Configurar e registre um Cisco VPN 3000 Concentrator a um roteador do Cisco IOS como um server de CA

Índice

Introdução

Este documento descreve como configurar um roteador de Cisco IOS® como um server do Certificate Authority (CA). Adicionalmente, ilustra como registrar um Cisco VPN 3000 Concentrator ao roteador do Cisco IOS para obter uma raiz e o certificado ID para a autenticação IPSec.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco 2600 Series Router que executa o Cisco IOS Software Release 12.3(4)T3

- Versão 4.1.2 do Concentrador Cisco VPN 3030

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Gerencia e exporte o par de chaves RSA para o servidor certificado

A primeira etapa é gerar o par de chaves RSA que o server de CA do Cisco IOS usa. No roteador (r1), gerencia as chaves RSA como visto aqui:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Note: Você deve usar o mesmo nome para o par de chaves (chave-*etiqueta*) esse você plano para usar-se para o servidor certificado (através do comando **cripto do *rótulo CS do* server do pki** coberto mais tarde).

Exporte o par de chaves gerado

As chaves precisam então de ser exportadas para o RAM não-volátil (NVRAM) ou o TFTP

(baseado em sua configuração). Neste exemplo, o NVRAM é usado. Baseado em sua aplicação, você pôde potencialmente querer usar um servidor TFTP separado para armazenar sua informação do certificado.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

Se você usa um servidor TFTP, você pode re-importação gerada o par de chaves como visto aqui:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable] passphrase
```

Note: Se você não quer a chave ser exportable de seu servidor certificado, importe-o de volta ao servidor certificado depois que foi exportado como um par de chaves NON-exportable. Consequentemente, a chave não pode ser decolada outra vez.

Verifique o par de chaves gerado

Você pode verificar o par de chaves gerado invocando o **comando show crypto key mypubkey rsa**:

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

Permita o Server do HTTP no roteador

O server de CA do Cisco IOS apoia somente os registros feitos através do protocolo simple certificate enrollment (SCEP). Consequentemente, a fim fazer este possível, o roteador deve executar o Server do HTTP incorporado do Cisco IOS. Para permiti-lo, use o **comando ip http server**:

```
R1(config)#ip http server
```

Permita e configurar o server de CA no roteador

Siga este procedimento.

1. Émuito importante recordar que o servidor certificado deve usar o mesmo nome que o par de chaves você apenas gerou manualmente. A etiqueta combina a etiqueta gerada do par de chaves:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Depois que você permitiu um servidor certificado, você pode usar os valores padrão preconfigured ou especificar valores através do CLI para a funcionalidade do servidor certificado.
2. **O comando url do base de dados** especifica o lugar onde todas as entradas no base de dados para o server de CA são escritas para fora.Se este comando não é especificado, todas as entradas no base de dados estão escritas para piscar.
   ```
   R1(cs-server)#database url nvram:
   ```

   Note: Se você usa um servidor TFTP, a URL precisa de ser **tftp:// <ip_address>/directory**.
3. Configurar o nível do base de dados:
   ```
   R1(cs-server)#database level minimum
   ```

   Este controles de comando que tipo de dados é armazenado no base de dados do certificado de registro.**Mínimo** — Bastante informação é armazenada para continuar somente a emitir Certificados novos sem conflito; o valor padrão.**Nomes** — Além do que a informação dada no nível mínimo, no número de série e no nome do sujeito de cada certificado.**Termine** — Além do que a informação dada nos níveis mínimos e dos nomes, cada certificado emitido é redigido ao base de dados.**Note**: A palavra-chave **completa** produz uma grande quantidade de informação. Se é emitida, você igualmente precisa de especificar um servidor TFTP externo em que para armazenar os dados através do **comando url do base de dados**.
4. Configurar o nome de emissor de CA à DN-corda especificada. Neste exemplo, o CN (Common Name) de cisco1.cisco.com, L (localidade) do RTP, e o C (país) dos E.U. são usados:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Especifique a vida, nos dias, de um certificado de CA ou de um certificado.Os valores válidos variam de *1 dia a 1825 dias*. A vida do certificado de CA do padrão é **3 anos** e a vida do certificado do padrão é **1 ano**. A duração máxima de certificado é *1 mês menos* do que a vida do certificado de CA. Por exemplo:
   ```
   R1(cs-server)#lifetime ca-certificate 365
   R1(cs-server)#lifetime certificate 200
   ```

6. Defina a vida, nas horas, do CRL que é usado pelo servidor certificado. O valor máximo da vida é **336 horas** (2 semanas). O valor padrão é **168 horas** (1 semana).
   ```
   R1(cs-server)#lifetime crl 24
   ```

7. Defina um ponto de distribuição da Lista de revogação de certificado (CDP) a ser usado nos Certificados que são emitidos pelo servidor certificado. A URL deve ser um URL DO HTTP.Por exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT de nosso server é 172.18.108.26.
   ```
   R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
   ```

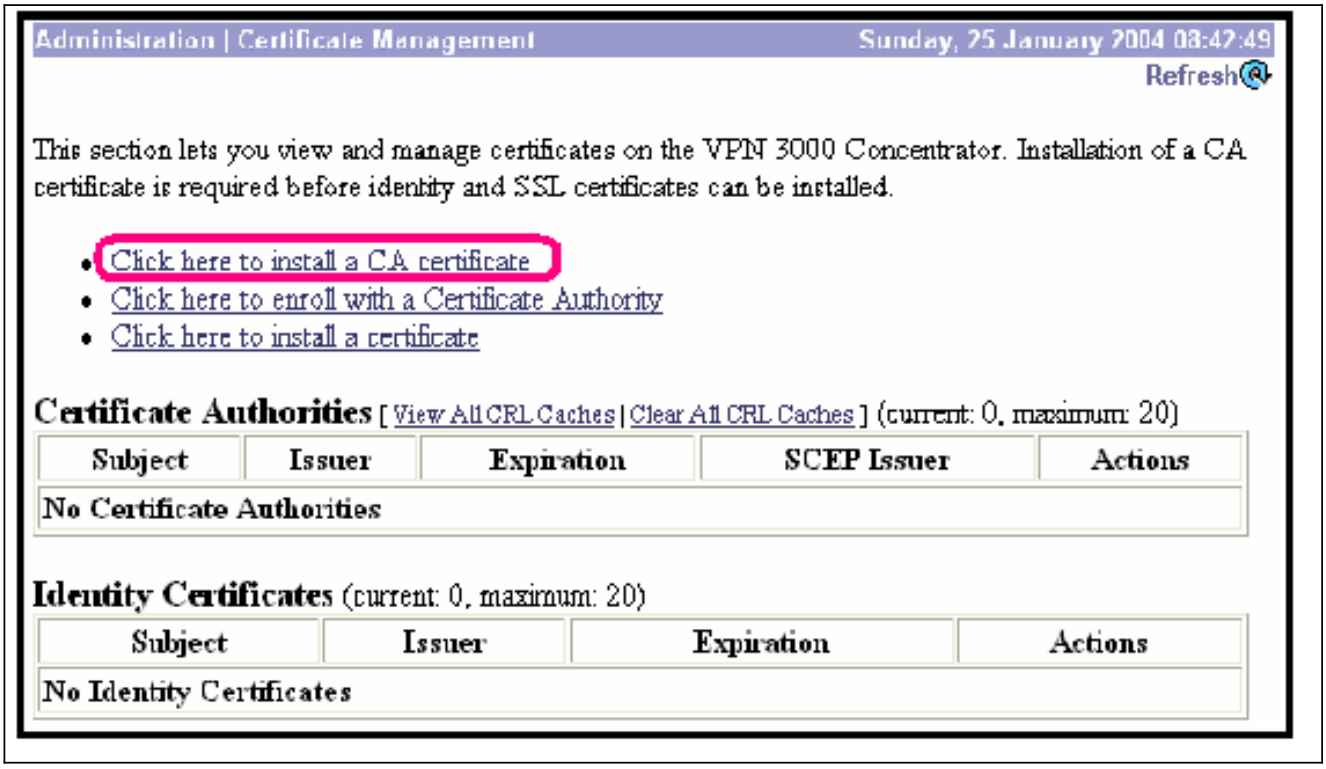
8. Permita o server de CA emitindo o **comando no shutdown**.
   ```
   R1(cs-server)#no shutdown
   ```

   Note: Emita este comando somente depois que você configurou completamente seu servidor certificado.

Configurar e registre o Cisco VPN 3000 Concentrator

Siga este procedimento.

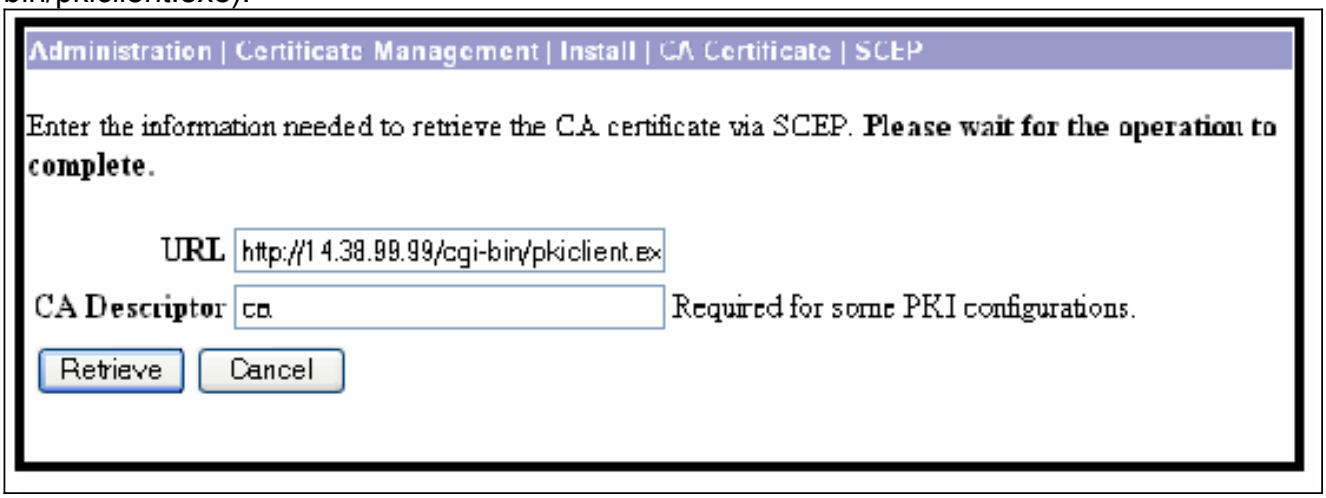
1. Selecionando o **administração > gerenciamento de certificado** e escolha **clicam aqui para instalar um certificado de CA** para recuperar o certificado de raiz do server de CA do Cisco IOS.



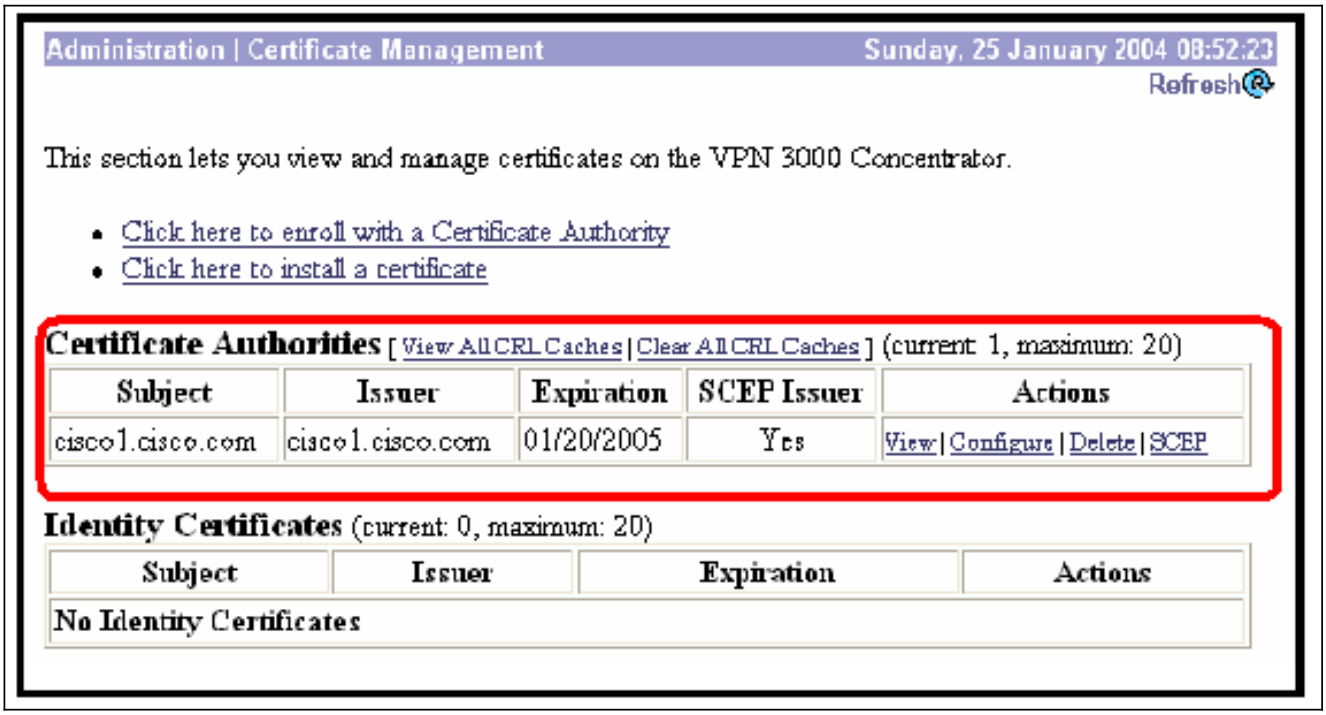
2. Selecione o **SCEP** como o método de

instalação.

3. Incorpore a URL do server de CA do Cisco IOS, um descritor de CA, e o clique **recupera**.**Note**: A URL correta neste exemplo é http://14.38.99.99/cgi-bin/pkiclient.exe (você deve incluir o caminho cheio de /cgi-bin/pkiclient.exe).

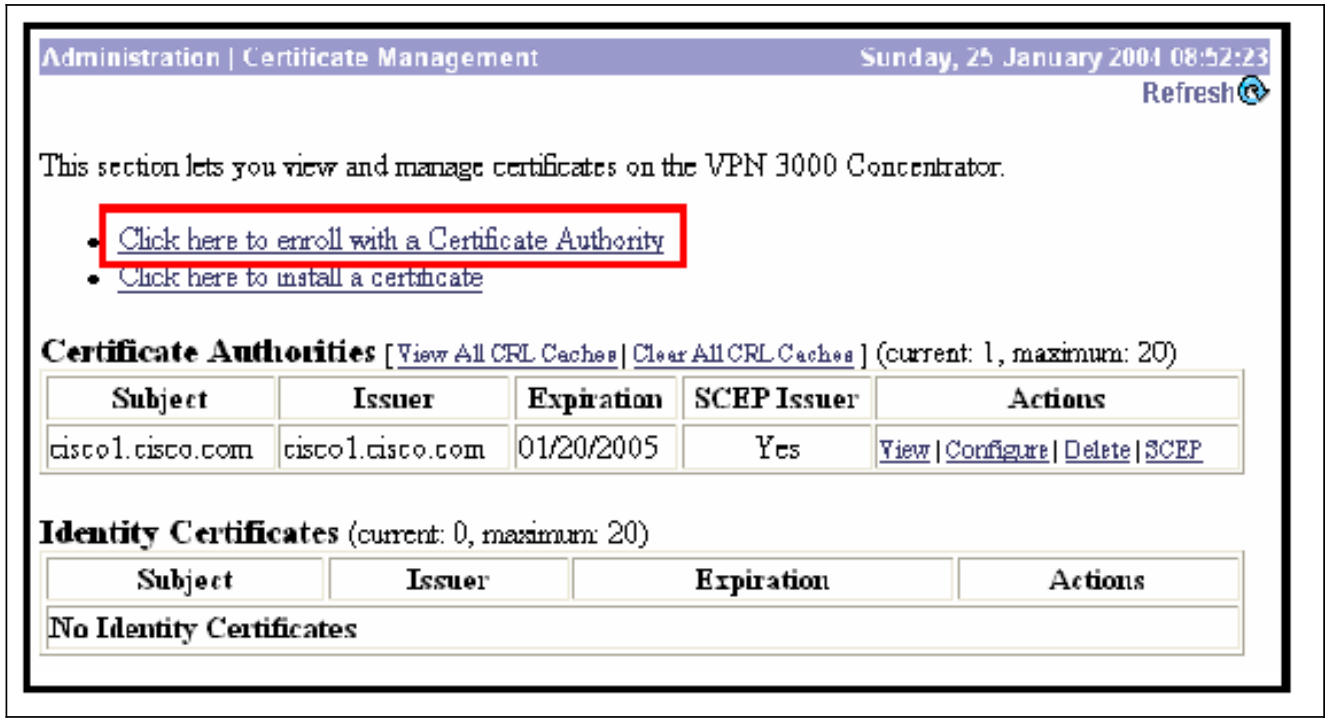


Selecione o **administração > gerenciamento de certificado** para verificar que o certificado de raiz esteve instalado. Esta figura ilustra os detalhes do certificado de raiz.



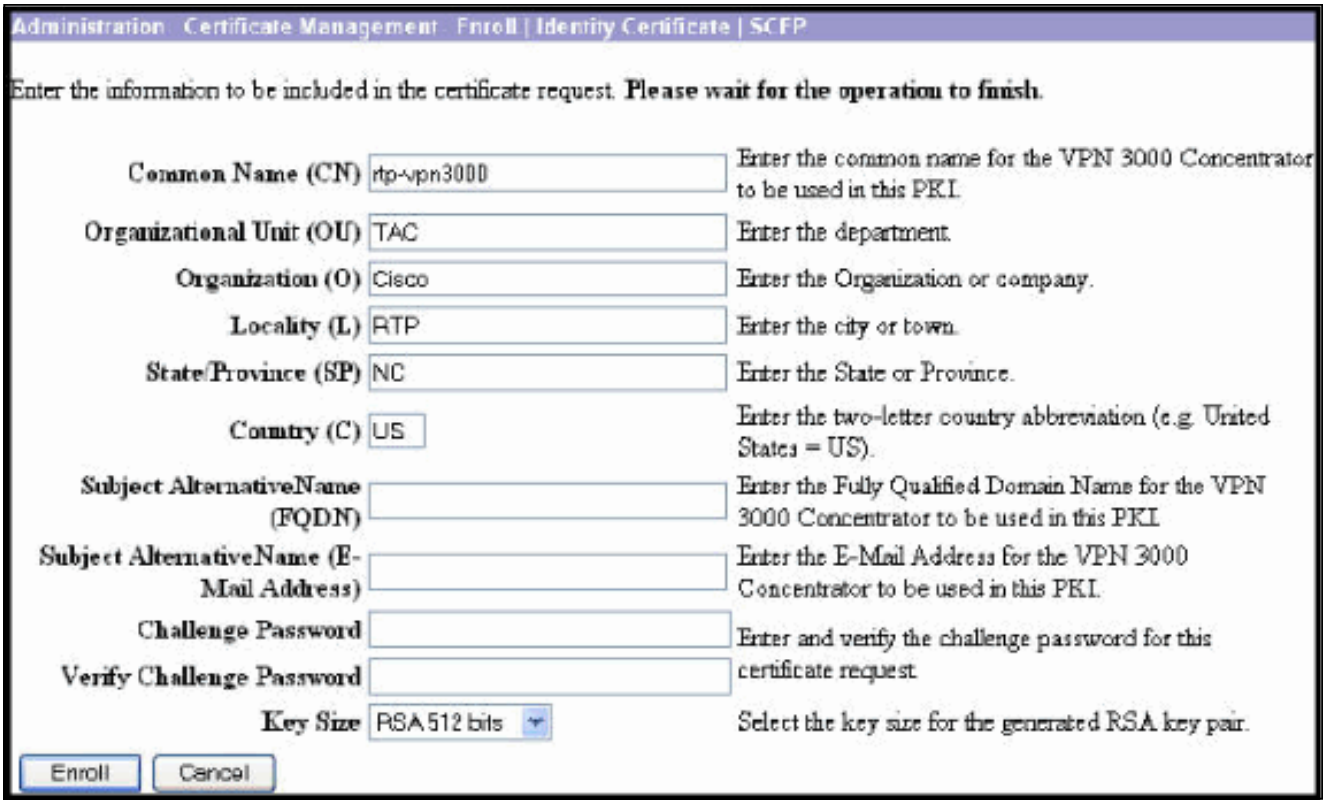
4. Selecione **clicam aqui para registrar-se com um Certificate Authority** para obter o certificado

ID do server de CA do Cisco
IOS.



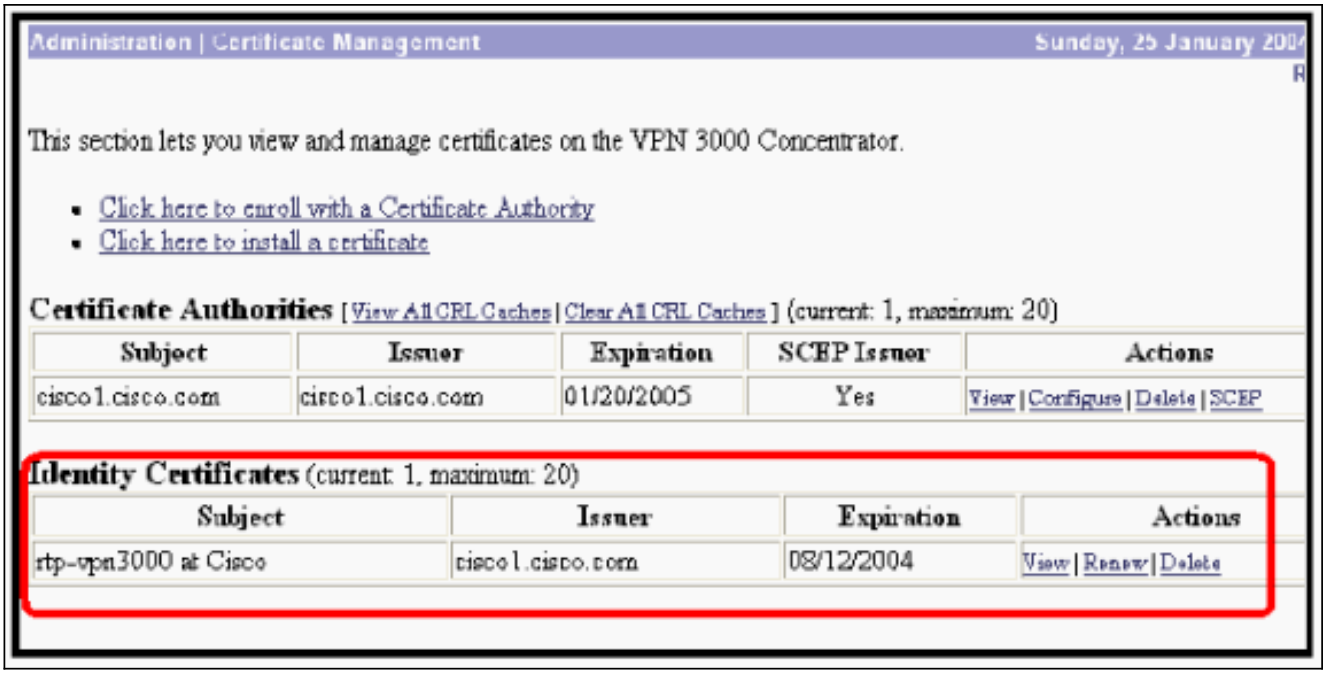
5. Seleto **registre através do SCEP em cisco1.cisco.com** (cisco1.cisco.com é o CN do server de CA do Cisco
IOS).

6. Termine o formulário do registro incorporando toda a informação a ser incluída dentro do pedido do certificado.Após conclusão do formulário, o clique **registra-se** para começar o pedido do registro ao server de
CA.



Depois que você clique se registra, o VPN 3000 concentrator indica “um pedido do certificado esteve
gerado”.

Note: O server de CA do Cisco IOS pode ser configurado para conceder automaticamente os Certificados com a **concessão do** subcommand do server de CA do Cisco IOS **automática**. Este comando é usado para este exemplo. Para considerar os detalhes do ID certificate, selecionam o **administração > gerenciamento de certificado**. O certificado indicado é similar a
este.



Verificar

Veja a verificação a seção gerada do par de chaves para a informação de verificação.

Troubleshooting

Para a informação de Troubleshooting, refira problemas de conexão do Troubleshooting no VPN 3000 concentrator ou Troubleshooting de Segurança IP - compreendendo e usando comandos debug.

Informações Relacionadas

- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems