ASA 8.x: Renove e instale o certificado SSL com ASDM

Índice

Introdução

O procedimento neste documento é um exemplo e pode ser usado como uma diretriz com todo o vendedor do certificado ou seu próprio server do certificado de raiz. As exigências especiais do parâmetro do certificado são exigidas às vezes por seu vendedor do certificado, mas este documento é pretendido fornecer as etapas gerais exigidas para renovar um certificado SSL e para instalá-lo em um ASA que use o software 8.0.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este procedimento refere-se as versões ASA 8.x com versão 6.0(2) ou mais recente ASDM.

O procedimento neste documento é baseado em uma configuração válida com um certificado instalado e usado para o acesso SSL VPN. Este procedimento não impacta sua rede enquanto o certificado atual não é suprimido. Este procedimento é um processo passo a passo em como emitir um CSR novo para um certificado atual com o mesmo certificado de raiz que emitiu a CA raiz original.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Procedimento

Conclua estes passos:

1. Selecione o certificado que você quer renovar abaixo da configuração > do Gerenciamento de dispositivos > dos certificados de identidade, e clique-o então **adicionam**.**Figura 1**
2. Sob adicionar o certificado de identidade, selecione **adicionar um** botão de rádio **novo do certificado de identidade**, e escolha seu par de chaves do menu suspenso.**Nota:** Não se recomenda usar o <Default-RSA-Key> porque se você regenera sua chave SSH, você invalida seu certificado. Se você não tem uma chave RSA, termine as etapas a e B. Se não continue a etapa 3.**Figura 2** (Opcional) termine estas etapas se você não tem uma chave RSA configurada ainda, se não faixa clara a etapa 3.Clique **novo…**Dê entrada com o nome do par de chaves no **campo de nome novo do par de chaves da entrada**, e o clique **gerencie agora**.**Figura 3**
3. Clique **seleto**.
4. Incorpore os atributos apropriados do certificado segundo as indicações de figura 4. Uma vez que terminado, clique a **APROVAÇÃO**. Clique então **adicionam o certificado**.**Figura 4** CLI output:
```
crypto ca trustpoint ASDM_TrustPoint0 keypair CertKey id-usage ssl-ipsec fqdn 5540-uwe
subject-name CN=ASA5540.company.com,OU=LAB,O=Cisco ystems,C=US,St=CA enrollment terminal
crypto ca enroll ASDM_TrustPoint0
```
5. Na janela pop-up do **pedido do certificado de identidade**, salvar sua solicitação de assinatura de certificado (CSR) a um arquivo de texto, e clique a **APROVAÇÃO**.**Figura 5**
6. (Opcional) verifique no ASDM que o CSR é pendente, segundo as indicações da figura 6.**Figura 6**
7. Submeta o pedido do certificado ao administrador do certificado, que emite o certificado no server. Isto pode ser através de uma interface da WEB, email, ou diretamente ao server da CA raiz para o processo da edição do certificado.
8. Termine estas etapas a fim instalar o certificado renovado.Selecione o pedido do certificado pendente sob a configuração > o Gerenciamento de dispositivos > os certificados de identidade, segundo as indicações da figura 6, e o clique **instala**.No indicador do certificado de identidade da instalação, selecione a **pasta os dados do certificado no** botão de rádio do **formato base-64**, e o clique **instala o certificado**.**Nota:** Alternativamente, se o certificado é emitido em um arquivo de .cer um pouco então um arquivo ou um email baseado texto, você pode igualmente selecionar **instala de um arquivo**, consulta ao arquivo apropriado em seu PC, clique **instala o arquivo certificado ID** e clica-o então **instala o certificado**.**Figura 7**CLI output:
```
crypto ca import ASDM_TrustPoint0 certificate
WIID2DCCAsCgAwIBAgIKYb9wewAAAAAAJzANBgkqhkiG9w0BAQUFADAQMQ !--- output truncated
wPevLEOl6TsMwng+izPQZG/f0+AnXukWHQiUPwrYw83jqNIxi5aDV/4atBbgiiBa
6duUocUGyQ+SgegCcmmEyMSd5UtbWAc4xOMMFw== quit
```
9. Um indicador aparece que confirme o certificado seja instalado com sucesso. " OK " do

clique a confirmar.**Figura 8**

10. Assegure-se de que seu certificado novo apareça sob certificados de identidade.**Figura 9**
11. Termine estas etapas a fim ligar o certificado novo à relação:Escolha a **configuração > o Gerenciamento de dispositivos > avançou > ajustes SSL**, segundo as indicações da figura 10.Selecione sua relação sob Certificados, e o clique **edita**.**Figura 10**
12. Escolha seu certificado novo do menu suspenso, clique a **APROVAÇÃO**, e o clique **aplica-se**.`ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1`
    `ssl trust-point ASDM_TrustPoint0 outside`**Figura 11**
13. Salvar sua configuração no ASDM ou no CLI.

Verificar

Você pode usar a interface CLI a fim verificar que o certificado novo está instalado ao ASA corretamente, segundo as indicações deste exemplo de saída:

```
ASA(config)#show crypto ca certificates Certificate Status: Available Certificate Serial Number:
61bf707b000000000027 Certificate Usage: General Purpose Public Key Type: RSA (1024 bits) Issuer
Name: cn=MS-CA Subject Name: cn=ASA5540.company.com !---new certificate ou=LAB o=Cisco Systems
st=CA c=US CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 22:39:31 UTC Aug 29 2008
end date: 22:49:31 UTC Aug 29 2009 Associated Trustpoints: ASDM_TrustPoint0 CA Certificate
Status: Available Certificate Serial Number: 211020a79cfd96b34ba93f3145d8e571 Certificate Usage:
Signature Public Key Type: RSA (2048 bits) Issuer Name: cn=MS-CA Subject Name: cn=MS-CA !---
'old' certificate CRL Distribution Points: [1] http://win2k3-base1/CertEnroll/MS-CA.crl [2]
file://\\win2k3-base1\CertEnroll\MS-CA.crl Validity Date: start date: 00:26:08 UTC Jun 8 2006
end date: 00:34:01 UTC Jun 8 2011 Associated Trustpoints: test Certificate Status: Available
Certificate Serial Number: 611f8630000000000026 Certificate Usage: General Purpose Public Key
Type: RSA (1024 bits) Issuer Name: cn=MS-CA Subject Name: cn=*.vpn1.com CRL Distribution Points:
[1] http://win2k3-base1/CertEnroll/MS-CA.crl [2] file://\\win2k3-base1\CertEnroll\MS-CA.crl
Validity Date: start date: 23:53:16 UTC Mar 10 2008 end date: 00:03:16 UTC Mar 11 2009
Associated Trustpoints: test ASA(config)#
```

Troubleshooting

(Opcional) verifique no CLI que o certificado correto está aplicado à relação:

```
ASA(config)#show running-config ssl ssl trust-point ASDM_TrustPoint0 outside !--- Shows that the
correct trustpoint is tied to the outside interface that terminates SSL VPN. ASA(config)#
```

Como copiar Certificados SSL de um ASA a outro

Isto pode ser feito se você tinha gerado chaves exportable. Você precisa de exportar o certificado para um arquivo PKCS. Isto inclui a exportação de todas as chaves associadas.

Use este comando exportar seu certificado através do CLI:

```
ASA(config)#crypto ca export <trust-point-name> pkcs12 <passphrase>
```

Nota: Frase de passagem - usada para proteger o arquivo do pkcs12.

Use este comando importar seu certificado através do CLI:

```
SA(config)#crypto ca import <trust-point-name> pkcs12 <passphrase>
```

Nota: Esta frase de passagem deve ser a mesma que usada ao exportar o arquivo.

Isto pode igualmente ser feito com o ASDM para um par de failover ASA. Termine estas etapas para executar isto:

1. Entre ao ASA preliminar através do ASDM e escolha **ferramentas--> configuração de backup**.
2. Você pode backup tudo ou apenas os Certificados.
3. No à espera, o ASDM aberto e escolhe **ferramentas --> configuração da restauração**.

Informações Relacionadas

- Página de suporte adaptável da ferramenta de segurança de Cisco (ASA)
- O ASA 8.x instala manualmente Certificados do vendedor da 3ª parte para o uso com exemplo de configuração WebVPN
- Suporte Técnico e Documentação - Cisco Systems