Cree un pedido de firma de certificado en un ESA

Contenido

Introducción

Este documento describe cómo crear un pedido de firma de certificado (CSR) en un dispositivo de seguridad del correo electrónico (ESA).

Cree un CSR en un ESA

A partir de AsyncOS 7.1.1, el ESA puede crear un certificado autofirmado para su propio uso y generar un CSR para someter a un Certificate Authority y para obtener el certificado público. El Certificate Authority devuelve un certificado público de confianza firmado por una clave privada. Utilice la página de la **red > de los Certificados** en el GUI o el comando del **certconfig** en el CLI para crear el certificado autofirmado, generar el CSR, y instalar el certificado público de confianza.

Si usted adquiere o crea un certificado por primera vez, busque Internet para “los Certificados de servidor SSL de los servicios del Certificate Authority” y elija el servicio que ese mejor cubre las necesidades de su organización. Siga las instrucciones del servicio para obtener un certificado.

Pasos para la configuración en el GUI

1. Para crear un certificado autofirmado, el tecleo **agrega el certificado** en la página de la red > de los Certificados en el GUI (o el comando del **certconfig** en el CLI). En la página del certificado del agregar, elija **crean el certificado autofirmado**.
2. Ingrese esta información para el certificado autofirmado: Common Name - El Nombre de dominio totalmente calificado (FQDN).Organización - El nombre legal exacto de la organización.Unidad organizativa - Sección de la organización.Ciudad (lugar) - La ciudad en donde la organización se localiza legalmente.Estado (provincia) - El estado, el condado, o la región donde la organización se localiza legalmente.País - La abreviatura del International Organization for Standardization de dos cartas (ISO) del país en donde la organización se localiza legalmente.Duración antes de la expiración - El número de días antes del certificado expira.Tamaño de la clave privada - Tamaño de la clave privada a generar para el CSR.

Solamente se soportan 2048-bit y 1024-bit.
3. Haga clic **después** para ver el certificado y la información de firma.
4. Ingrese un nombre para el certificado. AsyncOS asigna el Common Name por abandono.
5. Si usted quiere someter un CSR para el certificado autofirmado a un Certificate Authority, haga clic el **pedido de firma de certificado de la descarga** para salvar el CSR en el formato de Privacy Enhanced Mail (PEM) a un local o a una máquina de la red.
6. El tecleo **somete** para salvar el certificado y confiar sus cambios. Si usted deja los cambios sin compromiso, la clave privada conseguirá perdida y el certificado firmado no puede ser instalado.

Cuando el Certificate Authority devuelve el certificado público confiado en firmado por una clave privada, haga clic el nombre del certificado en la página de los Certificados y ingrese la trayectoria al archivo en su máquina local o red para cargar el certificado. Aseegurese que el certificado público de confianza que usted recibe está en el formato PEM o un formato que usted puede convertir al PEM antes de que esté cargado al dispositivo. Las herramientas para completar esto se incluyen con el OpenSSL, software gratuito disponible en http://www.openssl.org.

Si usted carga el certificado del Certificate Authority, el certificado existente está sobregrabado. Usted puede también cargar un certificado intermedio relacionado con el certificado autofirmado. Usted puede utilizar el certificado con un módulo de escucha público o privado, los servicios HTTPS de una interfaz IP, la interfaz del Lightweight Directory Access Protocol (LDAP), o todas las conexiones salientes de Transport Layer Security (TLS) a los dominios del destino.

Información Relacionada

- Guía completa de la configuración para TLS en el ESA
- Soporte Técnico y Documentación - Cisco Systems