¿Cómo generar y instalar un certificado digital en el S A?

Contenido

Introducción

Este documento describe cómo generar un certificado en el dispositivo de seguridad del correo electrónico (ESA) que se puede utilizar en el dispositivo de la Administración de seguridad (S A).

¿Cómo generar y instalar un certificado digital en el S A?

Antecedente

El S A no soporta la generación de los Certificados en el dispositivo sí mismo. En lugar es posible generar un certificado firmado del uno mismo en el ESA. Esto se puede utilizar como solución alternativa para crear un certificado para que utilizan el S A sea importado y.

Cree y certificado de exportación en el ESA

1. Cree un certificado firmado del uno mismo bajo el **GUI: La red > certifica > Add el certificado.** Es importante, al crear un certificado firmado del uno mismo, para que el Common Name (CN) utilice el nombre de host del S A y no del ESA, para poder utilizar correctamente el certificado. Someta y confíe los cambios.
2. Uso **GUI: La red > certifica > los Certificados de exportación al** certificado de exportación. Déle un nombre del archivo (e.g mycert) y la contraseña que sean utilizados al convertir el certificado.

Convierta el certificado exportado

El certificado exportado estará en el formato del **.pfx**. El S A soporta solamente el formato del **.pem** para importar, así que este certificado necesita ser convertido. Para convertir el certificado

del formato del .pfx al formato del .pem, utilice por favor el sintaxis siguiente del OpenSSL.

```
openssl pkcs12 -in mycert.pfx -out mycert.pem -nodes
```

Después de convertir el certificado al formato correcto, el certificado y la clave privada correspondiente en el formato del .pem deben estar presentes. Es importante tener el certifcate **y** clave privada disponibles. Solamente el certifcate sin la clave privada no se puede importar en el S A. Es recomendado para firmar el certificado por una autoridad confiable de certificación (CA). Cisco no recomienda CA específico. Para firmar el **"pedido de firma de certificado** selecto de la **descarga**" en el GUI del ESA y sométalo a CA de confianza de la opción.

Import Certificate (Importar certificado) al S A - Opción 1

El certificado firmado de CA o el certificado firmado del uno mismo y la clave privada en el .pem formatan, se pueden ahora importar en el S A. Para aprender cómo hacerlo, lea por favor la Nota Técnica "cómo instalo los Certificados en un S A?" según lo referido abajo.

Import Certificate (Importar certificado) al S A - Opción 2

En vez de convertir el certificado del .pfx en el .pem usted puede salvar simplemente un wihtout del archivo de configuración que enmascara las contraseñas en el ESA. Abra el archivo XML y la búsqueda para la etiqueta del <certificate>. Usted encontrará el certificado y la clave privada ya en el formato PEM. Copie el certificado y la clave privada para importar lo mismo en el S A según lo descrito en la Nota Técnica "cómo instalo los Certificados en un S A?" según lo referido abajo.

> Nota: Si usted va para la opción 2 y si usted hace el certificado firmar por CA usted primero necesita importar el certificado firmado de nuevo al ESA antes de guardar el archivo de configuración para hacer una copia del certificado y de la clave privada. La importación puede ser hecha haciendo clic en el nombre del certificado en ESA GUI y la opción "certificado firmado del uso de la carga".

Verifique el certificado importado

1. Acceda el S A GUI vía el HTTPS (IP de https:// <SMA u hostname>) y ponga en sus credenciales
2. Al lado del URL en la barra de dirección en su navegador, haga clic la validez del icono y del control del bloqueo del certificado, del vencimiento, del etc.
3. Haga clic en el trayecto de certificación para marcar el encadenamiento de los Certificados

Información Relacionada

- ¿Cómo instalo los Certificados en un S A?
- Convertidor en línea SSL