L2TP sobre el IPSec entre el Windows 2000 y el concentrador VPN 3000 usando el ejemplo de configuración de los Certificados digitales

Contenido

Introducción

Este documento muestra el procedimiento paso a paso usado para conectar con un concentrador VPN 3000 de un cliente del Windows 2000 que usa al cliente del accesorio del L2TP/IPSec. Se asume que usted utiliza los Certificados digitales (autoridades de certificación raíz independientes (CA) sin el Certificate Enrollment Protocol (el CEP)) para autenticar su conexión al concentrador VPN. Este documento utiliza el Microsoft Certificate Service para el ejemplo. Refiera al sitio Web de Microsoft para la documentación en cómo configurarla.

Nota: Esto es un ejemplo solamente porque el aspecto de las pantallas del Windows 2000 puede cambiar.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento está para el Cisco VPN 3000 Concentrator Series.

Objetivos

En este procedimiento, usted completa estos pasos:

1. Obtenga un certificado raíz.
2. Obtenga un certificado de identidad para el cliente.
3. Cree una conexión al VPN 3000 con la ayuda del asistente de conexión de red.
4. Configure el concentrador VPN 3000.

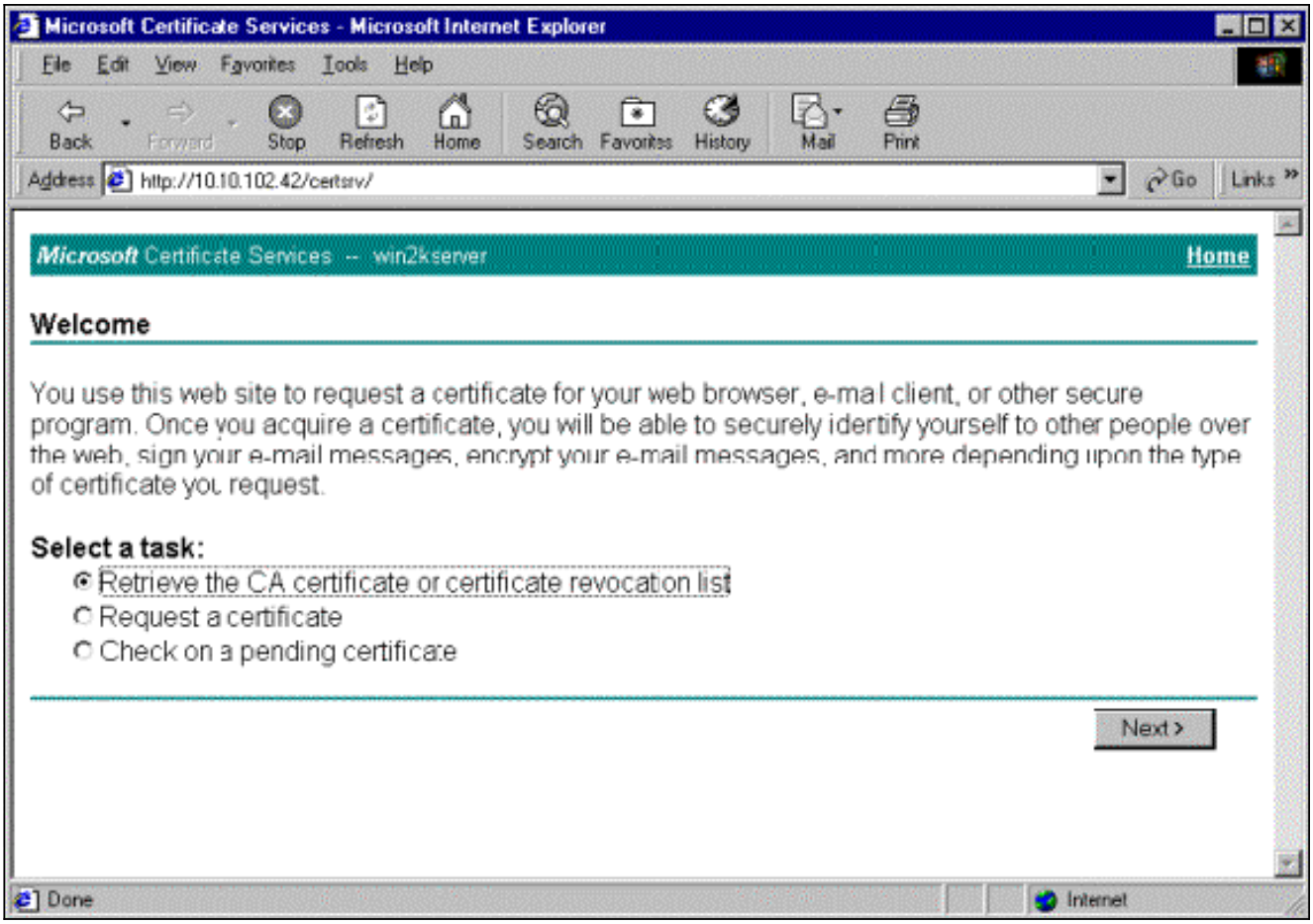
Convenciones

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

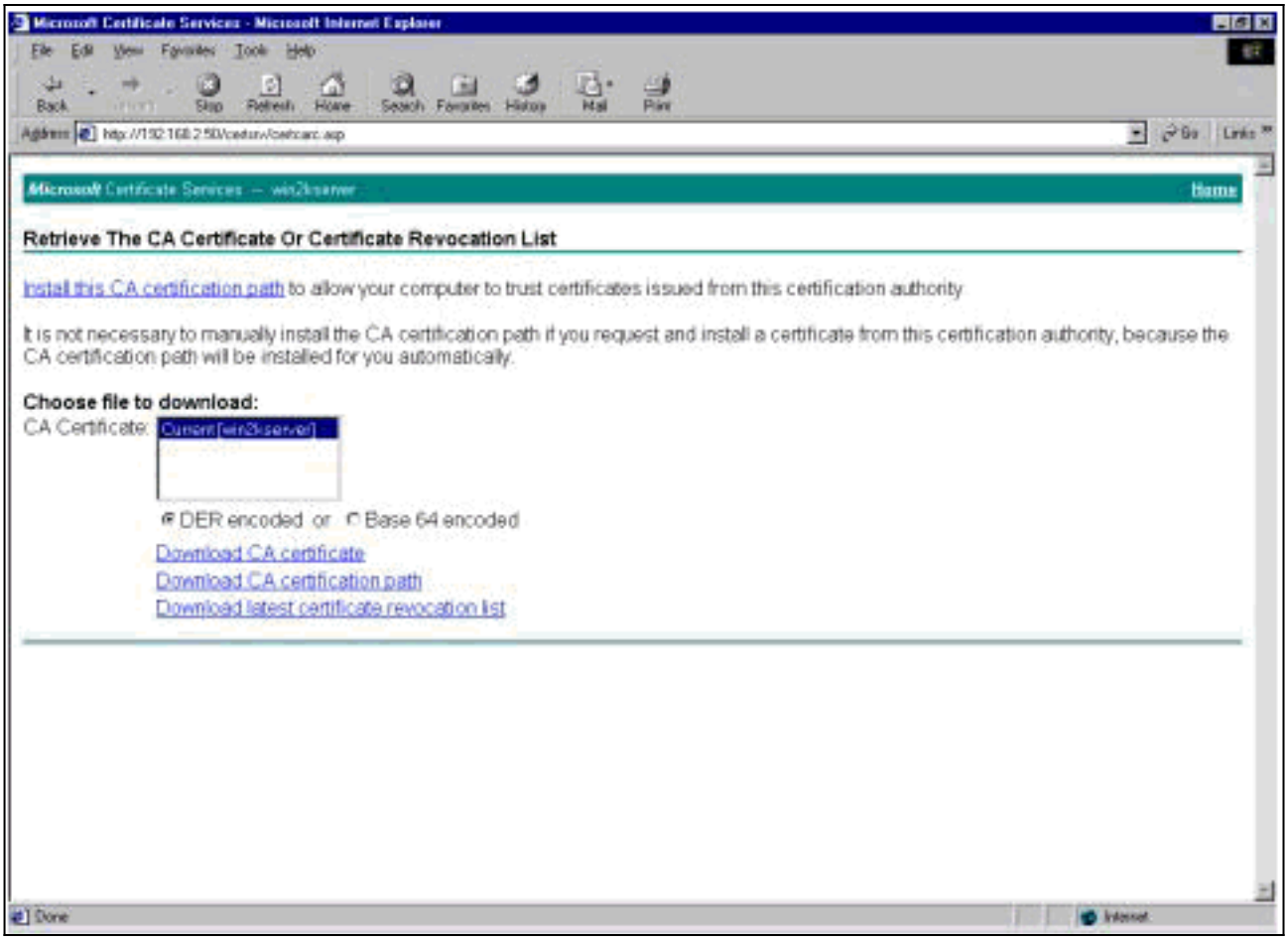
Obtenga un certificado raíz

Complete estas instrucciones para obtener un certificado raíz:

1. Abra una ventana del buscador y teclee adentro el URL para el Microsoft Certificate Authority (generalmente http://servername o la dirección IP de CA/certsrv).La ventana agradable para las recuperaciones de certificados y pide las visualizaciones.
2. En la ventana agradable debajo seleccione una tarea, elija **extraen el certificado de CA o el Lista de revocación de certificados (CRL)** y hacen clic **después**.



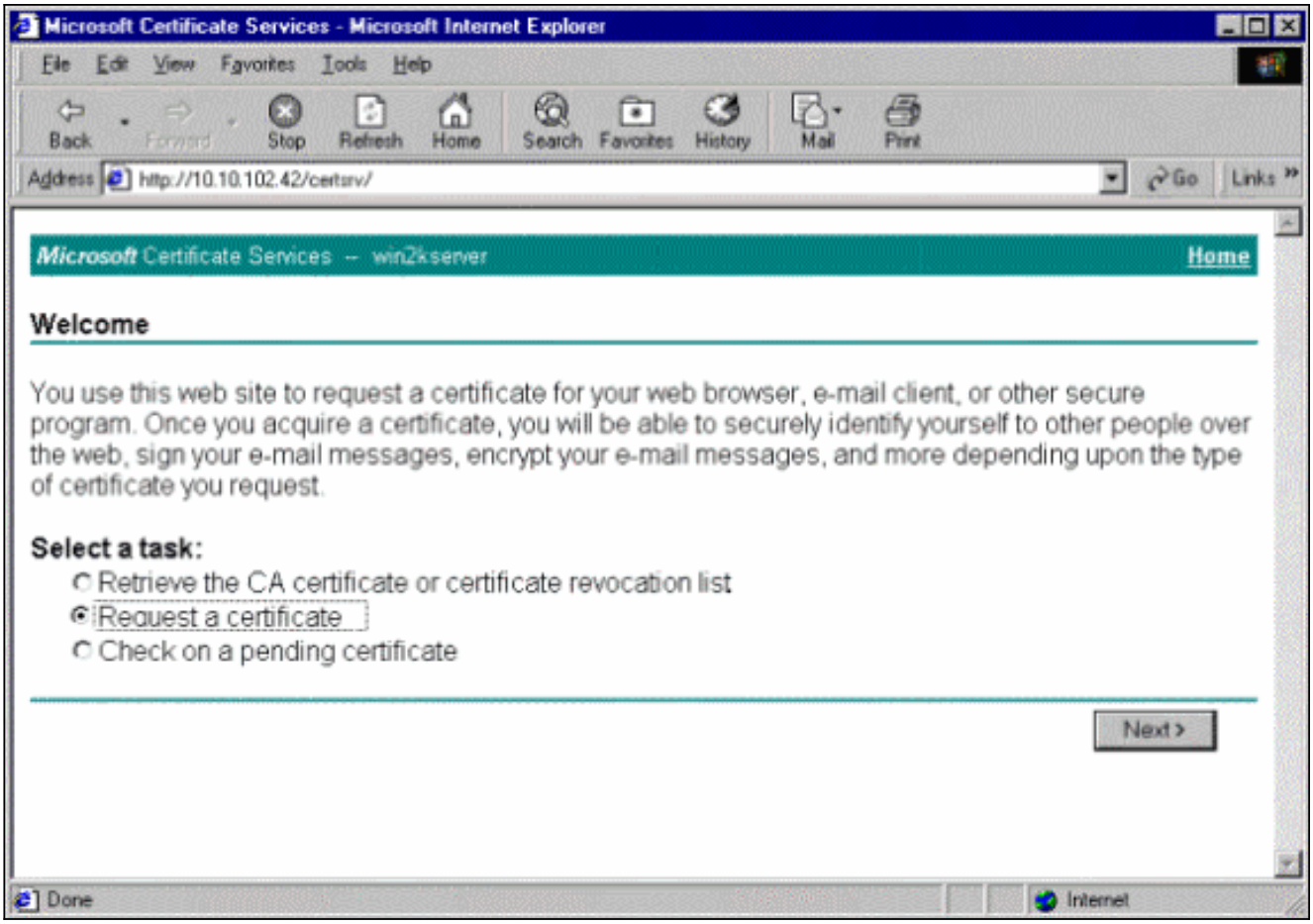
3. Del extraer el certificado de CA o la ventana del Lista de revocación de certificados (CRL), tecleo **instala este trayecto de certificación de CA** en la esquina izquierda.Esto agrega el certificado de CA al almacén de las autoridades de certificación de la Raíz confiable. Esto significa que cualquier Certificados que este CA publique a este cliente está confiado en.



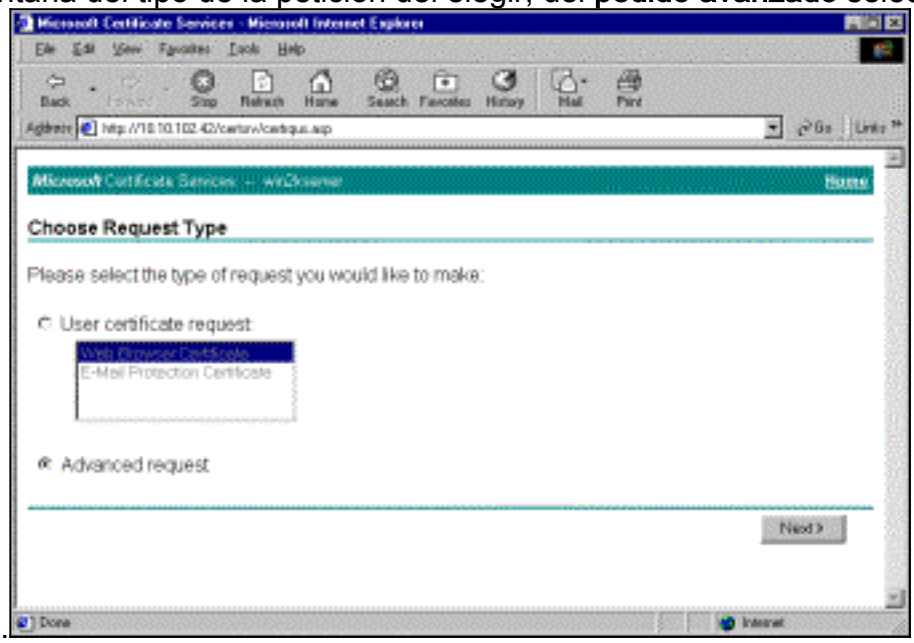
Obtenga un certificado de identidad para el cliente

Complete estos pasos para obtener un certificado de identidad para el cliente:

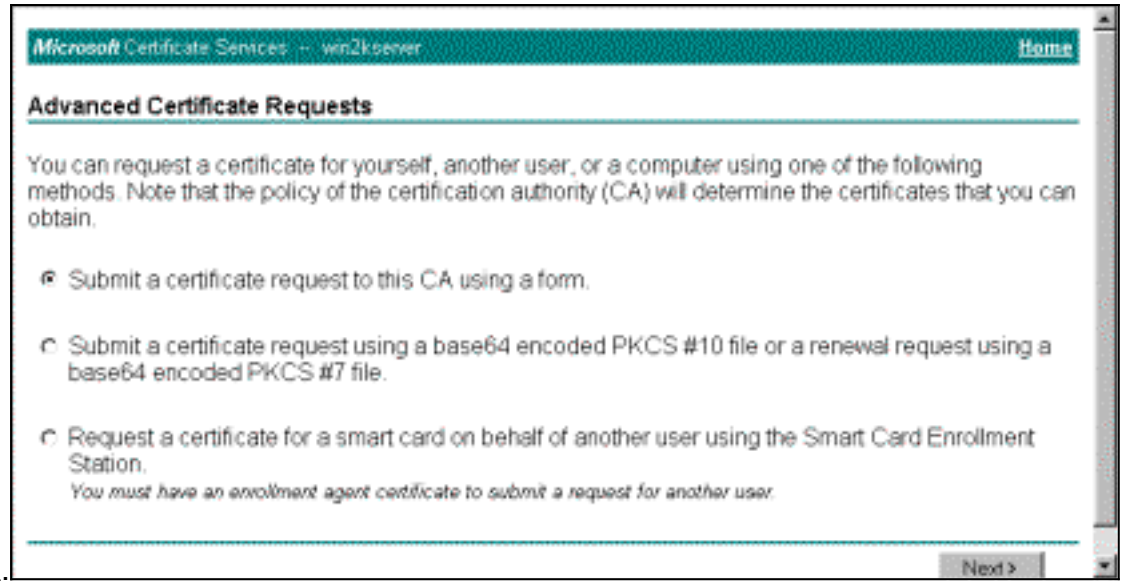
1. Abra una ventana del buscador y ingrese el URL para el Microsoft Certificate Authority (generalmente http://servername o IP Address de CA/certsrv).La ventana agradable para las recuperaciones de certificados y pide las visualizaciones.
2. De la ventana agradable, debajo seleccione una tarea, elija la **petición un certificado**, y haga clic
después.



3. De la ventana del tipo de la petición del elegir, del **pedido avanzado** selecto y del tecleo **después**.

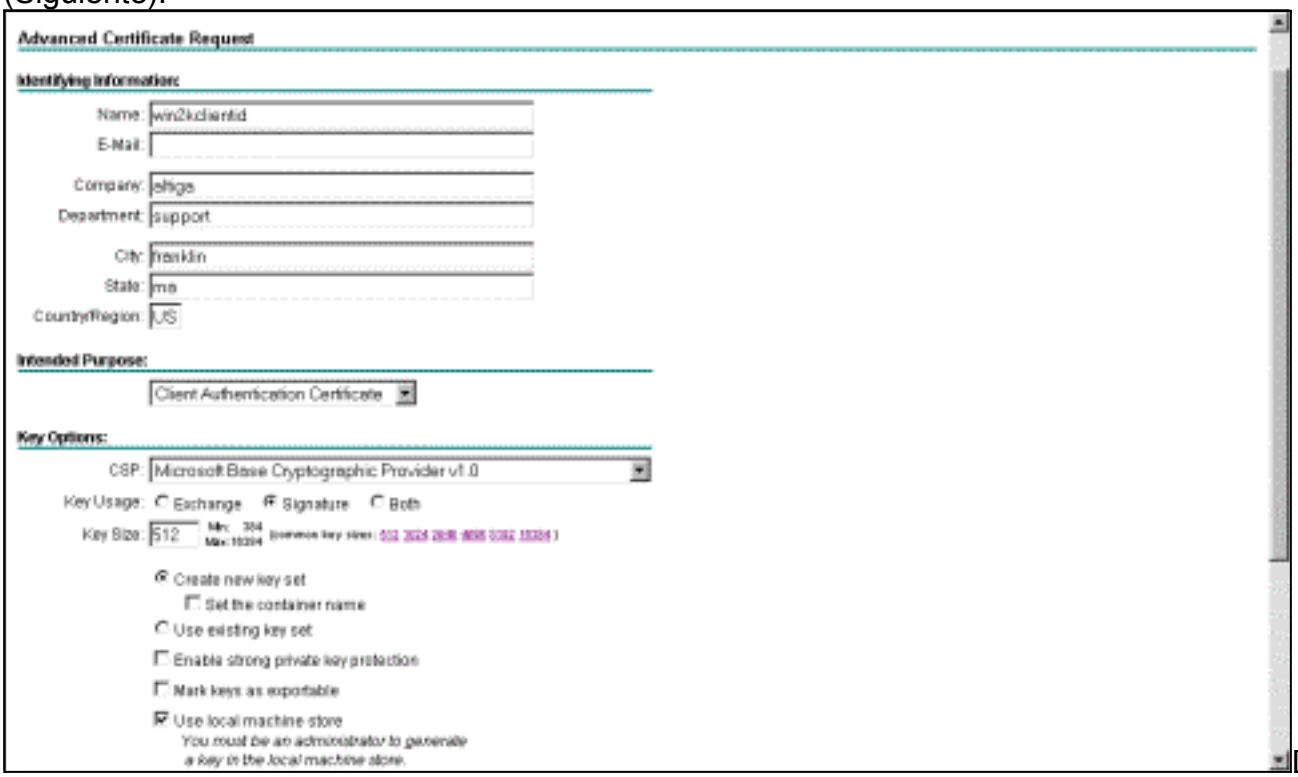


4. De la ventana avanzada de los pedidos de certificado, selecta **presente un pedido de certificado a este CA usando una**



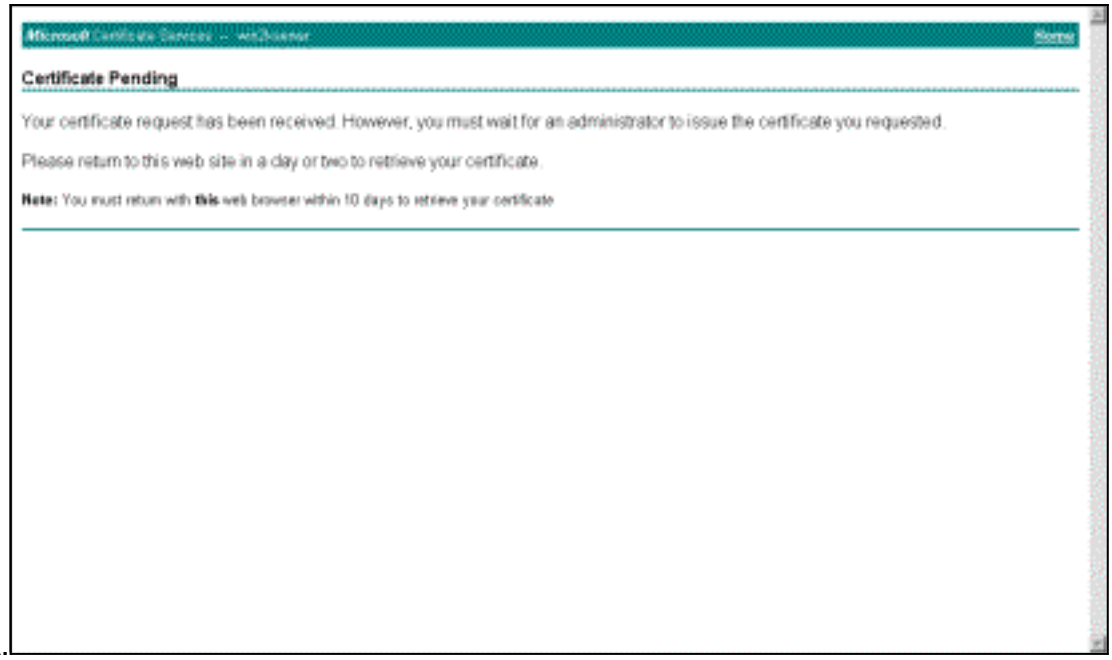
forma.

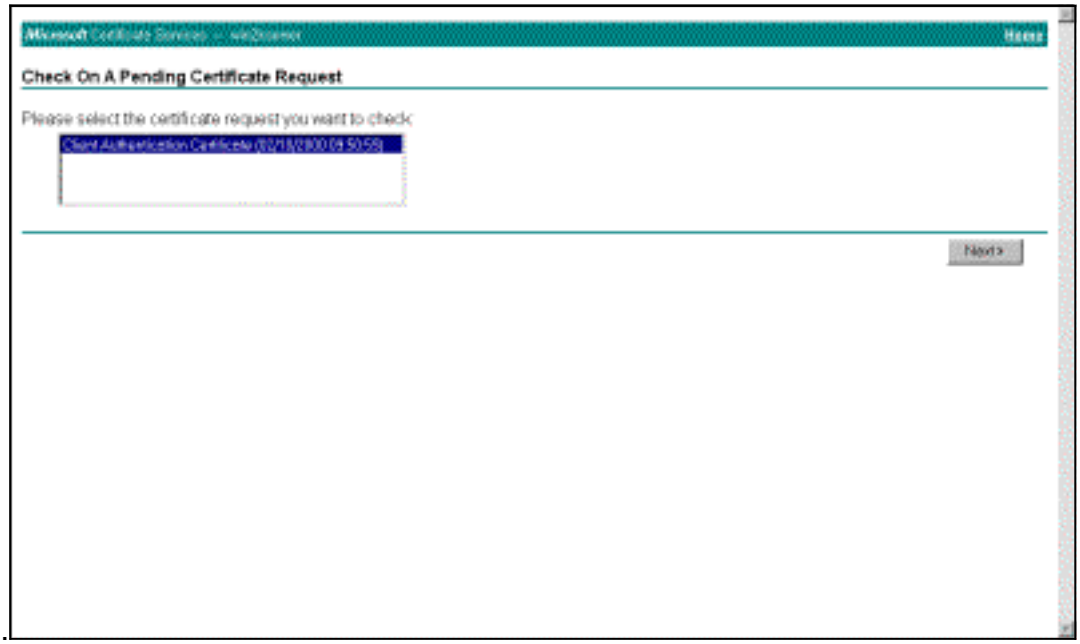
5. Complete los campos como en este ejemplo.El valor para que necesidades del departamento (unidad organizativa) hagan juego al grupo configurado en el concentrador VPN. No especifique un tamaño de clave más grande de 1024. Esté seguro de seleccionar el checkbox para el **almacenamiento de máquina local del uso**. Cuando haya finalizado, haga clic en Next
(Siguiente).

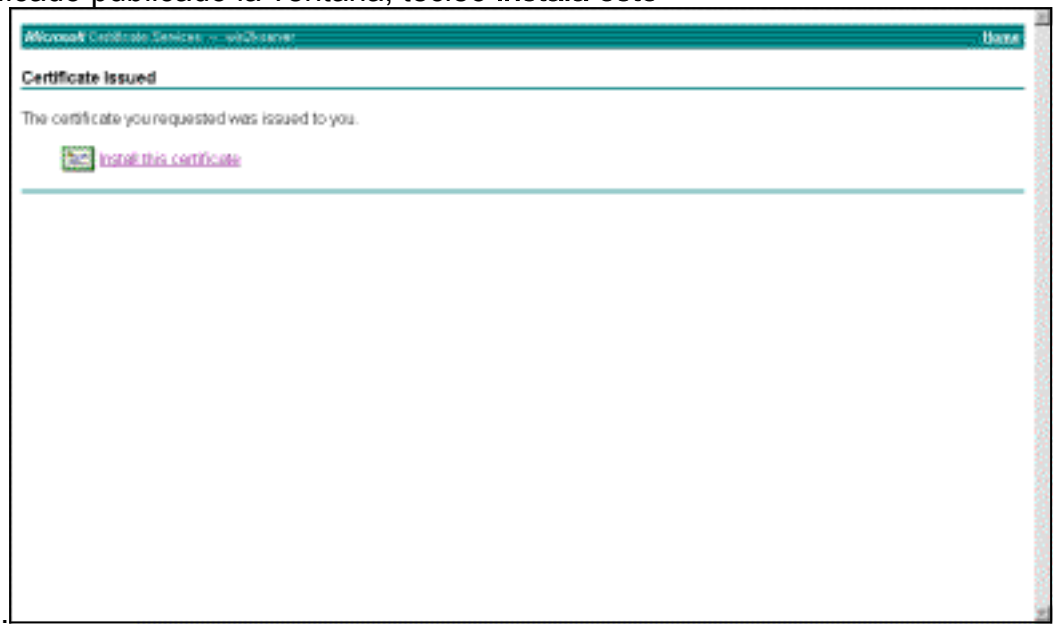


D

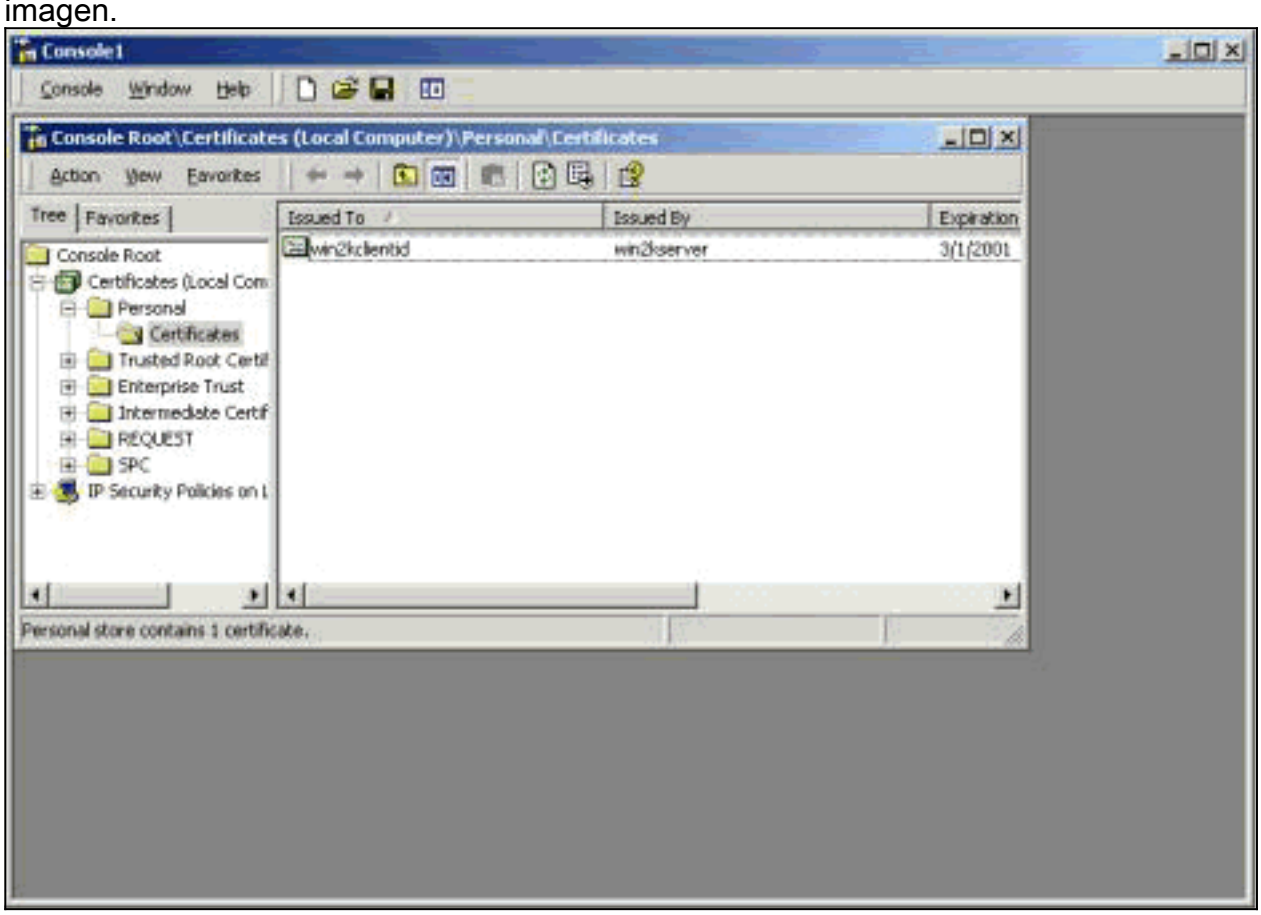
e acuerdo con cómo se configura el servidor de CA, esta ventana aparece a veces. Si hace, entrar en contacto al administrador de

CA. 

6. **Hogar del** tecleo a volver a la pantalla principal, **control** selecto **en el certificado pendiente**, y a hacer clic **después**. 

7. En el certificado publicado la ventana, tecleo **instala este certificado**. 

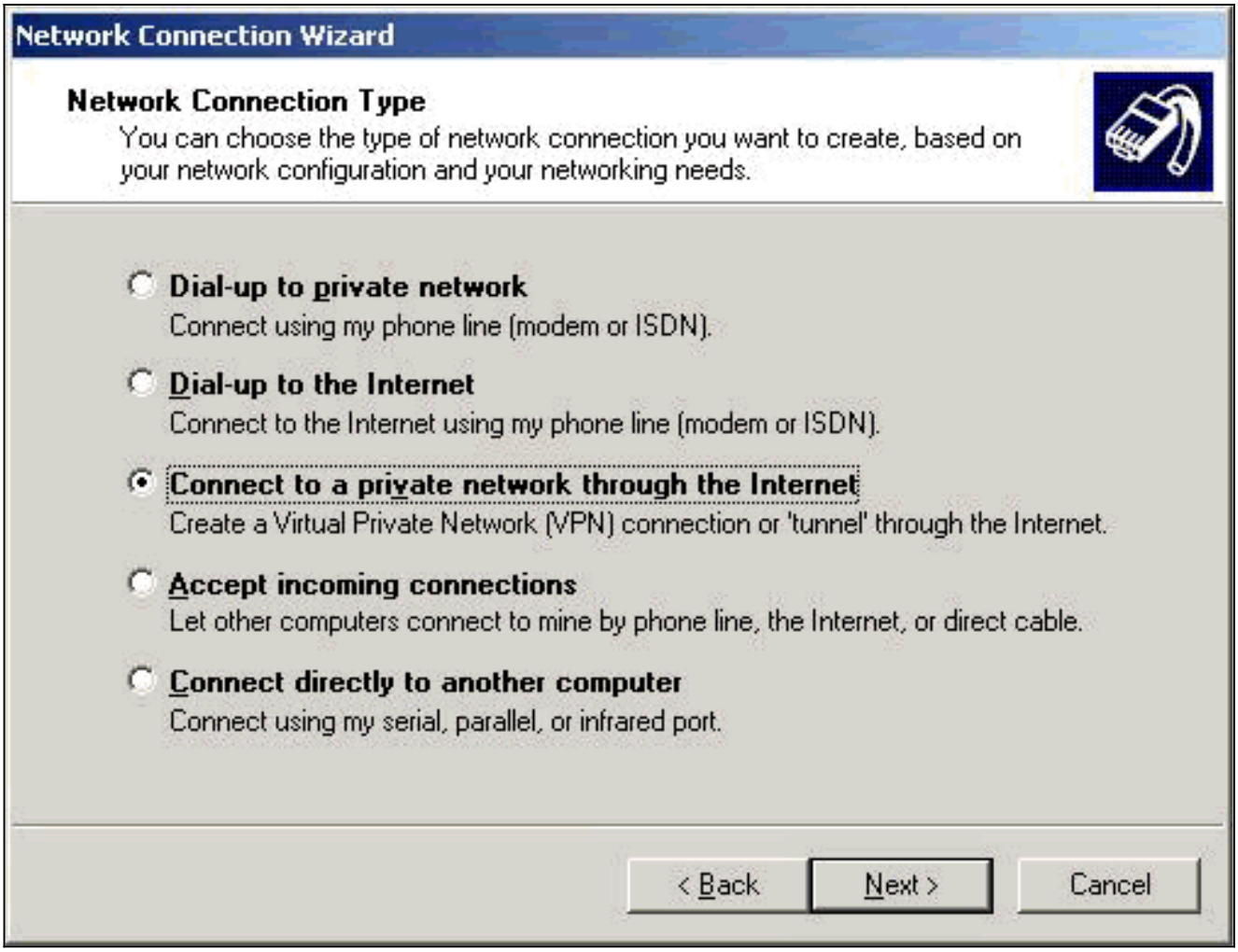
8. Para ver su certificado del cliente, seleccione el **Start (Inicio) > Run (Ejecutar)**, y realice el Microsoft Management Console (MMC).
9. Haga clic la **consola** y elija **agregan/quitan Broche-en**.
10. El tecleo **agrega** y elige el **certificado de la** lista.
11. Cuando aparece una ventana que le pide el alcance del certificado, elija la **cuenta de la Computadora**.
12. Verifique que el certificado del servidor de CA esté situado bajo Trusted Root Certification Authority. También verifique que usted tenga un certificado seleccionando la **Raíz de la consola** > el **certificado (computadora local) > personal** > los **Certificados**, tal y como se muestra en de esta
imagen.



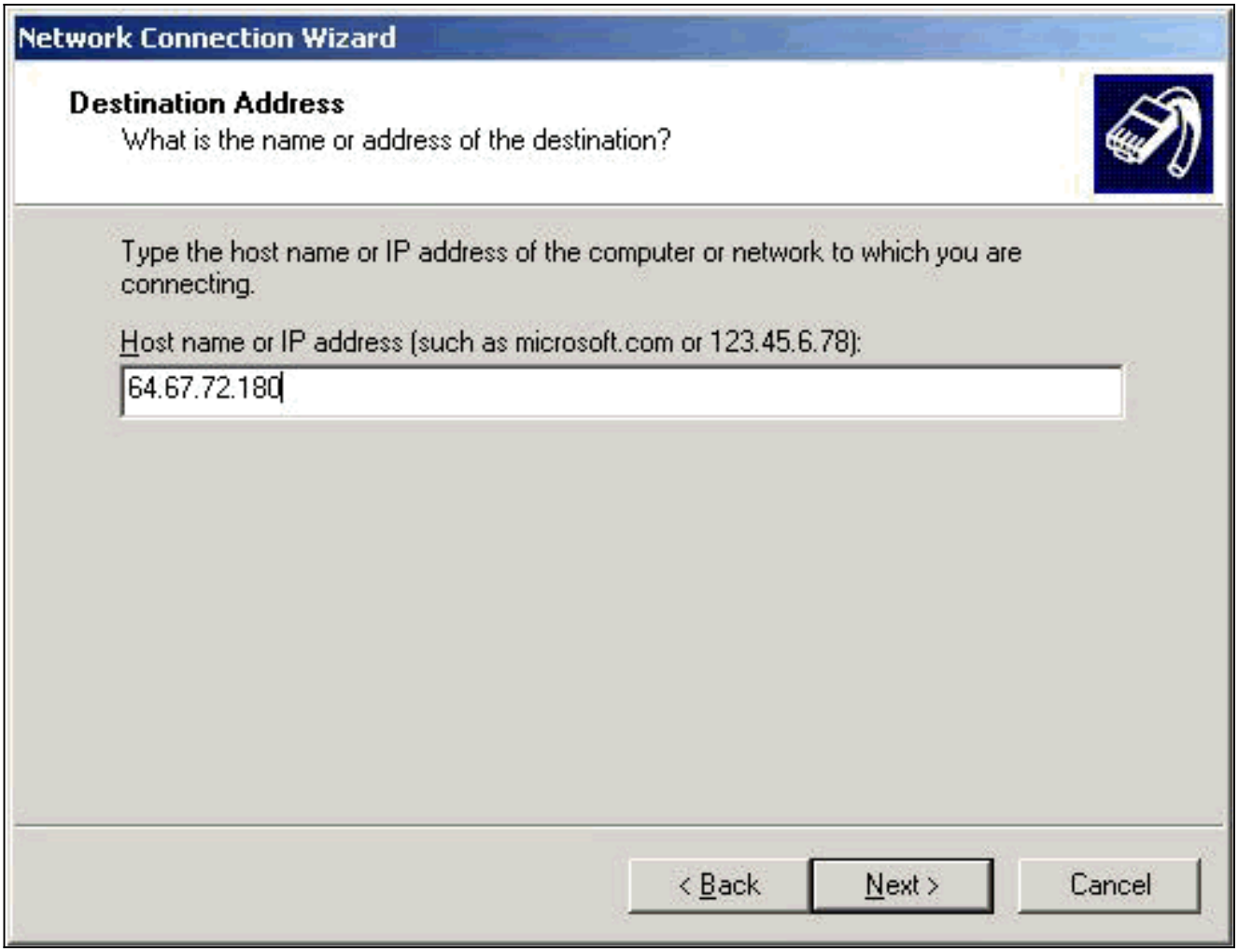
Cree una conexión al VPN 3000 usando el asistente de conexión de red

Complete este procedimiento para crear una conexión al VPN 3000 con la ayuda del asistente de conexión de red:

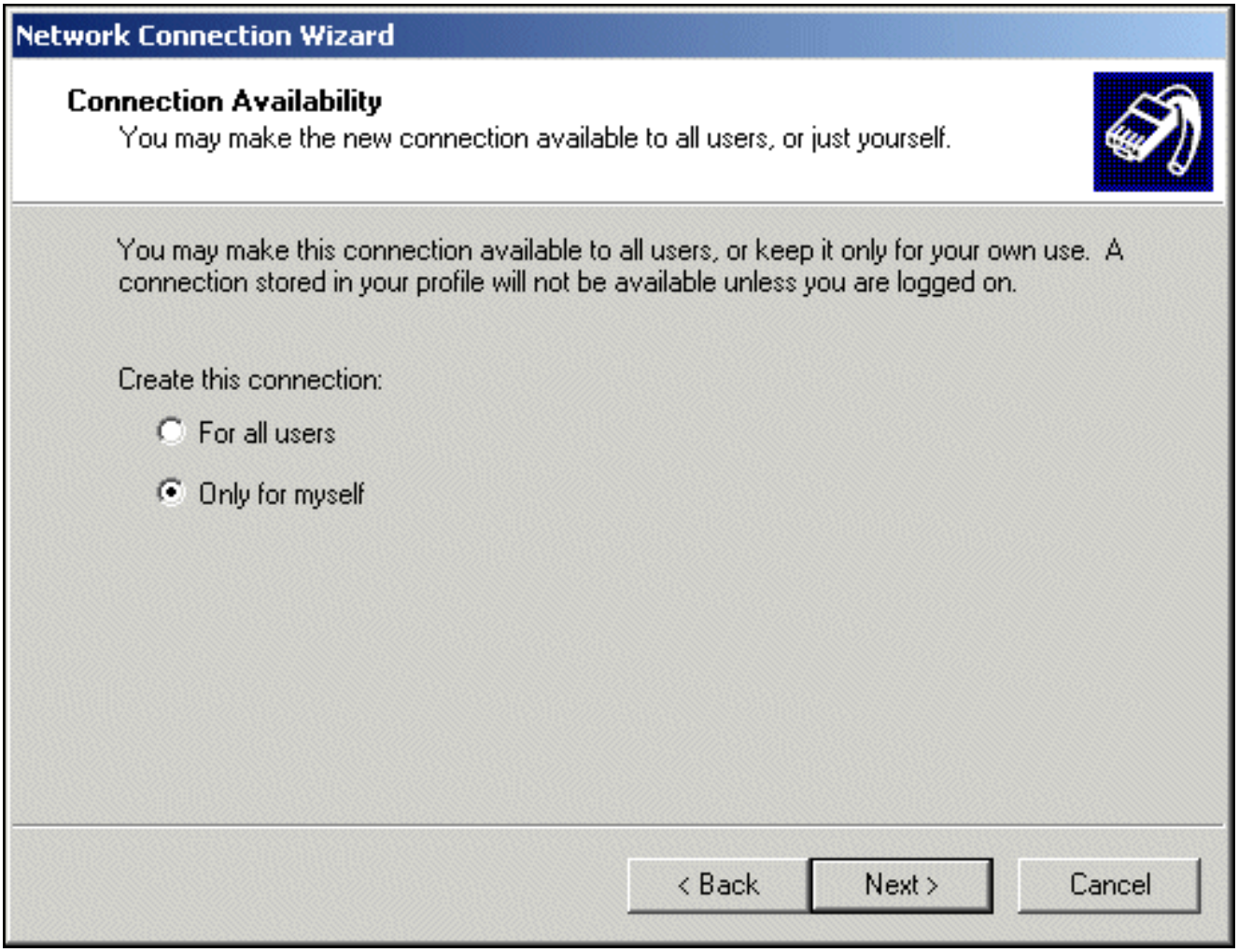
1. El click derecho **My Network Places**, elige las **propiedades** y hace clic el **Make New Connection**.
2. De la ventana del tipo de conexión de red, elija **conectan con una red privada a través de Internet** y después hacen clic
después.



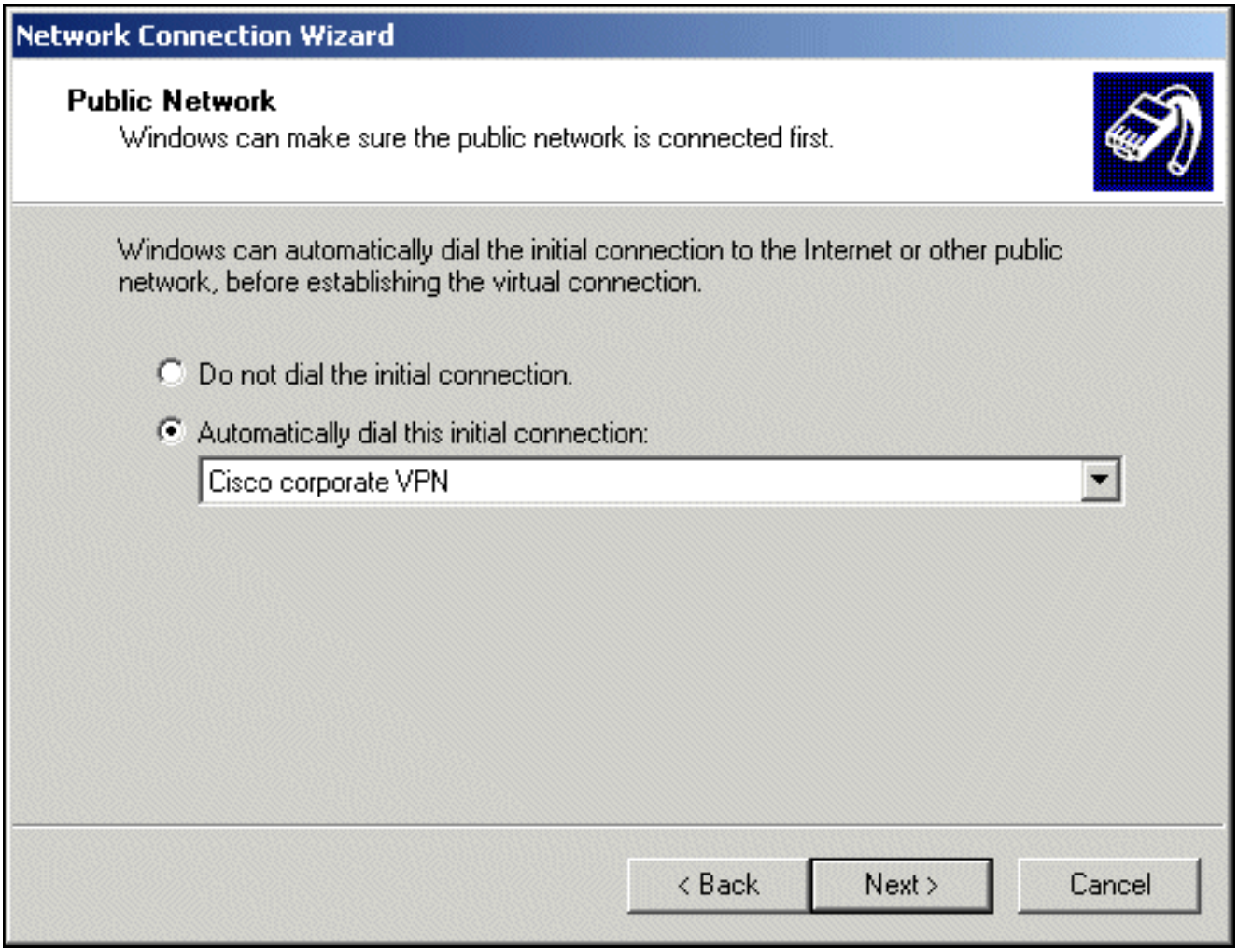
3. Ingrese el nombre del host o el IP Address de la interfaz pública del concentrador VPN, y haga clic
después.



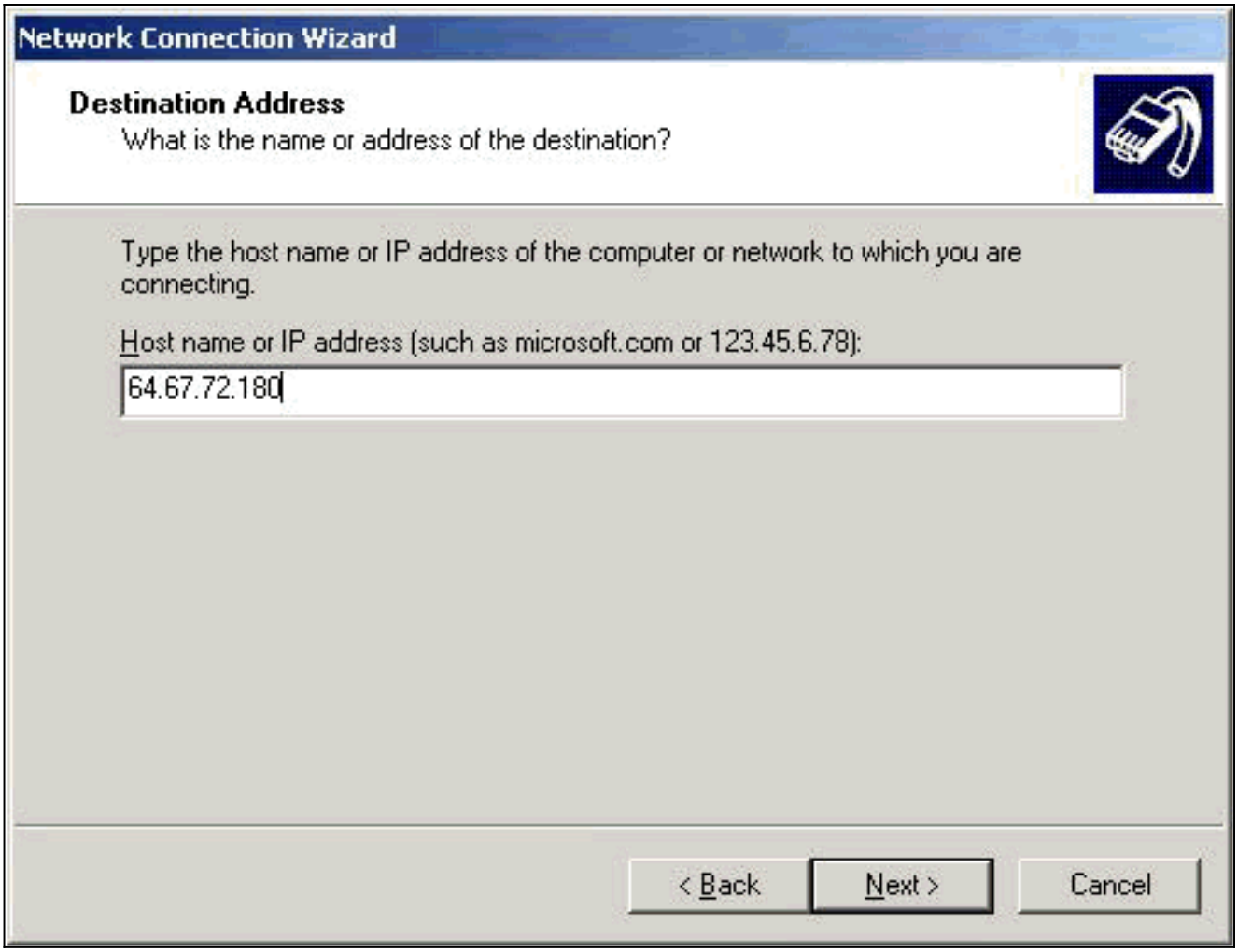
4. En de la ventana de la conexión la Disponibilidad, seleccione **solamente para mí mismo** y haga clic
después.



5. En la ventana de la red pública, seleccione si marcar la conexión inicial (la cuenta ISP) automáticamente.

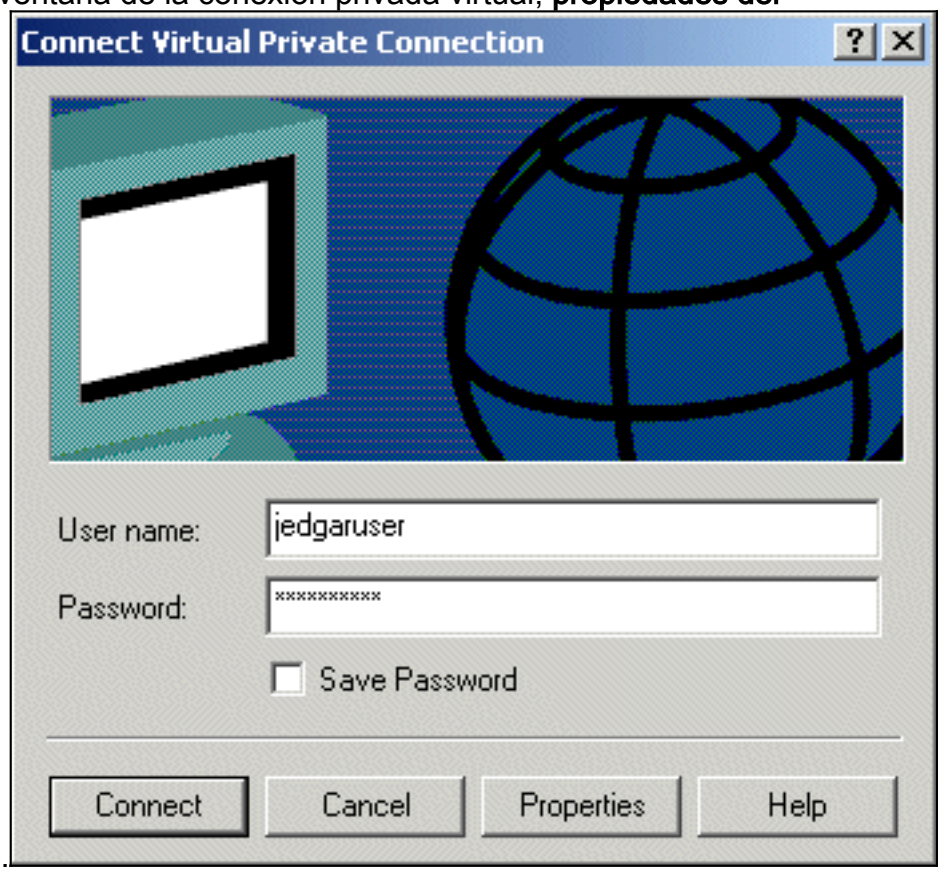


6. En la pantalla de la dirección destino, ingrese el nombre del host o el IP Address del concentrador VPN 3000, y haga clic
después.



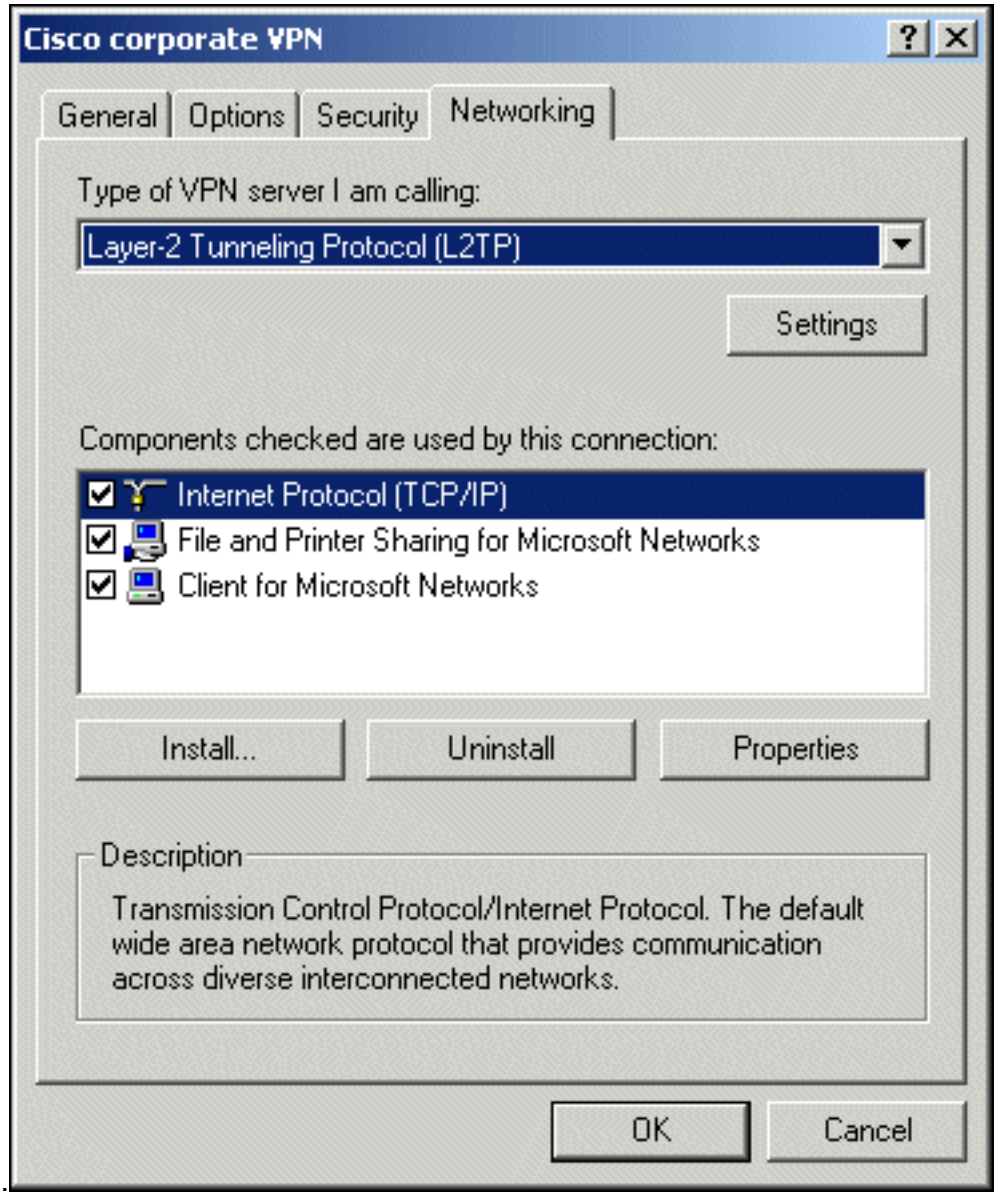
7. En la ventana del asistente de conexión de red, ingrese un nombre para la conexión y haga clic el **final**.En este ejemplo, la conexión se nombra “Cisco VPN corporativo.”

8. En la ventana de la conexión privada virtual, **propiedades del**



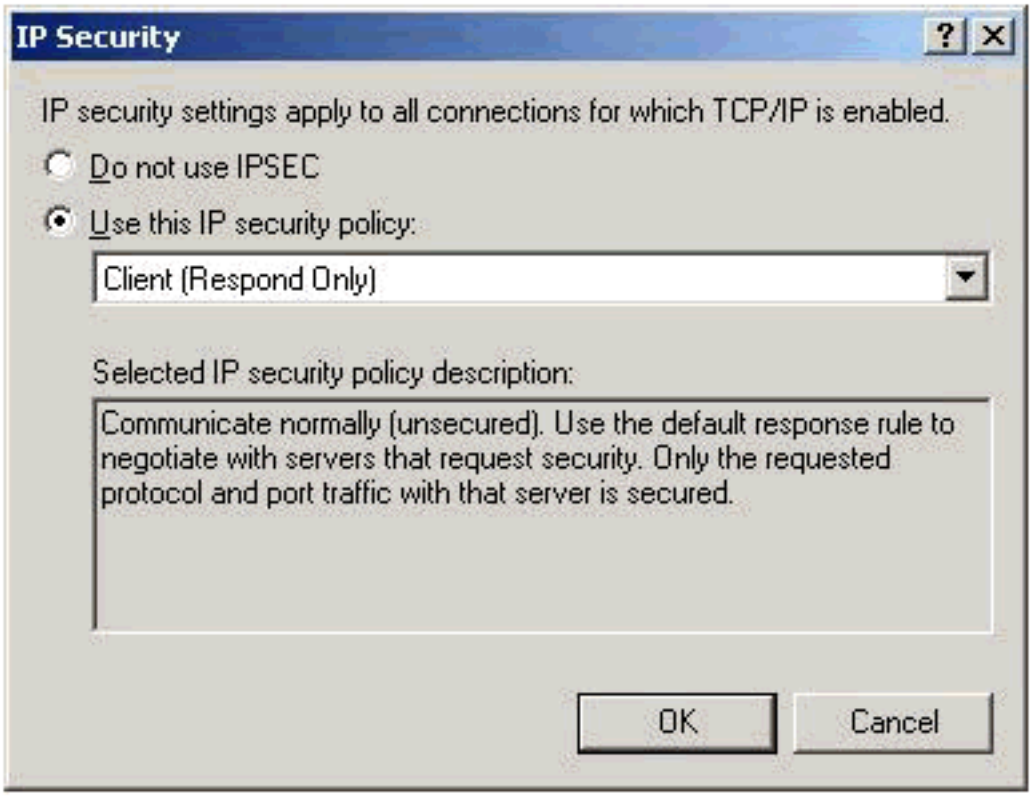
tecleo.

9. En la ventana de pPropiedades, seleccione la ficha de interconexión de redes.
10. Bajo el tipo de servidor VPN que estoy llamando, que elija el **L2TP del** menú desplegable, que resalte el **protocolo de Internet TCP/IP**, y que haga clic las



propiedades.

11. Seleccione el **Advanced (Avanzada) > Options (Opciones) > Properties (Propiedades)**
12. En la ventana de la seguridad IP, elija el **uso esta directiva de seguridad**



IP.

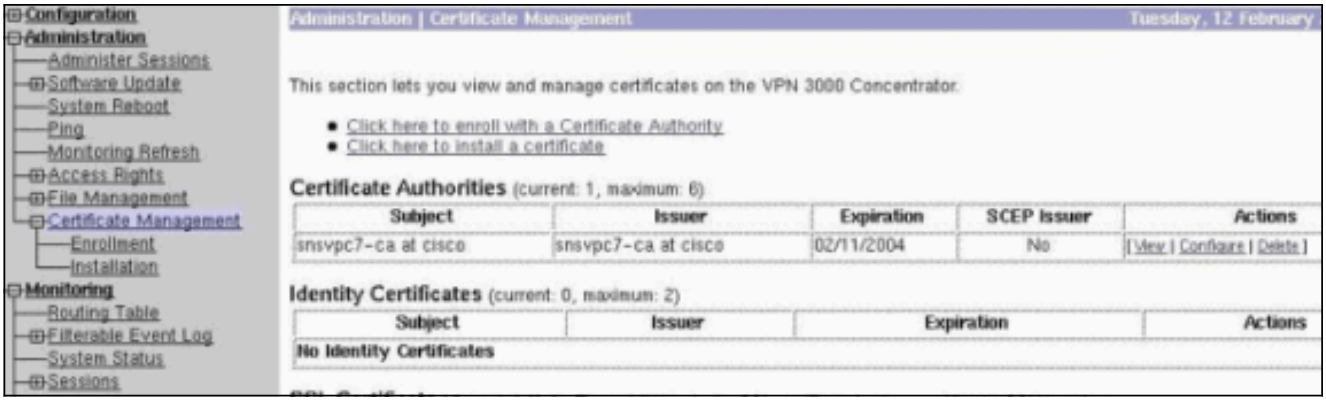
13. Elija la directiva del **cliente (responda solamente) del** menú desplegable, y haga clic la **AUTORIZACIÓN** varias veces hasta que usted vuelva a la pantalla de la conexión.
14. Para iniciar una conexión, ingresar su nombre de usuario y contraseña, y el tecleo **conecta**.

Configurar el concentrador VPN 3000

Obtenga un certificado raíz

Complete estos pasos para obtener un certificado raíz para el concentrador VPN 3000:

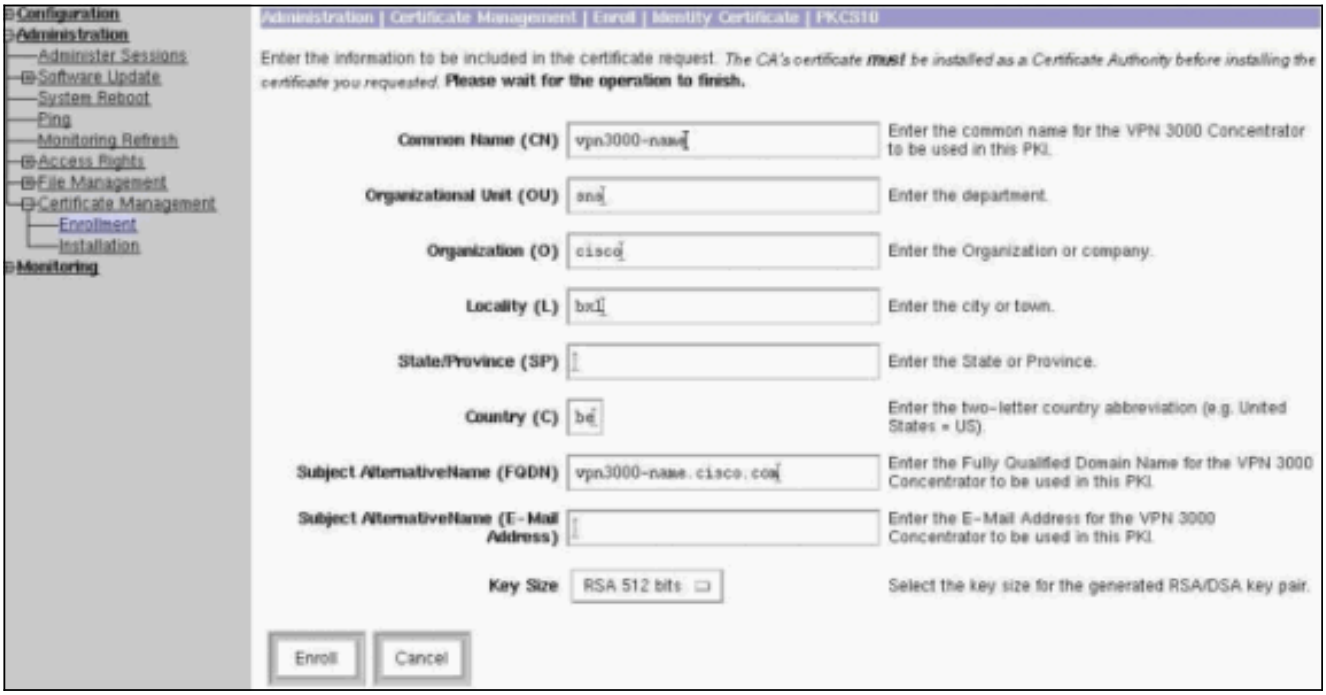
1. Señale a su navegador a su CA (generalmente algo tal como http://ip_add_of_ca/certsrv/), **extrae el certificado de CA o el Lista de revocación de certificados (CRL)**, y hace clic **después**.
2. Haga clic el **certificado de CA de la descarga** y salve el archivo en alguna parte en su disco local.
3. En el concentrador VPN 3000, el **Administration (Administración) > Certificate Management (Administración de certificados)** selecto, y el tecleo **hacen clic aquí para instalar un certificado** y **para instalar el certificado de CA**.
4. **Archivo de la carga del** tecleo del **puesto de trabajo**.
5. Haga clic **hojean** y seleccionan el archivo del certificado de CA que usted acaba de descargar.
6. Resalte el nombre de fichero y el tecleo **instala**.



Obtenga un certificado de identidad para el concentrador VPN 3000

Complete estos pasos para obtener un certificado de identidad para el concentrador VPN 3000:

1. **El Certificate Management (Administración de certificados)** selecto de **ConfAdministration > alista > certificado de identidad**, después hace clic **alista vía la petición PKCS10 (manual)**. Rellene el impreso como se muestra aquí y el tecleo **alista**.



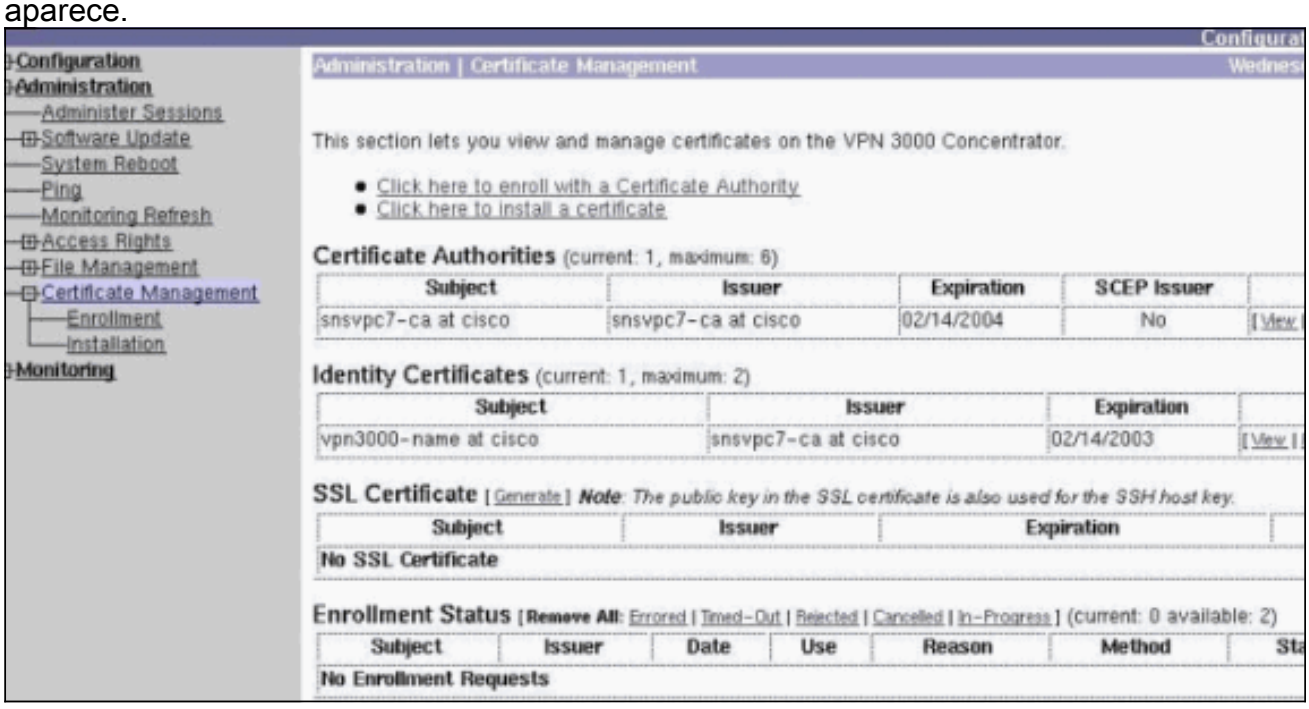
   Una ventana del buscador surge con el pedido de certificado. Necesita contener el texto similar a esta salida:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBPDCB5wIBADBQMRUwEwYDVQQDEwx2cG4zMDAwLW5hbWUxDDAKBgNVBAsTA3Nu
czEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAcTA2J4bDELMAkGA1UEBhMCYmUwWjAN
BgkqhkiG9w0BAQEFAANJADBGAkEAx7K+pvE004qILNNw3kPVWXrdlqZV4yeOIPdh
C8/V5Yuqq5tMWY3L1W6DC0p256bvGqzd5fhqSkOhBVnNJ1Y/KQIBA6A0MDIGCSqG
SIb3DQEJDjElMCMwIQYDVR0RBBowGIIWdnBuMzAwMC1uYW1lLmNpc2NvLmNvbTAN
BgkqhkiG9w0BAQQFAANBABzcG3IKaWnDLFtrNf1QDi+D7w8dxPu74b/BRHn9fsKI
X6+X0ed0EuEgm1/2nfj8Ux0nV5F/c5wukUfysMmJ/ak=
-----END NEW CERTIFICATE REQUEST-----
```

2. Señale a su navegador a su servidor de CA, marque la **petición un certificado**, y haga clic **después**.
3. Marque el **pedido avanzado**, haga clic **después**, y 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**.

4. Haga clic en Next (Siguiente). Corte y pegar el texto del pedido de certificado mostrado previamente en la área de texto. Haga clic en Submit (Enviar).
5. De acuerdo con cómo se configura el servidor de CA, usted puede hacer clic el **certificado de CA de la descarga**. O como pronto el certificado ha sido publicado por CA, vuelva a su servidor de CA y marque el **control en un certificado pendiente**.
6. Haga clic **siguiente**, seleccione su petición, y haga clic **después** otra vez.
7. Haga clic el **certificado de CA de la descarga**, y salve el archivo en el disco local.
8. En el concentrador VPN 3000, el **Administration (Administración) > Certificate Management (Administración de certificados) > Install (Instalar)** selecto**,** y el tecleo **instalan el certificado obtenido vía la inscripción**.Usted entonces ve su petición pendiente con un estatus de “en curso,” como en esta
imagen.

9. El tecleo **instala**, seguido por el **archivo de la carga del puesto de trabajo**.
10. Haga clic **hojean** y seleccionan el archivo que contiene su certificado publicado por CA.
11. Resalte el nombre de fichero y el tecleo **instala**.
12. Seleccione el **Administration (Administración) > Certificate Management (Administración de certificados)**. Una pantalla similar a esta imagen
aparece.



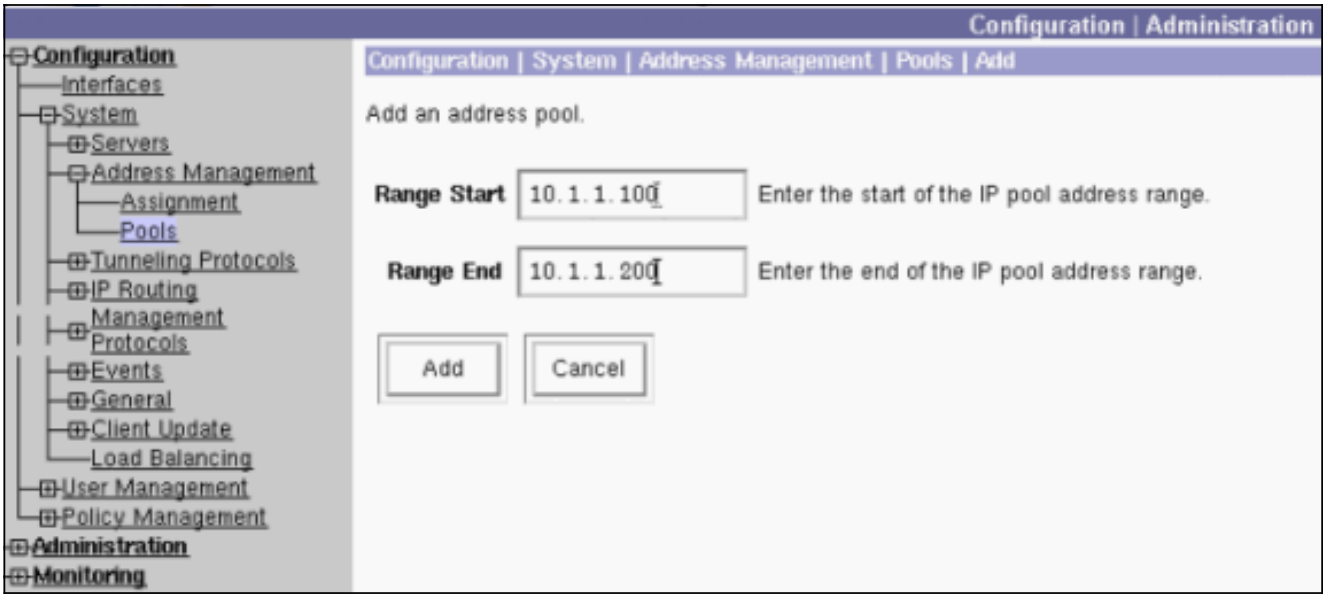
Configure un pool para los clientes

Complete este procedimiento para configurar un pool para los clientes:

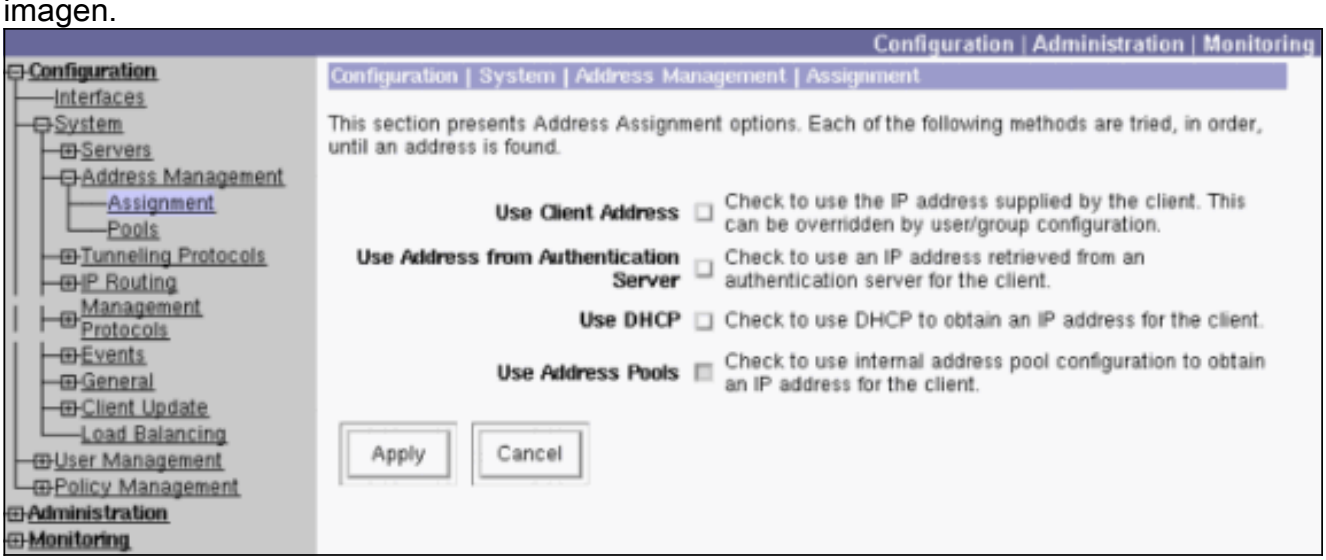
1. Para asignar un rango disponible de los IP Addresses, señale a un navegador a la interfaz interior del concentrador VPN 3000 y seleccione el **Configuration (Configuración) > System**

(Sistema) > Address Management (Administración de direcciones) > Pools (Agrupaciones) > Add (Agregar).

2. Especifique un rango de los IP Addresses que no están en conflicto con ninguna otros dispositivos en la red interna, y del haga click en Add



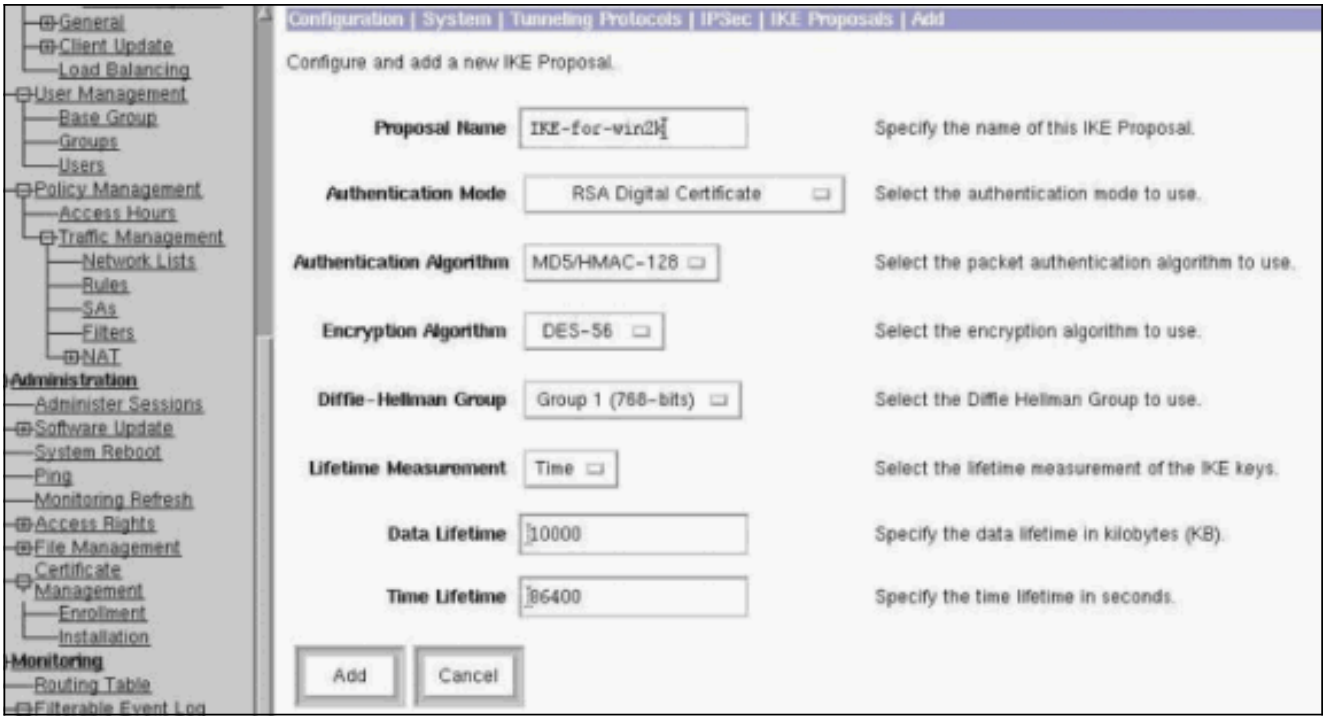
3. Para decir el concentrador VPN 3000 para utilizar el pool, el **Configuration (Configuración) > System (Sistema) > Address Management (Administración de direcciones) > Assigment (Asignación)** selecto, para marcar el cuadro de las **agrupaciones de direcciones del uso**, y el tecleo **se aplican**, como en esta imagen.



Configure una propuesta IKE

Complete estos pasos para configurar una propuesta IKE:

1. Seleccione el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE)**, tecleo **agregan** y seleccionan los parámetros, tal y como se muestra en de esta imagen.



2. El tecleo **agrega**, resalta la nueva oferta en la columna derecha, y el tecleo **activa**.

Configure el SA

Complete este procedimiento para configurar la asociación de seguridad (SA):

1. Seleccione el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > el SA** y haga clic el **ESP-L2TP-TRANSPORT**.Si este SA no está disponible o si usted lo utiliza para un cierto otro propósito, cree un nuevo SA similar éste. Diversas configuraciones para el SA son aceptables. Cambie este parámetro basado en su política de seguridad.
2. Seleccione el certificado digital que usted ha configurado previamente bajo menú desplegable del **certificado digital**. Seleccione la oferta del Internet Key Exchange (IKE) **IKE-for-win2k**.**Nota:** Esto no es obligatorio. Cuando el cliente del L2TP/IPSec conecta con el concentrador VPN, todas las propuestas IKE configuradas conforme a la columna activa del **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > IKE Proposals (Propuestas IKE) de la** página se intentan en la orden.Esta imagen muestra la configuración necesaria para el SA:

Configure el grupo y al usuario

Complete este procedimiento para configurar el grupo y al usuario:

1. Seleccione el **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)**.
2. Conforme a la ficha general, aseegurese que el **L2TP sobre el IPSec** está marcado.
3. Bajo lengueta del IPSec, seleccione **ESP-L2TP-TRANSPORT** SA.
4. Bajo lengueta PPTP/L2TP, desmarque todas las **opciones de encripción L2TP**.
5. Seleccione **configuration > user management > Users** y haga click en Add
6. Ingrese el nombre y la contraseña que usted utiliza para conectar de su cliente del Windows 2000. Aseegurese que usted selecciona al **grupo base** bajo Group Selection (Selección de grupos).
7. Conforme a la ficha general, marque el **L2TP sobre tunelización de IPSec el** protocolo.
8. Bajo lengueta del IPSec, seleccione **ESP-L2TP-TRANSPORT** SA.
9. Bajo lengueta PPTP/L2TP, desmarque todas las **opciones de encripción L2TP**, y el haga click en AddUsted puede ahora conectar con la ayuda del cliente del Windows 2000 del L2TP/IPSec.**Nota:** Usted ha elegido configurar al grupo base para validar la conexión remota del L2TP/IPSec. Es también posible configurar a un grupo que haga juego el campo del organization unit (OU) del SA para validar la conexión entrante. La configuración es idéntica.

Información acerca de la depuración

```
269 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3868 10.48.66.76
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7
```

```
271 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3869 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

274 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3870 10.48.66.76
Proposal # 1, Transform # 2, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

279 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3871 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

282 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3872 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

285 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3873 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

288 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3874 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

291 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3875 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

294 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3876 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

297 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3877 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

300 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3878 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

303 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3879 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

306 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3880 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

309 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3881 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

312 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3882 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

315 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3883 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

318 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3884 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 7

321 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3885 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 2
    Cfg'd: Oakley Group 1

324 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3886 10.48.66.76
Proposal # 1, Transform # 3, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

329 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3887 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

332 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3888 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

335 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3889 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
```

```
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

338 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3890 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

341 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3891 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

344 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3892 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

347 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3893 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

350 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3894 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

353 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3895 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

356 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3896 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

358 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3897 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

361 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3898 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

364 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3899 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

367 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3900 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

370 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3901 10.48.66.76
  Phase 1 failure against global IKE proposal # 16:
  Mismatched attr types for class Hash Alg:
    Rcv'd: SHA
    Cfg'd: MD5

372 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3902 10.48.66.76
Proposal # 1, Transform # 4, Type ISAKMP, Id IKE
Parsing received transform:
  Phase 1 failure against global IKE proposal # 1:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

377 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3903 10.48.66.76
  Phase 1 failure against global IKE proposal # 2:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

380 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3904 10.48.66.76
  Phase 1 failure against global IKE proposal # 3:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

383 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3905 10.48.66.76
  Phase 1 failure against global IKE proposal # 4:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

386 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3906 10.48.66.76
  Phase 1 failure against global IKE proposal # 5:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

389 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3907 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

392 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3908 10.48.66.76
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

395 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3909 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

398 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3910 10.48.66.76
  Phase 1 failure against global IKE proposal # 9:
  Mismatched attr types for class DH Group:
```

```
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

401 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3911 10.48.66.76
  Phase 1 failure against global IKE proposal # 10:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

404 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3912 10.48.66.76
  Phase 1 failure against global IKE proposal # 11:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

407 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3913 10.48.66.76
  Phase 1 failure against global IKE proposal # 12:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

410 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3914 10.48.66.76
  Phase 1 failure against global IKE proposal # 13:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

413 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3915 10.48.66.76
  Phase 1 failure against global IKE proposal # 14:
  Mismatched attr types for class Encryption Alg:
    Rcv'd: DES-CBC
    Cfg'd: Triple-DES

416 02/15/2002 12:47:24.430 SEV=8 IKEDBG/0 RPT=3916 10.48.66.76
  Phase 1 failure against global IKE proposal # 15:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

419 02/15/2002 12:47:24.430 SEV=7 IKEDBG/28 RPT=20 10.48.66.76
IKE SA Proposal # 1, Transform # 4 acceptable
Matches global IKE entry # 16

420 02/15/2002 12:47:24.440 SEV=9 IKEDBG/0 RPT=3917 10.48.66.76
constructing ISA_SA for isakmp

421 02/15/2002 12:47:24.490 SEV=8 IKEDBG/0 RPT=3918 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + SA (1) + NONE (0) ... total length : 80

423 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3919 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

425 02/15/2002 12:47:24.540 SEV=8 IKEDBG/0 RPT=3920 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + NONE (0) ... total length : 152

427 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3921 10.48.66.76
processing ke payload

428 02/15/2002 12:47:24.540 SEV=9 IKEDBG/0 RPT=3922 10.48.66.76
processing ISA_KE
```

```
429 02/15/2002 12:47:24.540 SEV=9 IKEDBG/1 RPT=104 10.48.66.76
processing nonce payload

430 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3923 10.48.66.76
constructing ke payload

431 02/15/2002 12:47:24.600 SEV=9 IKEDBG/1 RPT=105 10.48.66.76
constructing nonce payload

432 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3924 10.48.66.76
constructing certreq payload

433 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3925 10.48.66.76
Using initiator's certreq payload data

434 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=61 10.48.66.76
constructing Cisco Unity VID payload

435 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=62 10.48.66.76
constructing xauth V6 VID payload

436 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=39 10.48.66.76
Send IOS VID

437 02/15/2002 12:47:24.600 SEV=9 IKEDBG/38 RPT=20 10.48.66.76
Constructing VPN 3000 spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 20000001)

439 02/15/2002 12:47:24.600 SEV=9 IKEDBG/46 RPT=63 10.48.66.76
constructing VID payload

440 02/15/2002 12:47:24.600 SEV=9 IKEDBG/48 RPT=40 10.48.66.76
Send Altiga GW VID

441 02/15/2002 12:47:24.600 SEV=9 IKEDBG/0 RPT=3926 10.48.66.76
Generating keys for Responder...

442 02/15/2002 12:47:24.610 SEV=8 IKEDBG/0 RPT=3927 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + KE (4) + NONCE (10) + CERT_REQ (7) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + VENDOR (13) + NONE (0) ... total length : 229

445 02/15/2002 12:47:24.640 SEV=8 IKEDBG/0 RPT=3928 10.48.66.76
RECEIVED Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + CERT_REQ (7) + NONE (0)
... total length : 1186

448 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=106 10.48.66.76
Processing ID

449 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3929 10.48.66.76
processing cert payload

450 02/15/2002 12:47:24.640 SEV=9 IKEDBG/1 RPT=107 10.48.66.76
processing RSA signature

451 02/15/2002 12:47:24.640 SEV=9 IKEDBG/0 RPT=3930 10.48.66.76
computing hash

452 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3931 10.48.66.76
processing cert request payload

453 02/15/2002 12:47:24.650 SEV=9 IKEDBG/0 RPT=3932 10.48.66.76
Storing cert request payload for use in MM msg 4
```

```
454 02/15/2002 12:47:24.650 SEV=9 IKEDBG/23 RPT=20 10.48.66.76
Starting group lookup for peer 10.48.66.76

455 02/15/2002 12:47:24.650 SEV=9 IKE/21 RPT=12 10.48.66.76
No Group found by matching IP Address of Cert peer 10.48.66.76

456 02/15/2002 12:47:24.650 SEV=9 IKE/20 RPT=12 10.48.66.76
No Group found by matching OU(s) from ID payload:
 ou=sns,

457 02/15/2002 12:47:24.650 SEV=9 IKE/0 RPT=12 10.48.66.76
Group [VPNC_Base_Group]
No Group name for IKE Cert session, defaulting to BASE GROUP

459 02/15/2002 12:47:24.750 SEV=7 IKEDBG/0 RPT=3933 10.48.66.76
Group [VPNC_Base_Group]
Found Phase 1 Group (VPNC_Base_Group)

460 02/15/2002 12:47:24.750 SEV=7 IKEDBG/14 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
Authentication configured for Internal

461 02/15/2002 12:47:24.750 SEV=9 IKEDBG/19 RPT=20 10.48.66.76
Group [VPNC_Base_Group]
IKEGetUserAttributes: default domain = fenetwork.com

462 02/15/2002 12:47:24.770 SEV=5 IKE/79 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Validation of certificate successful
(CN=my_name, SN=6102861F000000000005)

464 02/15/2002 12:47:24.770 SEV=7 IKEDBG/0 RPT=3934 10.48.66.76
Group [VPNC_Base_Group]
peer ID type 9 received (DER_ASN1_DN)

465 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=108 10.48.66.76
Group [VPNC_Base_Group]
constructing ID

466 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3935 10.48.66.76
Group [VPNC_Base_Group]
constructing cert payload

467 02/15/2002 12:47:24.770 SEV=9 IKEDBG/1 RPT=109 10.48.66.76
Group [VPNC_Base_Group]
constructing RSA signature

468 02/15/2002 12:47:24.770 SEV=9 IKEDBG/0 RPT=3936 10.48.66.76
Group [VPNC_Base_Group]
computing hash

469 02/15/2002 12:47:24.800 SEV=9 IKEDBG/46 RPT=64 10.48.66.76
Group [VPNC_Base_Group]
constructing dpd vid payload

470 02/15/2002 12:47:24.800 SEV=8 IKEDBG/0 RPT=3937 10.48.66.76
SENDING Message (msgid=0) with payloads :
HDR + ID (5) + CERT (6) + SIG (9) + VENDOR (13) + NONE (0)
... total length : 1112

473 02/15/2002 12:47:24.800 SEV=4 IKE/119 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 1 COMPLETED
```

```
474 02/15/2002 12:47:24.800 SEV=6 IKE/121 RPT=4 10.48.66.76
Keep-alive type for this connection: None

475 02/15/2002 12:47:24.800 SEV=6 IKE/122 RPT=4 10.48.66.76
Keep-alives configured on but peer does not support keep-alives (type = None)

476 02/15/2002 12:47:24.800 SEV=7 IKEDBG/0 RPT=3938 10.48.66.76
Group [VPNC_Base_Group]
Starting phase 1 rekey timer: 21600000 (ms)

477 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3939 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 1108

480 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3940 10.48.66.76
Group [VPNC_Base_Group]
processing hash

481 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3941 10.48.66.76
Group [VPNC_Base_Group]
processing SA payload

482 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=110 10.48.66.76
Group [VPNC_Base_Group]
processing nonce payload

483 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=111 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

484 02/15/2002 12:47:24.810 SEV=5 IKE/25 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received remote Proxy Host data in ID Payload:
Address 10.48.66.76, Protocol 17, Port 1701

487 02/15/2002 12:47:24.810 SEV=9 IKEDBG/1 RPT=112 10.48.66.76
Group [VPNC_Base_Group]
Processing ID

488 02/15/2002 12:47:24.810 SEV=5 IKE/24 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Received local Proxy Host data in ID Payload:
Address 10.48.66.109, Protocol 17, Port 0

491 02/15/2002 12:47:24.810 SEV=8 IKEDBG/0 RPT=3942
QM IsRekeyed old sa not found by addr

492 02/15/2002 12:47:24.810 SEV=5 IKE/66 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IKE Remote Peer configured for SA: ESP-L2TP-TRANSPORT

493 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3943 10.48.66.76
Group [VPNC_Base_Group]
processing IPSEC SA

494 02/15/2002 12:47:24.810 SEV=7 IKEDBG/27 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
IPSec SA Proposal # 1, Transform # 1 acceptable

495 02/15/2002 12:47:24.810 SEV=7 IKEDBG/0 RPT=3944 10.48.66.76
Group [VPNC_Base_Group]
IKE: requesting SPI!
```

```
496 02/15/2002 12:47:24.810 SEV=8 IKEDBG/6 RPT=4
IKE got SPI from key engine: SPI = 0x10d19e33

497 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3945 10.48.66.76
Group [VPNC_Base_Group]
oakley constucting quick mode

498 02/15/2002 12:47:24.810 SEV=9 IKEDBG/0 RPT=3946 10.48.66.76
Group [VPNC_Base_Group]
constructing blank hash

499 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3947 10.48.66.76
Group [VPNC_Base_Group]
constructing ISA_SA for ipsec

500 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=113 10.48.66.76
Group [VPNC_Base_Group]
constructing ipsec nonce payload

501 02/15/2002 12:47:24.820 SEV=9 IKEDBG/1 RPT=114 10.48.66.76
Group [VPNC_Base_Group]
constructing proxy ID

502 02/15/2002 12:47:24.820 SEV=7 IKEDBG/0 RPT=3948 10.48.66.76
Group [VPNC_Base_Group]
Transmitting Proxy Id:
  Remote host: 10.48.66.76  Protocol 17  Port 1701
  Local host:  10.48.66.109  Protocol 17  Port 0

506 02/15/2002 12:47:24.820 SEV=9 IKEDBG/0 RPT=3949 10.48.66.76
Group [VPNC_Base_Group]
constructing qm hash

507 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3950 10.48.66.76
SENDING Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0)
... total length : 156

510 02/15/2002 12:47:24.820 SEV=8 IKEDBG/0 RPT=3951 10.48.66.76
RECEIVED Message (msgid=781ceadc) with payloads :
HDR + HASH (8) + NONE (0) ... total length : 48

512 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3952 10.48.66.76
Group [VPNC_Base_Group]
processing hash

513 02/15/2002 12:47:24.830 SEV=9 IKEDBG/0 RPT=3953 10.48.66.76
Group [VPNC_Base_Group]
loading all IPSEC SAs

514 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=115 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

515 02/15/2002 12:47:24.830 SEV=9 IKEDBG/1 RPT=116 10.48.66.76
Group [VPNC_Base_Group]
Generating Quick Mode Key!

516 02/15/2002 12:47:24.830 SEV=7 IKEDBG/0 RPT=3954 10.48.66.76
Group [VPNC_Base_Group]
Loading host:
  Dst: 10.48.66.109
  Src: 10.48.66.76
```

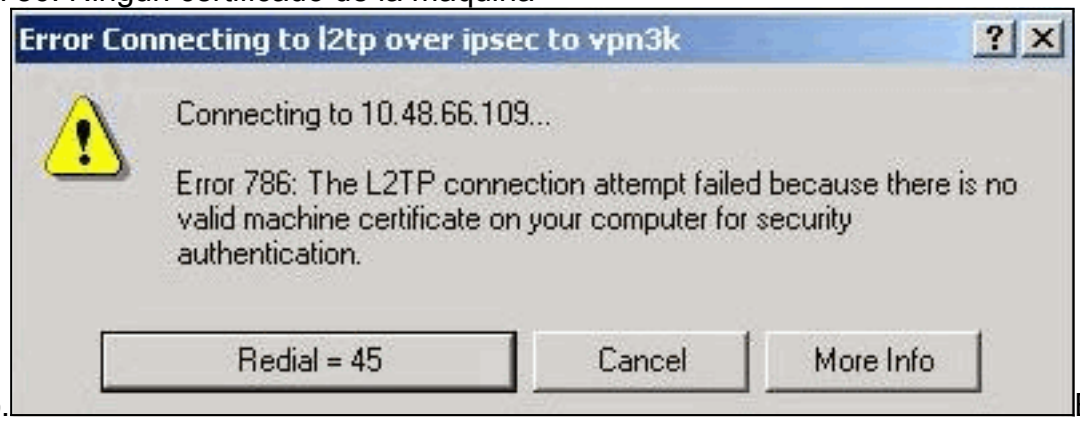
```
517 02/15/2002 12:47:24.830 SEV=4 IKE/49 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
Security negotiation complete for User ()
Responder, Inbound SPI = 0x10d19e33, Outbound SPI = 0x15895ab9

520 02/15/2002 12:47:24.830 SEV=8 IKEDBG/7 RPT=4
IKE got a KEY_ADD msg for SA: SPI = 0x15895ab9

521 02/15/2002 12:47:24.830 SEV=8 IKEDBG/0 RPT=3955
pitcher: rcv KEY_UPDATE, spi 0x10d19e33

522 02/15/2002 12:47:24.830 SEV=4 IKE/120 RPT=4 10.48.66.76
Group [VPNC_Base_Group]
PHASE 2 COMPLETED (msgid=781ceadc)

523 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3956
pitcher: recv KEY_SA_ACTIVE spi 0x10d19e33

524 02/15/2002 12:47:24.840 SEV=8 IKEDBG/0 RPT=3957
KEY_SA_ACTIVE no old rekey centry found with new spi 0x10d19e33, mess_id 0x0
```

Información del Troubleshooting

Esta sección ilustra algunos problemas comunes y los métodos de Troubleshooting para cada uno.

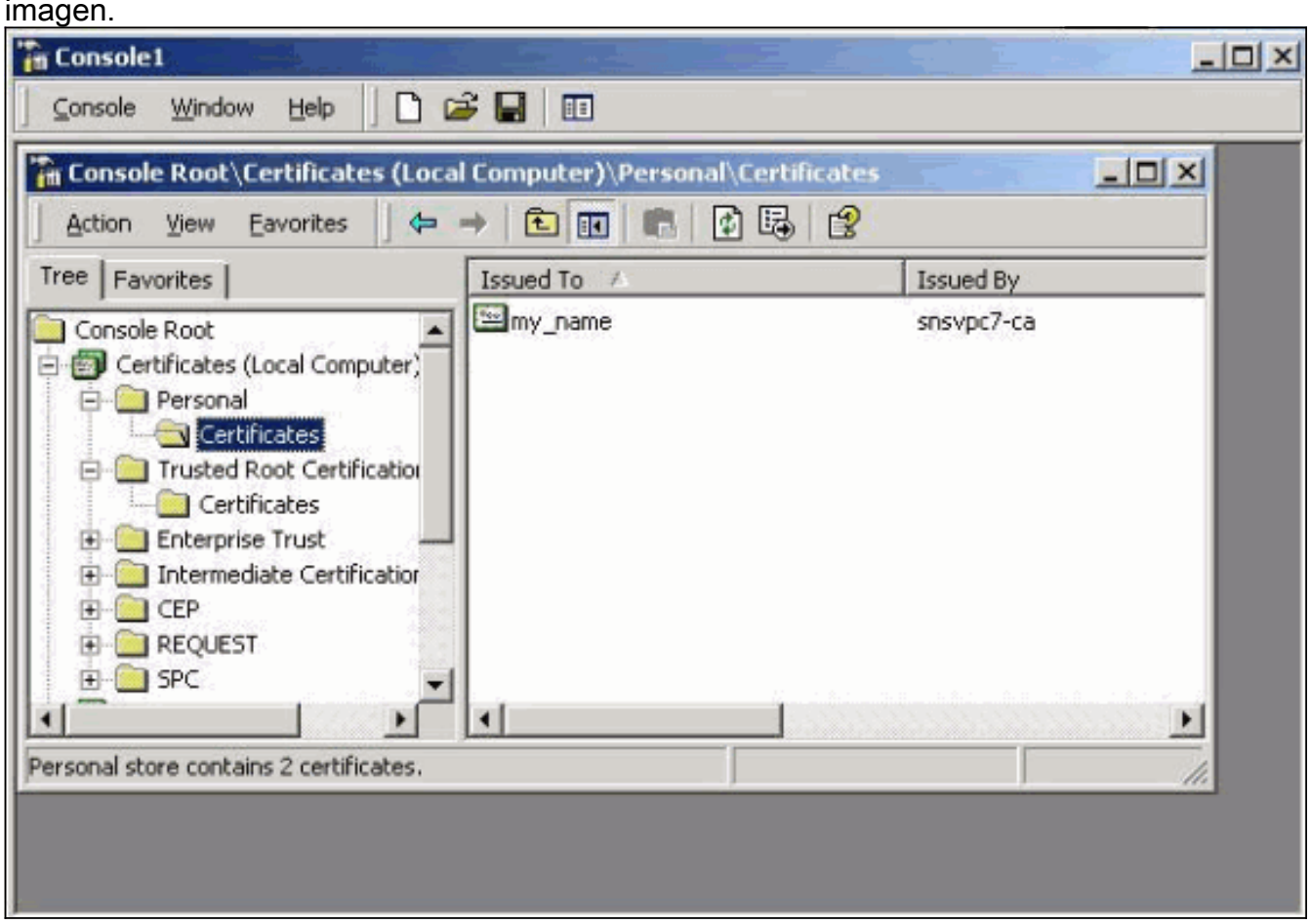
- El servidor no puede ser encendido.

  Muy probablemente, no comienzan al servicio IPSec. Seleccione el **Start (Inicio) > Programs (Programas) > Administrative Tools (Herramientas administrativas) > el servicio** y aseegurese que habilitan al **servicio IPSec**.
- Error 786: Ningún certificado de la máquina válido.



  Este error indica un problema con el certificado en la máquina local. Para mirar fácilmente su certificado, seleccione el **Start (Inicio) > Run (Ejecutar)**, y ejecute el MMC. Haga clic la **consola** y elija **agregan/quitan Broche-en**. El tecleo **agrega** y elige el **certificado de la** lista. Cuando aparece una ventana que le pide el alcance del certificado, elija la **cuenta de la Computadora**.Ahora usted puede verificar que el certificado del servidor de CA esté situado bajo **Trusted Root**

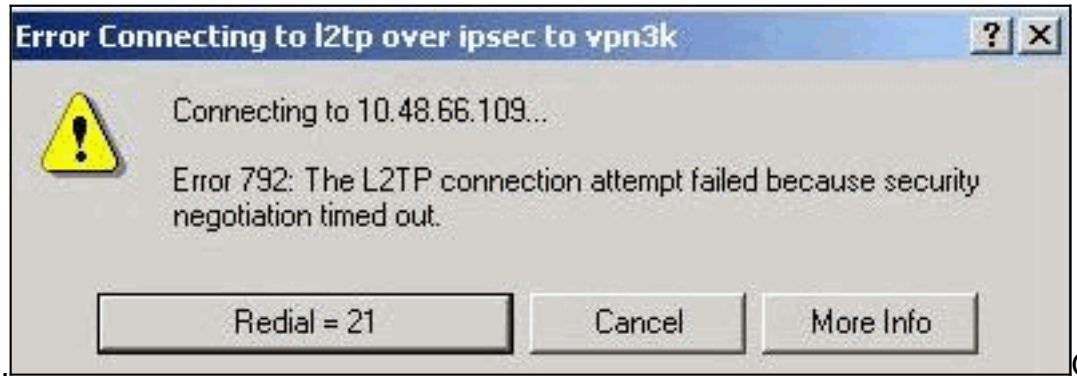
Certification Authority. Usted puede también verificar que usted tenga un certificado seleccionando la **Raíz de la consola > el certificado (computadora local) > personal > los Certificados**, tal y como se muestra en de esta imagen.



Haga clic el **certificado**. Verifique que todo esté correcto. En este ejemplo, hay una clave privada asociada al certificado. Sin embargo, este certificado ha expirado. Ésta es la causa

del problema.

- Error 792: Descanso de la negociación de seguridad.Este mensaje aparece después de un período



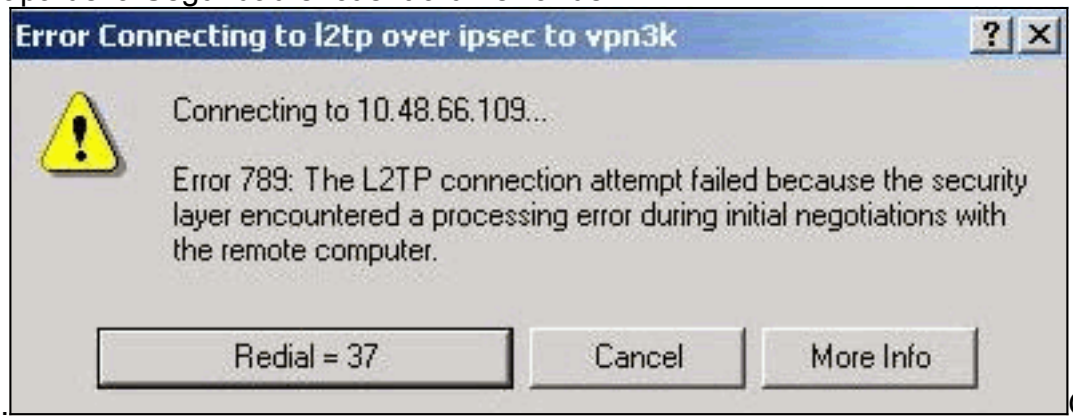
prolongado.Gire los debugs relevantes como se explica en el Cisco VPN 3000 Concentrator FAQ. Lea a través de ellos. Usted necesita ver algo similar a esta salida:

```
9337 02/15/2002 15:06:13.500 SEV=8
IKEDBG/0 RPT=7002 10.48.66.76
  Phase 1 failure against global IKE proposal # 6:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 2

9340 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7003 10.48.66.76
```

```
  Phase 1 failure against global IKE proposal # 7:
  Mismatched attr types for class Auth Method:
    Rcv'd: RSA signature with Certificates
    Cfg'd: Preshared Key

9343 02/15/2002 15:06:13.510 SEV=8 IKEDBG/0 RPT=7004 10.48.66.76
  Phase 1 failure against global IKE proposal # 8:
  Mismatched attr types for class DH Group:
    Rcv'd: Oakley Group 1
    Cfg'd: Oakley Group 7

9346 02/15/2002 15:06:13.510 SEV=7 IKEDBG/0 RPT=7005 10.48.66.76
All SA proposals found unacceptable

9347 02/15/2002 15:06:13.510 SEV=4 IKE/48 RPT=37 10.48.66.76
Error processing payload: Payload ID: 1

9348 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7006 10.48.66.76
IKE SA MM:261e40dd terminating:
flags 0x01000002, refcnt 0, tuncnt 0

9349 02/15/2002 15:06:13.510 SEV=9 IKEDBG/0 RPT=7007
sending delete message
```

Esto indica que la propuesta IKE no se ha configurado correctamente. Verifique la información de configurar una sección de la propuesta IKE de este documento.

- Error 789: La capa de la Seguridad encuentra un error de procesamiento.



Gire los debugs relevantes como se explica en el Cisco VPN 3000 Concentrator FAQ. Lea a través de ellos. Usted necesita ver algo similar a esta salida:

```
11315 02/15/2002 15:36:32.030
SEV=8 IKEDBG/0 RPT=7686
Proposal # 1, Transform # 2, Type ESP, Id DES-CBC
Parsing received transform:
  Phase 2 failure:
  Mismatched attr types for class Encapsulation:
    Rcv'd: Transport
    Cfg'd: Tunnel

11320 02/15/2002 15:36:32.030 SEV=5 IKEDBG/0 RPT=7687
AH proposal not supported

11321 02/15/2002 15:36:32.030 SEV=4 IKE/0 RPT=27 10.48.66.76
Group [VPNC_Base_Group]
All IPSec SA proposals found unacceptable!
```

- Versión usadaSeleccione el **Monitoring (Monitoreo) > System Status (Estado del sistema)** para ver esta salida:

```
VPN Concentrator Type: 3005
Bootcode Rev: Altiga Networks/VPN Concentrator Version 2.2.int_9 Jan 19 2000 05:36:41
Software Rev: Cisco Systems, Inc./VPN 3000 Concentrator Version 3.5.Rel Nov 27 2001 13:35:16
Up For: 44:39:48
Up Since: 02/13/2002 15:49:59
RAM Size: 32 MB
```

Información Relacionada

- Soporte de productos de la Negociación IPSec/Protocolos IKE
- Soporte Técnico - Cisco Systems