Configurando o cliente VPN 3.x para obter um certificado digital

Índice

Introdução

Este documento demonstra como configurar o Cisco VPN Client 3.x para obter um certificado digital.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em um PC que execute o Cisco VPN Client 3.x.

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.

Configurar o VPN Client

Termine estas etapas para configurar o cliente VPN.

1. Selecione o **Iniciar > Programas > Cliente de VPN de Cisco Systems Inc. > Gerenciador de Certificado** para lançar o gerenciador certificado do cliente VPN.
2. Selecione a aba dos certificados pessoais e clique **novo**.**Note**: Os certificados da máquina para autenticar usuários para conexões de VPN não podem ser feitos com IPsec.
3. Quando o cliente VPN o alerta para uma senha, especifique uma senha para proteger o certificado. Toda a operação que exigir o acesso à chave privada do certificado exige a senha especificada continuar.
4. Selecione o **arquivo** para pedir um certificado usando o formato PKCS #10 na página do registro. Em seguida, clique em Avançar.
5. O clique **consulta**, e especifica um nome de arquivo para o arquivo do pedido do certificado. Para o tipo de arquivo, o **PEM** seleto **codificou o arquivo do pedido (*.req)** e a **salvaguarda do** clique.
6. Clique **em seguida na** página do registro do cliente VPN.
7. Complete os campos no formulário do registro.Este exemplo mostra os campos:Common Name = usuário1Departamento = IPSECCERT (isto deve combinar a unidade organizacional (OU) e o nome do grupo no VPN 3000 concentrator.)Empresa = Cisco SystemsEstado = North CarolinaPaís = E.U.Email = User1@email.comEndereço IP de Um ou Mais Servidores Cisco ICM NT = (opcional; usado para especificar o endereço IP de Um ou Mais Servidores Cisco ICM NT no pedido do certificado)Domínio = cisco.comClique **em seguida** quando você for feito.
8. **Revestimento do** clique a continuar com o registro.
9. Selecione a aba dos pedidos do registro para verificar o pedido no gerenciador certificado do cliente VPN.
10. Traga acima o server do Certification Authority (CA) e o cliente VPN conecta simultaneamente para submeter o pedido.
11. Selecione o **pedido um certificado** e clique-o **em seguida no** server de CA.
12. Selecione o **pedido avançado** para o tipo de pedido e clique-o **em seguida**.
13. 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** sob pedidos do certificado avançados, e clique-o então **em seguida**.
14. Destaque o arquivo do pedido do cliente VPN, e cole-o ao server de CA sob a solicitação salva. Clique então **submetem-se**.
15. No server de CA, emita o certificado de identidade para o pedido do cliente VPN.
16. Transfira a raiz e os certificados de identidade ao cliente VPN. No server de CA, selecione a **verificação em um certificado pendente**, e clique-a então **em seguida**.
17. Selecione **Base64 codificou**. Clique então o **certificado de CA da transferência no** server de CA.
18. Selecione um arquivo para transferir a recuperação da página do certificado de CA ou da lista de revogação de certificado para obter o certificado de raiz no server de CA. Em seguida, clique em Avançar.
19. Selecione o **Gerenciador de Certificado > Certificado CA > Importar no VPN Client**, e selecione então o arquivo da CA raiz para instalar a raiz e os certificados de identidade.
20. Selecione o **Gerenciador de Certificado > Certificados Pessoais > Importar**, e escolha o arquivo de certificado de identidade.
21. Assegure-se de que o certificado de identidade apareça sob a aba dos certificados pessoais.

22. Assegure-se de que o certificado de raiz apareça sob a aba dos certificados de CA.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Quando você tenta se registrar com o Microsoft CA server, pode gerar este Mensagem de Erro.

```
Initiating online request
Generating key pair
Generating self-signed Certificate
Initiating online request
Received a response from the CA
Your certificate request was denied
```

Se você recebe este Mensagem de Erro, refira os logs de Microsoft CA para detalhes, ou refira estes recursos para mais informação.

- Windows não pode encontrar um Certificate Authority que processa o pedido
- XCCC: “Seu pedido do certificado esteve negado” o Mensagem de Erro ocorre quando você pede um certificado para conferências seguras

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems