Uso del certificado WSA para el desciframiento HTTPS

Contenido

Introducción

Este documento describe el tipo de certificado que debe ser utilizado para el desciframiento HTTPS en un dispositivo de seguridad de la red de Cisco (WSA).

Descripción del certificado

El WSA tiene la capacidad de utilizar un certificado y una clave privada actuales para el uso con el desciframiento HTTPS. Sin embargo, pudo haber confusión sobre el tipo de certificado que debe ser utilizado, puesto que no todos los Certificados x.509 trabajan.

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

- **Entidad sujeta de Type=End** - Certificado de servidor
- **Type=CA sujeto** - Certificado raíz

> **Note**: Usted debe utilizar un certificado raíz, también referido como un Certificate Authority (CA) firmando el certificado, para el desciframiento HTTPS en el WSA.

Certificados raíz

Un certificado raíz se crea específicamente para firmar los certificados de servidor. Usted puede crear y actuar su propio CA y firmar sus propios certificados de servidor.

Note: Puesto que un certificado raíz firma solamente otros Certificados, no puede ser utilizado en un servidor Web para realizar el cifrado y el desciframiento HTTPS.

El WSA debe utilizar un certificado raíz para generar activamente los certificados de servidor para el desciframiento HTTPS. Hay dos opciones disponibles para el uso del certificado raíz:

- Genere un certificado raíz en el WSA. El WSA crea su propio certificado raíz y clave privada, y utiliza este par clave para firmar los certificados de servidor.
- Usted puede cargar un certificado raíz actual y su clave privada en el WSA. El campo del Common Name (CN) en un certificado raíz identifica la entidad (típicamente un nombre de la sociedad) esa las confianzas cualquier certificado de servidor que contenga su firma.

  Note: Antes de que un certificado de servidor pueda ser confiado en, debe ser firmado por un certificado raíz que tenga una clave pública presente en el buscador Web.

Certificados de servidor

Un certificado de servidor se crea específicamente para ser utilizado en el cifrado y el desciframiento HTTPS y para verificar la autenticidad de un servidor específico. Los certificados de servidor son firmados por CA con el uso del certificado raíz de CA. Un ejemplo común de CA es Verisign o Thawte.

Note: Un certificado de servidor no se puede utilizar para firmar otros Certificados; por lo tanto, el desciframiento HTTPS no trabaja si un certificado de servidor está instalado en el WSA.

El campo CN en un certificado de servidor especifica el host para el cual el certificado se piensa para ser utilizado. Por ejemplo, **https://www.verisign.com** utiliza un certificado de servidor con un CN de **www.verisign.com**.

Información Relacionada

- Uso del certificado del dispositivo de seguridad de la red (WSA) (desciframiento HTTPS, inicio de sesión de interfaz gráfica de usuario, cifrado credencial)
- Pasos para habilitar el proxy HTTPS en WSA y la opción del pedido de firma de certificado (CSR)
- Pasos para habilitar el proxy HTTPS encendido (WSA) y cargando la raíz/la opción intermedia del certificado
- Soporte Técnico y Documentación - Cisco Systems