Configurar al cliente VPN 3.x para conseguir un certificado digital

Contenido

Introducción

Este documento muestra cómo configurar el Cisco VPN Client 3.x para conseguir un certificado digital.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en un PC que funcione con al Cliente Cisco VPN 3.x.

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.

Convenciones

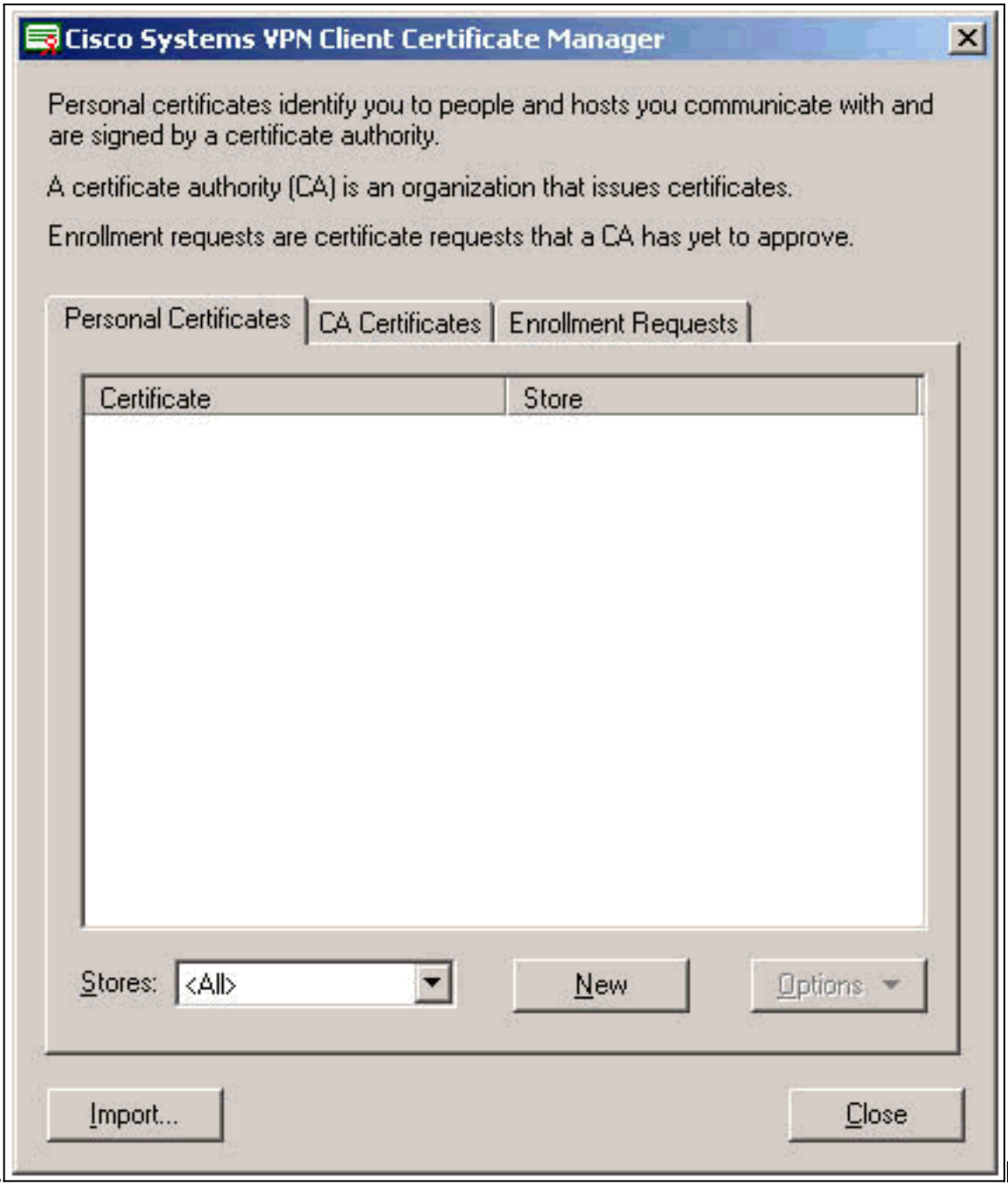
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configure el cliente VPN

Complete estos pasos para configurar al cliente VPN.

1. Seleccione **Start > Programs > cliente VPN > Certificate Manager de Cisco Systems Inc.** para iniciar al Certificate Manager del cliente VPN.

2. Seleccione la lengueta de los certificados personales y haga clic

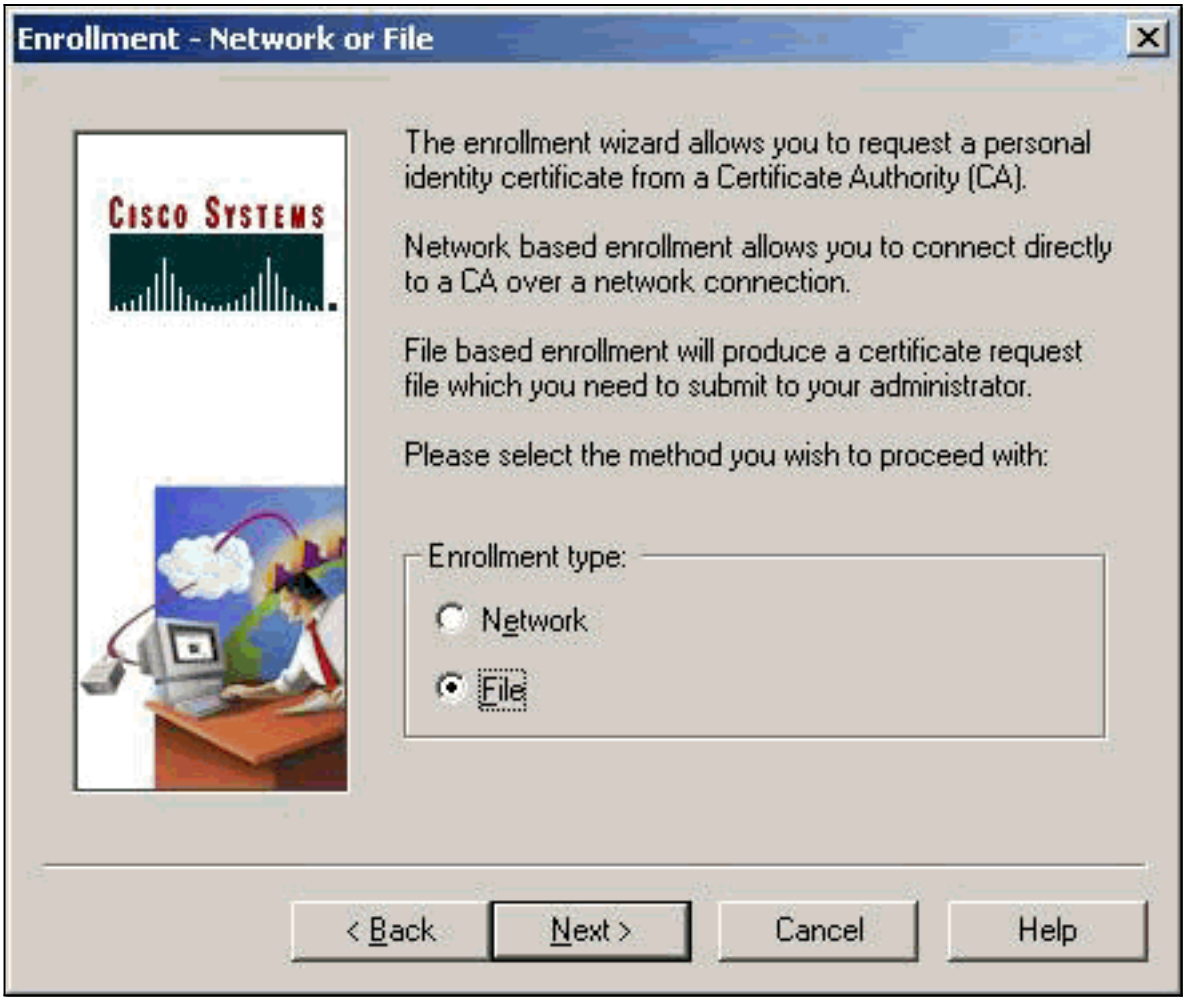


nuevo. **Nota:** Los certificados de la máquina para autenticar a los usuarios para las conexiones VPN no se pueden hacer con el IPSec.

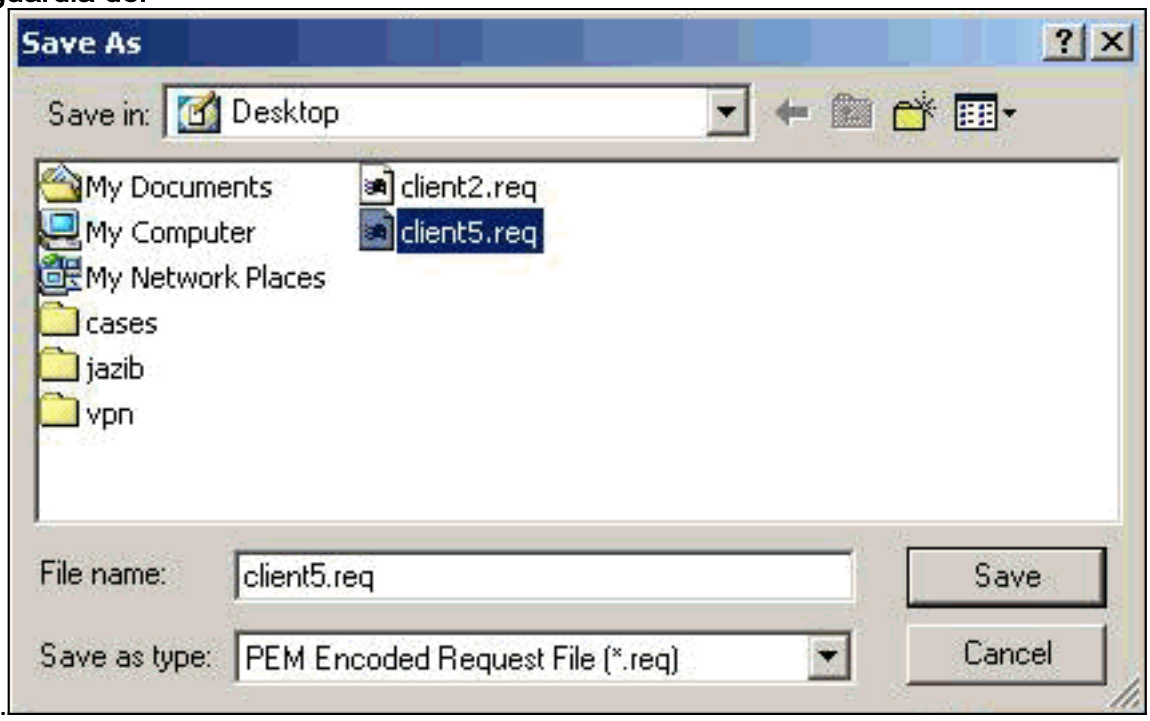
3. Cuando el cliente VPN le indica para una contraseña, especifique una contraseña para proteger el certificado. Cualquier operación que requiera el acceso a la clave privada del certificado requiere la contraseña especificada

continuar.

4. **Archivo** selecto para pedir un certificado usando PKCS-10 el formato en la página de la inscripción. Luego haga clic en Next
(Siguiente).

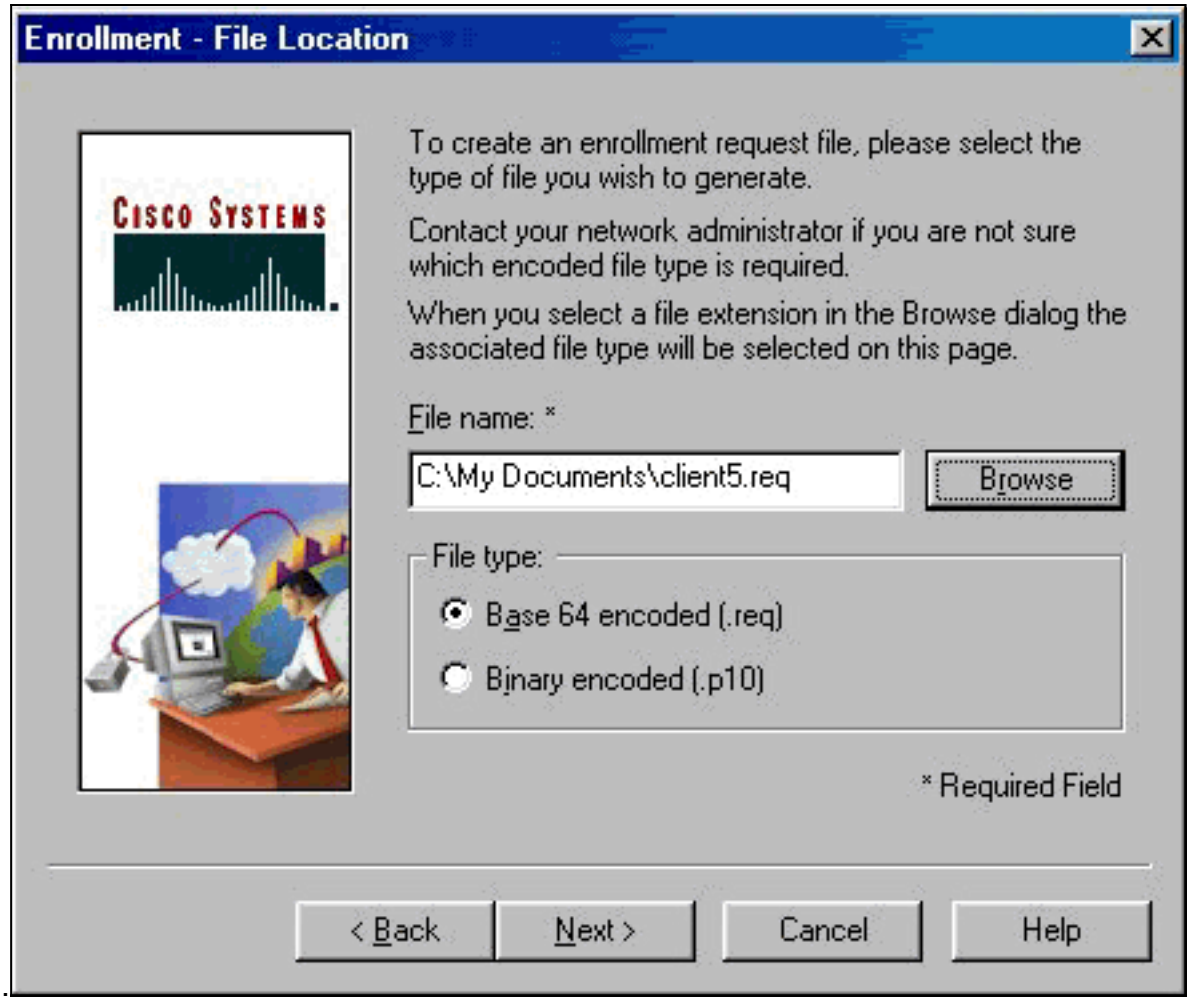


5. El tecleo **hojea**, y especifica un nombre de fichero para el archivo del pedido de certificado. Para el tipo de archivo, el **PEM** selecto **codificó el archivo de la petición (*.req)** y la **salvaguardia del**



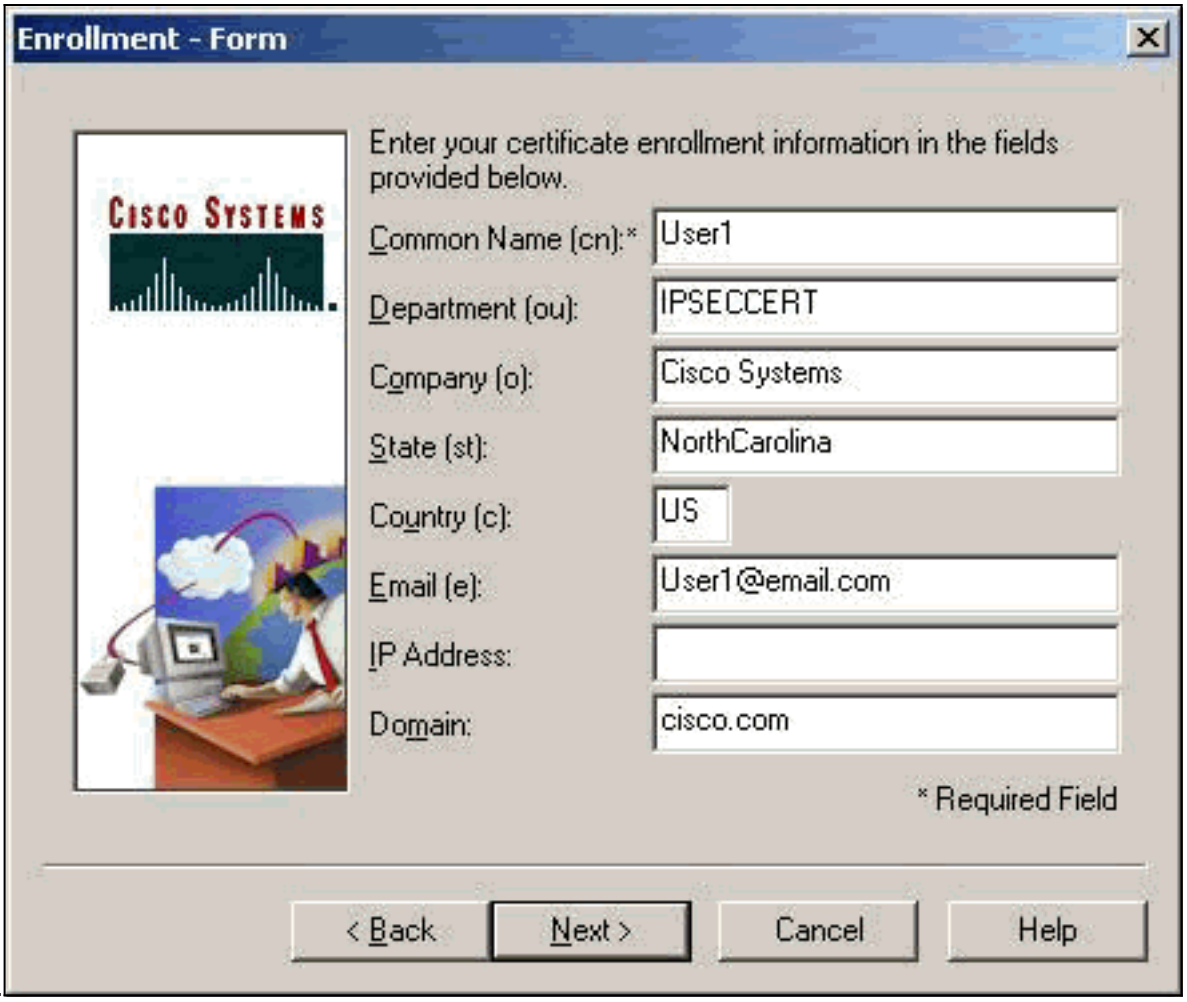
tecleo.

6. Tecleo **después** en la página de la inscripción del cliente



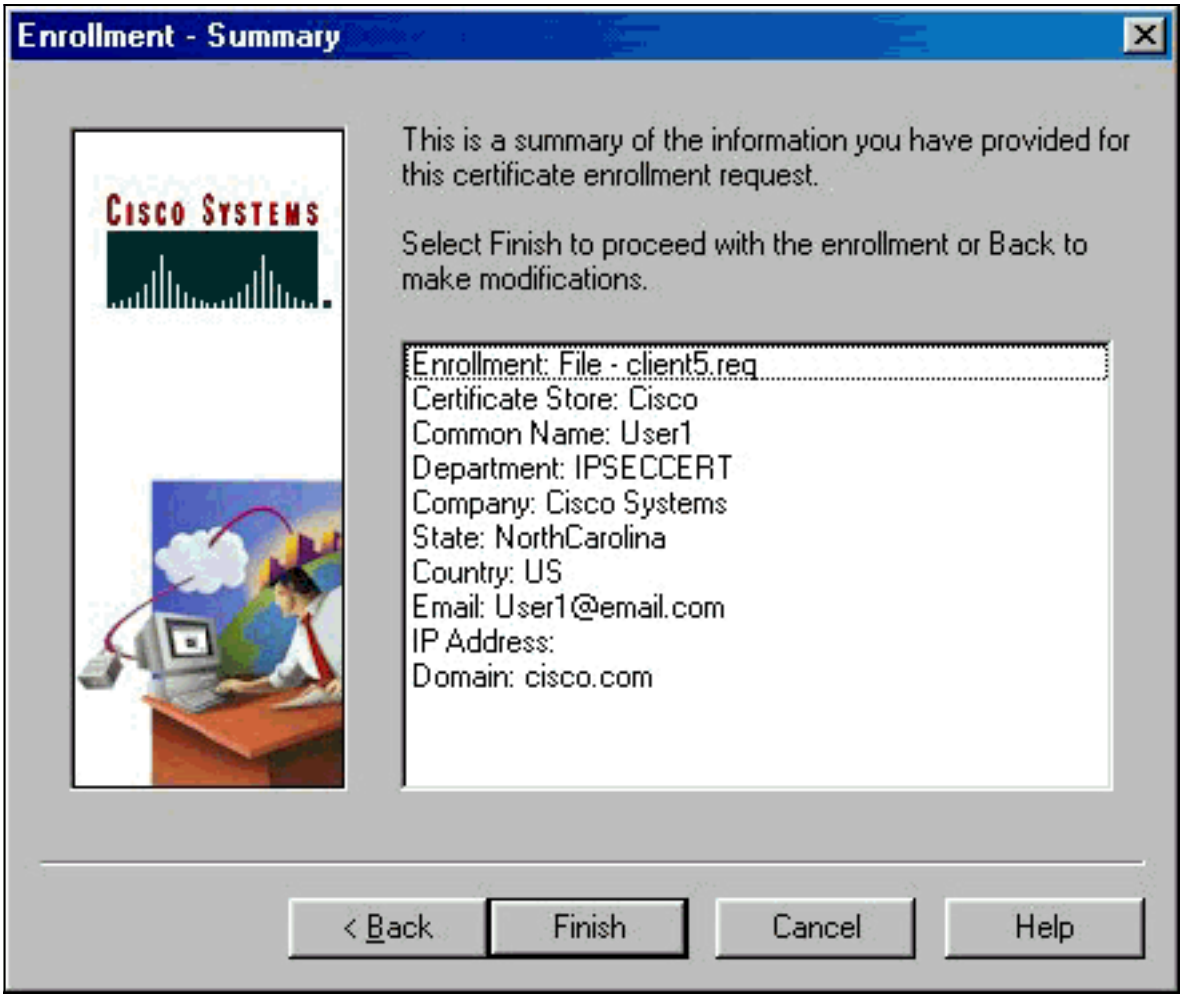
VPN.

7. Complete los campos en el formulario de la inscripción.Este ejemplo muestra los campos:Common Name = user1Departamento = IPSECCERT (esto debe hacer juego la unidad organizativa (OU) y el nombre del grupo en el concentrador VPN 3000.)Compañía = Cisco SystemsEstado = Carolina del NortePaís = los E.E.U.U.Correo electrónico = User1@email.comDirección IP = (opcional; utilizado para especificar la dirección IP en el pedido de certificado)Dominio = cisco.comTecleo **después** cuando le

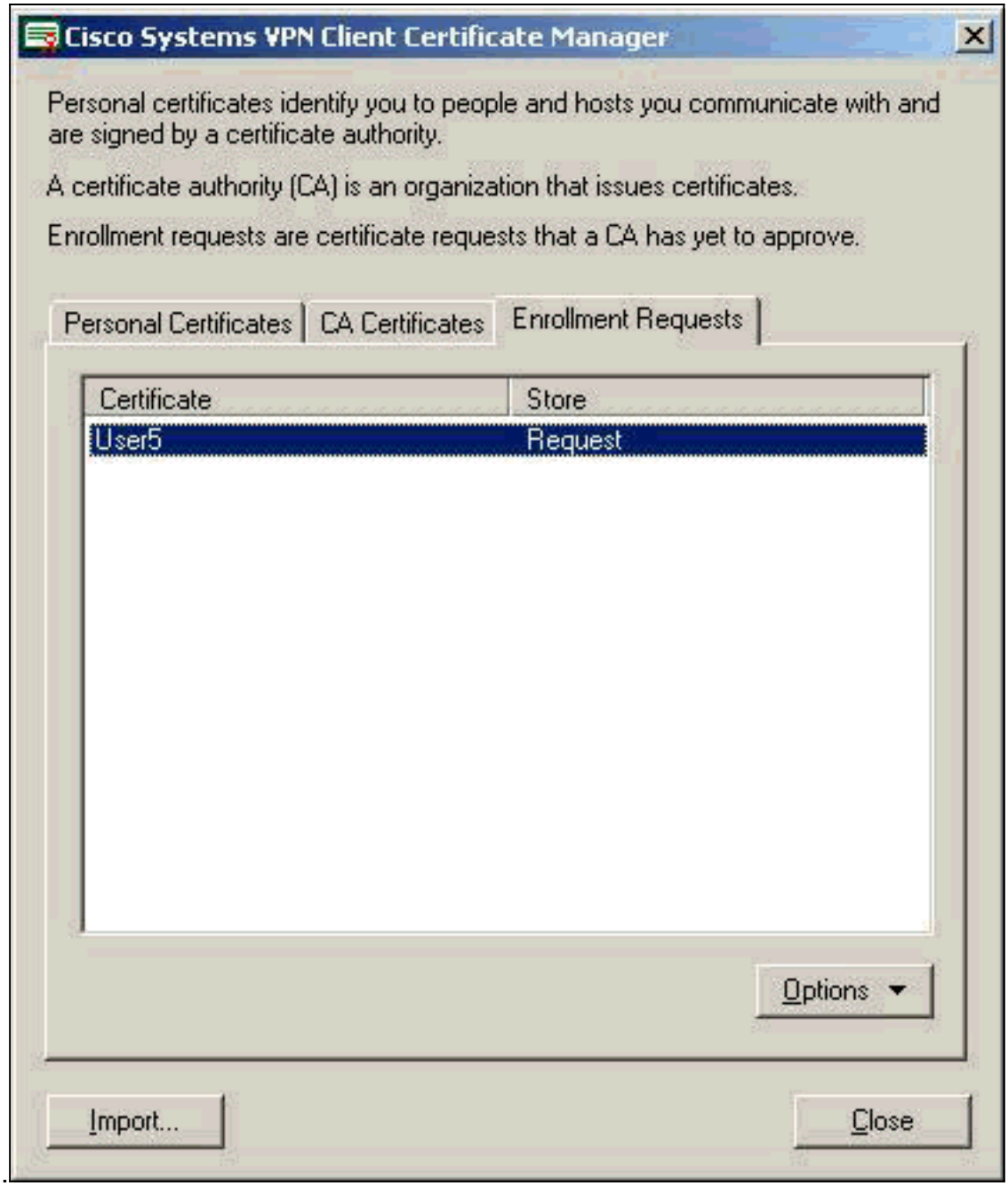


hacen.

8. Clic en Finalizar a proceder con la inscripción.

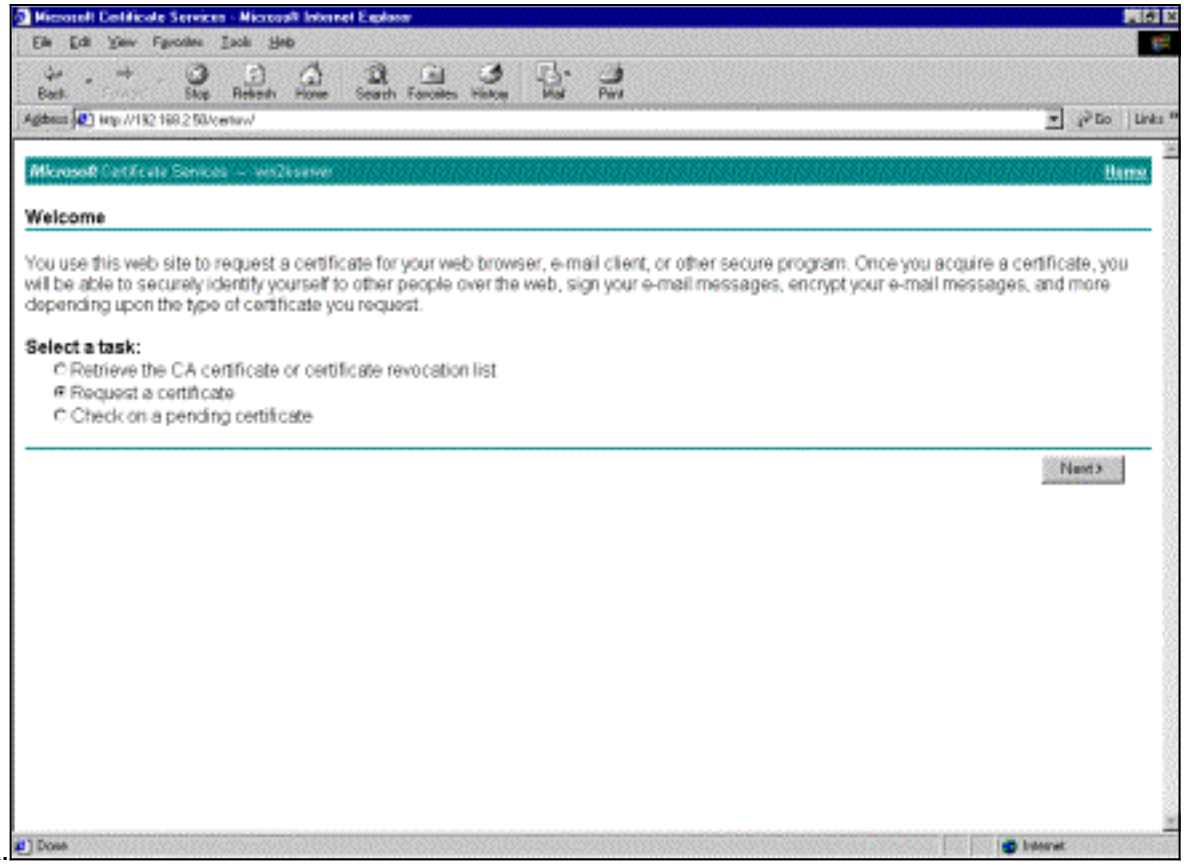


9. Seleccione la lengueta de las peticiones de la inscripción para marcar la petición en el Certificate Manager del cliente



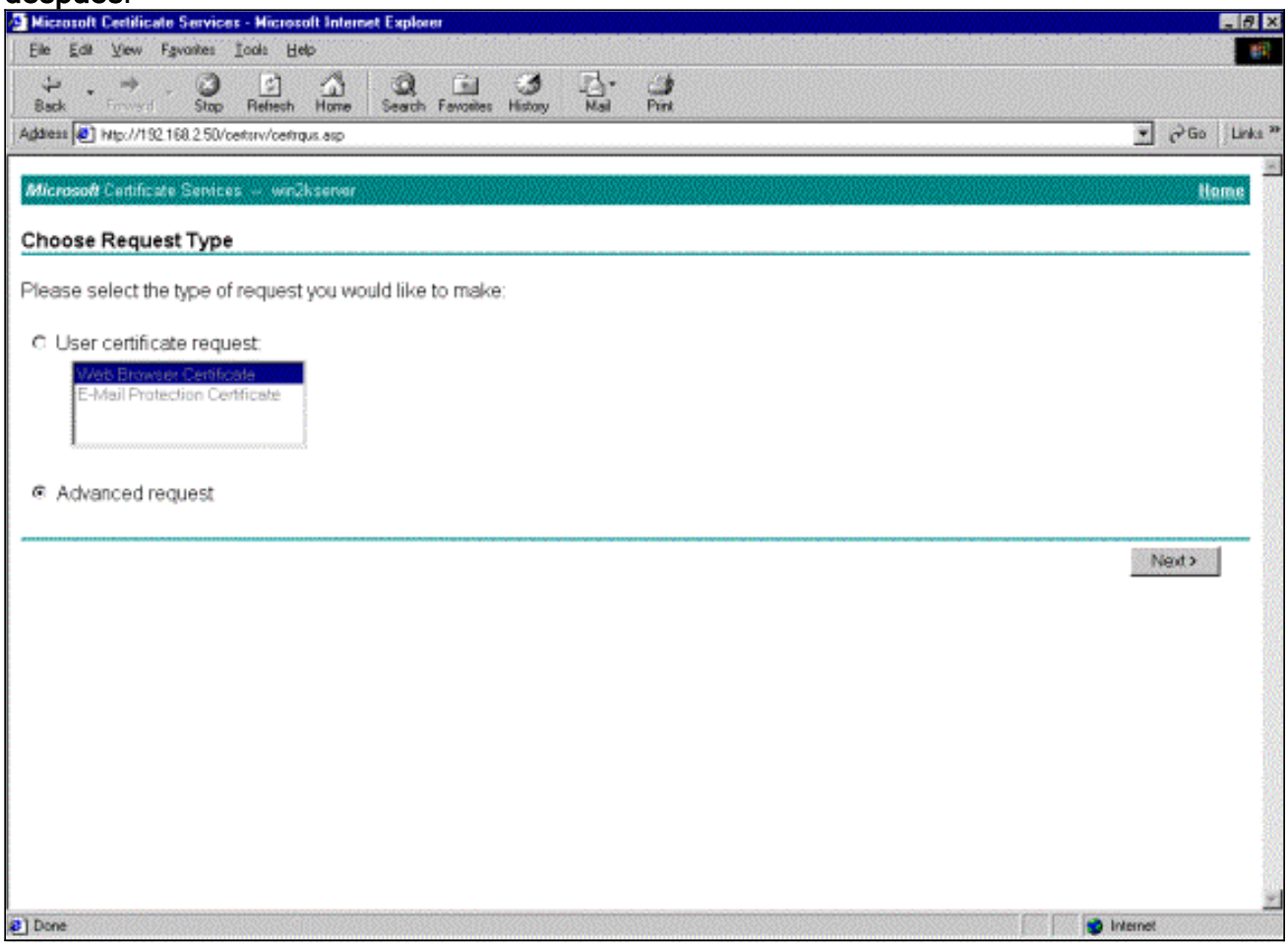
VPN.

10. Traiga para arriba el servidor del Certification Authority (CA) y el cliente VPN interconecta en paralelo para someter la petición.
11. Seleccione la **petición un certificado** y haga clic **después** en el servidor de



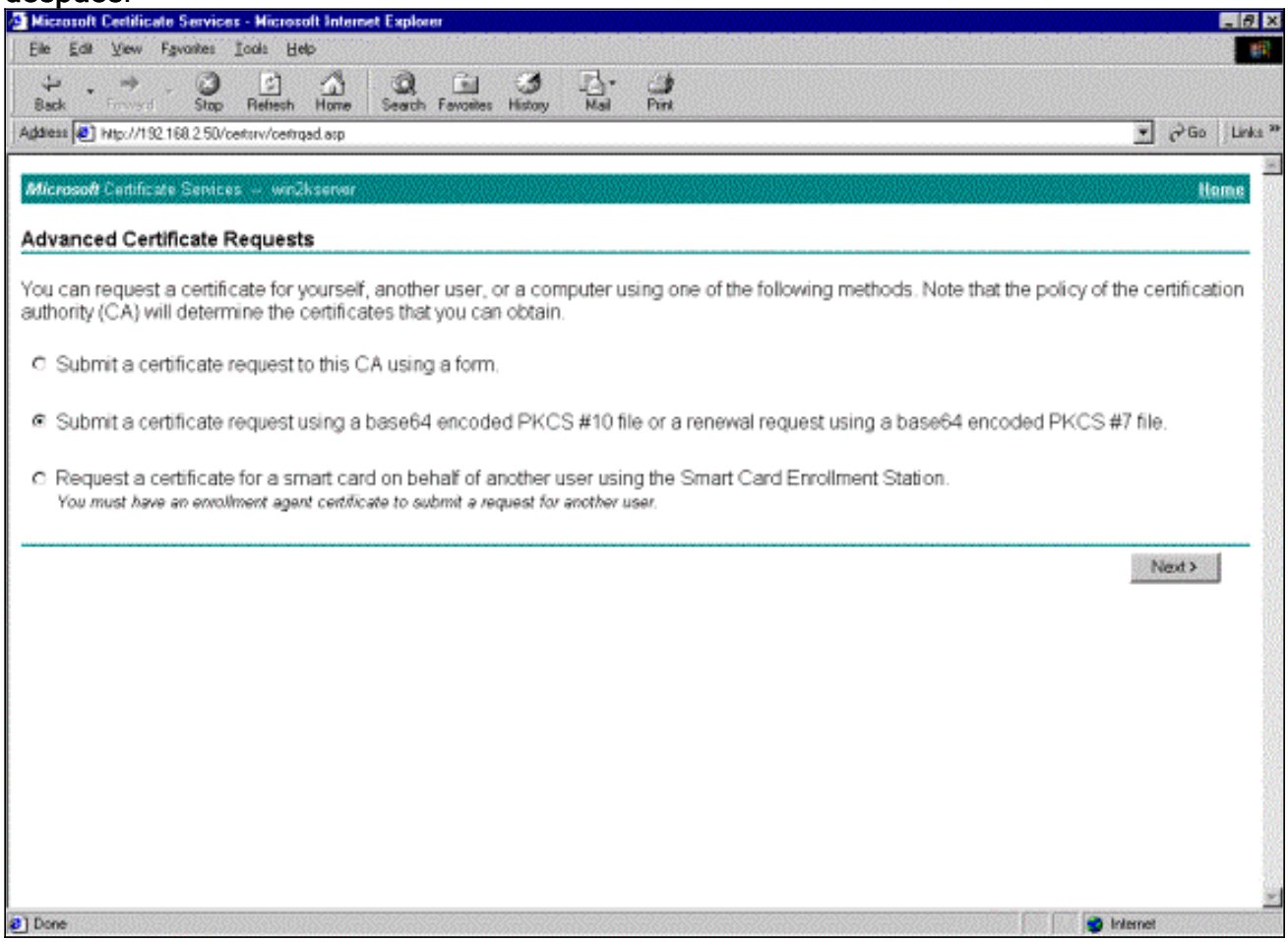
CA.

12. Seleccione el **pedido avanzado** el tipo de petición y haga clic **después**.

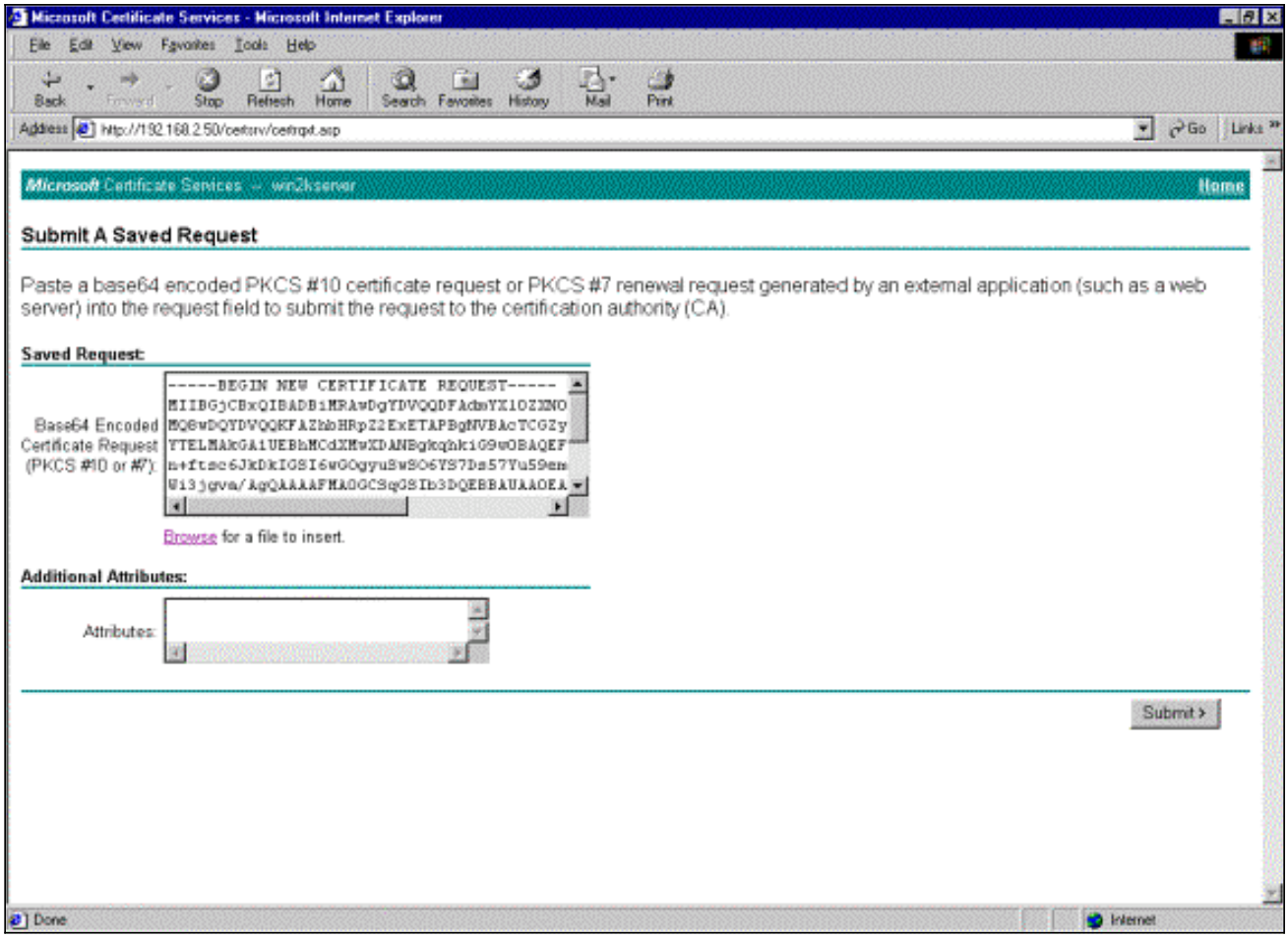


13. Selecto **presente un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64** conforme a los pedidos de certificado avanzados, y después haga clic

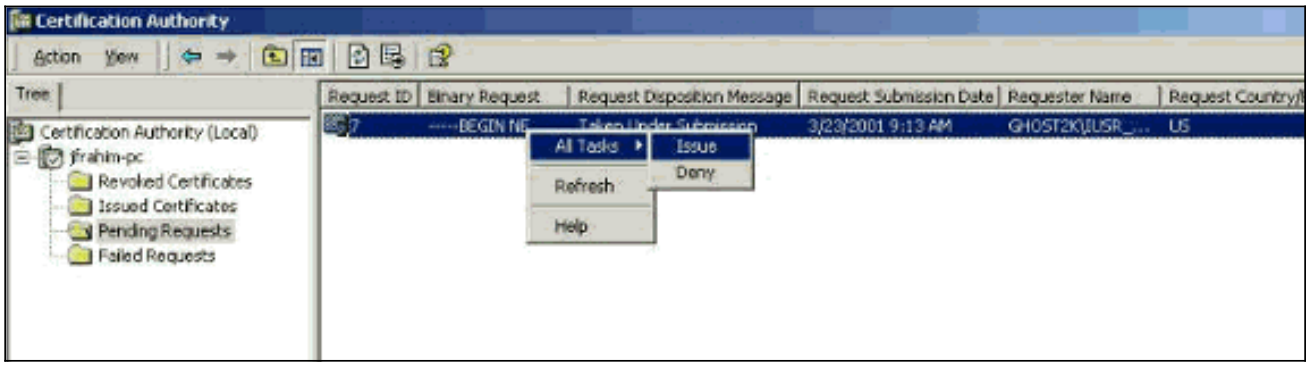
después.



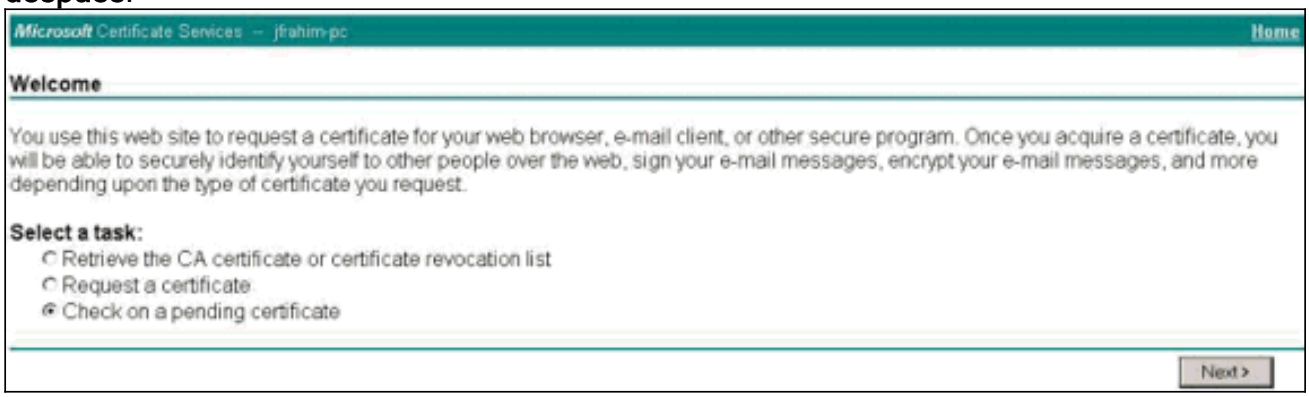
14. Resalte el archivo de la petición del cliente VPN, y pegúelo al servidor de CA bajo el Saved Request. Entonces haga clic
someten.



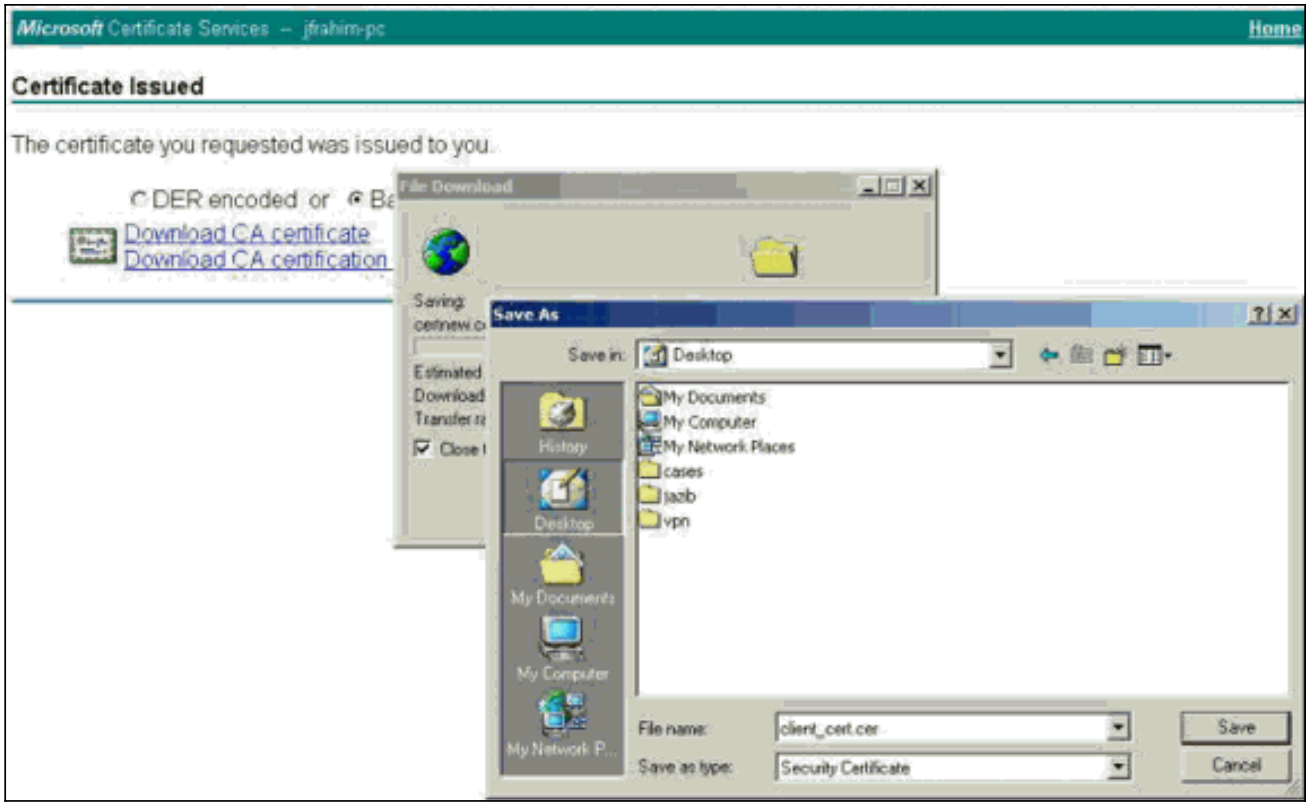
15. En el servidor de CA, publique el certificado de identidad para la petición del cliente VPN.



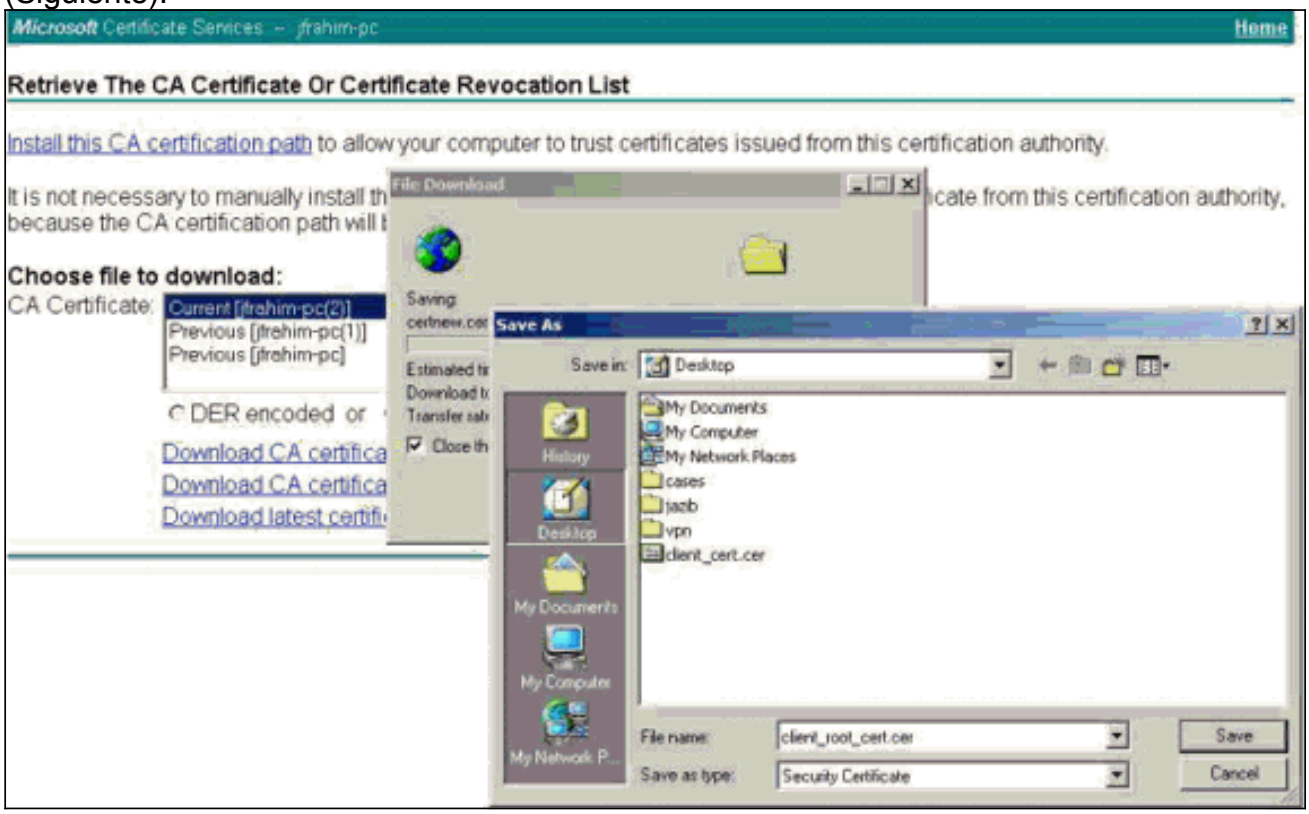
16. Descargue la raíz y los certificados de identidad al cliente VPN. En el servidor de CA, seleccione el **control en un certificado pendiente**, y después haga clic **después**.



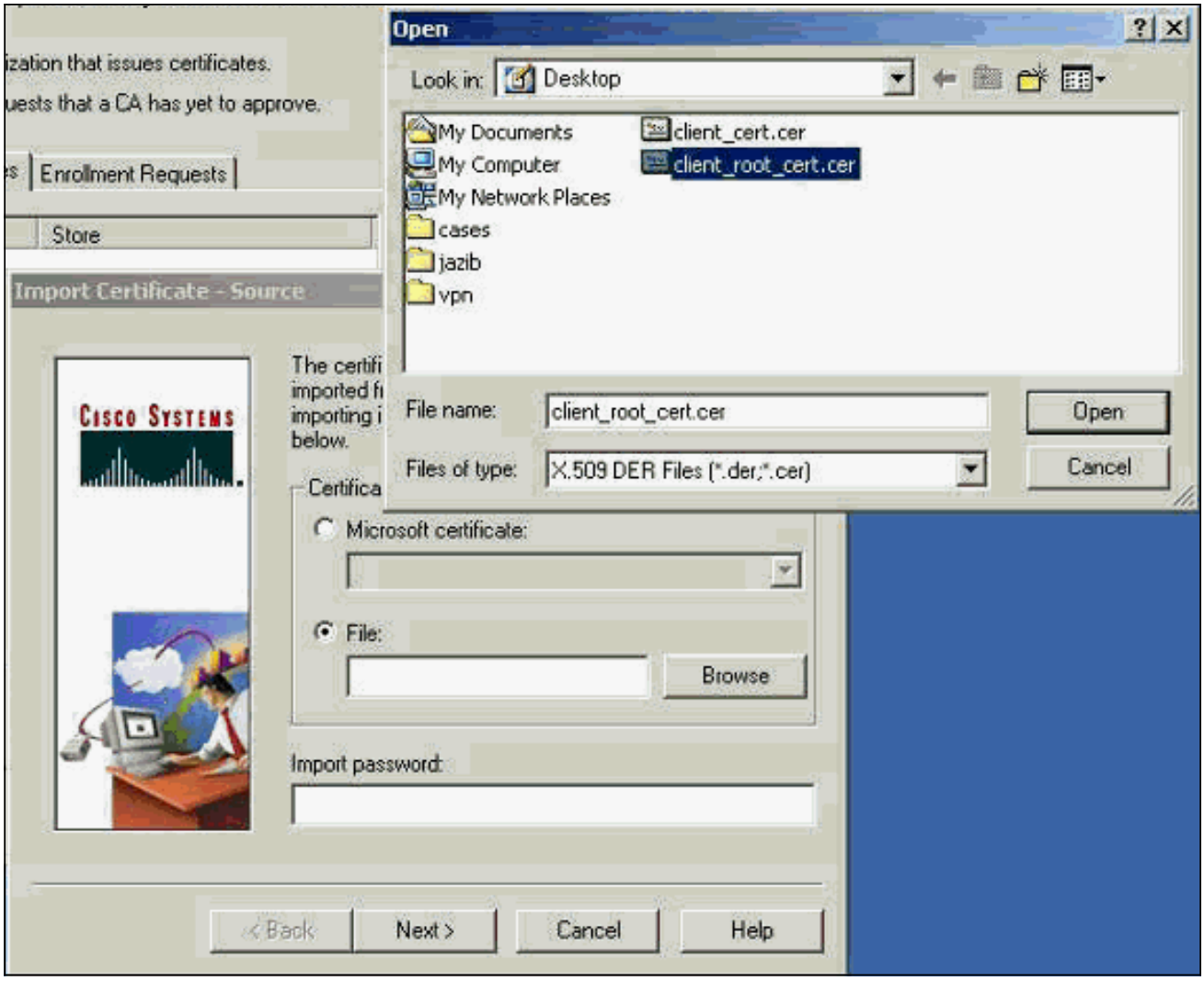
17. Seleccione el **base 64 codificado**. Entonces haga clic el **certificado de CA de la descarga** en el servidor de
CA.



18. Seleccione un archivo para descargar el extraer de la página del certificado de CA o del Lista de revocación de certificados (CRL) para conseguir el certificado raíz en el servidor de CA. Luego haga clic en Next
(Siguiente).

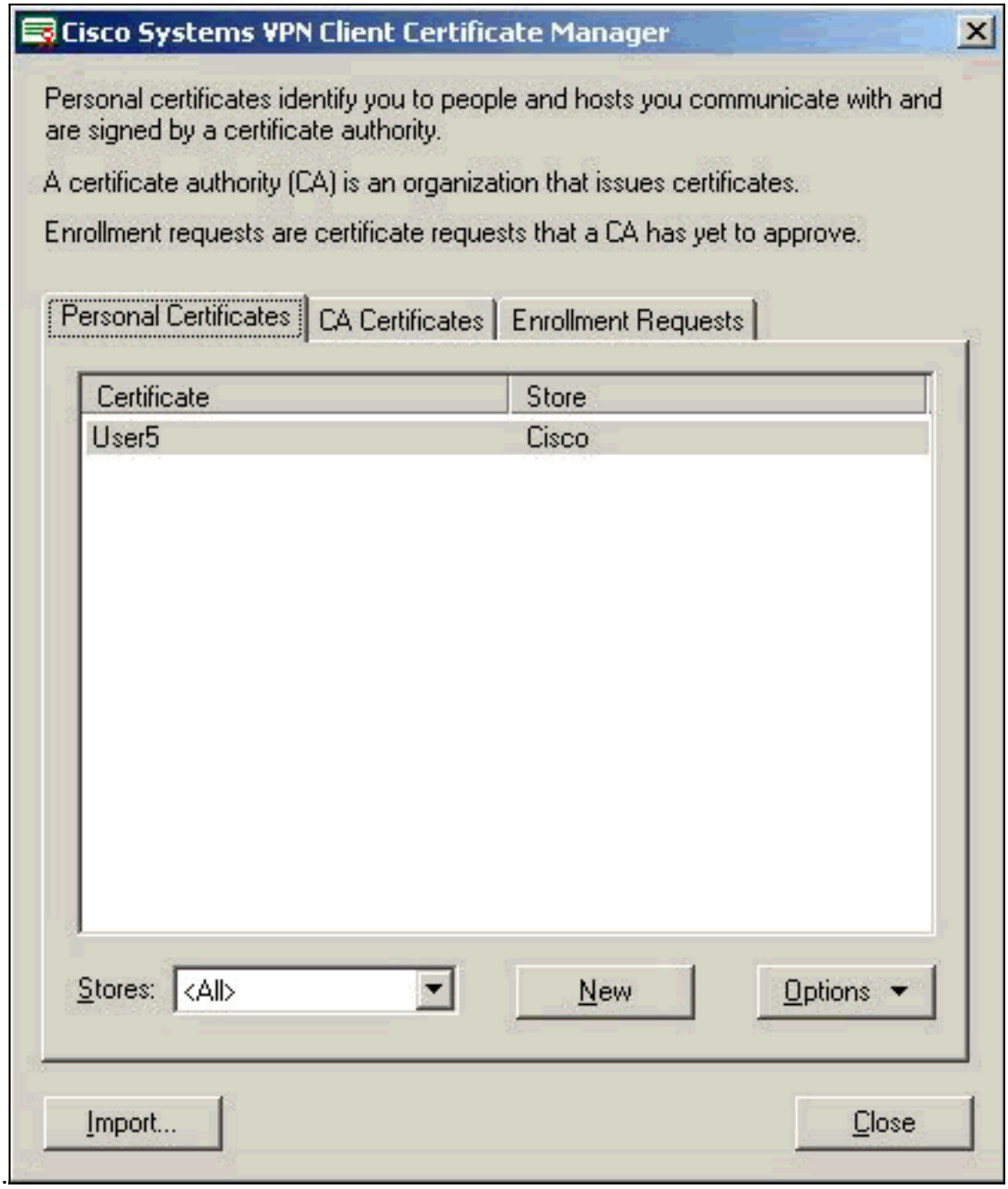


19. Seleccione el **Certificate Manager (Administrador de certificados) > CA Certificate (Certificado de CA) > Import on the VPN Client (Importar en Cliente VPN)**, y después seleccione raíz CA el archivo para instalar la raíz y los certificados de identidad.



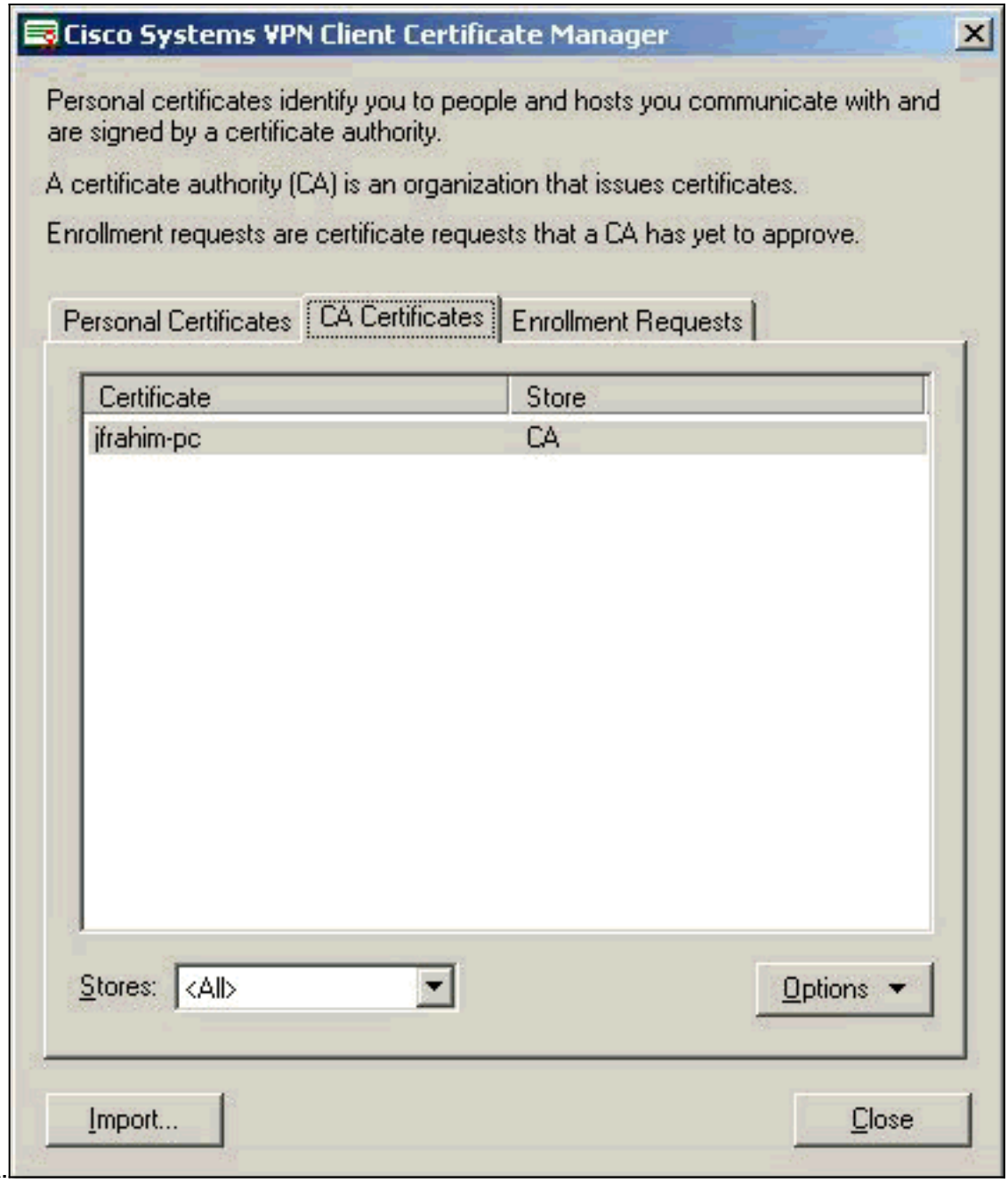
20. Seleccione el **Certificate Manager (Administración de certificados) > Personal Certificates (Certificados personales)> Import (Importar)**, y elija el archivo de certificado de identidad.

21. Asegúrese de que el certificado de identidad aparezca bajo lengueta de los certificados



personales.

22. Asegúrese de que el certificado raíz aparezca bajo lengueta de los Certificados de



CA.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Cuando usted intenta alistar con el Microsoft CA server, puede generar este mensaje de error.

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

Si usted recibe este mensaje de error, refiera a los registros de Microsoft CA para los detalles, o refiera a estos recursos para más información.

- Windows no puede encontrar un Certificate Authority que procesa la petición
- XCCC: El mensaje de error "su petición de certificado fue denegada" ocurre cuando usted pide un certificado para las conferencias seguras

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems