Configurar el Cisco VPN 3000 Concentrator 4.7.x para conseguir un certificado digital y un certificado SSL

Contenido

Introducción

Este documento incluye las instrucciones paso a paso en cómo configurar el Concentradores Cisco VPN de la serie 3000 para autenticar con el uso de digital o de los certificados de identidad y de los Certificados SSL.

Note: En el concentrador VPN, el Equilibrio de carga debe ser inhabilitado antes de que usted genere otro certificado SSL puesto que éste previene la generación del certificado.

Refiérase a cómo obtener un certificado digital de Microsoft Windows CA usando el ASDM en un ASA para aprender un escenario más casi igual con el PIX/ASA 7.x.

Refiera a la inscripción del certificado del Cisco IOS usando el ejemplo aumentado de los comandos Configuration de la inscripción para aprender un escenario más casi igual con las Plataformas de Cisco IOS®.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Cisco VPN 3000 Concentrator que funciona con la versión 4.7.

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.

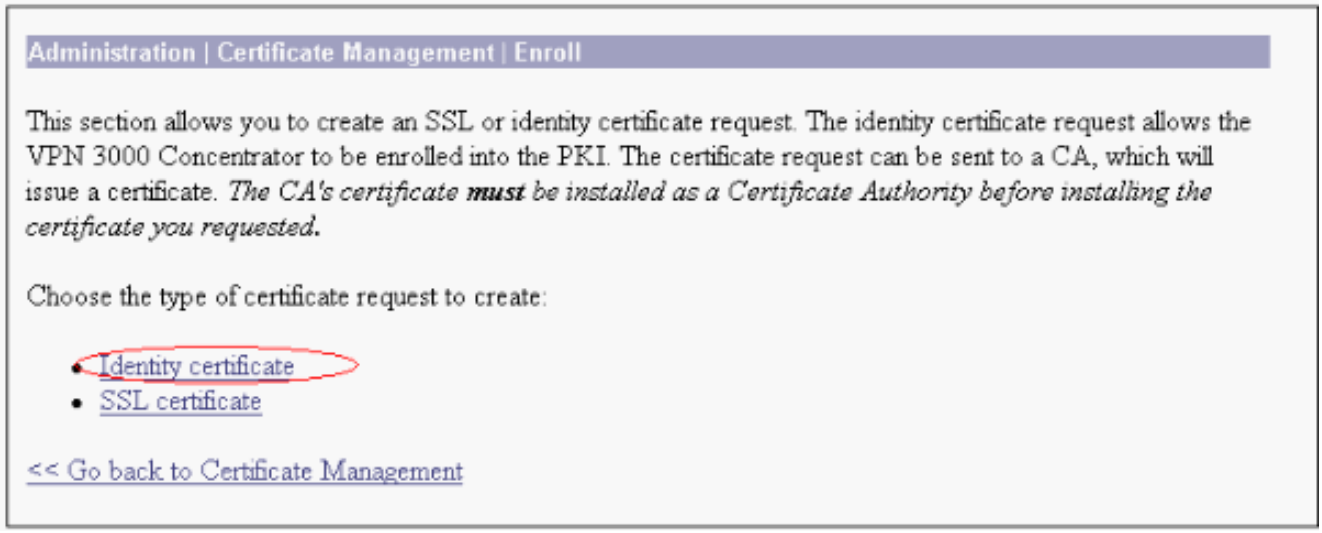
Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

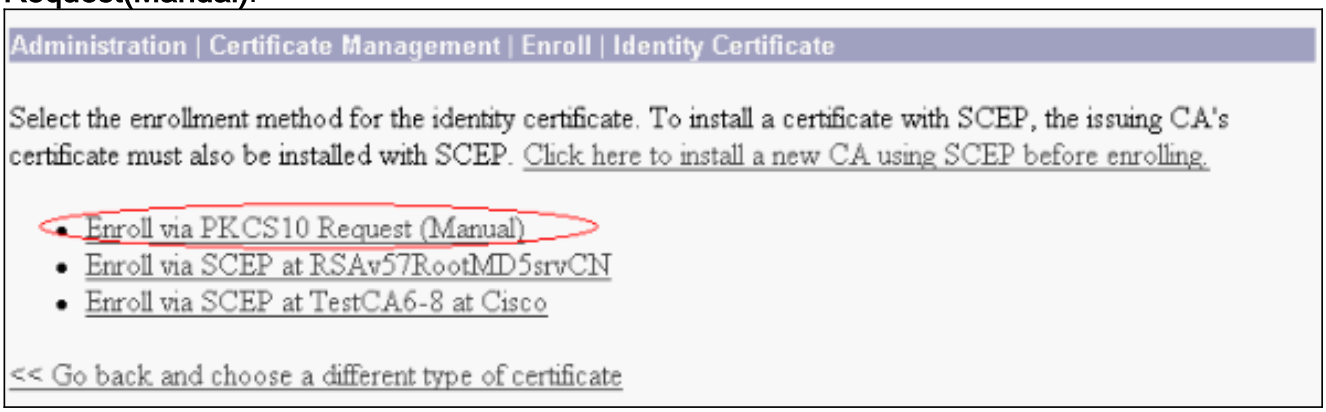
Instale los Certificados digitales en el concentrador VPN

Complete estos pasos:

1. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > Enroll (Registrar)** para seleccionar la petición digital o del certificado de identidad.

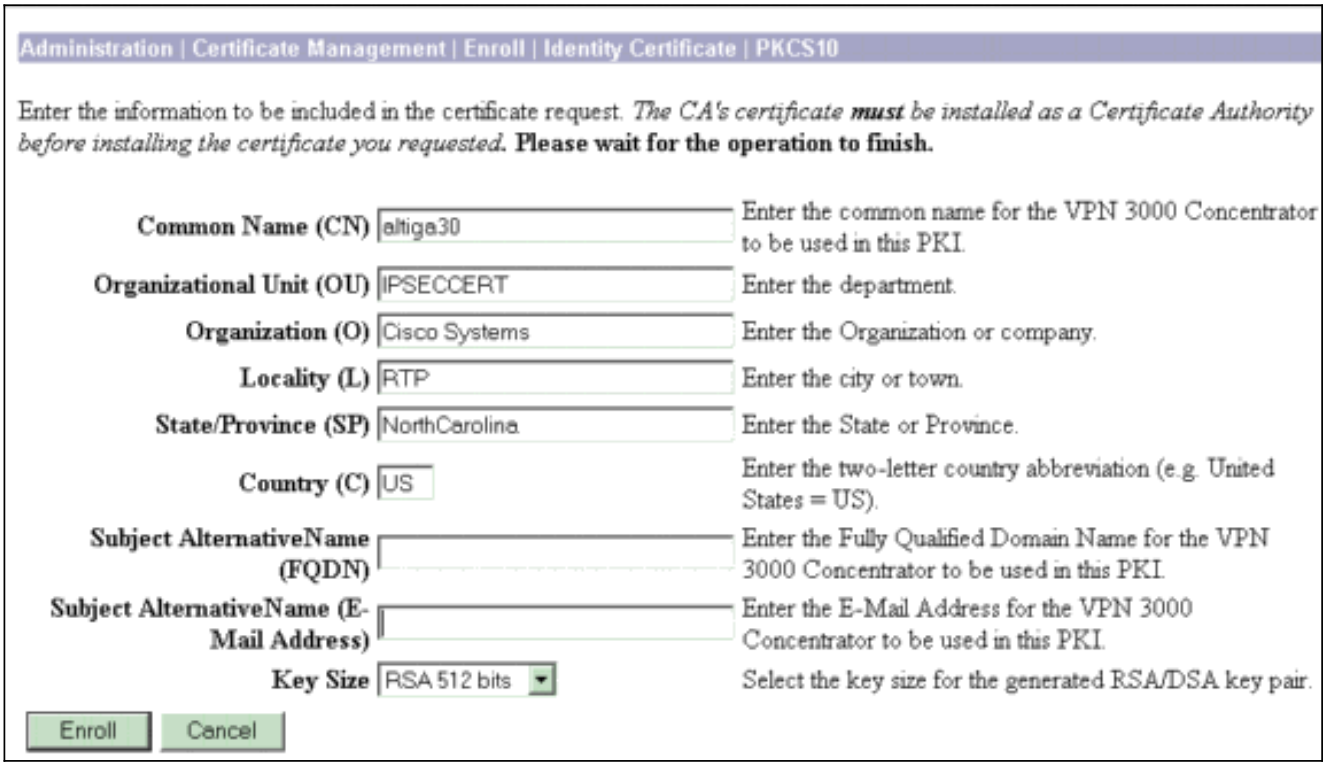


2. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > Enrollment (Inscripción) > Identity Certificate (Certificado de identidad)** y el tecleo **alista vía PKCS10 Request(Manual)**.

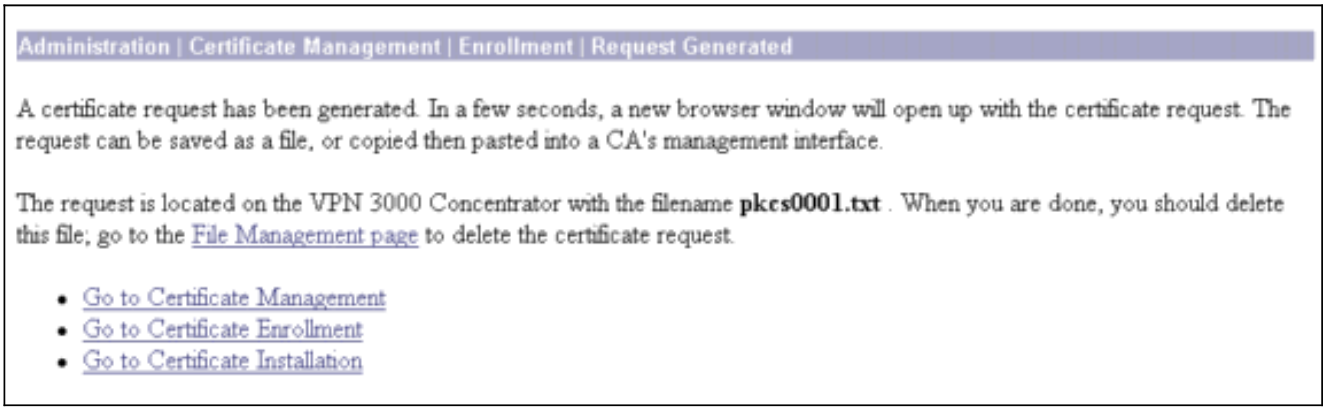


3. Complete los campos pedidos, y después haga clic **alistan**.Estos campos se completan hacia fuera este ejemplo.**Common Name** — altiga30**Unidad organizativa** — IPSECCERT (el OU debe hacer juego el nombre de grupo configurado del IPSec)**Organización** — Cisco Systems**Lugar** — RTP**Estado/provincia** — Carolina del Norte**País** — Los E.E.U.U.**Nombre de dominio totalmente calificado (FQDN)** — (no utilizado aquí)**Tamaño de clave** — 512**Note**: Si

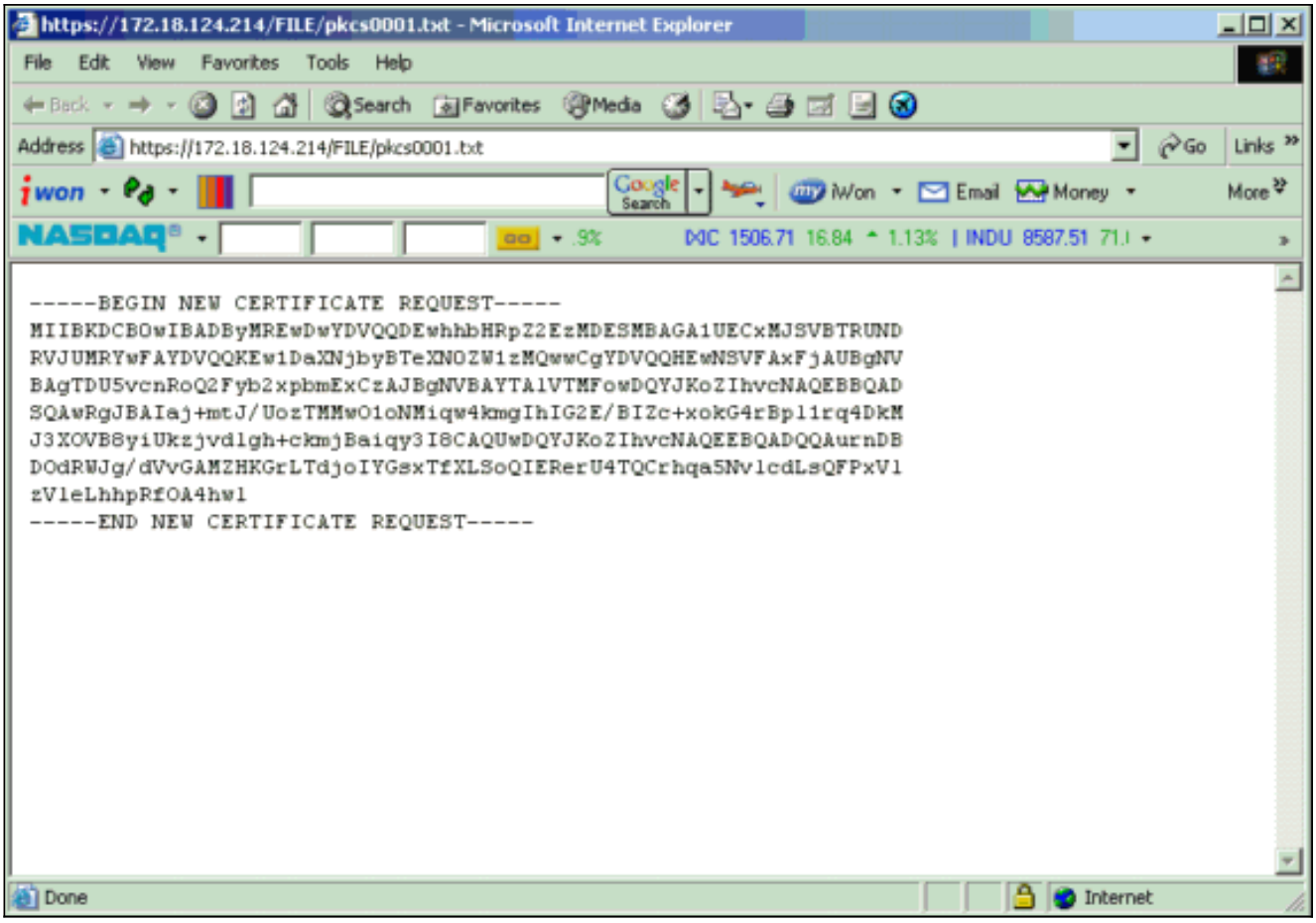
usted pide un certificado SSL o un certificado de identidad usando el protocolo simple certificate enrollment (SCEP), éstas son las únicas opciones de RSA disponibles.Bits RSA 512Bits RSA 768Bits RSA 1024Bits RSA 2048Bits DSA 512Bits DSA 768Bits DSA 1024



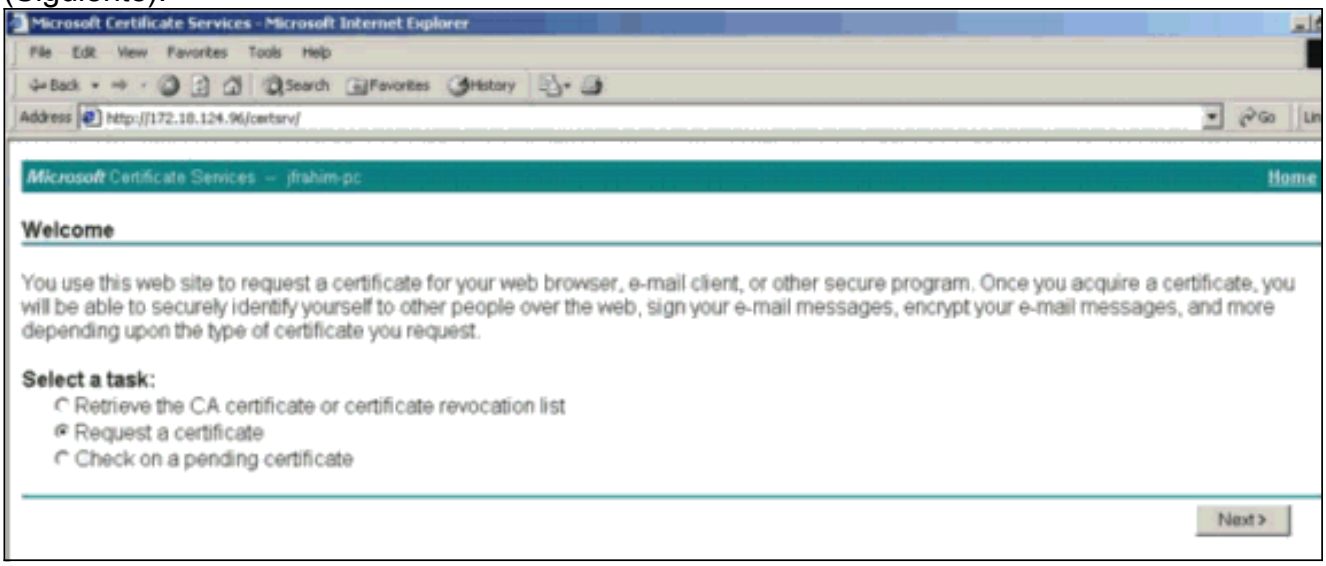
4. Después de que usted tecleo **aliste**, varias ventanas aparecen. La primera ventana confirma que usted ha pedido un certificado.



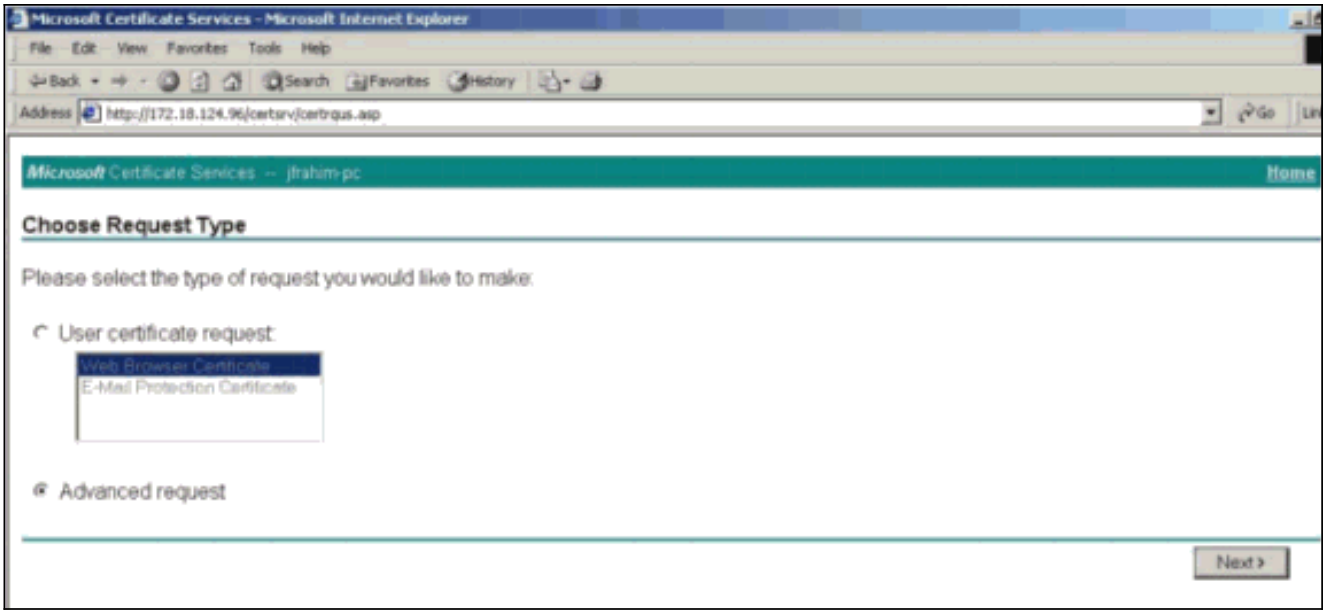
Una nueva ventana del buscador también abre y visualiza su archivo de la petición PKCS.



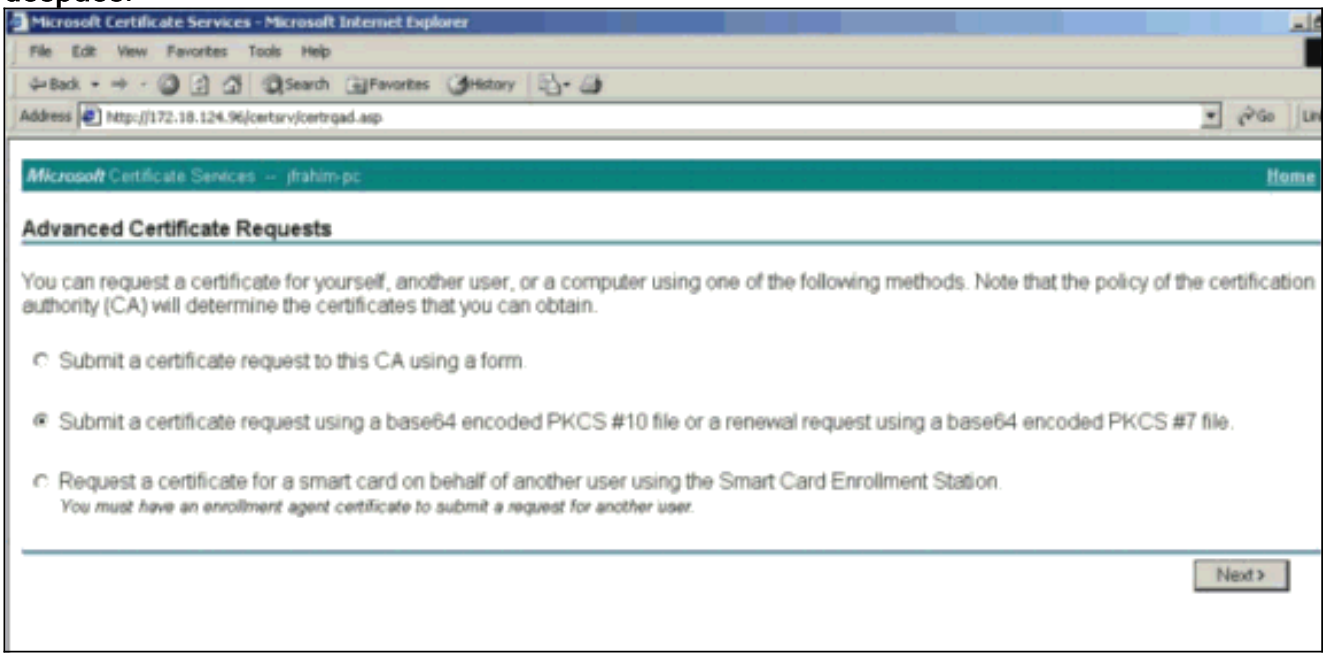
5. En su servidor del Certification Authority (CA), resalte la petición y pegúela en su servidor de CA para someter su petición. Haga clic en Next (Siguiente).



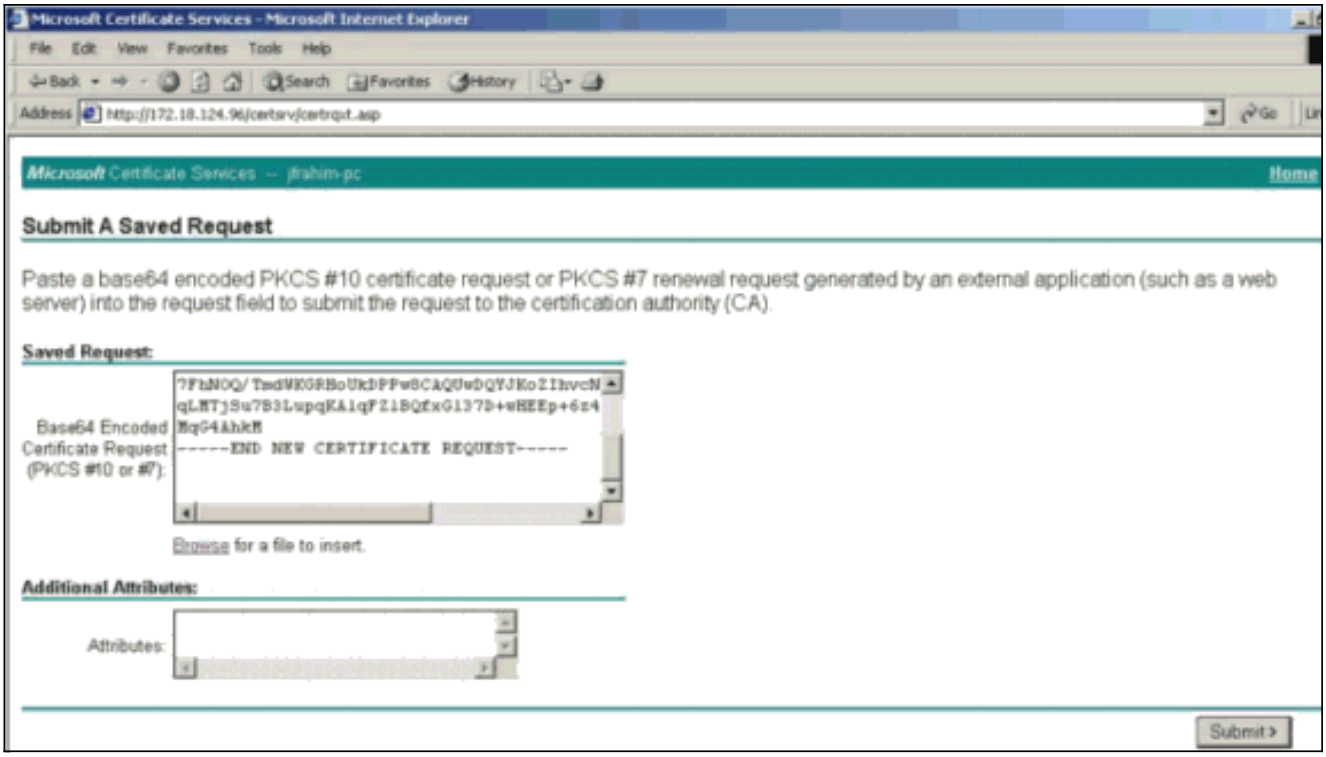
6. Seleccione el **pedido avanzado** y haga clic **después**.



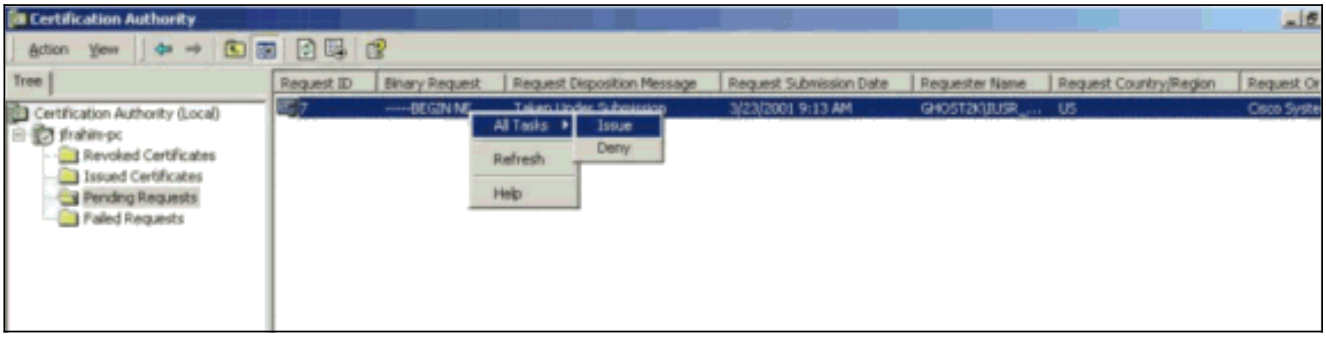
7. Selecto **presente un pedido de certificado usando PKCS-10 un archivo codificado base64 o un pedido de renovación usando PKCS-7 un archivo codificado base64**, y después haga clic **después**.



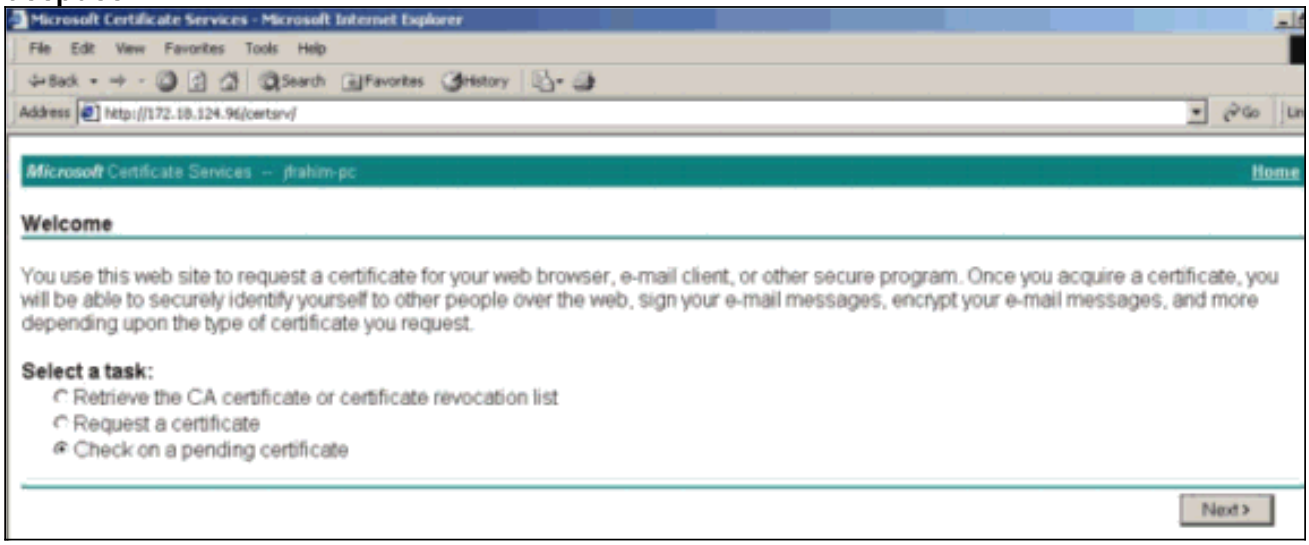
8. Corte y pegar su archivo PKCS en el campo de texto bajo sección del Saved Request. Entonces haga clic
someten.



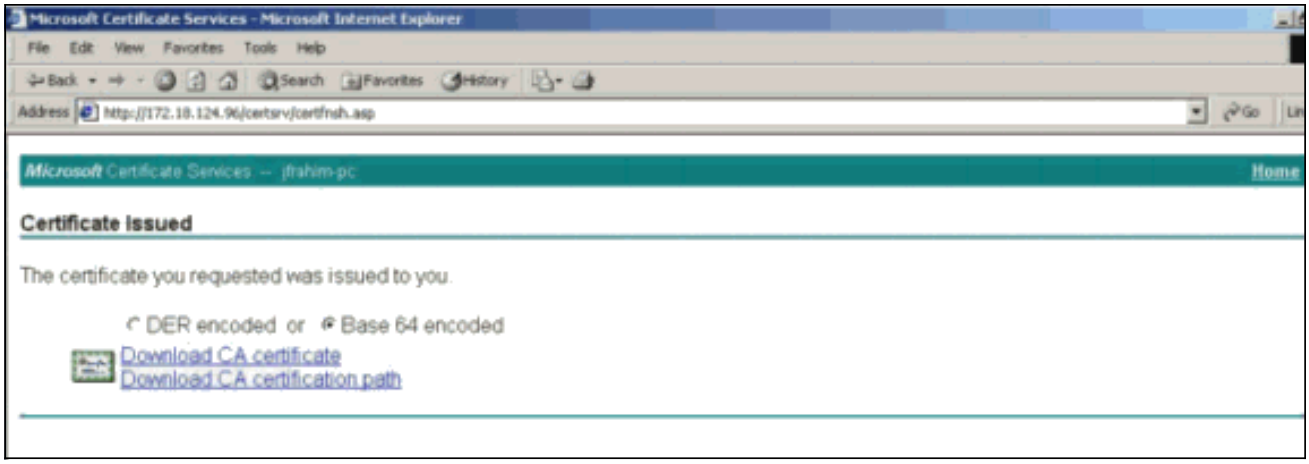
9. Publique el certificado de identidad en el servidor de CA.



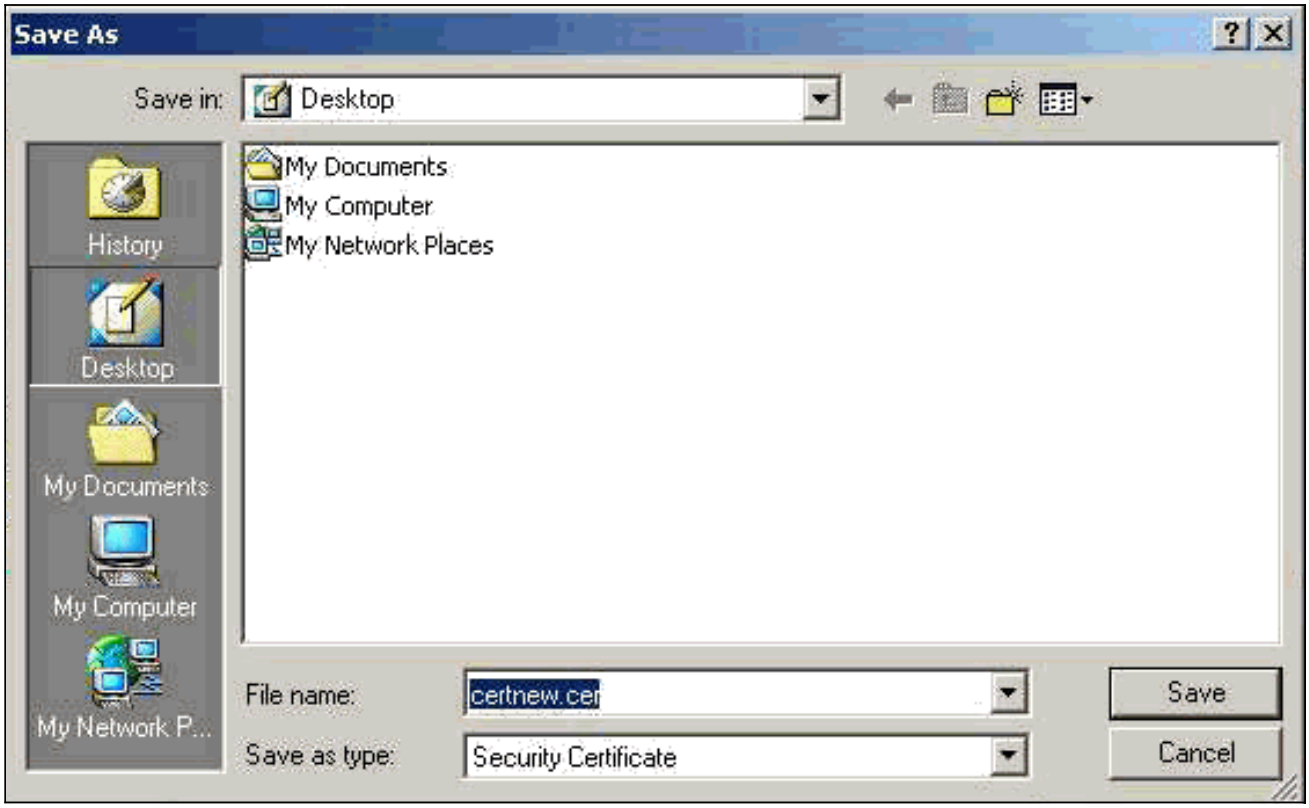
10. Descargue la raíz y los certificados de identidad. En su servidor de CA, seleccione el **control en un certificado pendiente**, y haga clic **después**.



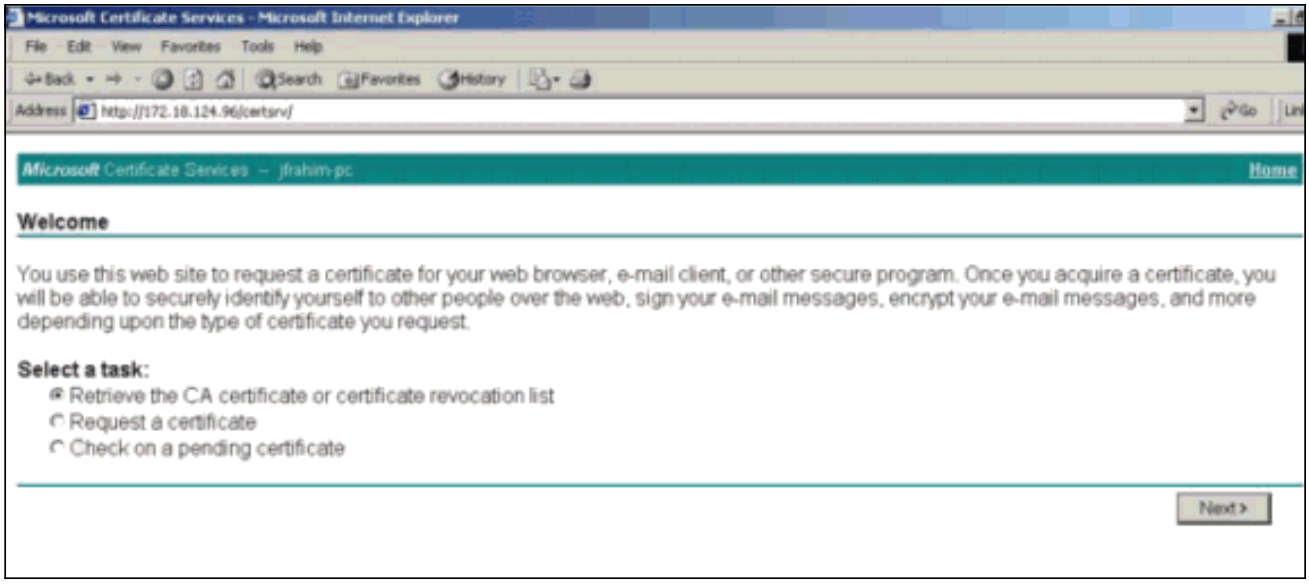
11. Seleccione el **base 64 codificado**, y haga clic el **certificado de CA de la descarga** en el servidor de CA.



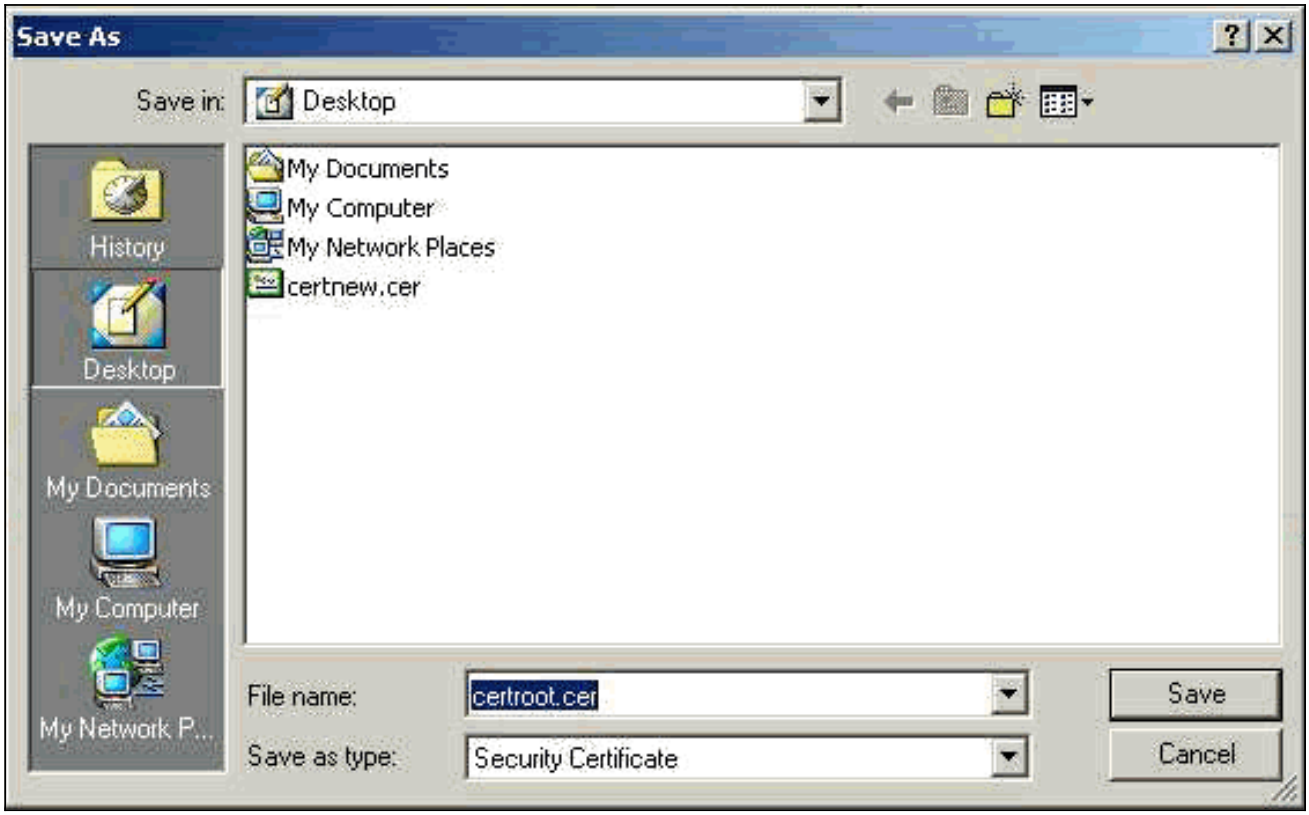
12. Salve el certificado de identidad en su unidad local.



13. En el servidor de CA, selecto **extraiga el certificado de CA o el Lista de revocación de certificados (CRL)** para conseguir el certificado raíz. Luego haga clic en Next (Siguiente).



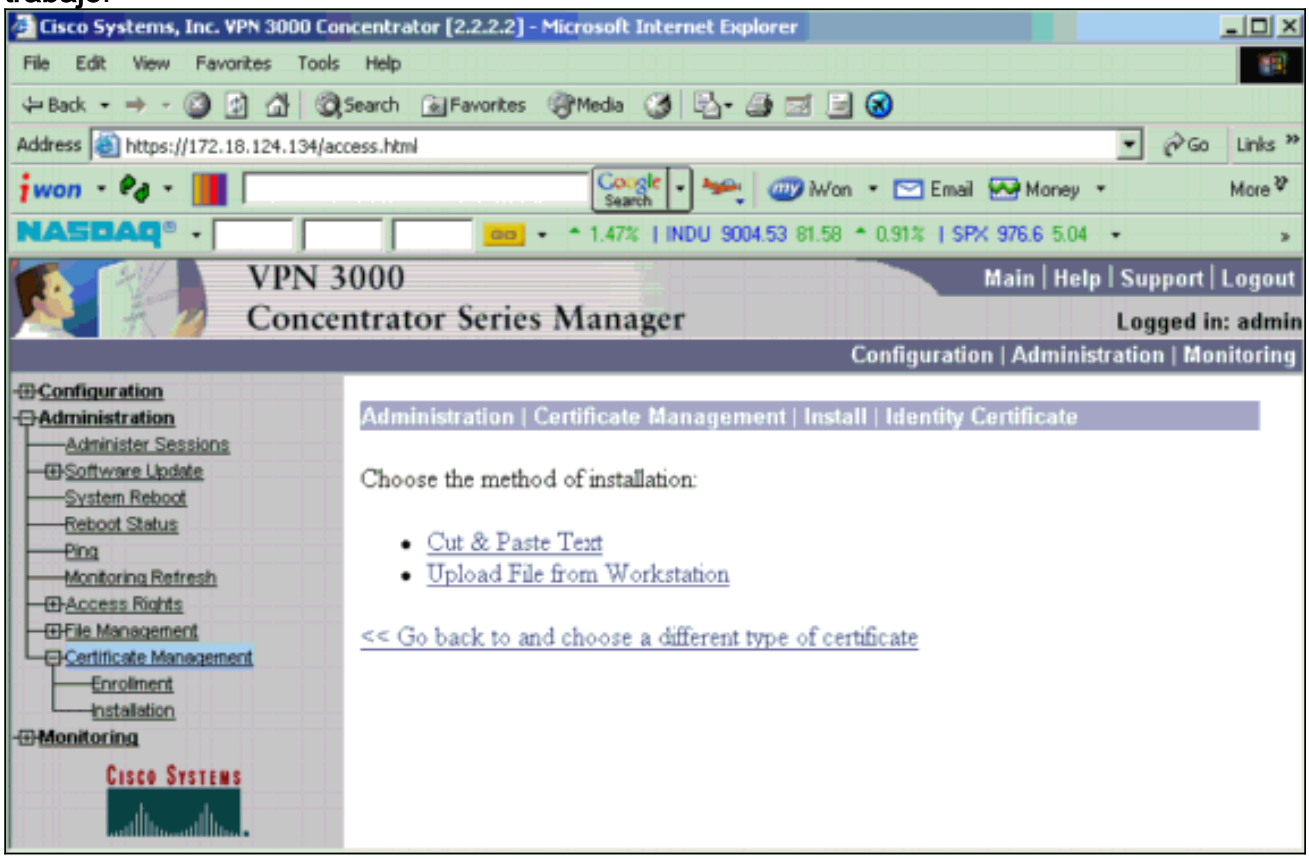
14. Salve el certificado raíz en su unidad local.



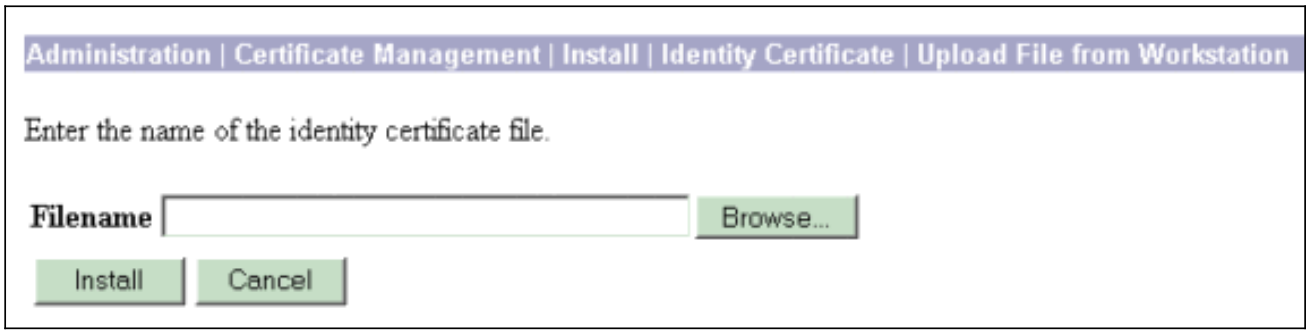
15. Instale la raíz y los certificados de identidad en el concentrador VPN 3000. Para hacer esto, la **administración** selecta > el **Certificate Manager** > la **instalación > instalan el certificado obtenido vía la inscripción**. Bajo estatus de la inscripción, el tecleo **instala**.

16. **Archivo de la carga del** tecleo del **puesto de**

trabajo.



17. Haga clic **hojean** y seleccionan el archivo de certificado raíz que usted guardó a su unidad local.Selecto **instale** para instalar el certificado de identidad en el concentrador VPN. La administración | La ventana de la administración de certificados aparece como confirmación, y su nuevo certificado de identidad aparece en la tabla de los certificados de identidad.



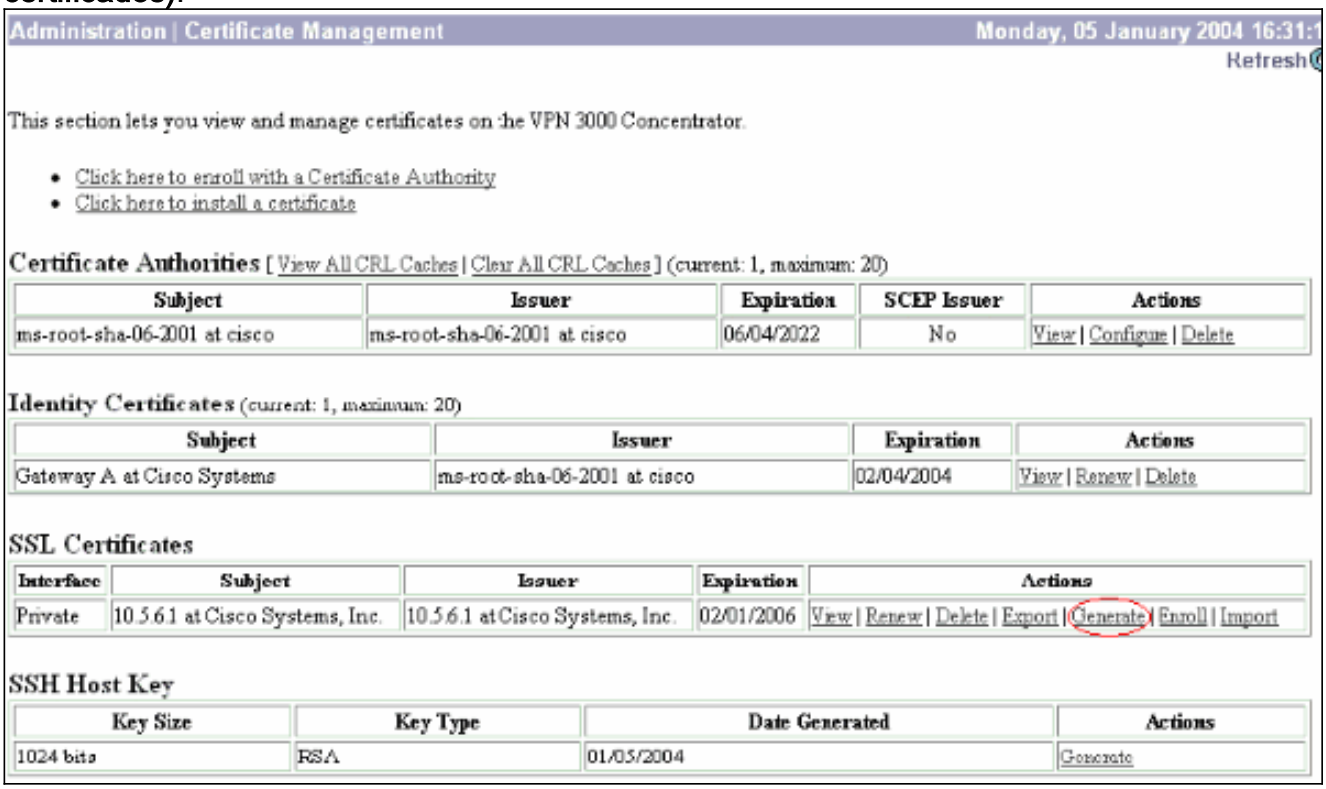
Note: Complete estos pasos para generar un nuevo certificado si el certificado falla.Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)**.Haga clic la **cancelación** en el cuadro de las acciones para el anuncio del certificado SSL.Seleccione la **reinicialización de la administración >** del **sistema**.Seleccione la **salvaguardia la configuración activa en la época de la reinicialización**, **ahora** elija, y el tecleo **se aplica**. Usted puede ahora generar un nuevo certificado después de que la recarga sea completa.

Instale los Certificados SSL en el concentrador VPN

Si usted utiliza una conexión segura entre su navegador y el concentrador VPN, el concentrador VPN requiere un certificado SSL. Usted también necesita un certificado SSL en la interfaz que usted utiliza para manejar el concentrador VPN y para el WebVPN, y para cada interfaz que termine los túneles del WebVPN.

Los Certificados de la interfaz SSL, si son inexistentes, se generan automáticamente cuando las reinicializaciones concentradoras VPN 3000 después de que usted actualice el software concentrador VPN 3000. Porque uno mismo-se genera un certificado autofirmado, este certificado no es comprobable. Ningún Certificate Authority ha garantizado su identidad. Pero este certificado permite que usted haga el contacto inicial con el concentrador VPN usando el navegador. Si usted quiere substituirlo por otro certificado uno mismo-firmado SSL, complete estos pasos:

1. Elija el **Administration (Administración) > Certificate Management (Administración de certificados)**.



2. El tecleo **genera** para visualizar el nuevo certificado en la tabla del certificado SSL y substituir el existencia.Esta ventana permite que usted configure los campos para el SSL certifica el concentrador VPN genera automáticamente. Estos Certificados SSL están para las interfaces y para el Equilibrio de carga.

Si usted quiere obtener un certificado comprobable SSL (es decir, uno publicado por un Certificate Authority), vea los Certificados digitales del instalar en la sección del concentrador VPN de este documento para utilizar el mismo procedimiento que usted utiliza para obtener

los certificados de identidad. Pero este vez, en la ventana del **Administration (Administración) > Certificate Management (Administración de certificados) > Enroll (Registrar)**, **certificado del** tecleo **SSL** (en vez del certificado de identidad).**Note**: Refiera a la *administración | Sección de administración de certificados del* volumen de referencia concentrador VPN 3000 II: La administración y la supervisión liberan 4.7 para toda la información sobre los Certificados digitales y los Certificados SSL.

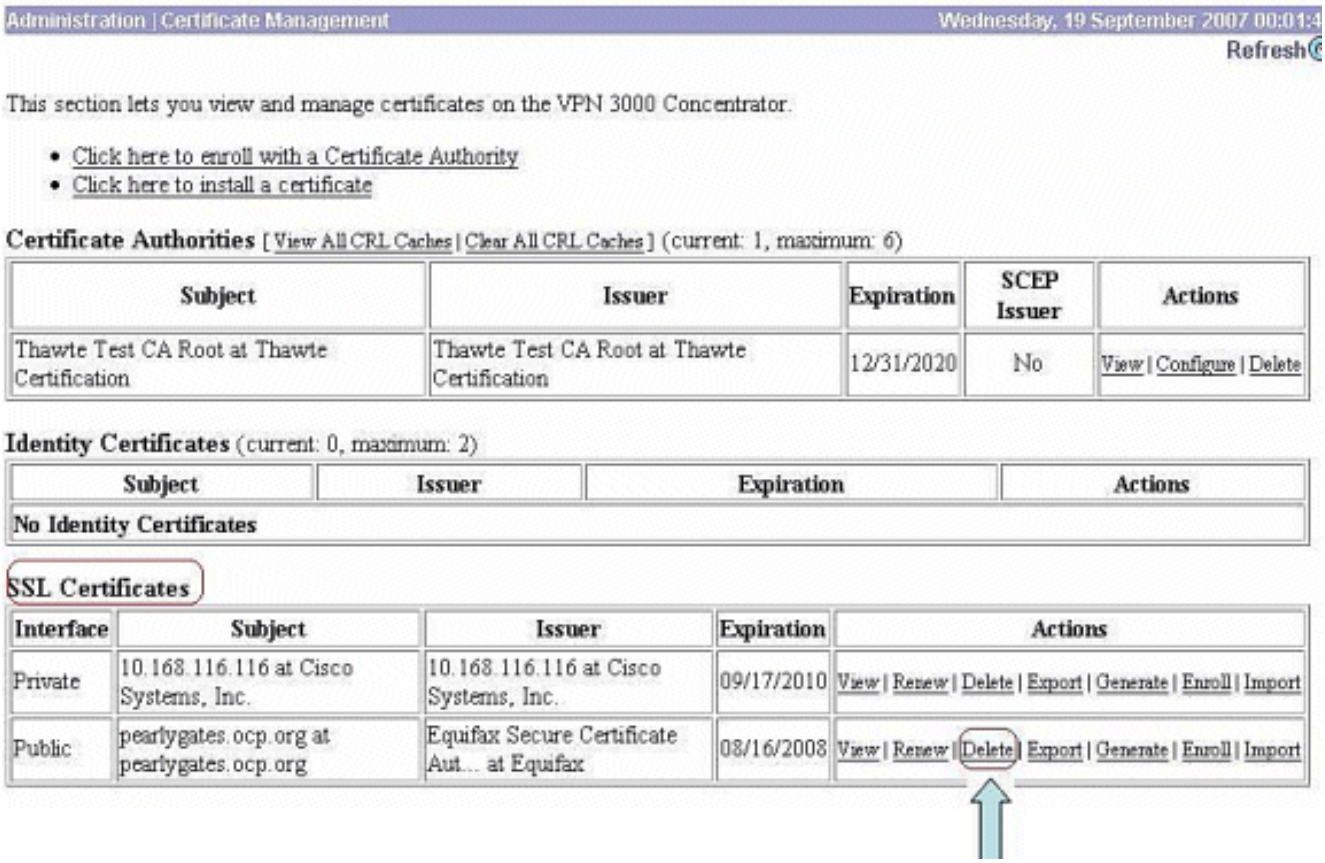
Renueve los Certificados SSL en el concentrador VPN

Esta sección describe cómo renovar los Certificados SSL:

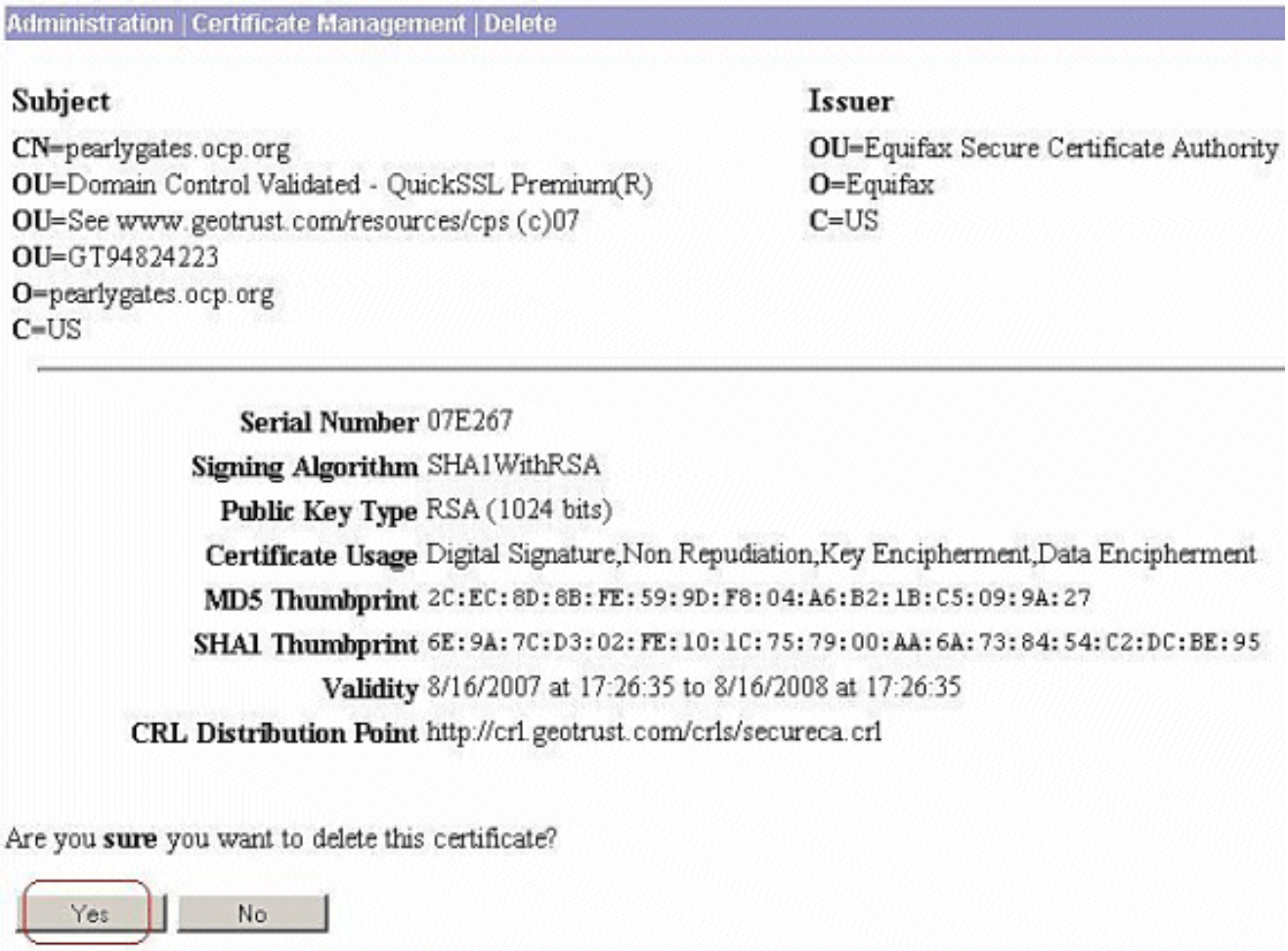
Si esto está para el certificado SSL generado por el concentrador VPN, vaya al **Administration (Administración) > Certificate Management (Administración de certificados)** en la sección SSL. Haga clic la opción de la **renovación**, y eso renueva el certificado SSL.

Si esto está para un certificado concedido por un servidor externo de CA, complete estos pasos:

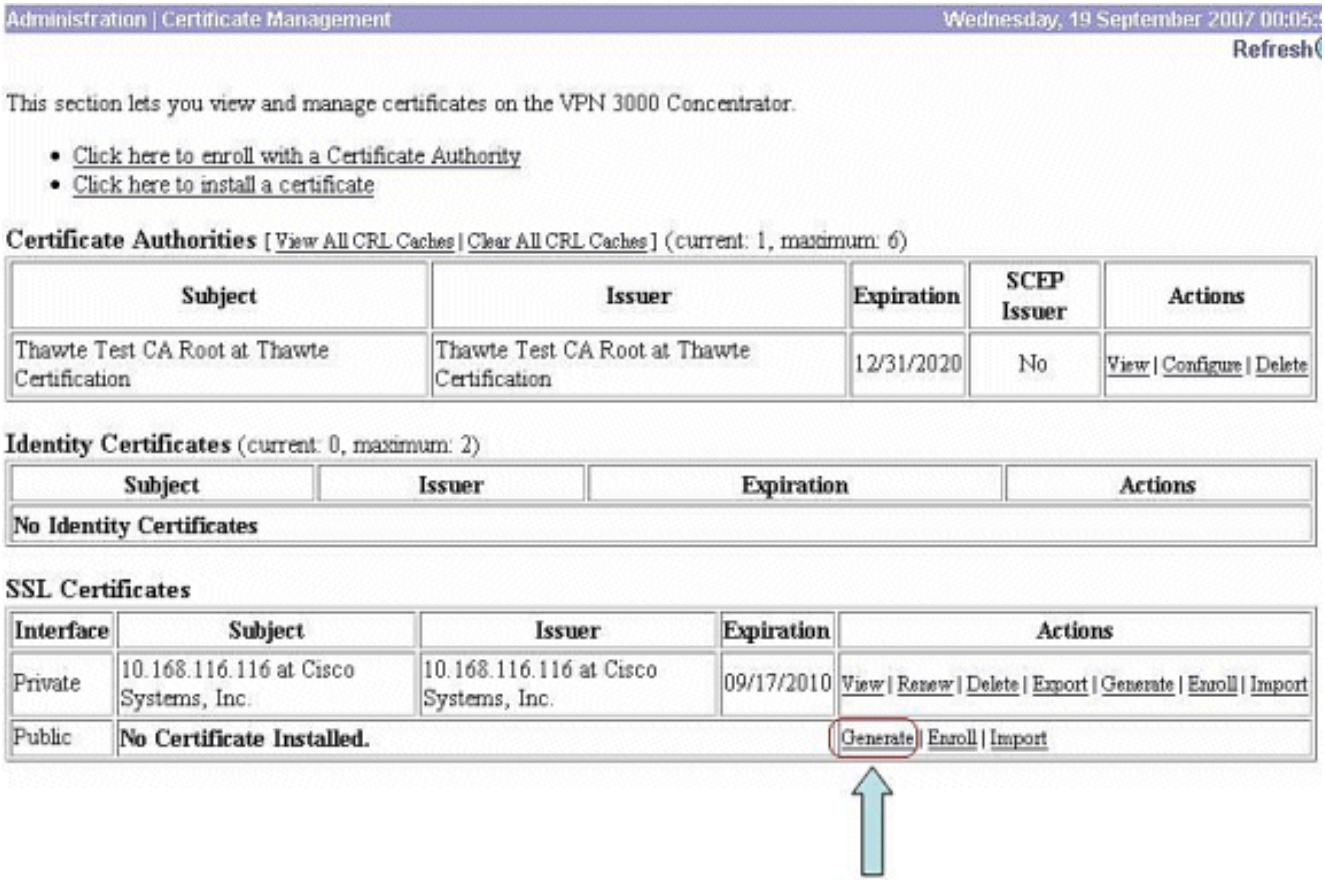
1. Elija el **>Delete del Administration (Administración) > Certificate Management (Administración de certificados)** conforme a los *Certificados SSL* para borrar los certificados vencidos de la interfaz
pública.



Tecleo **sí** para confirmar la cancelacíon del certificado SSL.

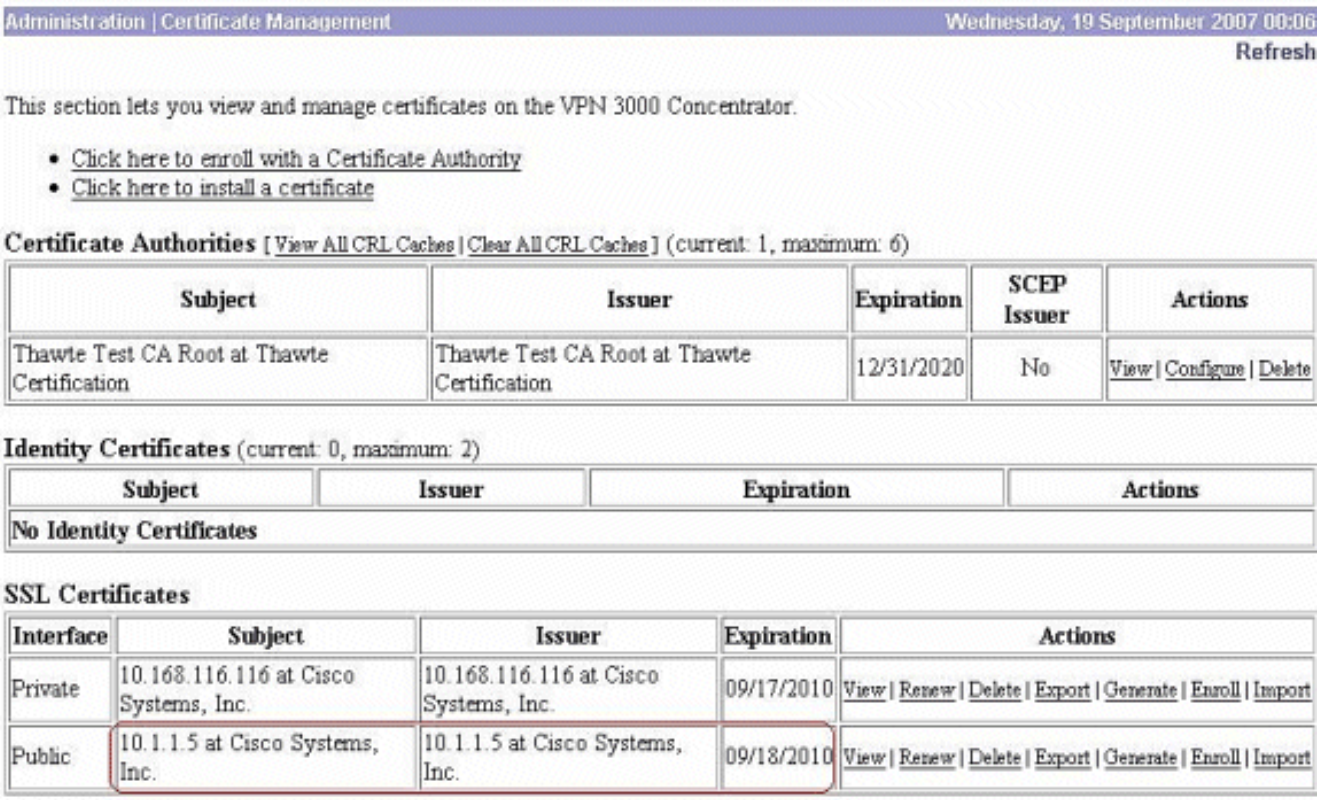


2. Elija el **Administration (Administración) > Certificate Management (Administración de certificados) > generan** para generar el nuevo certificado SSL.



El nuevo certificado SSL para la interfaz pública

aparece.



Administration | Certificate Management — Wednesday, 19 September 2007 00:06

Refresh

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- Click here to enroll with a Certificate Authority
- Click here to install a certificate

Certificate Authorities [View All CRL Caches | Clear All CRL Caches] (current: 1, maximum: 6)

Subject	Issuer	Expiration	SCEP Issuer	Actions
Thawte Test CA Root at Thawte Certification	Thawte Test CA Root at Thawte Certification	12/31/2020	No	View | Configure | Delete

Identity Certificates (current: 0, maximum: 2)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

SSL Certificates

Interface	Subject	Issuer	Expiration	Actions
Private	10.168.116.116 at Cisco Systems, Inc.	10.168.116.116 at Cisco Systems, Inc.	09/17/2010	View | Renew | Delete | Export | Generate | Enroll | Import
Public	10.1.1.5 at Cisco Systems, Inc.	10.1.1.5 at Cisco Systems, Inc.	09/18/2010	View | Renew | Delete | Export | Generate | Enroll | Import

Información Relacionada

- Página de soporte del concentrador de la serie Cisco VPN 3000
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems