Verificação CRL sobre HTTP em um Cisco VPN 3000 Concentrator

Índice

Introdução

Este documento descreve como permitir o Certificate Revocation List (CRL) que verifica para ver se há Certificados de Certification Authority (CA) instalados no Cisco VPN 3000 Concentrator usando o modo de HTTP.

Um certificado é esperado normalmente ser válido para seu período de validade inteiro. Contudo, se um certificado assenta bem no inválido devido a coisas como uma alteração de nome, mudança da associação entre o assunto e o CA, e acordo da Segurança, CA revoga o certificado. Sob o X.509, os CA revogam Certificados periodicamente emitindo um CRL assinado, onde cada certificado revogado seja identificado por seu número de série. Permitir a verificação CRL significa que cada vez que o concentrador VPN usa o certificado para a autenticação, igualmente verifica o CRL para se assegurar de que o certificado que está sendo verificado não esteja revogado.

Bases de dados do Lightweight Directory Access Protocol (LDAP) /HTTP do uso CA para armazenar e distribuir CRL. Puderam igualmente usar outros meios, mas o concentrador VPN confia no acesso LDAP/HTTP.

A verificação CRL HTTP é introduzida na versão 3.6 ou mais recente do concentrador VPN. Contudo, a verificação CRL LDAP-baseada foi introduzida nas liberações 3.x mais adiantadas. Este documento discute somente a verificação CRL usando o HTTP.

Note: O tamanho de cache CRL do VPN 3000 series concentrators depende da plataforma e não pode ser configurado de acordo com o desejo do administrador.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Você estabeleceu com sucesso o túnel de IPsec dos clientes da ferragem VPN 3.x que usam Certificados para a autenticação do Internet Key Exchange (IKE) (sem a verificação CRL permitida).
- Seu concentrador VPN tem a Conectividade ao server de CA em todas as vezes.
- Se seu server de CA é conectado para fora à interface pública, a seguir você abriu regras necessárias no filtro público (do padrão).

Componentes Utilizados

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

- C da versão 4.0.1 do VPN 3000 concentrator
- Cliente da ferragem VPN 3.x
- Microsoft CA server para a geração e a verificação CRL do certificado que são executado em um servidor do Windows 2000.

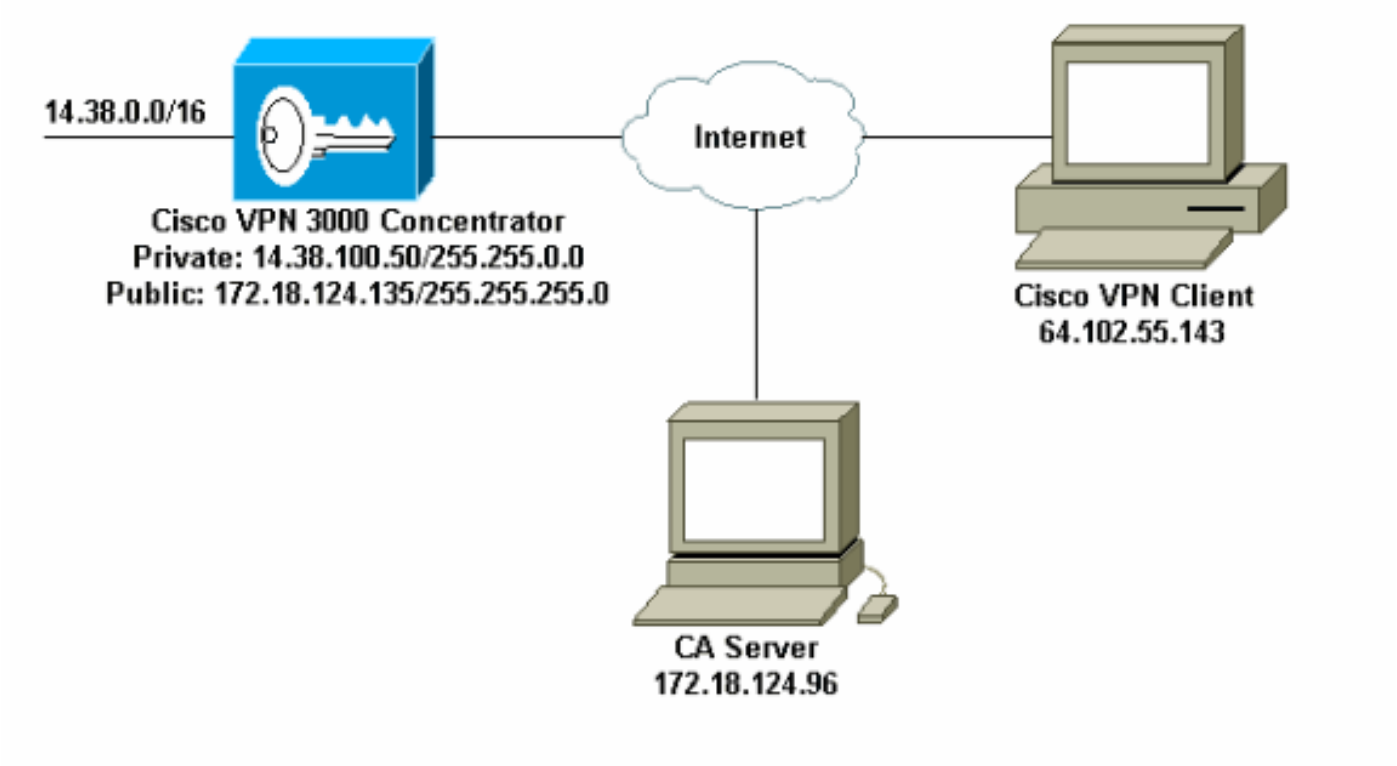
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer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

Convenções

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

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

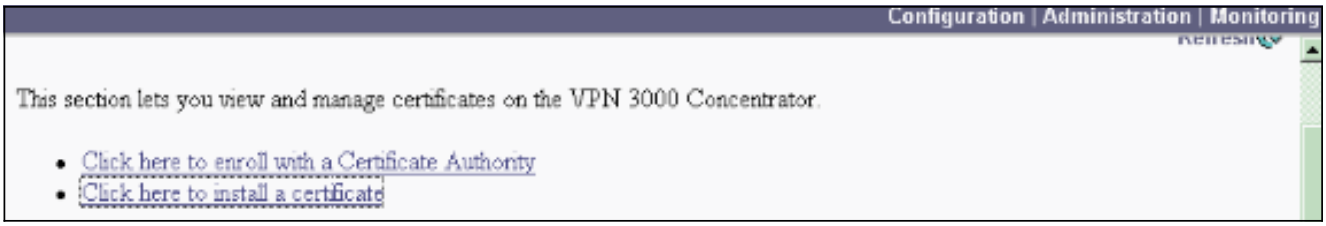


Configurar o VPN 3000 Concentrator

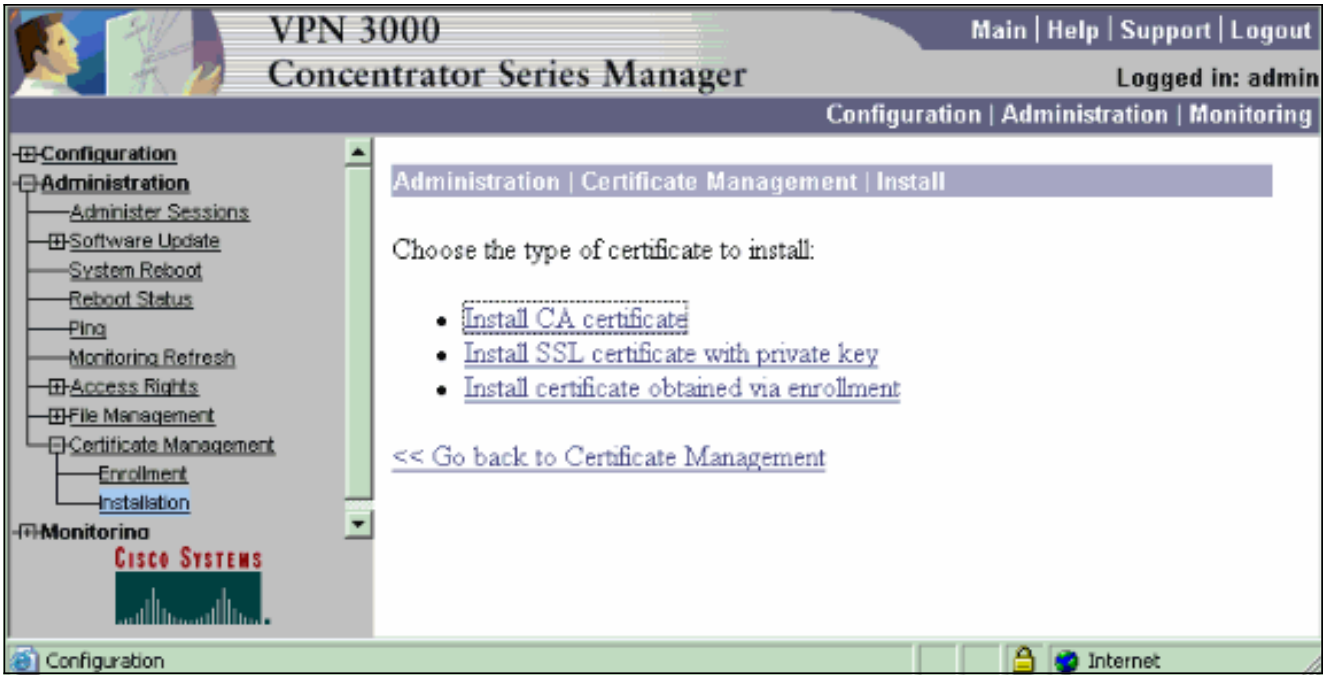
Instruções passo a passo

Termine estas etapas para configurar o VPN 3000 concentrator:

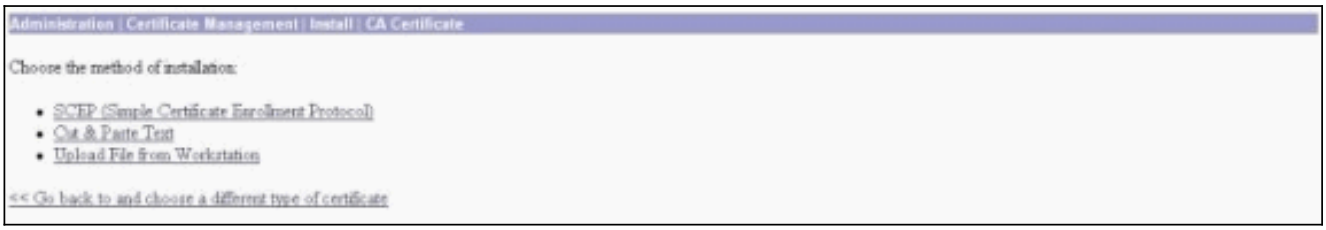
1. Selecione o **administração > gerenciamento de certificado** para pedir um certificado se você não tem um certificado.Selecione **clicam aqui para instalar um certificado** para instalar o certificado de raiz no concentrador VPN.



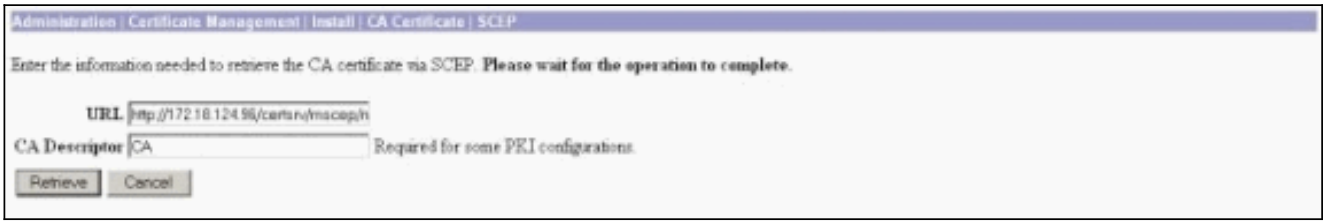
2. Seleto **instale o certificado de CA**.



3. Selecione **SCEP (protocolo simple certificate enrollment)** para recuperar os certificados de CA.

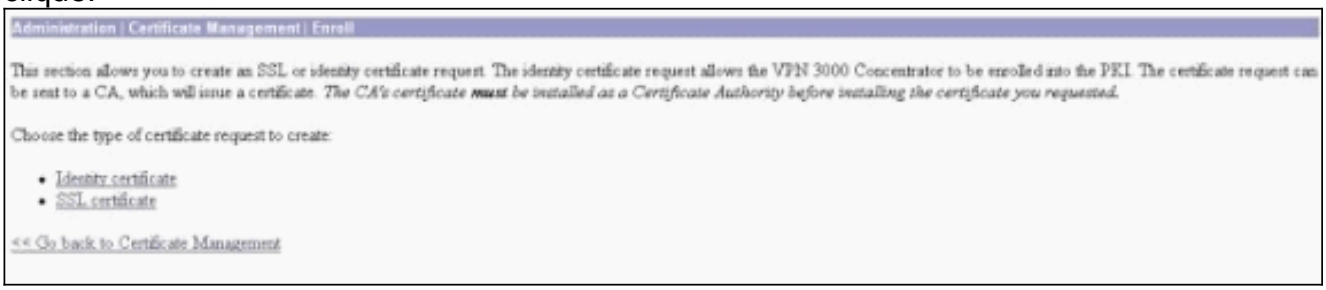


4. Da janela SCEP, incorpore a URL completa do server de CA à caixa de diálogo URL.Neste exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT do server de CA é 172.18.124.96. Desde que este exemplo usa o server de CA de Microsoft, a URL completa é http://172.18.124.96/certsrv/mscep/mscep.dll. Em seguida, inscreva um descritor de uma palavra na caixa de diálogo do descritor de CA. Este exemplo usa CA.

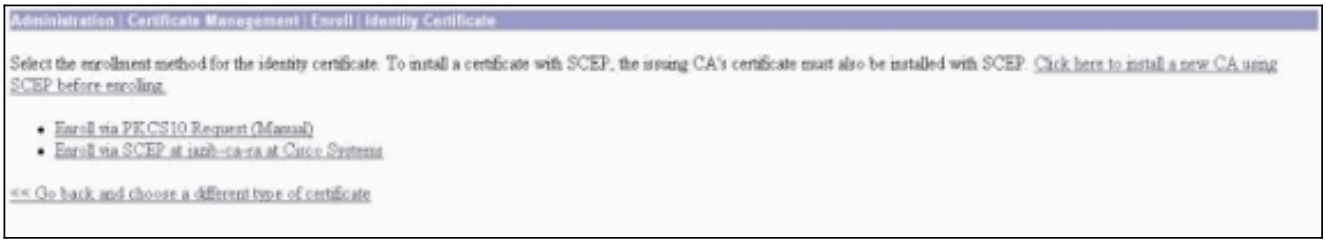


5. O clique **recupera**.Seu certificado de CA deve aparecer sob o indicador do administração > gerenciamento de certificado. Se você não vê um certificado, passe para trás a etapa 1 e siga o procedimento outra vez.

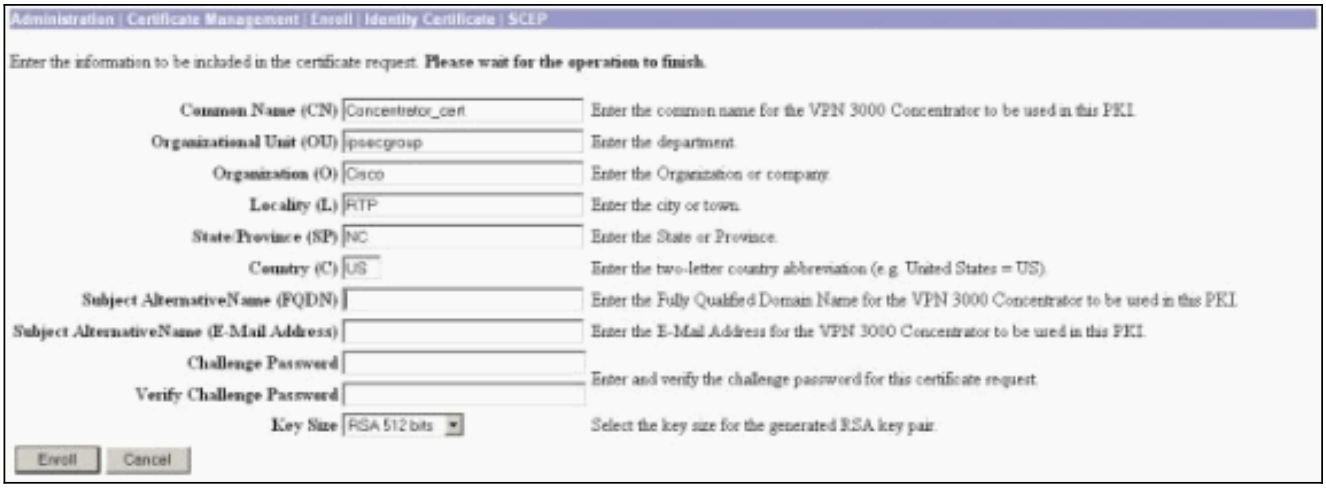
6. Uma vez que você tem o certificado de CA, o **Administração > Gerenciamento de Certificado > Registrar** seleto, e o **certificado de identidade do** clique.



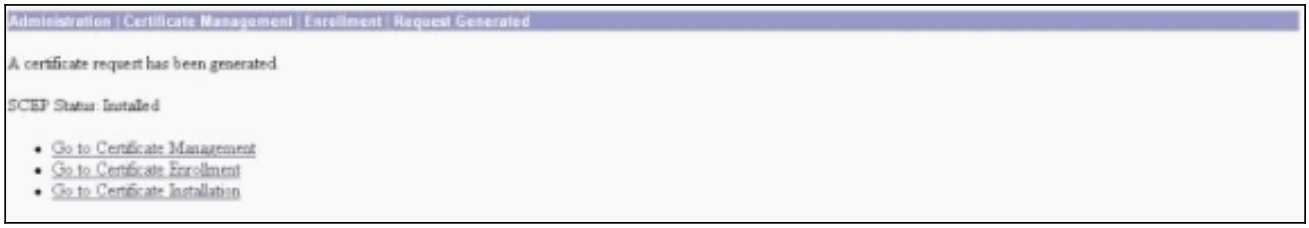
7. O clique **registra-se através do SCEP em…** para aplicar-se para o certificado de identidade.



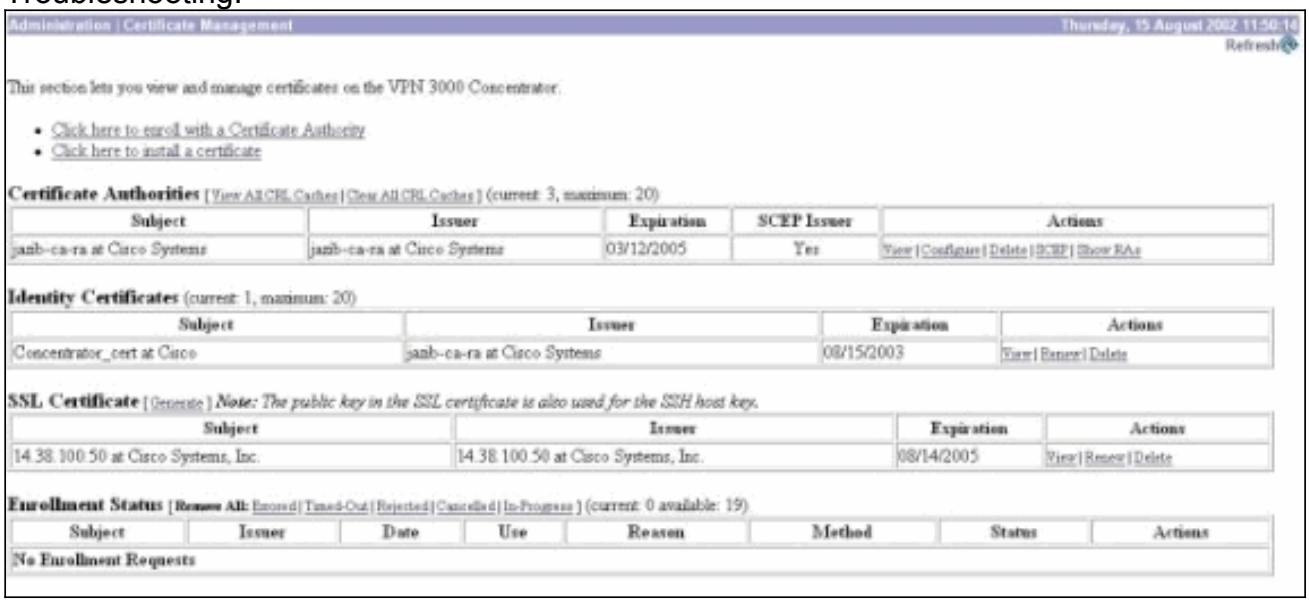
8. Termine estas etapas para completar o formulário do registro:Incorpore o Common Name para que o concentrador VPN seja usado no Public Key Infrastructure (PKI) ao campo do Common Name (CN).Incorpore seu departamento ao campo da unidade organizacional (OU). O OU deve combinar o nome do grupo de IPSec configurado.Incorpore sua organização ou empresa à organização (O) campo.Entre em sua cidade ou cidade na localidade (L) campo.Inscreva sua estado ou província no campo do estado/província (SP).Entre em seu país no campo do país (c).Incorpore o nome de domínio totalmente qualificado (FQDN) para que o concentrador VPN seja usado no PKI ao campo do nome de domínio totalmente qualificado (FQDN).Incorpore o endereço email para que o concentrador VPN seja usado no PKI ao campo alternativo sujeito do nome (endereço email).Incorpore a senha do desafio para o pedido do certificado ao campo de senha do desafio.Reenter a senha do desafio no campo de senha do desafio da verificação.Selecione o tamanho chave para o par de chaves gerado RSA da lista de drop-down do tamanho chave.



9. Seleto **registre** e veja o status de SCEP no estado de polling.
10. Vá a seu server de CA aprovar o certificado de identidade. Uma vez que é aprovado no server de CA, seu status de SCEP deve ser instalado.



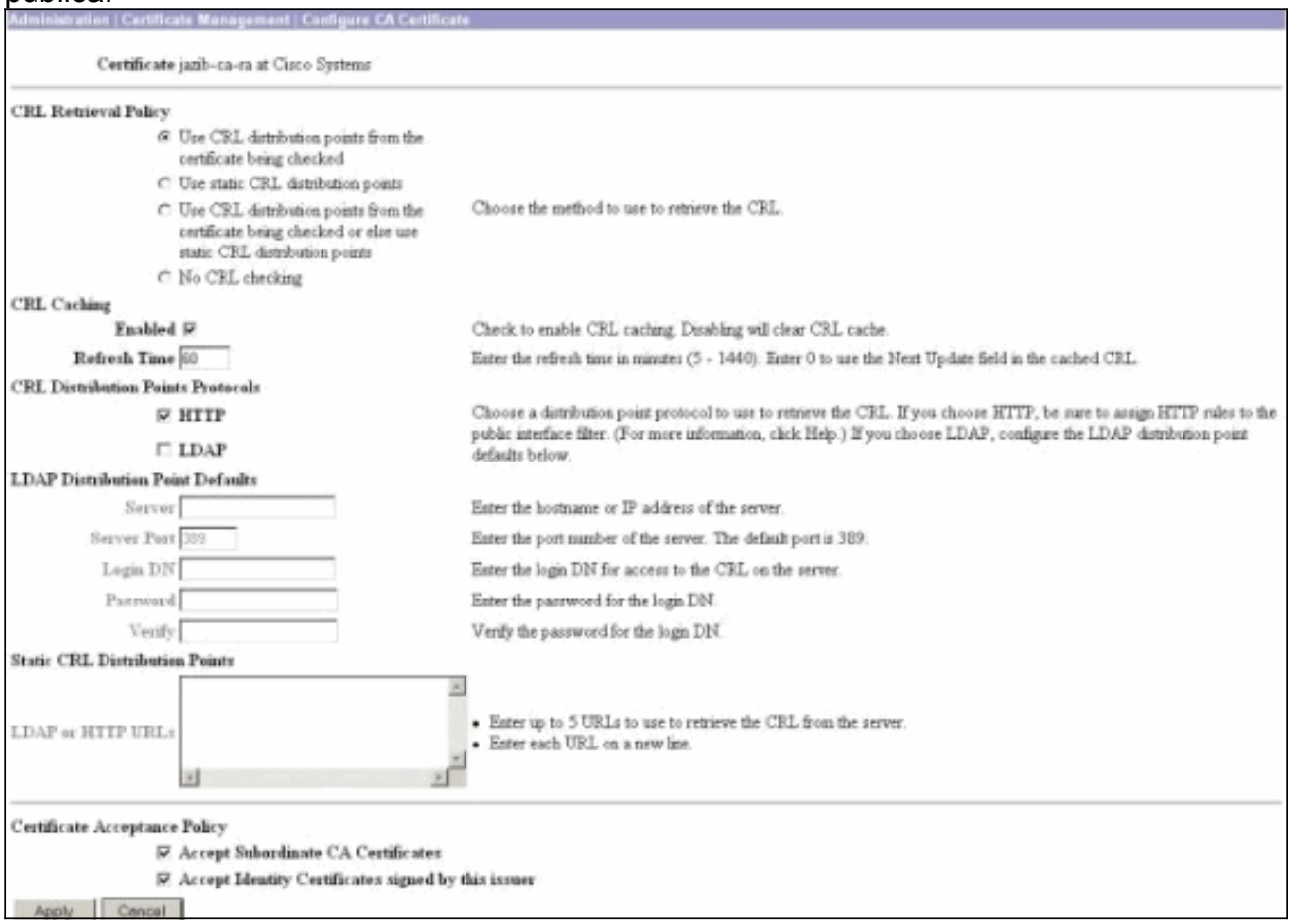
11. Sob o gerenciamento certificado, você deve ver seu certificado de identidade.Se você não faz, para verificar entra seu server de CA para mais Troubleshooting.



12. Selecione a **vista em** seu certificado recebido para ver se seu certificado tem um CRL Distribution Point (CDP).O CDP alista todos os pontos da distribuição de CRL do expedidor deste certificado. Se você tem o CDP em seu certificado, e você usa um nome de DNS para enviar uma pergunta ao server de CA, certifique-se de que você tem servidores DNS definidos em seu concentrador VPN para resolver o hostname com um endereço IP de Um ou Mais Servidores Cisco ICM NT. Neste caso, o nome de host do server de CA do exemplo é o jazib-PC que resolve a um endereço IP de Um ou Mais Servidores Cisco ICM NT de 172.18.124.96 no servidor DNS.

13. O clique **configura em** seu certificado de CA para permitir a verificação CRL nos Certificados recebidos.Se você tem o CDP em seu certificado recebido e você gostaria do usar, a seguir selecione **pontos da distribuição de CRL do uso do certificado que está sendo verificado**.Desde que o sistema tem que recuperar e examinar o CRL de um ponto de distribuição da rede, permitir a verificação CRL pôde retardar o tempo de resposta de sistema. Também, se a rede é lenta ou congestionada, a verificação CRL pôde falhar. Permita o CRL que põe em esconderijo para abrandar estes problemas potenciais. Isto armazena os CRL recuperados na memória volátil local e permite consequentemente que o concentrador VPN verifique o status de revogação dos Certificados mais rapidamente.Com pôr em esconderijo CRL permitido, as primeiras verificações do concentrador VPN se o CRL exigido existe no esconderijo e verifica o número de série do certificado contra a lista de números de série no CRL quando precisar de verificar o status de revogação de um certificado. O certificado está considerado revogado se seu número de série é encontrado. O concentrador VPN recupera um CRL de um servidor interno qualquer um quando não encontra o CRL exigido no esconderijo, quando o período de validade do CRL posto em esconderijo expirou, ou quando as horas da atualização configuradas decorreram. Quando o concentrador VPN recebe um CRL novo de um servidor interno, atualiza o esconderijo com o CRL novo. O esconderijo pode conter até 64 CRL.**Note**: O esconderijo CRL existe na memória. Consequentemente, recarregar o concentrador VPN cancela o esconderijo CRL. O concentrador VPN preencher novamente o esconderijo CRL com os CRL actualizados como ele processa novas requisições de autenticação de peer.Se você seleciona **pontos estáticos da distribuição de CRL do uso**, a seguir você pode usar até cinco pontos estáticos da distribuição de CRL, como especificado neste indicador. Se você escolhe esta opção, você deve incorporar pelo menos uma URL.Você pode igualmente selecionar **pontos da distribuição de CRL do uso do certificado que está sendo verificado**, ou selecionar **pontos estáticos da distribuição de CRL do uso**. Se o concentrador VPN não pode encontrar cinco pontos da distribuição de CRL no certificado, adiciona pontos estáticos da distribuição de CRL, até um limite de cinco. Se você escolhe esta opção, permita pelo menos um protocolo do CRL Distribution Point. Você igualmente deve incorporar pelo menos pontos estáticos de uma (e não mais de cinco) distribuição de CRL.Não selecione **nenhuma verificação CRL** se você quer desabilitar a verificação CRL.Sob o CRL que põe em esconderijo, selecione a caixa **permitida** para permitir que o concentrador VPN ponha em esconderijo CRL recuperados. O padrão não é permitir pôr em esconderijo CRL. Quando você desabilitar o CRL que põe em esconderijo (unselect a caixa), o esconderijo CRL está cancelado.Se você configurou uma política de recuperação de CRL que use pontos da distribuição de CRL do certificado que está sendo verificado,

escolha um protocolo do ponto de distribuição usar-se para recuperar o CRL. Escolha o **HTTP** neste caso recuperar o CRL. Atribua regras HTTP ao filtro da interface pública se seu server de CA é para a interface
pública.



Monitoramento

Selecione o **administração > gerenciamento de certificado** e clique sobre a **vista todos os esconderijos CRL** para ver se seu concentrador VPN pôs em esconderijo algum CRL do server de CA.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração funciona adequadamente.

Logs do concentrador

Permita estes eventos no concentrador VPN a fim certificar-se de que a verificação CRL trabalha.

1. Selecione o **configuração > sistema > eventos > classes** para ajustar os níveis de registro.
2. Sob o nome de classe selecione o **IKE**, o **IKEDBG**, o **IPSEC**, o **IPSECDBG**, ou o **CERT**.
3. Clique **adicionam** ou **alteram**, e escolhem a **severidade registrar a opção 1-13**.
4. O clique **aplica-se** se você quer alterar, ou **adiciona-se** se você quer adicionar uma entrada nova.

Registros de concentrador concluídos com sucesso

Se sua verificação CRL é bem sucedida, estas mensagens estão consideradas nos log filtrável de eventos.

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)

1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2

1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)

1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

Refira logs bem sucedidos do concentrador para as saídas completas de um log bem sucedido do concentrador.

Logs falhados

Se sua verificação CRL em não bem sucedido, estas mensagens é considerada nos log filtrável de eventos.

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5

1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.

1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

Refira log revogado de concentrador para as saídas completas de um log falhado do concentrador.

Refira logs bem sucedidos do cliente para as saídas completas de um log bem sucedido do cliente.

Refira log revogado de cliente para as saídas completas de um log falhado do cliente.

Troubleshooting

Refira pesquisando defeitos problemas de conexão no VPN 3000 concentrator para mais informação de Troubleshooting.

Informações Relacionadas

- Página de suporte do Concentradores Cisco VPN série 3000
- Página de suporte ao Cisco VPN 3000 Client
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems