Configurando o Cisco VPN 3000 Concentrator 4.7.x para obter um certificado digital e um certificado SSL

Índice

Introdução

Este documento inclui instruções passo a passo em como configurar o Concentradores Cisco VPN série 3000 para autenticar com o uso de digital ou de certificados de identidade e de Certificados SSL.

Note: No concentrador VPN, o Balanceamento de carga deve ser desabilitado antes que você gerencia um outro certificado SSL desde que este impede a geração do certificado.

Refira como obter um certificado digital de Microsoft Windows CA usando o ASDM em um ASA a fim aprender uma encenação mais mais ou menos idêntica com PIX/ASA 7.x.

Refira o certificado de registro do Cisco IOS usando o exemplo aumentado dos comandos Configuration do registro a fim aprender uma encenação mais mais ou menos idêntica com Plataformas de Cisco IOS®.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no Cisco VPN 3000 Concentrator que executa a versão 4.7.

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

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

Instale Certificados digitais no concentrador VPN

Conclua estes passos:

1. Escolha o **Administração > Gerenciamento de Certificado > Registrar** a fim selecionar o pedido digital ou do certificado de identidade.
2. Escolha o **Administração > Gerenciamento Certificado > Registro > Certificado de Identidade** e o clique **registra-se através de PKCS10 Request(Manual)**.
3. Complete os campos pedidos, e clique-os então **registram-se**.Estes campos são completados neste exemplo.**Common Name** — altiga30**Unidade organizacional** — IPSECCERT (o OU deve combinar o nome de grupo configurado do IPsec)**Organização** — Cisco Systems**Localidade** — RTP**Estado/província** — North Carolina**País** — E.U.**Nome de domínio totalmente qualificado** — (não usado aqui)**Tamanho chave** — 512**Note**: Se você pede um certificado SSL ou um certificado de identidade usando o protocolo simple certificate enrollment (SCEP), estas são as únicas opções RSA disponíveis.Bit RSA 512Bit RSA 768Bit RSA 1024Bit RSA 2048Bit DSA 512Bit DSA 768Bit DSA 1024
4. Depois que você clique **se registra**, diversos indicadores aparecem. O primeiro indicador confirma que você pediu um certificado.Uma janela de navegador nova igualmente abre e indica seu arquivo do pedido PKCS.
5. Em seu server do Certification Authority (CA), destaque o pedido e cole-o em seu server de CA a fim submeter seu pedido. Clique em Next.
6. Selecione o **pedido avançado** e clique-o **em seguida**.
7. Seleto **submeta um pedido do certificado usando base64 um arquivo do PKCS codificado #10 ou uma requisição de renovação usando base64 um arquivo do PKCS codificado #7**, e clique-o então **em seguida**.
8. Cortare-col seu arquivo PKCS no campo de texto sob a seção da solicitação salva. Clique então **submetem-se**.
9. Emita o certificado de identidade no server de CA.
10. Transfira a raiz e os certificados de identidade. Em seu server de CA, selecione a **verificação em um certificado pendente**, e clique-a **em seguida**.
11. Selecione **Base64 codificado**, e clique o **certificado de CA da transferência no** server de CA.
12. Salvar o certificado de identidade em sua unidade local.
13. No server de CA, seleto **recupere o certificado de CA ou a lista de revogação de certificado** a fim obter o certificado de raiz. Em seguida, clique em Avançar.
14. Salvar o certificado de raiz em sua unidade local.
15. Instale a raiz e os certificados de identidade no VPN 3000 concentrator. A fim fazer isto, **certificado** seleto do **Administração > Gerenciador de Certificado > Instalação > Instalar**

obtido através do registro. Sob o estado do registro, o clique **instala**.
16. **Arquivo da transferência de arquivo pela rede do** clique da **estação de trabalho**.
17. Clique **consultam** e selecionam o arquivo de certificado de raiz que você salvar a sua unidade local.Seleto **instale** para instalar o certificado de identidade no concentrador VPN. A administração | O indicador do gerenciamento certificado aparece como uma confirmação, e seu certificado de identidade novo aparece na tabela dos certificados de identidade.**Note**: Termine estas etapas para gerar um certificado novo se o certificado falha.Selecione o **administração > gerenciamento de certificado**.Clique a **supressão na** caixa das ações para a lista do certificado SSL.Selecione a **repartição da administração >** do **sistema**.Selecione a **salvaguarda a configuração ativa na época da repartição**, escolha-a **agora**, e o clique **aplica-se**. Você pode agora gerar um certificado novo depois que o reload está completo.

Instale Certificados SSL no concentrador VPN

Se você usa uma conexão segura entre seu navegador e o concentrador VPN, o concentrador VPN exige um certificado SSL. Você igualmente precisa um certificado SSL na relação que você se usa para controlar o concentrador VPN e para o WebVPN, e para cada relação que termina túneis WebVPN.

Os Certificados da relação SSL, se inexistentes, estiverem gerados automaticamente quando as repartições do VPN 3000 concentrator depois que você promove o software do VPN 3000 concentrator. Porque um certificado auto-assinado auto-é gerado, este certificado não é passível de verificação. Nenhum Certificate Authority garantiu sua identidade. Mas este certificado permite que você faça o contato inicial com o concentrador VPN usando o navegador. Se você quer o substituir com um outro certificado auto-assinado SSL, termine estas etapas:

1. Escolha o **administração > gerenciamento de certificado**.
2. O clique **gerencie** a fim indicar o certificado novo na tabela do certificado SSL e substituir existente.Este indicador permite que você configure campos para Certificados que SSL o concentrador VPN gerencie automaticamente. Estes Certificados SSL são para relações e para o Balanceamento de carga.Se você quer obter um certificado passível de verificação SSL (isto é, um emitido por um Certificate Authority), veja os Certificados digitais da instalação na seção do concentrador VPN deste documento a fim usar o mesmo procedimento que você se usa para obter certificados de identidade. Mas esta vez, no indicador do **Administração > Gerenciamento de Certificado > Registrar**, **certificado do** clique **SSL** (em vez do certificado de identidade).**Note**: Refira a *administração | Seção de gerenciamento de certificado do* volume de referência II do VPN 3000 concentrator: A administração e a monitoração liberam 4.7 para obter informações completas sobre dos Certificados digitais e dos Certificados SSL.

Renove Certificados SSL no concentrador VPN

Esta seção descreve como renovar os Certificados SSL:

Se isto é para o certificado SSL gerado pelo concentrador VPN, vá ao **administração > gerenciamento de certificado na** seção SSL. Clique a opção da **renovação**, e isso renova o certificado SSL.

Se isto é para um certificado concedido por um server externo de CA, termine estas etapas:

1. Escolha o **>Delete do administração > gerenciamento de certificado** sob *Certificados SSL* a fim suprimir dos certificados expirados da interface pública.Clique **sim** a fim confirmar o supressão do certificado SSL.
2. Escolha o **administração > gerenciamento de certificado > gerenciem** a fim gerar o certificado novo SSL.O certificado novo SSL para a interface pública aparece.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems