Uso do certificado WSA para a descriptografia HTTPS

Índice

Introdução

Este documento descreve o tipo de certificado que deve ser usado para a descriptografia HTTPS em uma ferramenta de segurança da Web de Cisco (WSA).

Vista geral do certificado

O WSA tem a capacidade para usar um certificado e uma chave privada atuais para o uso com descriptografia HTTPS. Contudo, pôde haver uma confusão sobre o tipo de certificado que deve ser usado, desde que não todos os Certificados x.509 trabalham.

Há dois tipos principais de Certificados: **Certificados de servidor** e **certificados de raiz**. Todos os Certificados x.509 contêm um campo básico das limitações, que identifique o tipo de certificado:

- **Entidade sujeita de Type=End** - Certificado de servidor
- **Type=CA sujeito** - Certificado de raiz

> **Note**: Você deve usar um certificado de raiz, igualmente referido como um Certificate Authority (CA) assinando o certificado, para a descriptografia HTTPS no WSA.

Certificados de raiz

Um certificado de raiz é criado especificamente a fim assinar certificados de servidor. Você pode criar e operar seu próprio CA e assinar seus próprios certificados de servidor.

Note: Desde que um certificado de raiz assina somente outros Certificados, não pode ser usado em um servidor de Web a fim executar a criptografia e a descriptografia HTTPS.

O WSA deve usar um certificado de raiz a fim gerar ativamente certificados de servidor para a descriptografia HTTPS. Há duas opções disponíveis para o uso do certificado de raiz:

- Gerencia um certificado de raiz no WSA. O WSA cria seus próprios certificado de raiz e chave privada, e usa este par de chaves a fim assinar certificados de servidor.
- Você pode transferir arquivos pela rede um certificado de raiz atual e sua chave privada no WSA. O campo do Common Name (CN) em um certificado de raiz identifica a entidade (tipicamente um nome do corporaçõ) essa confianças todos os certificados de servidor que contiverem sua assinatura.

Note: Antes que um certificado de servidor possa ser confiado, deve ser assinado por um certificado de raiz que tenha uma chave pública atual no navegador da Web.

Certificados de servidor

Um certificado de servidor é criado especificamente a fim ser usado na criptografia e na descriptografia HTTPS e a fim verificar a autenticidade de um server específico. Os certificados de servidor são assinados por CA com uso do certificado de raiz de CA. Um exemplo comum de CA é Verisign ou Thawte.

Note: Um certificado de servidor não pode ser usado a fim assinar outros Certificados; consequentemente, a descriptografia HTTPS não trabalha se um certificado de servidor é instalado no WSA.

O campo do CN em um certificado de servidor especifica o host para que o certificado é pretendido ser usado. Por exemplo, **https://www.verisign.com** usa um certificado de servidor com um CN de **www.verisign.com**.

Informações Relacionadas

- Uso do certificado da ferramenta de segurança da Web (WSA) (descriptografia HTTPS, início de uma sessão GUI, criptografia credencial)
- Etapas para permitir o proxy HTTPS em WSA & em opção da solicitação de assinatura de certificado (CSR)
- Etapas para permitir sobre o proxy HTTPS (WSA) & a raiz transferindo arquivos pela rede/opção intermediária do certificado
- Suporte Técnico e Documentação - Cisco Systems