Verificação CRL sobre HTTP em um Cisco VPN 3000 Concentrator

Contents

Introduction

Este documento descreve como habilitar a verificação de lista de revogação de certificados (CRL) para certificados de autoridade de certificação (CA) instalados no Cisco VPN 3000 Concentrator usando o modo HTTP.

Normalmente, espera-se que um certificado seja válido para todo o seu período de validade. No entanto, se um certificado se tornar inválido devido a itens como uma alteração de nome, alteração de associação entre o assunto e a AC e comprometimento de segurança, a CA revogará o certificado. Em X.509, as CA revogam os certificados emitindo periodicamente um CRL assinado, em que cada certificado revogado é identificado pelo seu número de série. Habilitar verificação de CRL significa que cada vez que o VPN Concentrator usa o certificado para autenticação, ele também verifica a CRL para garantir que o certificado que está sendo verificado não foi revogado.

As CAs usam bancos de dados LDAP/HTTP para armazenar e distribuir CRLs. Eles também podem usar outros meios, mas o VPN Concentrator depende do acesso LDAP/HTTP.

A verificação de CRL de HTTP é introduzida no VPN Concentrator versão 3.6 ou posterior. No entanto, a verificação de CRL baseada em LDAP foi introduzida nas versões 3.x anteriores. Este documento discute somente a verificação de CRL usando HTTP.

Observação: o tamanho do cache de CRL dos VPN 3000 Series Concentrators depende da plataforma e não pode ser configurado de acordo com o desejo do administrador.

Prerequisites

Requirements

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

- Você estabeleceu com êxito o túnel IPsec dos Clientes de Hardware VPN 3.x usando certificados para autenticação do Internet Key Exchange (IKE) (sem verificação de CRL habilitada).
- O VPN Concentrator tem conectividade com o servidor CA o tempo todo.
- Se o servidor CA estiver conectado à interface pública, você abrirá as regras necessárias no filtro público (padrão).

Componentes Utilizados

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

- VPN 3000 Concentrator versão 4.0.1 C
- Cliente de hardware VPN 3.x
- Servidor Microsoft CA para geração de certificado e verificação CRL em execução em um servidor Windows 2000.

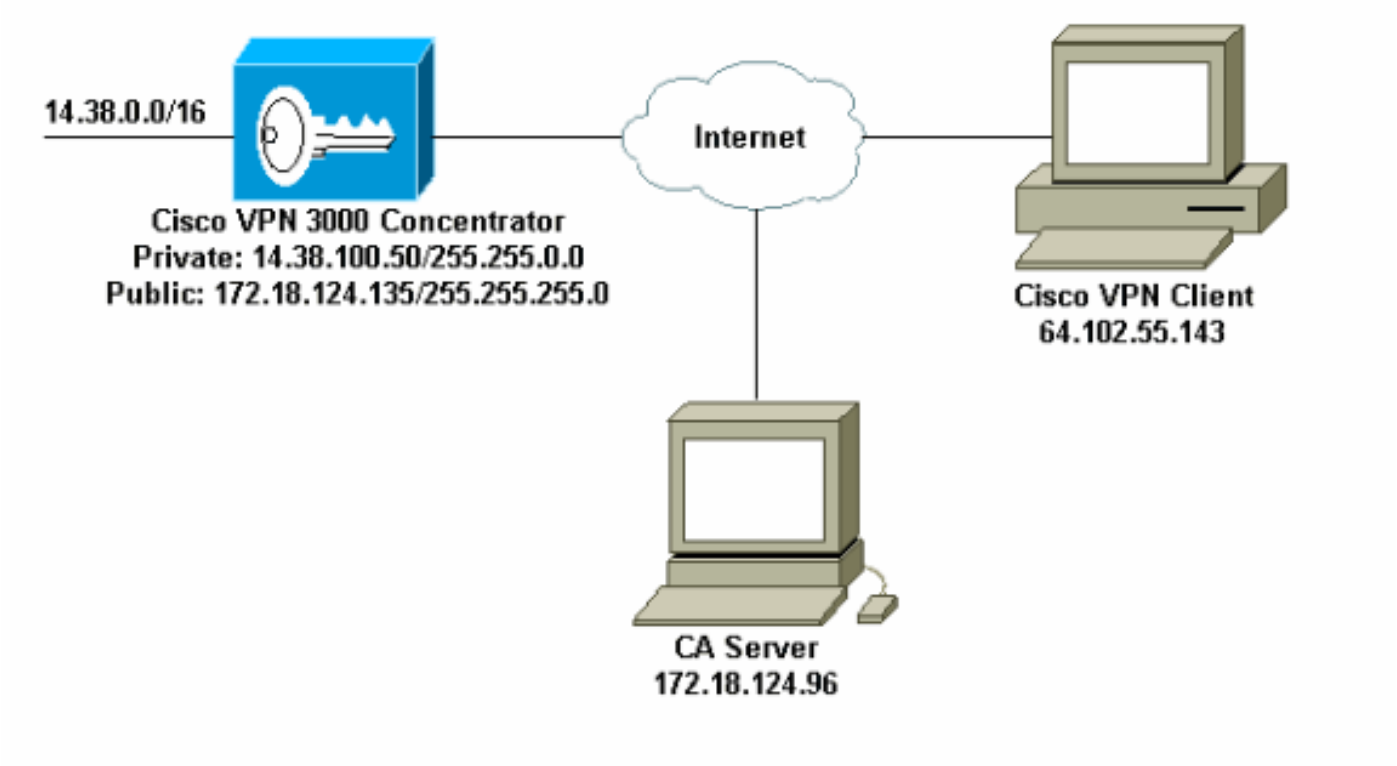
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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:

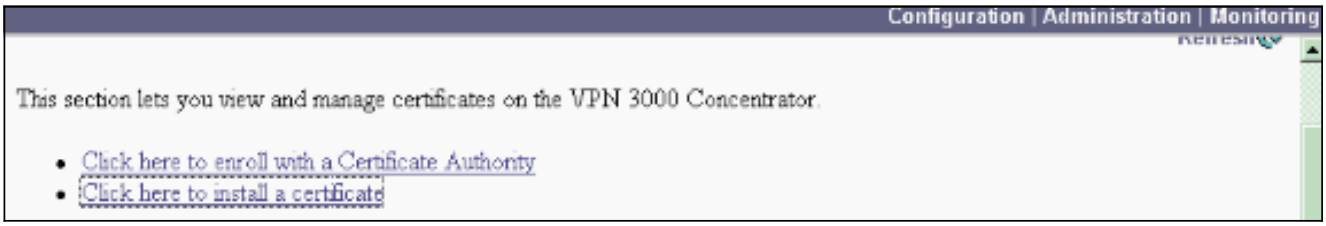


Configurar o VPN 3000 Concentrator

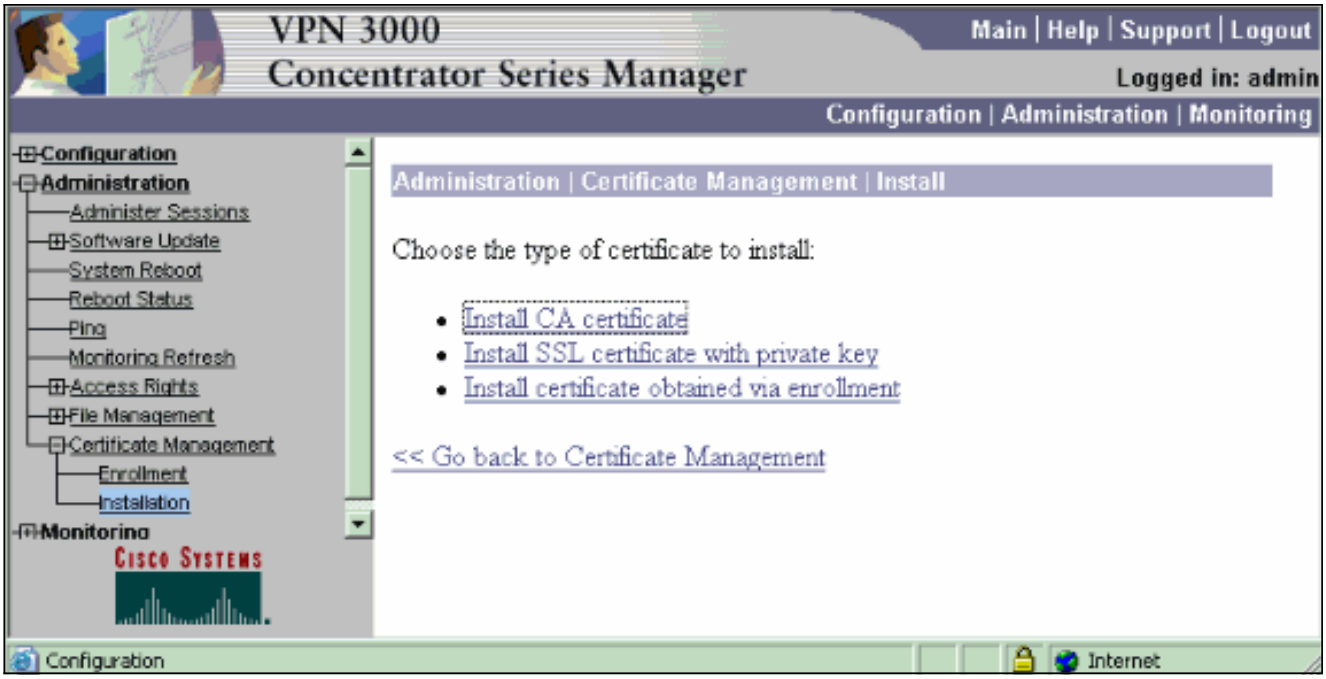
Step-by-Step Instructions

Conclua estes passos para configurar o VPN 3000 Concentrator:

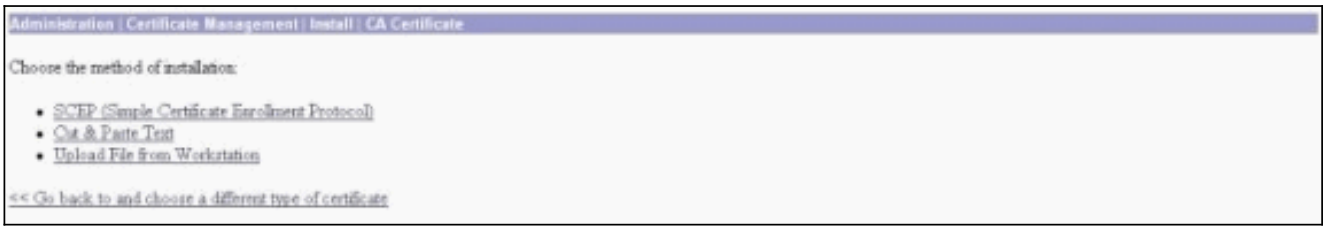
1. Selecione **Administration > Certificate Management** para solicitar um certificado se você não tiver um certificado.Selecione **Clique aqui para instalar um certificado** para instalar o certificado raiz no VPN Concentrator.



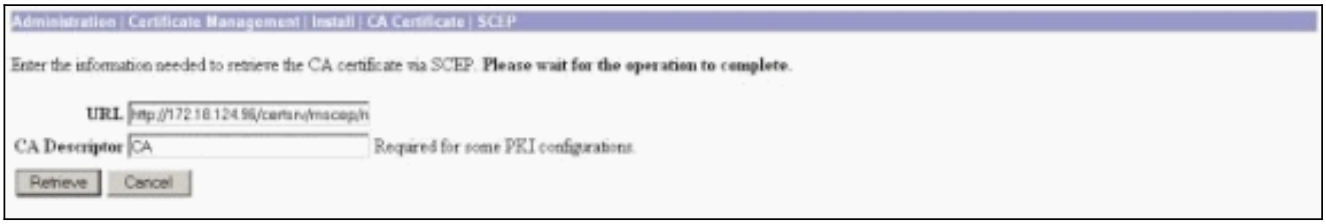
2. Selecione **Instalar certificado CA**.



3. Selecione **SCEP (Simple Certificate Enrollment Protocol)** para recuperar os certificados CA.

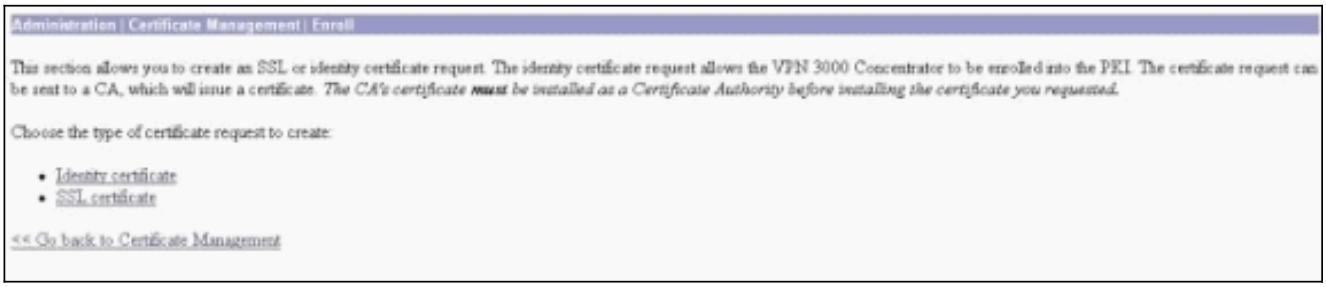


4. Na janela SCEP, digite a URL completa do servidor CA na caixa de diálogo URL.Neste exemplo, o endereço IP do servidor CA é 172.18.124.96. Como este exemplo usa o servidor CA da Microsoft, o URL completo é http://172.18.124.96/certsrv/mscep/mscep.dll. Em seguida, digite um descritor de uma palavra na caixa de diálogo Descritor de CA. Este exemplo usa
CA.

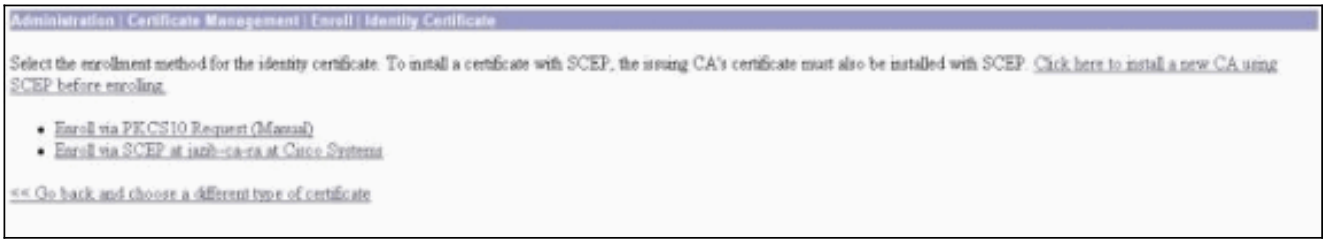


5. Clique em **Recuperar**.Seu certificado CA deve aparecer na janela Administration > Certificate Management. Se você não vir um certificado, volte para a Etapa 1 e siga o procedimento
novamente.

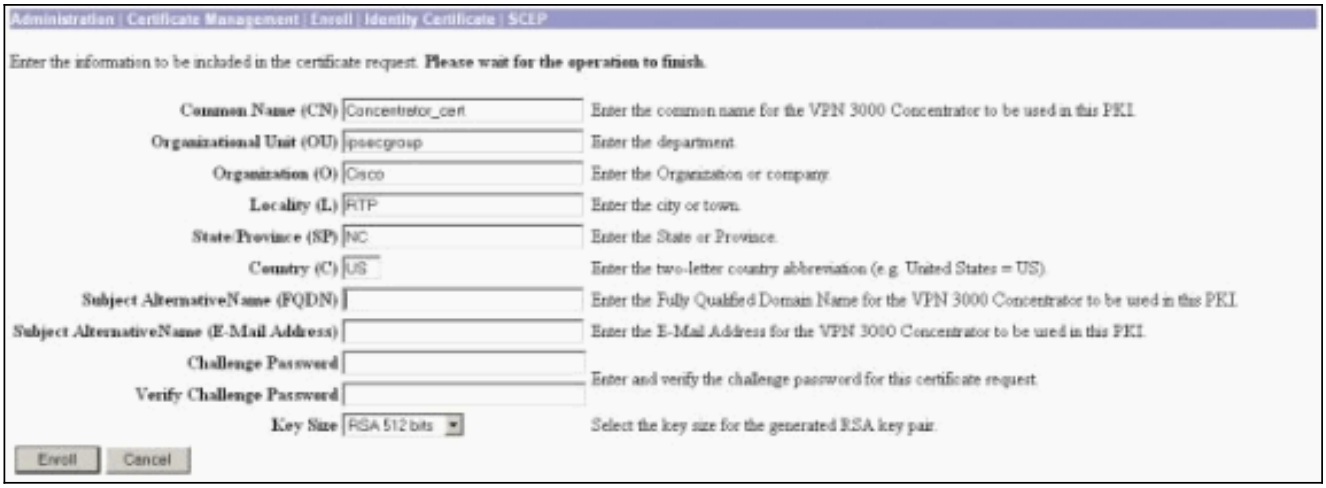
6. Depois de possuir o certificado CA, selecione **Administration > Certificate Management > Enroll** e clique em **Identity certificate**.



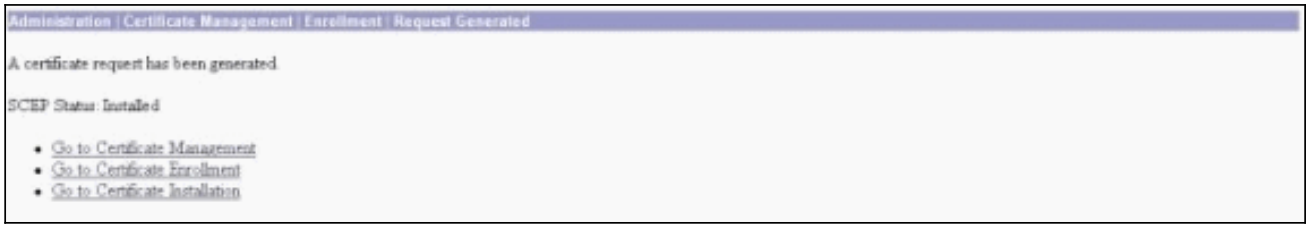
7. Clique em **Inscrever-se via SCEP em ...** para solicitar o certificado de identidade.



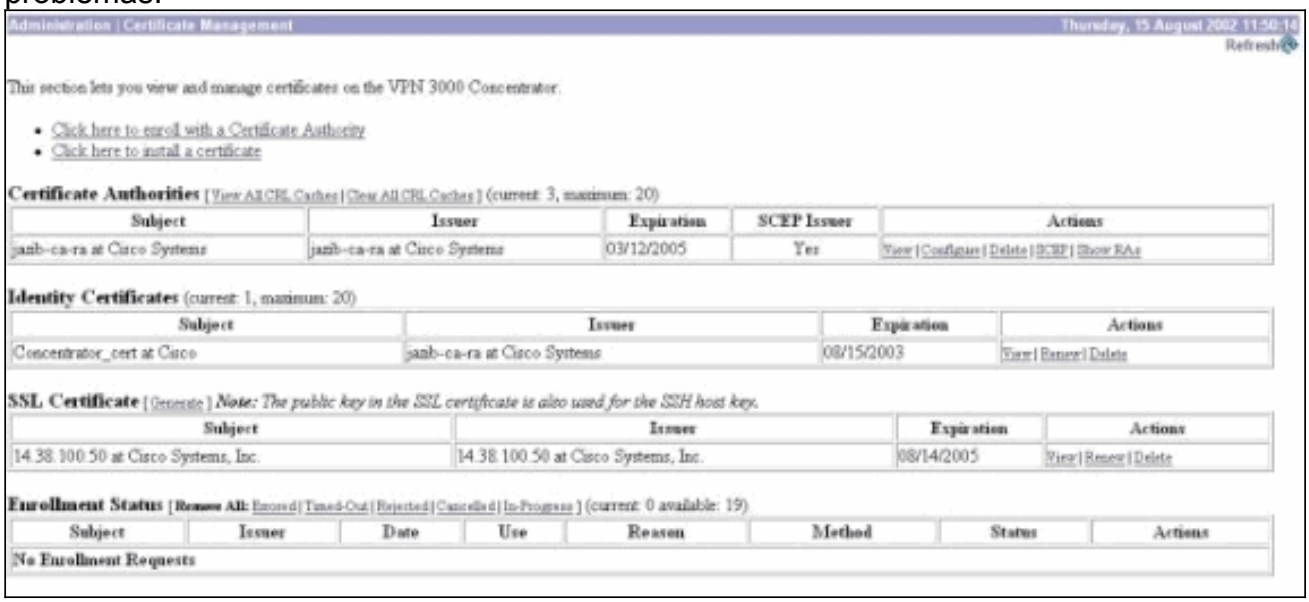
8. Conclua estes passos para preencher o formulário de inscrição:Insira o nome comum do VPN Concentrator a ser usado na infraestrutura de chave pública (PKI) no campo Common Name (CN).Insira seu departamento no campo Unidade organizacional (OU). A OU deve corresponder ao nome do grupo IPsec configurado.Digite sua organização ou empresa no campo Organização (O).Digite sua cidade ou cidade no campo Localidade (L).Insira seu estado ou província no campo Estado/Província (SP).Digite seu país no campo País (C).Insira o Nome de domínio totalmente qualificado (FQDN) para o VPN Concentrator a ser usado no PKI no campo Nome de domínio totalmente qualificado (FQDN).Insira o endereço de e-mail do VPN Concentrator a ser usado no PKI no campo Nome alternativo do assunto (endereço de e-mail).Insira a senha do desafio para a solicitação de certificado no campo Challenge Password (Senha do desafio).Insira novamente a senha do desafio no campo Verificar senha do desafio.Selecione o tamanho da chave para o par de chaves RSA gerado na lista suspensa Tamanho da chave.



9. Selecione **Inscrever** e exiba o status do SCEP no estado de pesquisa.
10. Vá para o servidor de AC para aprovar o certificado de identidade. Depois de aprovado no servidor CA, o status do SCEP deve ser
    Instalado.



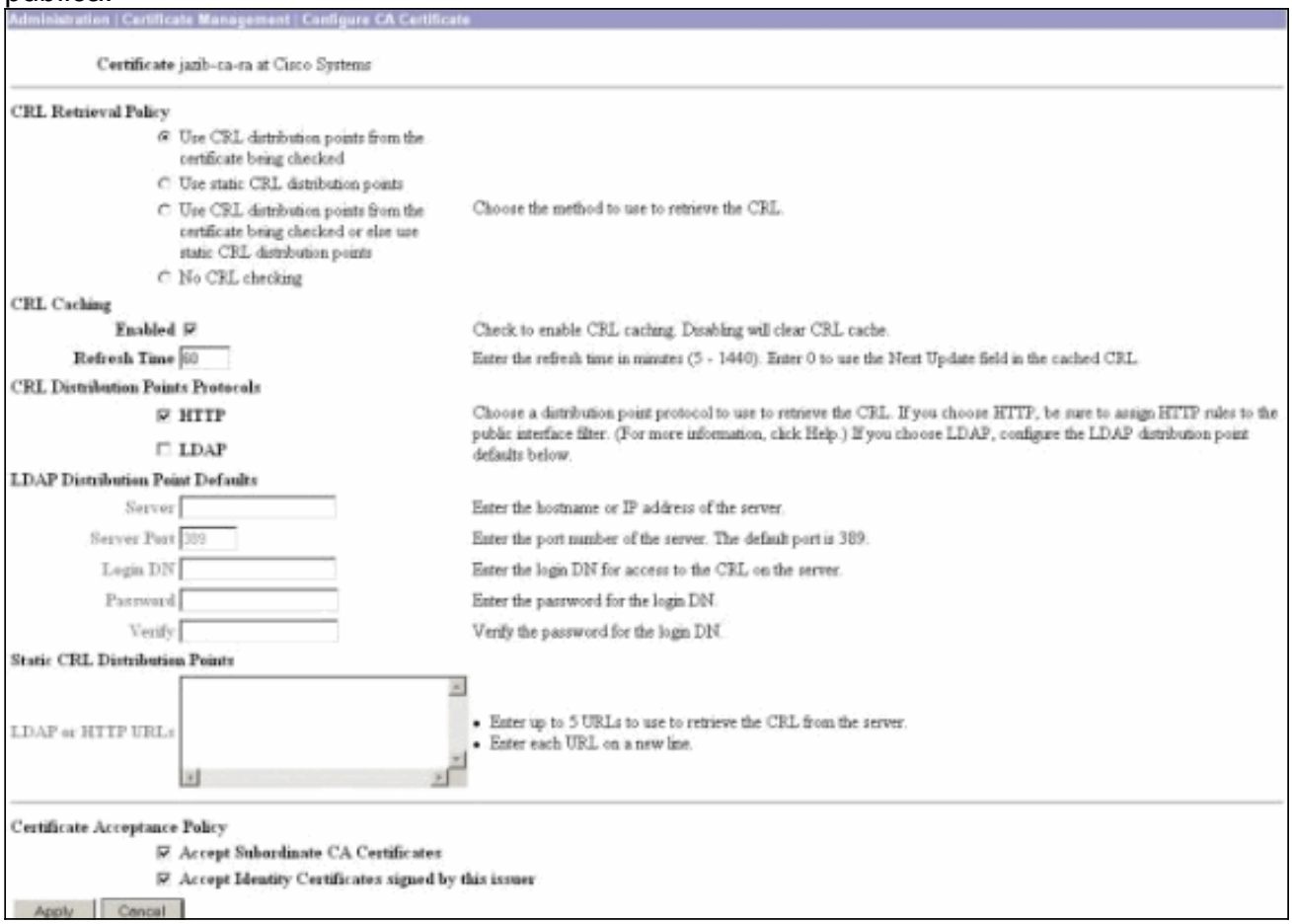
11. Em Gerenciamento de Certificados, você deve ver seu Certificado de Identidade.Caso contrário, verifique os registros no servidor CA para obter mais soluções de problemas.



12. Selecione **Exibir** no certificado recebido para ver se o certificado tem um Ponto de Distribuição de CRL (CDP).O CDP lista todos os pontos de distribuição de CRL do emissor deste certificado. Se você tiver o CDP em seu certificado e usar um nome DNS para enviar uma consulta ao servidor de CA, certifique-se de ter servidores DNS definidos em seu VPN Concentrator para resolver o nome do host com um endereço IP. Nesse caso, o nome de host do exemplo de servidor CA é jazib-pc que é resolvido para um endereço IP de 172.18.124.96 no servidor
    DNS.

13. Clique em **Configurar** no certificado CA para ativar a verificação de CRL nos certificados recebidos.Se você tiver o CDP no certificado recebido e quiser usá-lo, selecione **Usar pontos de distribuição CRL do certificado que está sendo verificado**.Como o sistema precisa recuperar e examinar a CRL de um ponto de distribuição de rede, habilitar a verificação de CRL pode retardar os tempos de resposta do sistema. Além disso, se a rede estiver lenta ou congestionada, a verificação de CRL poderá falhar. Habilite o cache de CRL para atenuar esses possíveis problemas. Isso armazena as CRLs recuperadas na memória volátil local e, portanto, permite que o VPN Concentrator verifique o status de revogação dos certificados mais rapidamente.Com o cache de CRL ativado, o VPN Concentrator primeiro verifica se a CRL necessária existe na cache e verifica o número de série do certificado em relação à lista de números de série na CRL quando precisa verificar o status de revogação de um certificado. O certificado é considerado revogado se seu número de série for encontrado. O VPN Concentrator recupera uma CRL de um servidor externo quando ele não encontra a CRL necessária no cache, quando o período de validade da CRL armazenada em cache expirou ou quando o tempo de atualização configurado expirou. Quando o VPN Concentrator recebe uma nova CRL de um servidor externo, ele atualiza o cache com a nova CRL. O cache pode conter até 64 CRLs.**Observação:** o cache de CRL existe na memória. Portanto, a reinicialização do VPN Concentrator limpa o cache de CRL. O VPN Concentrator preenche novamente o cache de CRL com CRLs atualizadas à medida que processa novas solicitações de autenticação de peer.Se você selecionar **Usar pontos de distribuição de CRL estáticos**, poderá usar até cinco pontos de distribuição de CRL estáticos, conforme especificado nesta janela. Se escolher esta opção, você deve digitar pelo menos um URL.Você também pode selecionar **Usar pontos de distribuição de CRL do certificado que está sendo marcado** ou selecionar **Usar pontos de distribuição de CRL estáticos**. Se o VPN Concentrator não puder encontrar cinco pontos de distribuição CRL no certificado, ele adicionará pontos de distribuição de CRL estáticos, até um limite de cinco. Se você escolher essa opção, ative pelo menos um Protocolo de Ponto de Distribuição CRL. Você também deve inserir pelo menos um (e no máximo cinco) pontos de distribuição de CRL estático.Selecione **No CRL Checking** se quiser desativar a verificação de CRL.Em Cache de CRL, selecione a caixa **Habilitado** para permitir que o VPN Concentrator armazene em cache as CRLs recuperadas. O padrão não é ativar o cache de CRL. Quando você desabilita o cache de CRL (desmarque a caixa), o cache de CRL é limpo.Se você configurou uma política de recuperação de CRL que usa pontos de distribuição de CRL do certificado que está sendo verificado, escolha um protocolo de ponto de distribuição a ser usado para recuperar a CRL. Escolha **HTTP** neste caso para recuperar a CRL. Atribua regras HTTP ao filtro de interface pública se o servidor

CA estiver em direção à interface pública.



Monitoramento

Selecione **Administration > Certificate Management** e clique em **View All CRL caches** para ver se o VPN Concentrator armazenou em cache qualquer CRL do servidor CA.

Verificar

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

Logs do concentrador

Ative esses eventos no VPN Concentrator para garantir que a verificação de CRL funcione.

1. Selecione **Configuration > System > Events > Classes** para definir os níveis de registro.
2. Em Nome da classe, selecione IKE, **IKEDBG**, **IPSEC**, **IPSECDBG** ou **CERT**.
3. Clique em **Add** ou **Modify** e escolha **Severity to Log (Gravidade para registro), opção 1-13**.
4. Clique em **Apply** se quiser modificar ou em **Add** se quiser adicionar uma nova entrada.

Registros de concentrador concluídos com sucesso

Se a verificação de CRL for bem-sucedida, essas mensagens serão vistas nos Logs de eventos filtráveis.

```
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)
```

Consulte Logs de Concentrador Bem-sucedidos para obter a saída completa de um log de concentrador bem-sucedido.

Logs com falha

Se a verificação de CRL não for bem-sucedida, essas mensagens serão vistas nos Logs de eventos filtráveis.

```
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.
```

Consulte Registros de Concentradores Revogados para obter a saída completa de um log de concentrador com falha.

Consulte Registros de Clientes Bem-Sucedidos para obter a saída completa de um log de cliente bem-sucedido.

Consulte Registros de Clientes Revogados para obter a saída completa de um log de cliente com falha.

Troubleshoot

Consulte Troubleshooting de Problemas de Conexão no VPN 3000 Concentrator para obter mais informações sobre Troubleshooting.

Informações Relacionadas

- Página de suporte de Cisco VPN 3000 Series Concentrators
- Página de suporte ao Cisco VPN 3000 Client
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems