Como instalar um certificado acorrentado SSL ao módulo de CSS SSL

Índice

Introdução

Um certificate chain é uma sequência dos Certificados, onde cada certificado na corrente é assinado pelo certificado subsequente. A finalidade do certificate chain é estabelecer uma corrente da confiança de um certificado de peer a um certificado da autoridade de certificação confiável (CA). CA responde pela identidade no certificado de peer assinando o. Se CA é um que você confia (indicado pela presença de uma cópia do certificado de CA em seu diretório do certificado de raiz), este implica-o pode confiar o certificado de peer assinado também.

Frequentemente, os clientes não aceitam os Certificados porque não foram criados por CA conhecido. O cliente indica tipicamente que a validez do certificado não pode ser verificada. Este é o caso quando o certificado é assinado por CA intermediário, que não está sabido ao navegador cliente. Nesses casos, é necessário usar um certificado SSL ou um grupo acorrentado do certificado. Este documento discute como instalar corretamente um certificado acorrentado do Secure Socket Layer (SSL) a um módulo de CSS SSL.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware:

- Módulo SSL CSS11506 (criptografia forte) - CSS 506-SSL-K9
- Módulo SSL CSS11501 (criptografia forte) - CSS 501-SSL-K9
- Somente módulo de switch CSS11506 - CSS 506-SM
- WebNS 7.10 e 7.20

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Instruções passo a passo

Esta seção mostra como instalar um certificado acorrentado no módulo de CSS SSL com o CSS11500.

Se o certificado acorrentado está nos arquivos múltiplos, use o procedimento esboçado abaixo.

1. Converta todos os Certificados ao mesmo formato. Se os Certificados são separados e não no formato do Privacy Enhanced Mail (PEM), você precisa de convertê-los ao formato PEM e de concatená-los então.
2. Concatene todos os Certificados em um arquivo; assegure-se de que estejam concatenados enquanto aparecem na corrente. O certificado de servidor deve ser primeiro na corrente, seguida pelos intermediários (certificados de servidor e certificados de CA intermediários).
3. Importe o arquivo certificado concatenado no CSS.
4. Associe o certificado ao SSL-server.
5. Aplique CA do SSL-server dentro da lista de proxy ssl.

Se todos estes Certificados estão acorrentados em um arquivo do PKCS-12 (tanto como dos Certificados do PKCS-12 seja), você deve importar o certificado acorrentado como um PKCS-12, e o associado/aplica-o como o normal. O PKCS-12 não é capaz da concatenação.

Nota: Os distintos formatos da regra da codificação (DER) não apoiam correntes, assim que esta não deve ser uma edição.

Para verificar, a chave que precisa de ser usada é a chave que gerou o arquivo da solicitação de assinatura de certificado (CSR) para criar o certificado de servidor. Há somente uma chave para um certificado, esteja ele acorrentou ou regular. Certifique-se verificar o certificado e a chave depois que são importados. Você pode emitir o comando mostrado abaixo.

```
(config)# ssl verify myrsacert1 myrsakey1 Certificate and key match
```

Informações Relacionadas

- CSS Advanced Configuration Guide
- Fixe/instalação de ID de servidor local PRO do comércio - Acelerador de e-Commerce de Intel NetStructure 7110
- Sustentação do produto dos Serviços de aplicação de rede
- Suporte Técnico e Documentação - Cisco Systems