Configure y aliste un Cisco VPN 3000 Concentrator a un router del Cisco IOS como servidor de CA

Contenido

Introducción

Este documento describe cómo configurar a un router de Cisco IOS® como servidor del Certificate Authority (CA). Además, ilustra cómo alistar un Cisco VPN 3000 Concentrator al router del Cisco IOS para obtener una raíz y el certificado ID para la Autenticación IPSec.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2600 Series Router que funciona con el Cisco IOS Software Release 12.3(4)T3

- Versión 4.1.2 del Concentrador Cisco VPN 3030

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Genere y exporte el par clave RSA para el servidor de certificados

El primer paso es generar el par clave RSA que el servidor de CA del Cisco IOS utiliza. En el router (r1), genere las claves RSA según lo visto aquí:

```
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: Usted debe utilizar el mismo nombre para el par clave (clave-*escritura de la etiqueta*) ese usted plan para utilizar para el servidor de certificados (vía el comando **crypto de la *escritura de la etiqueta del cs del* servidor pki** cubierto más adelante).

Exporte el par clave generado

Las claves entonces necesitan ser exportadas al RAM no volátil (NVRAM) o al TFTP (basado en

su configuración). En este ejemplo, se utiliza el NVRAM. De acuerdo con su implementación, usted puede ser que potencialmente quiera utilizar a un servidor TFTP separado para salvar su información del 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)#
```

Si usted utiliza a un servidor TFTP, usted puede reimportar generado el par clave según lo visto aquí:

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

Note: Si usted no quisiera que la clave fuera exportable de su servidor de certificados, impórtela de nuevo al servidor de certificados después de que se haya exportado como par clave NON-exportable. Por lo tanto, la clave no se puede sacar otra vez.

Verifique el par clave generado

Usted puede verificar el par clave generado invocando el **comando show crypto key mypubkey rsa**:

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

```
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
```

Habilite al servidor HTTP en el router

El servidor de CA del Cisco IOS soporta solamente las inscripciones hechas vía el protocolo simple certificate enrollment (SCEP). Por lo tanto, para hacer este posible, el router debe funcionar con al servidor HTTP incorporado del Cisco IOS. Para habilitarlo, utilice el **comando ip http server**:

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

Habilite y configure el servidor de CA en el router

Siga este procedimiento.

1. Es muy importante recordar que el servidor de certificados debe utilizar el mismo nombre que el par clave usted acaba de generar manualmente. La escritura de la etiqueta hace juego la escritura de la etiqueta generada del par clave:
   ```
   R1(config)#crypto pki server cisco1
   ```

   Después de que usted haya habilitado a un servidor de certificados, usted puede utilizar los valores predeterminados preconfigurados o especificar los valores vía el CLI para las funciones del servidor de certificados.
2. **El comando url de la base de datos** especifica la ubicación en donde todas las entradas de la base de datos para el servidor de CA se ponen en escrito.Si este comando no se especifica, todas las entradas de la base de datos se escriben para contellear.
   ```
   R1(cs-server)#database url nvram:
   ```

   Note: Si usted utiliza a un servidor TFTP, el URL necesita ser **tftp:// <ip_address>/directory**.
3. Configure el nivel de la base de datos:
   ```
   R1(cs-server)#database level minimum
   ```

   Este controles de comandos salvan a qué tipo de datos en la base de datos de la inscripción del certificado.**Mínimo** — Bastante información se salva para continuar solamente publicando los nuevos Certificados sin el conflicto; el valor predeterminado.**Nombres** — Además de la información dada en el nivel mínimo, el número de serie y el asunto de cada certificado.**Completo** — Además de la información dada en los niveles mínimos y de los nombres, cada certificado publicado se escribe a la base de datos.**Note**: La palabra clave **completa** presenta una gran cantidad de información. Si se publica, usted también necesita especificar a un servidor TFTP externo en quien salvar los datos vía el **comando url de la base de datos**.
4. Configure el nombre del emisor de CA a la DN-cadena especificada. En este ejemplo, el CN (Common Name) de cisco1.cisco.com, L (lugar) de RTP, y el C (país) de los E.E.U.U. se utilizan:
   ```
   R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
   ```

5. Especifique el curso de la vida, en los días, de un certificado de CA o de un certificado.Los valores válidos se extienden a partir de *1 día a 1825 días*. El curso de la vida predeterminado del certificado de CA es **3 años** y el curso de la vida predeterminado del certificado es **1 año**. La vida útil máxima del certificado es *1 mes menos* que el curso de la vida del certificado de CA. Por ejemplo:
   ```
   R1(cs-server)#lifetime ca-certificate 365
   ```

```
R1(cs-server)#lifetime certificate 200
```

6. Defina el curso de la vida, en las horas, del CRL que es utilizado por el servidor de certificados. El valor máximo del curso de la vida es **336 horas** (2 semanas). El valor predeterminado es **168 horas** (1 semana).
```
R1(cs-server)#lifetime crl 24
```

7. Defina un punto de distribución de la Lista de Revocación de Certificados (CRL) (CDP) que se utilizará en los Certificados que son publicados por el servidor de certificados. El URL debe ser HTTP URL.Por ejemplo, la dirección IP de nuestro servidor es 172.18.108.26.
```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

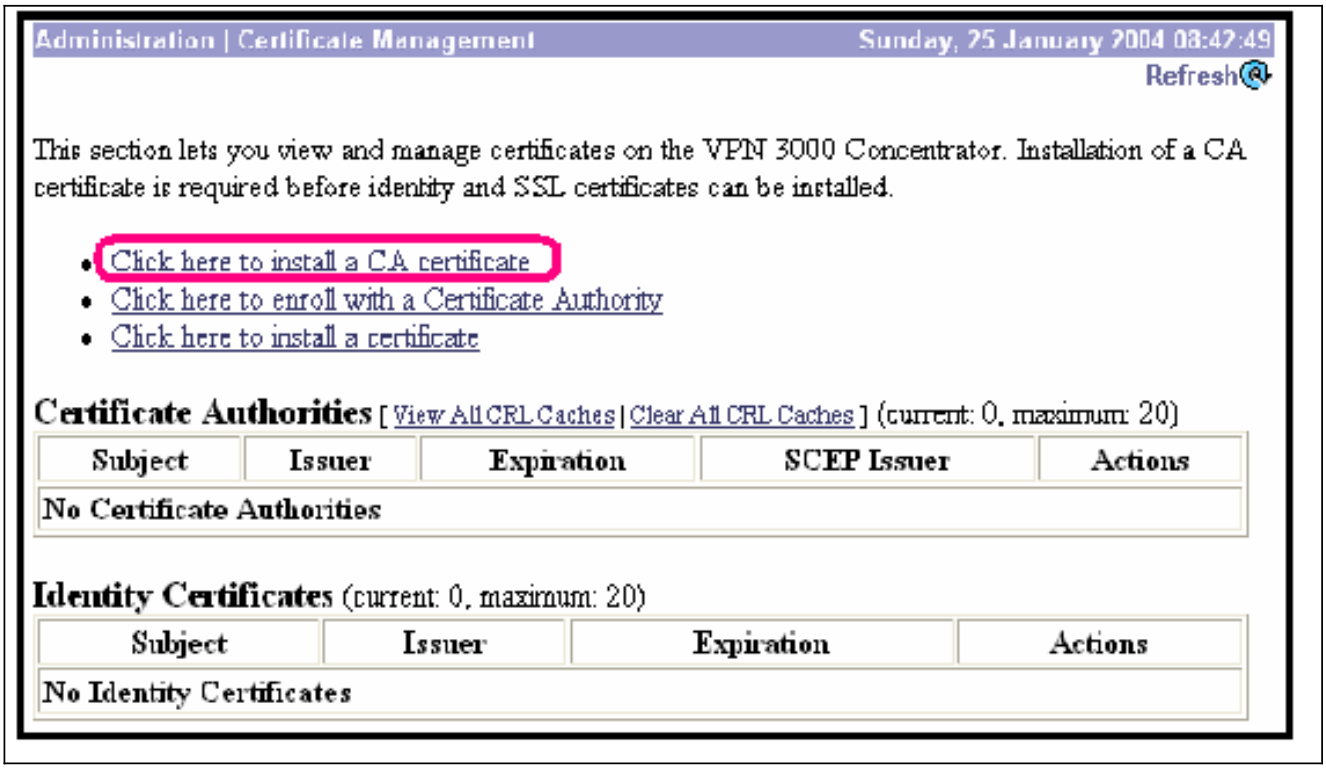
8. Habilite el servidor CA publicando el **comando no shutdown**.
```
R1(cs-server)#no shutdown
```

   Note: Publique este comando solamente después que usted ha configurado totalmente a su servidor de certificados.

Configure y aliste el Cisco VPN 3000 Concentrator

Siga este procedimiento.

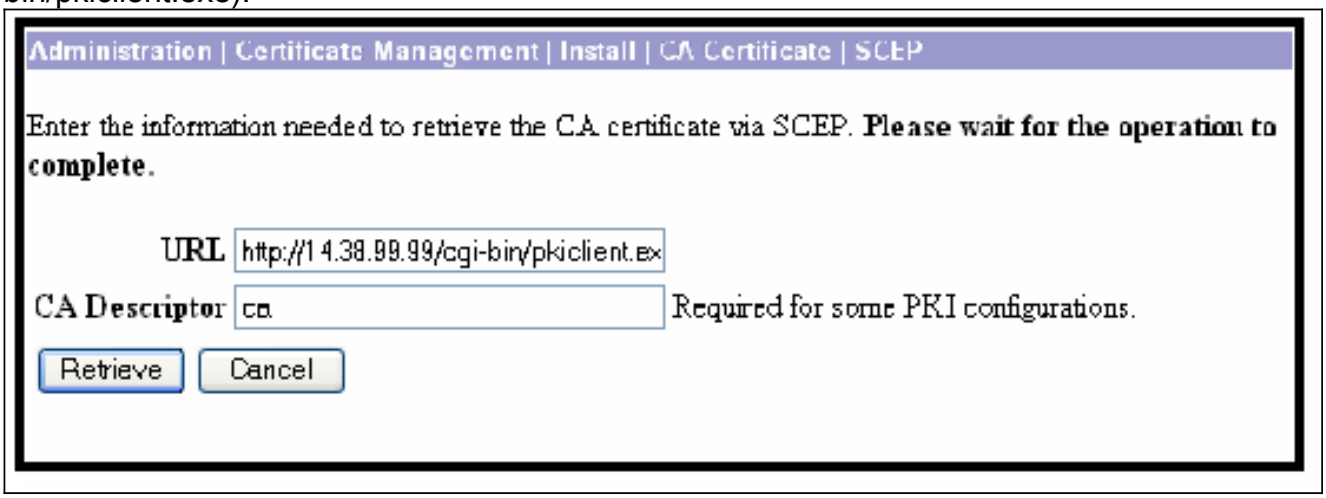
1. Seleccionando el **Administration (Administración) > Certificate Management (Administración de certificados)** y elija **hacen clic aquí para instalar un certificado de CA** para extraer el certificado raíz del servidor de CA del Cisco IOS.



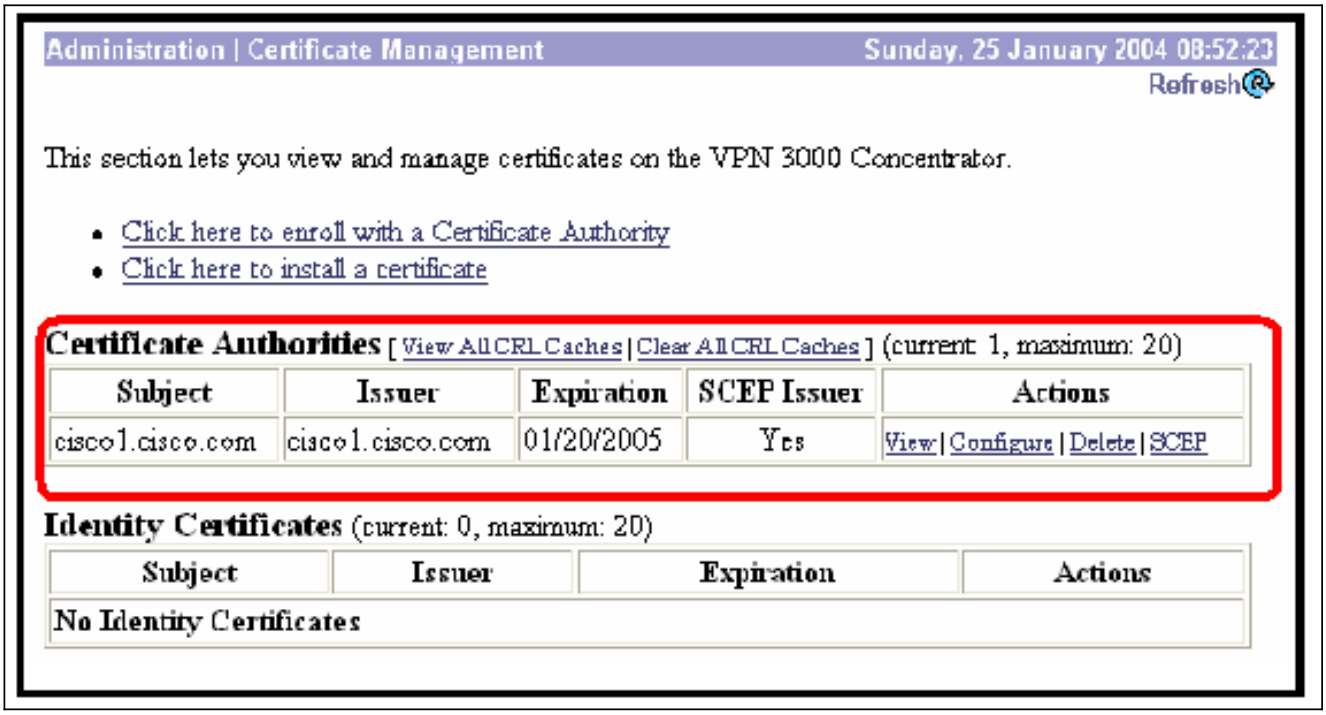
2. Seleccione el **SCEP** como el método de

instalación.

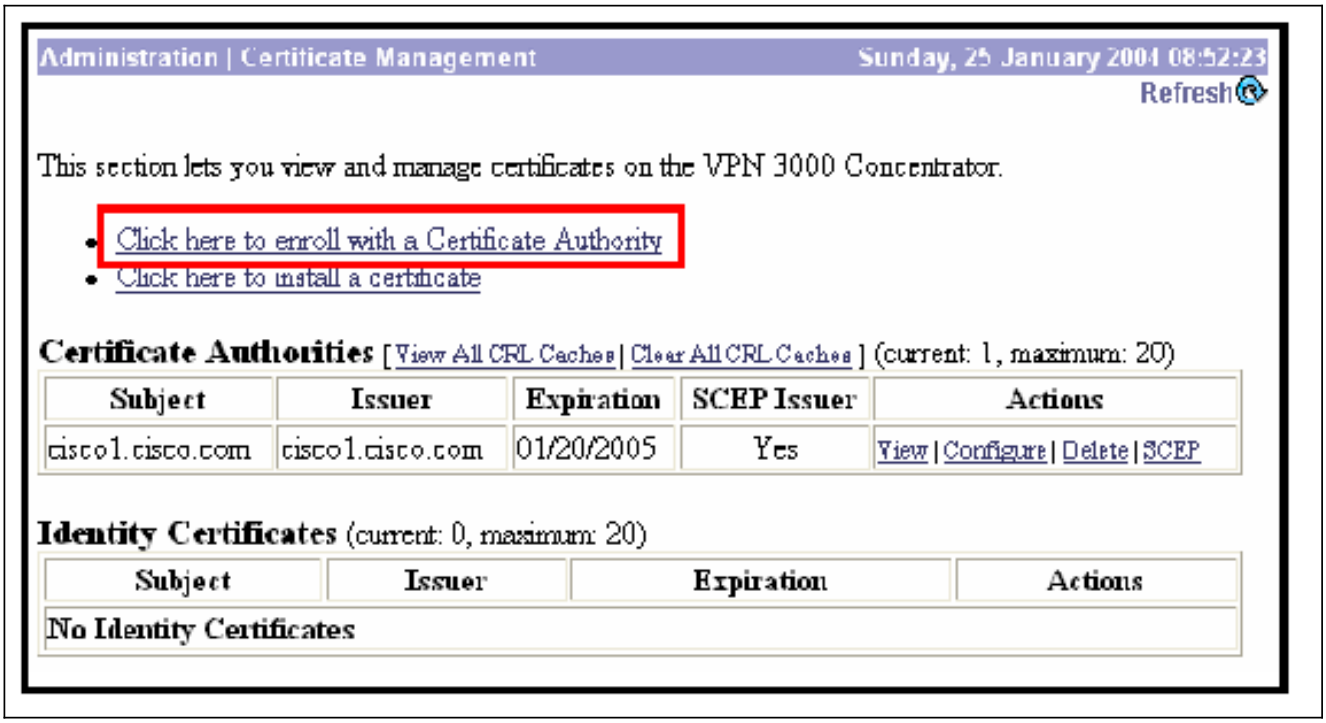
3. Ingrese el URL del servidor del Cisco IOS CA, un descriptor CA, y el tecleo **extrae**.**Note**: El URL correcto en este ejemplo es http://14.38.99.99/cgi-bin/pkiclient.exe (usted debe incluir la ruta completa de /cgi-bin/pkiclient.exe).



Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)** para verificar que el certificado raíz ha estado instalado. Esta figura ilustra los detalles del certificado raíz.

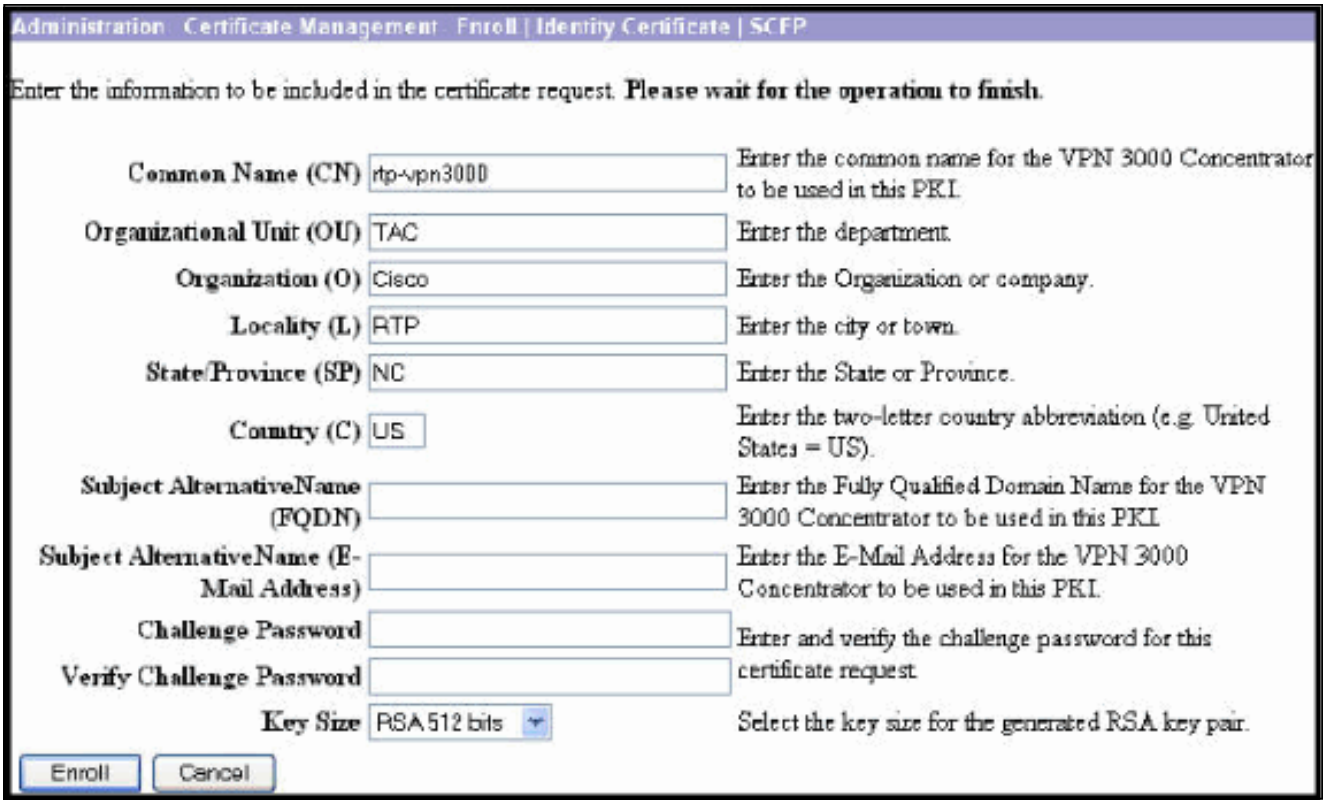


4. Seleccione **hacen clic aquí para alistar con un Certificate Authority** para obtener el certificado ID del servidor de CA del Cisco
IOS.

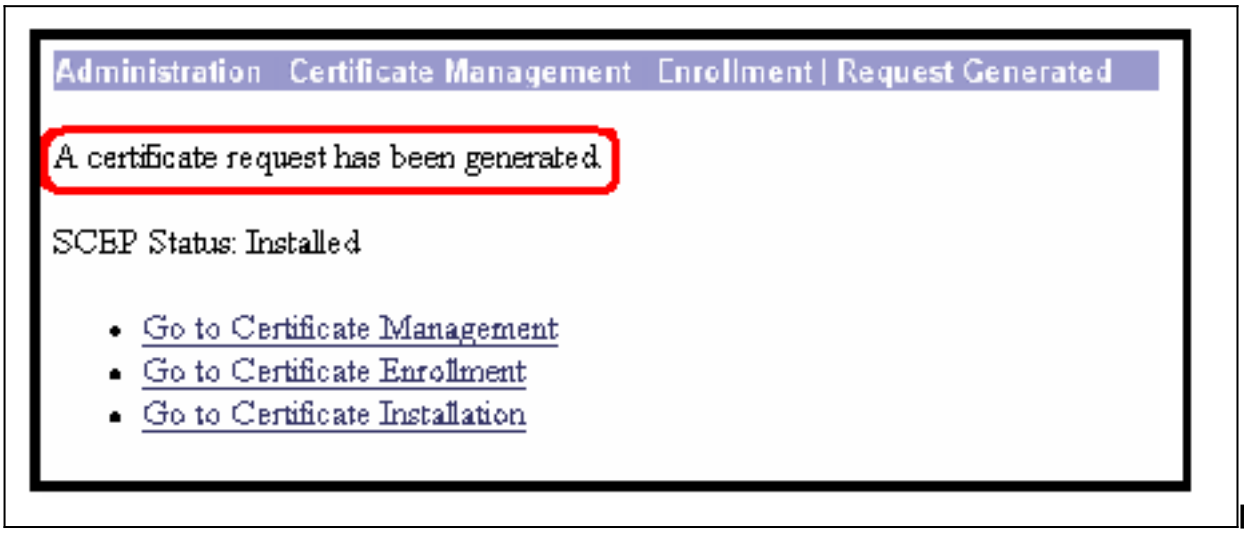


5. Selecto **aliste vía el SCEP en cisco1.cisco.com** (cisco1.cisco.com es el CN del servidor de CA del Cisco
IOS).

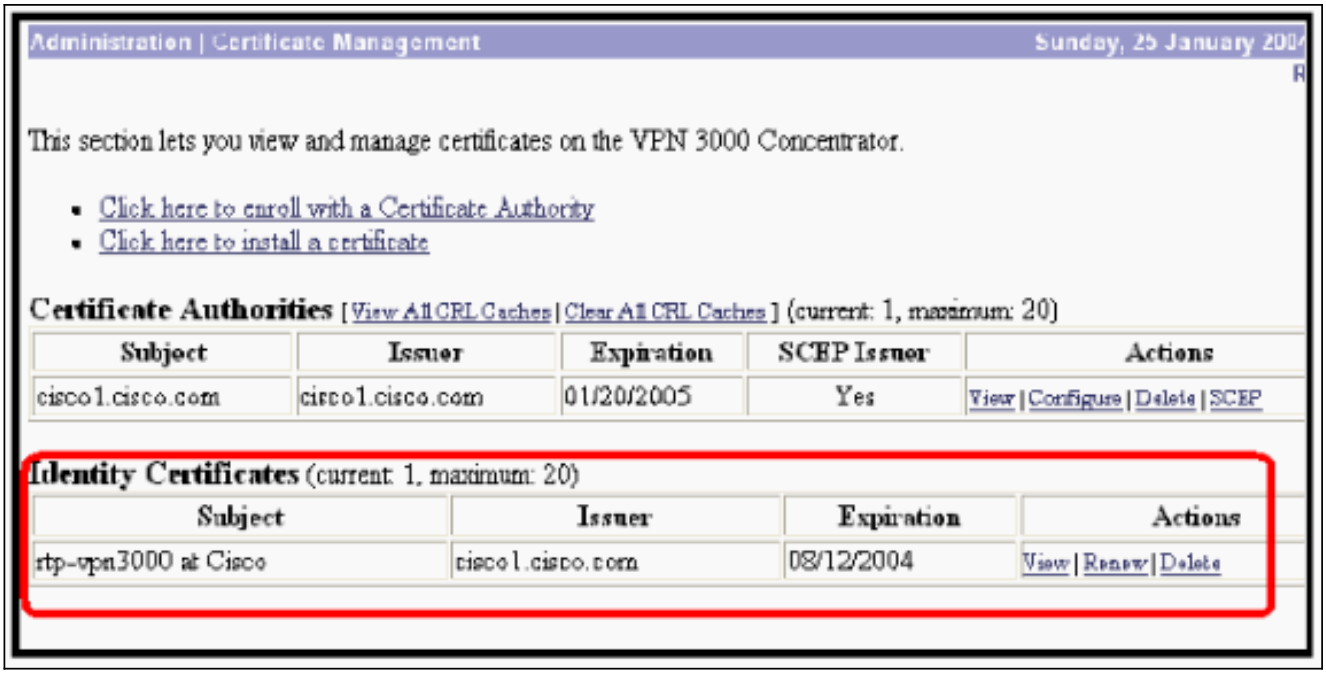
6. Llene el formulario la inscripción ingresando toda la información que se incluirá dentro del pedido de certificado.Tras completar la forma, el tecleo **alista** para comenzar la petición de la inscripción al servidor de
CA.



Después de que usted tecleo aliste, se han generado las visualizaciones concentradoras VPN 3000 “un pedido de certificado”.



Note: El servidor de CA del Cisco IOS se puede configurar para conceder automáticamente los Certificados con la **concesión del** submandato del servidor de CA del Cisco IOS **automática**. Este comando se utiliza para este ejemplo. Para considerar los detalles del ID certifican, seleccionan el **Administration (Administración) > Certificate Management (Administración de certificados)**. El certificado visualizado es similar a esto.



Verificación

Vea el verificar la sección generada del par clave para la información de verificación.

Troubleshooting

Para la información de Troubleshooting, refiera a los Problemas de conexión del troubleshooting en el concentrador VPN 3000 o al Troubleshooting de IP Security - entendiendo y con los comandos debug.

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems