Crie uma solicitação de assinatura de certificado em um ESA

Índice

Introdução

Este documento descreve como criar uma solicitação de assinatura de certificado (CSR) em uma ferramenta de segurança do email (ESA).

Crie um CSR em um ESA

Até à data de AsyncOS 7.1.1, o ESA pode criar um certificado auto-assinado para seu próprio uso e gerar um CSR para submeter-se a um Certificate Authority e para obter o certificado público. O Certificate Authority retorna um certificado público confiado assinado por uma chave privada. Use a página da **rede > dos Certificados no** GUI ou o comando do **certconfig no** CLI a fim criar o certificado auto-assinado, gerar o CSR, e instalar o certificado público confiado.

Se você adquire ou cria um certificado pela primeira vez, procure o Internet do “por Certificados de servidor SSL dos serviços Certificate Authority” e escolha o serviço que esse melhor encontra as necessidades de sua organização. Siga as instruções do serviço a fim obter um certificado.

Etapas de configuração no GUI

1. A fim criar um certificado auto-assinado, o clique **adiciona o certificado na** página da rede > dos Certificados no GUI (ou o comando do **certconfig no** CLI). Na página do certificado adicionar, escolha **criam o certificado auto-assinado**.
2. Incorpore esta informação para o certificado auto-assinado: Common Name - O nome de domínio totalmente qualificado.Organização - O nome legal exato da organização.Unidade organizacional - Seção da organização.Cidade (localidade) - A cidade onde a organização é encontrada legalmente.Estado (província) - O estado, o condado, ou a região onde a organização é encontrada legalmente.País - A abreviatura de duas letras do International Organization for Standardization (ISO) do país onde a organização é encontrada legalmente.Duração antes da expiração - O número de dias antes do certificado expira.Tamanho da chave privada - Tamanho da chave privada a gerar para o CSR.

Somente 2048-bit e 1024-bit são apoiados.
3. Clique **em seguida** a fim ver o certificado e a informação de assinatura.
4. Dê entrada com um nome para o certificado. AsyncOS atribui o Common Name à revelia.
5. Se você quer submeter um CSR para o certificado auto-assinado a um Certificate Authority, clique a **solicitação de assinatura de certificado da transferência** a fim salvar o CSR no formato do Privacy Enhanced Mail (PEM) a um local ou a uma máquina da rede.
6. O clique **submete-se** a fim salvar o certificado e comprometer suas mudanças. Se você deixa as mudanças descomprometidos, a chave privada obterá perdida e o certificado assinado não pode ser instalado.

Quando o Certificate Authority retorna o certificado público confiado assinado por uma chave privada, clique o nome do certificado na página dos Certificados e entre no trajeto ao arquivo em sua máquina local ou rede a fim transferir arquivos pela rede o certificado. Certifique-se de que o certificado público confiado que você recebe está no formato PEM ou em um formato que você pode converter ao PEM antes que esteja transferido arquivos pela rede ao dispositivo. As ferramentas para terminar isto são incluídas com OpenSSL, software gratuito disponível em http://www.openssl.org.

Se você transfere arquivos pela rede o certificado do Certificate Authority, o certificado existente overwritten. Você pode igualmente transferir arquivos pela rede um certificado intermediário relativo ao certificado auto-assinado. Você pode usar o certificado com ouvinte público ou privado, serviços HTTPS de uma interface IP, relação do Lightweight Directory Access Protocol (LDAP), ou todas as conexões que parte do Transport Layer Security (TLS) aos domínios do destino.

Informações Relacionadas

- Guia detalhado da instalação para o TLS no ESA
- Suporte Técnico e Documentação - Cisco Systems