ejecutar sudo update-ca-certificates.

Nota: En algunas versiones, debe instalar el paquete ca-certificates con este comando: sudo apt-get install -y ca-certificates.

Importar certificado SWA en CentOS 6

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Abra el archivo de certificado en el editor de texto y copie todo el contenido dentro del archivo.
Paso 3. Cree un nuevo archivo en /etc/pki/ca-trust/source/anchors/ con la extensión .crt.
Paso 4. Edite el archivo con el editor de texto deseado y copiado texto pasado en el nuevo

archivo, y guarde.
Paso 5. Instale el paquete ca-certificates:

```
yum install ca-certificates
```

Paso 6. Ejecute este comando para actualizar los certificados en el sistema operativo:

```
update-ca-trust extract
```



Consejo: Si tiene el certificado almacenado localmente en el cliente, puede copiar el certificado en /etc/pki/ca-trust/source/anchors/ y ejecutar update-ca-trust extract después de instalar los ca-certificates.

Importar certificado SWA en CentOS 5

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Abra el archivo de certificado en el editor de texto y copie todo el contenido dentro del archivo.
Paso 3. Cree un nuevo archivo en la carpeta actual con la extensión .crt (por ejemplo, SWA.crt).
Paso 4. Edite el archivo /etc/pki/tls/certs/ca-bundle.crt con el editor de texto que desee, pegue el texto copiado al final del archivo y guárdelo.



Consejo: Si tiene el certificado almacenado localmente en el cliente (en este ejemplo, el nombre de archivo es SWA.crt), puede anexar el certificado con este comando: cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

Importar certificado SWA en Mozilla Firefox

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Cambie el nombre de la extensión de archivo a .crt.
Paso 3. Abre Firefox y haz clic en el Menú (tres barras en la esquina superior derecha).
Paso 4. Seleccione Configuración (en algunas versiones es Opciones).
Paso 5. Haga clic en Privacidad y seguridad en el menú de la izquierda y desplácese hasta Certificados.

Paso 6. Haga clic en Ver certificados.
Paso 7. Haga clic en la pestaña Autoridades y luego en Importar.
Paso 8. Elija el archivo de certificado y haga clic en Abrir.
Paso 9. Haga clic en Aceptar.

Importar certificado SWA en Google Chrome

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Cambie el nombre de la extensión de archivo a .crt.
Paso 3. Abra Google Chrome y haga clic en Personalizar y controlar Google Chrome (tres puntos en la esquina superior derecha).
Paso 4. Seleccione Configuración.
Paso 5. Haga clic en Privacidad y seguridad en el menú de la izquierda.
Paso 6. Seleccione Seguridad.
Paso 7. Desplácese hasta Administrar certificados y haga clic en el botón de la derecha.
Paso 8. Elija la pestaña Entidades de certificación raíz de confianza y haga clic en Importar.
Paso 9. Elija el archivo de certificado y haga clic en Abrir.
Paso 10. Haga clic en Aceptar.



Nota: Si instala el certificado SWA en el sistema operativo, Google Chrome confía en ese certificado y no hay necesidad de importar el certificado por separado a su navegador.

Importar certificado SWA en Microsoft Edge/Internet Explorer

Microsoft Edge e Internet Explorer (IE) utilizan certificados de sistema operativo. Si instala el certificado SWA en el sistema operativo, no es necesario importar el certificado por separado en el explorador.

Importar certificado SWA en Safari

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Cambie el nombre de la extensión de archivo a .crt.
Paso 3. En el Launchpad, seleccione Acceso de llavero.
Paso 4. En el menú Archivo, haga clic en Agregar llavero.
Paso 5. Elija el archivo de certificado SWA y haga clic en Agregar.
Paso 6. Seleccione Seguridad.
Paso 7. Desplácese hasta Administrar certificados y haga clic en el botón de la derecha.
Paso 8. Elija la pestaña Entidades de certificación raíz de confianza y haga clic en Importar.

Paso 9. Elija el archivo de certificado y haga clic en Abrir.
Paso 10. Haga clic en Aceptar.

Importar certificado SWA de directiva de grupo a clientes

Para distribuir certificados a equipos cliente mediante la directiva de grupo desde Active Directory, siga estos pasos:

Paso 1. Descargue el certificado de proxy HTTPS de SWA.
Paso 2. Cambie el nombre de la extensión de archivo a .crt.
Paso 3. Copie el archivo de certificado en el controlador de dominio.
Paso 4. En el controlador de dominio, haga clic en Inicio y abra el complemento Administración de directivas de grupo.
Paso 5. Busque el objeto de directiva de grupo (GPO) deseado o cree un nuevo GPO que contenga el certificado SWA para importar al cliente.
Paso 6. Haga clic con el botón secundario en GPO y haga clic en Editar.
Paso 7. En el menú de la izquierda, navegue hasta Configuración del equipo > Directivas > Configuración de Windows > Configuración de seguridad > Directivas de clave pública.
Paso 8. Haga clic con el botón secundario en Entidades de certificación raíz de confianza y haga clic en Importar.
Paso 9. Haga clic en Siguiente en la página Bienvenido al Asistente para importación de certificados.
Paso 10. Elija el archivo de certificado SWA para importar y haga clic en Next (Siguiente).
Paso 11. Haga clic en Colocar todos los certificados en el siguiente almacén y, a continuación, haga clic en Siguiente.
Paso 12. Compruebe que la información proporcionada es precisa y haga clic en Finalizar.



Nota: En algunas condiciones, debe reiniciar el cliente o ejecutar gpupdate /force para aplicar los cambios en el equipo cliente de Active Directory.

Contenido relacionado

- Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD (implementación general)
- Distribuir certificados a equipos cliente mediante una directiva de grupo | Microsoft Learn
- 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).