Configuración del Concentrador VPN 3000 de Cisco para bloquear con filtros y la asignación de filtro RADIUS

Contenido

Introducción

En esta configuración de muestra, queremos utilizar los filtros para permitir que un usuario acceda solamente un servidor (10.1.1.2) dentro de la red y bloquee el acceso al resto de los recursos. El Cisco VPN 3000 Concentrator se puede configurar para controlar el IPSec, el Point-to-Point Tunneling Protocol (PPTP), y el acceso al cliente L2TP a los recursos de red con los filtros. Los filtros consisten en las reglas, que son similares a las Listas de acceso en un router. Si configuraron a un router para:

```
access-list 101 permit ip any host 10.1.1.2
access-list 101 deny ip any any
```

el equivalente del concentrador VPN sería configurar un filtro con las reglas.

Nuestra primera regla del concentrador VPN es el **permit_server_rule**, que es equivalente al **IP del permiso del** router **cualquier** comando de **10.1.1.2 del host**. Nuestra segunda regla del concentrador VPN es **deny_server_rule** que es equivalente al **comando deny ip any any del** router.

Nuestro filtro del concentrador VPN es **filter_with_2_rules**, que es equivalente a la lista de acceso del router 101; utiliza el **permit_server_rule** y el **deny_server_rule** (en esa orden). Se asume que los clientes pueden conectar correctamente antes de agregar los filtros; reciben sus IP Addresses de un pool en el concentrador VPN.

Refiera al ASDM del PIX/ASA 7.x: Restrinja el acceso a la red de los usuarios del VPN de acceso remoto para aprender más sobre el escenario donde el bloque del PIX/ASA 7.x el acceso de los usuarios de VPN.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

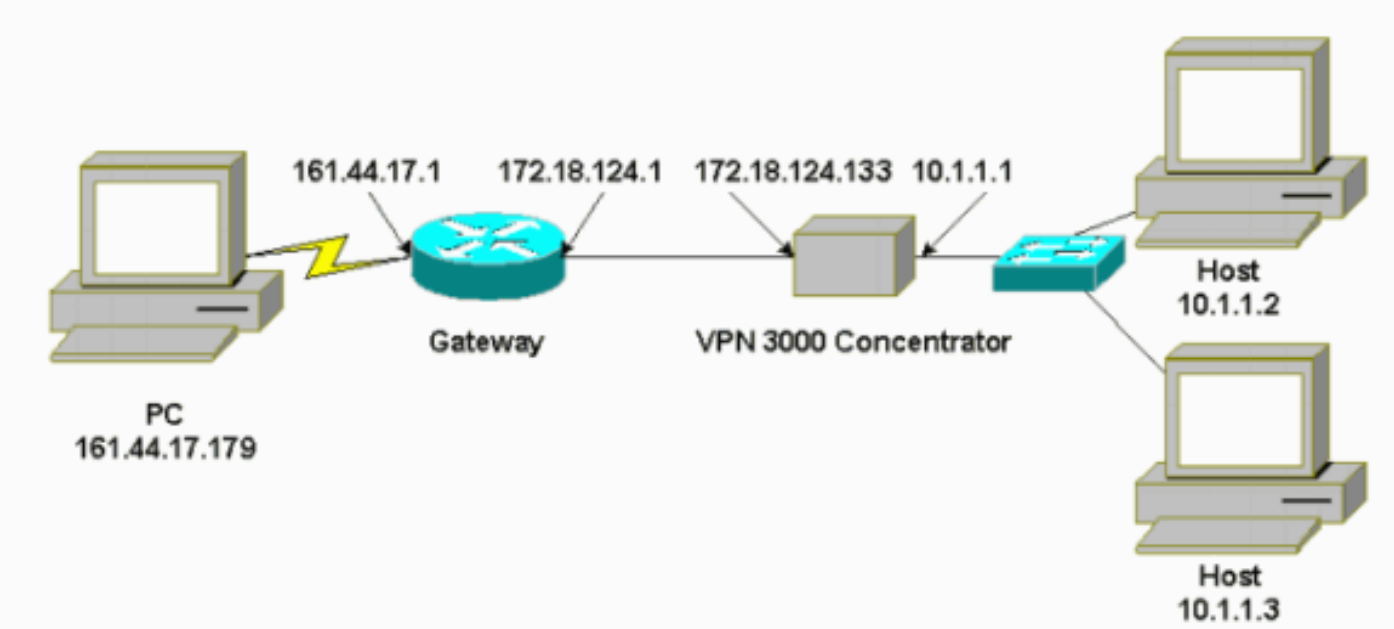
Componentes Utilizados

La información en este documento se basa en la versión 2.5.2.D del Cisco VPN 3000 Concentrator.

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:



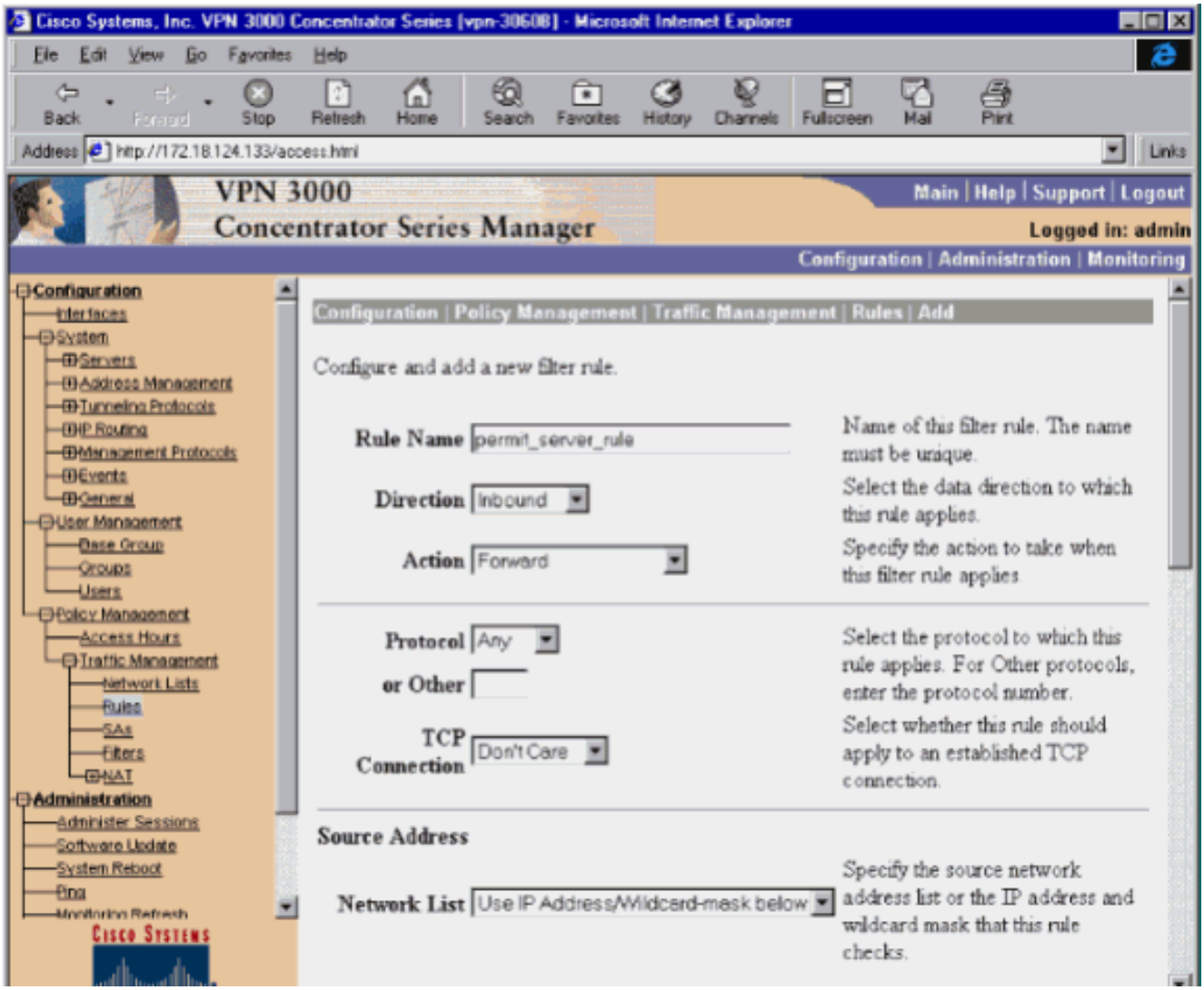
Convenciones

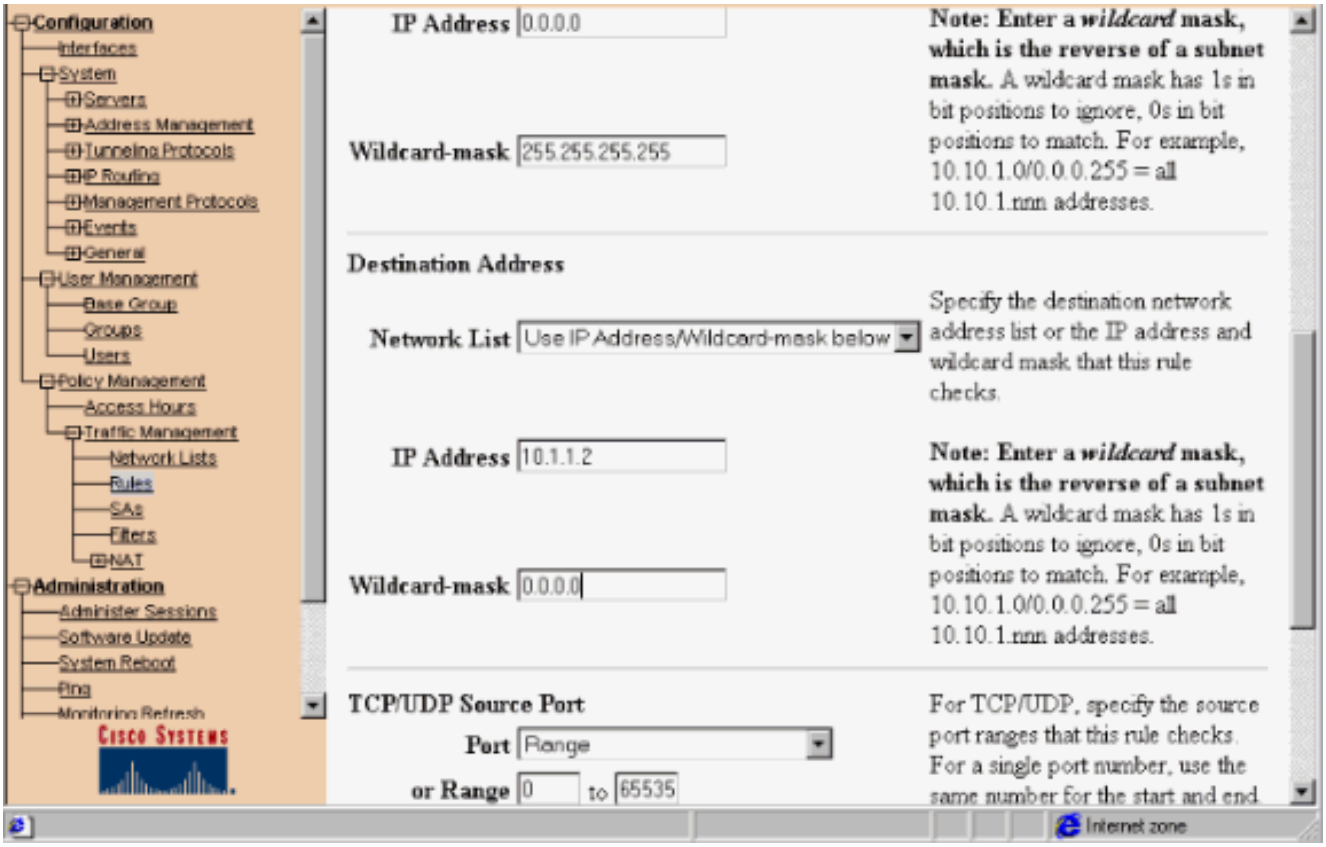
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración de VPN 3000

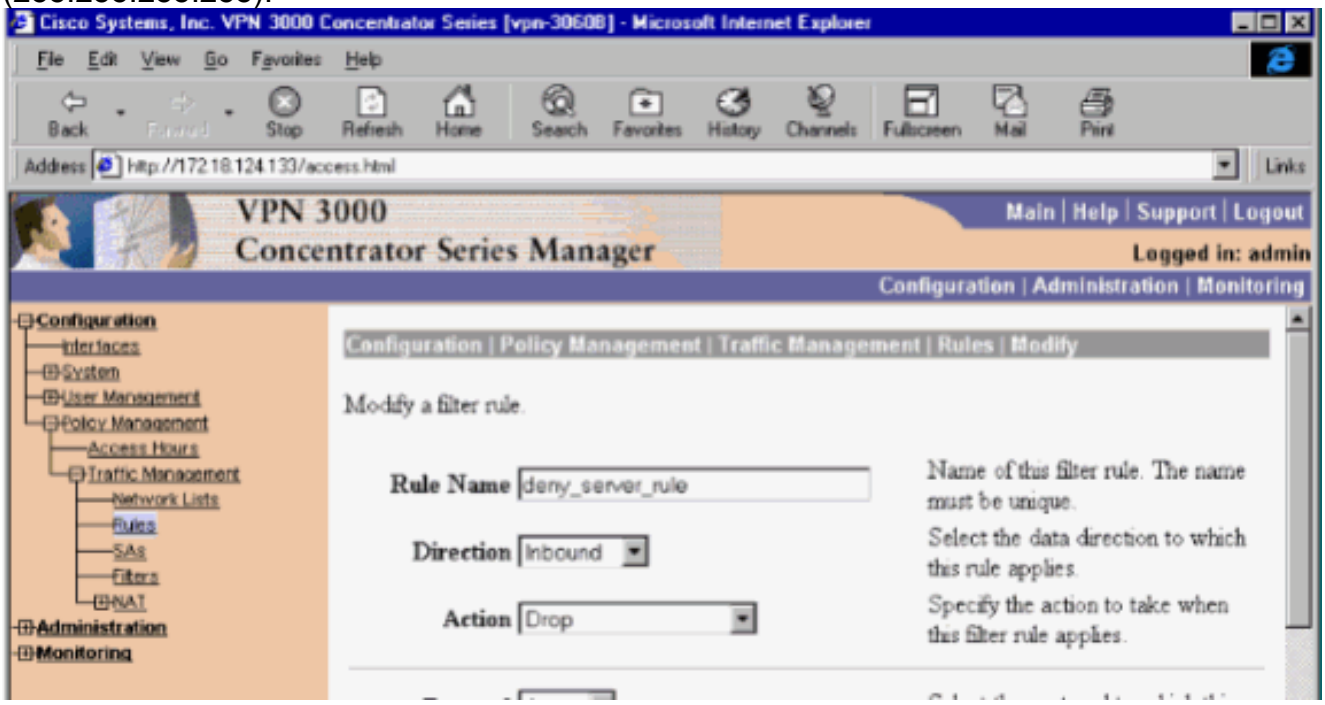
Complete estos pasos para configurar el concentrador VPN 3000.

1. Elija la **Administración del >Policy de la configuración > Traffic Management > las reglas > Add** y defina primera el **permit_server_rule** llamado del concentrador VPN regla con estas configuraciones:Dirección — **Entrante**Acción — **Delantero**Dirección de origen — **255.255.255.255**Dirección destino — **10.1.1.2**Máscara comodín — **0.0.0.0**

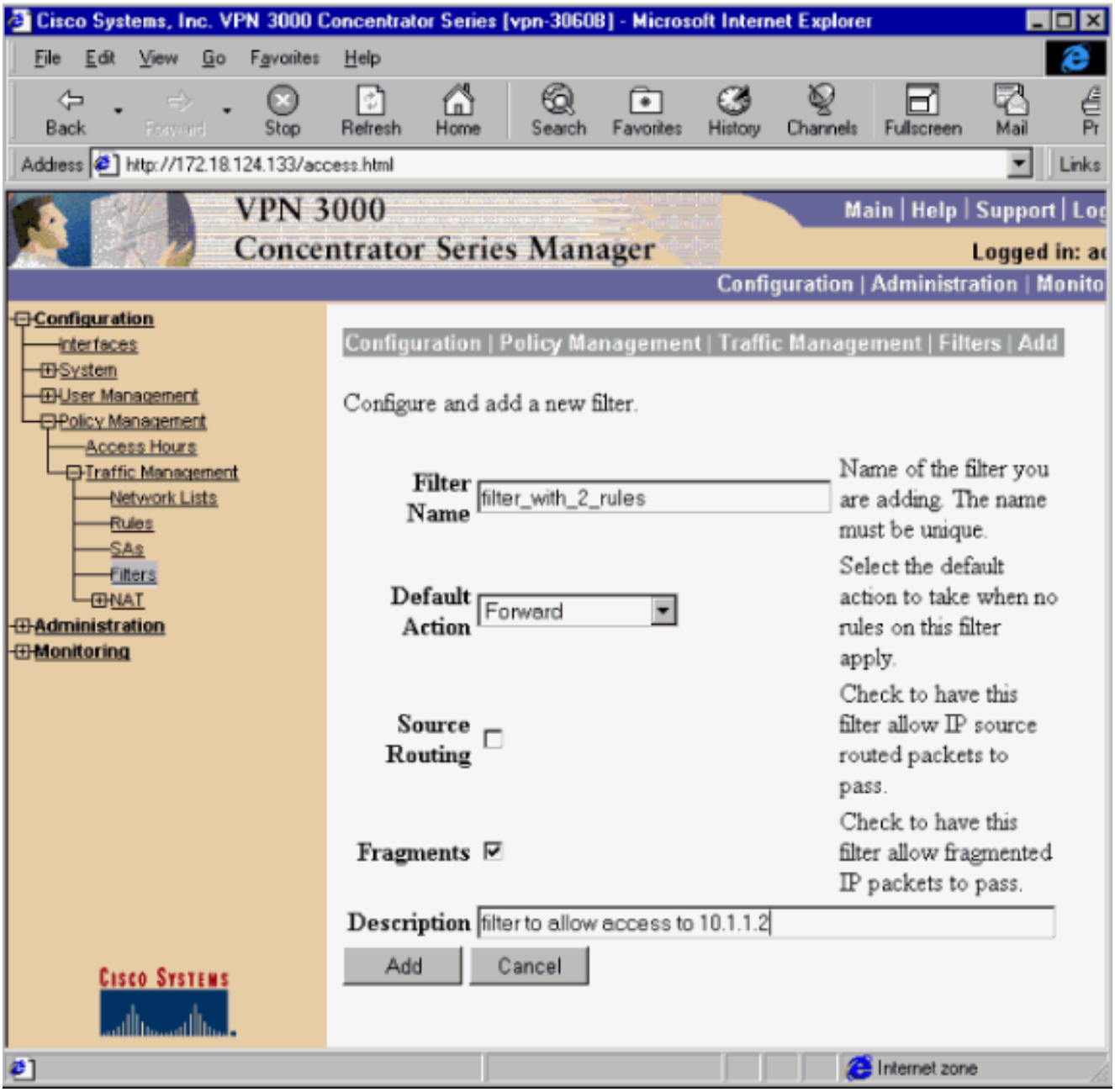




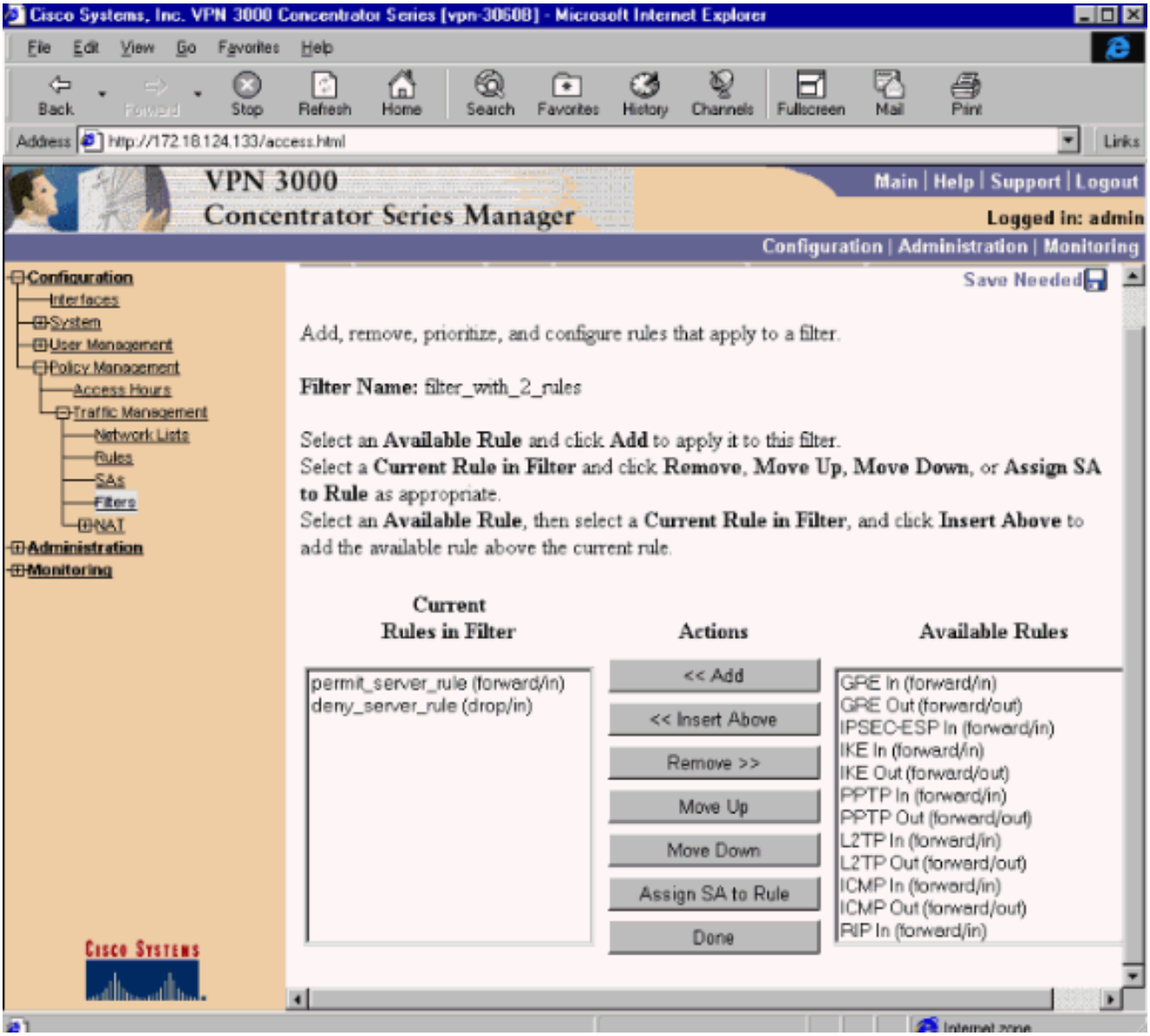
2. En la misma área, defina la segunda regla del concentrador VPN llamada **deny_server_rule** con estos valores por defecto:Dirección — **Entrante**Acción — **Descenso**Direcciones de origen y de destino cualquier cosa (255.255.255.255):



3. Elija el **Configuration (Configuración) > Policy Management (Administración de políticas) > Traffic Management (Administración de tráfico) > Filters (Filtros)** y agregue su filtro del **filter_with_2_rules**.



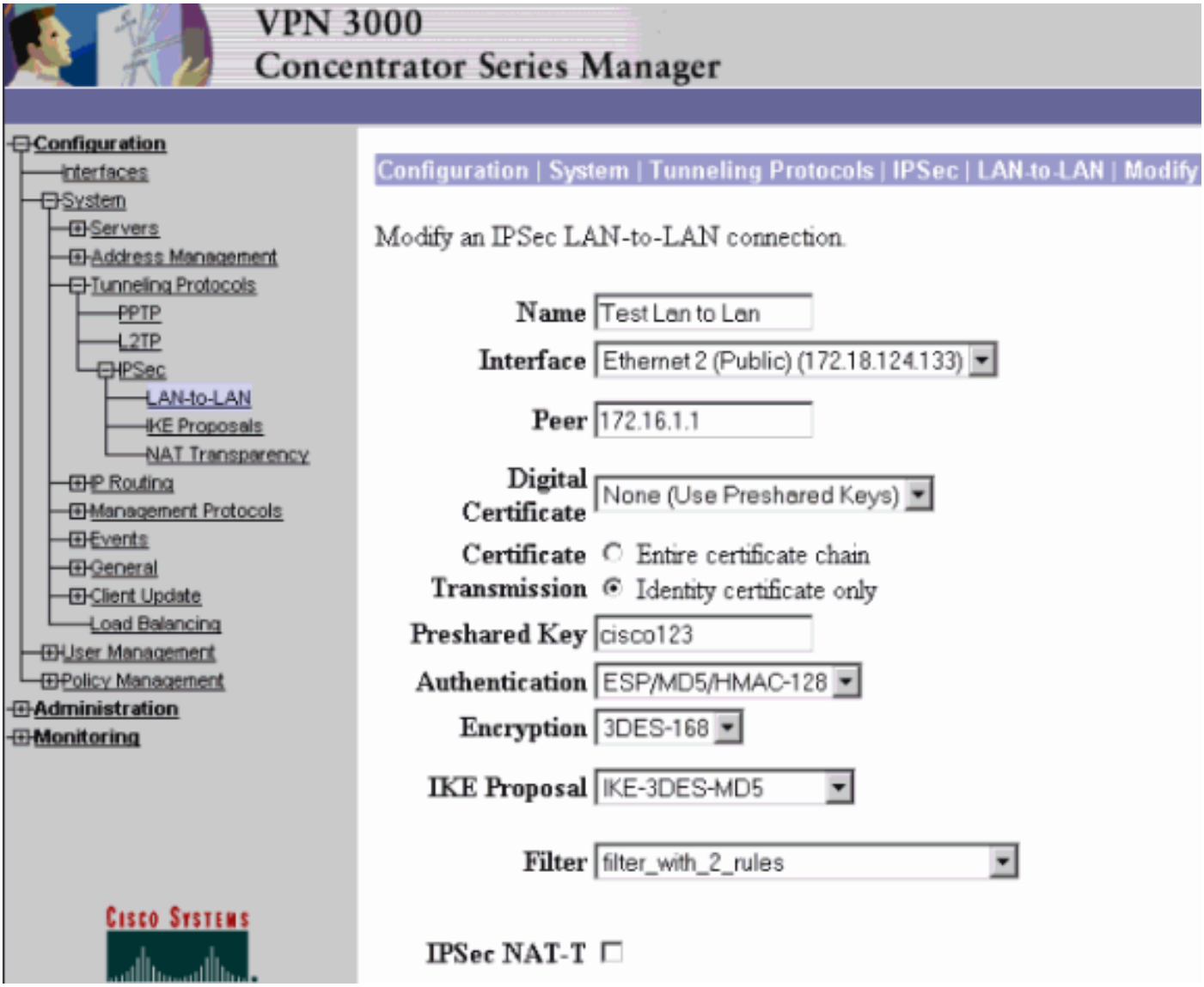
4. Agregue las dos reglas al filter_with_2_rules:



5. Elija el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)** y aplique el filtro al grupo:

Filtros para un túnel VPN de LAN a LAN

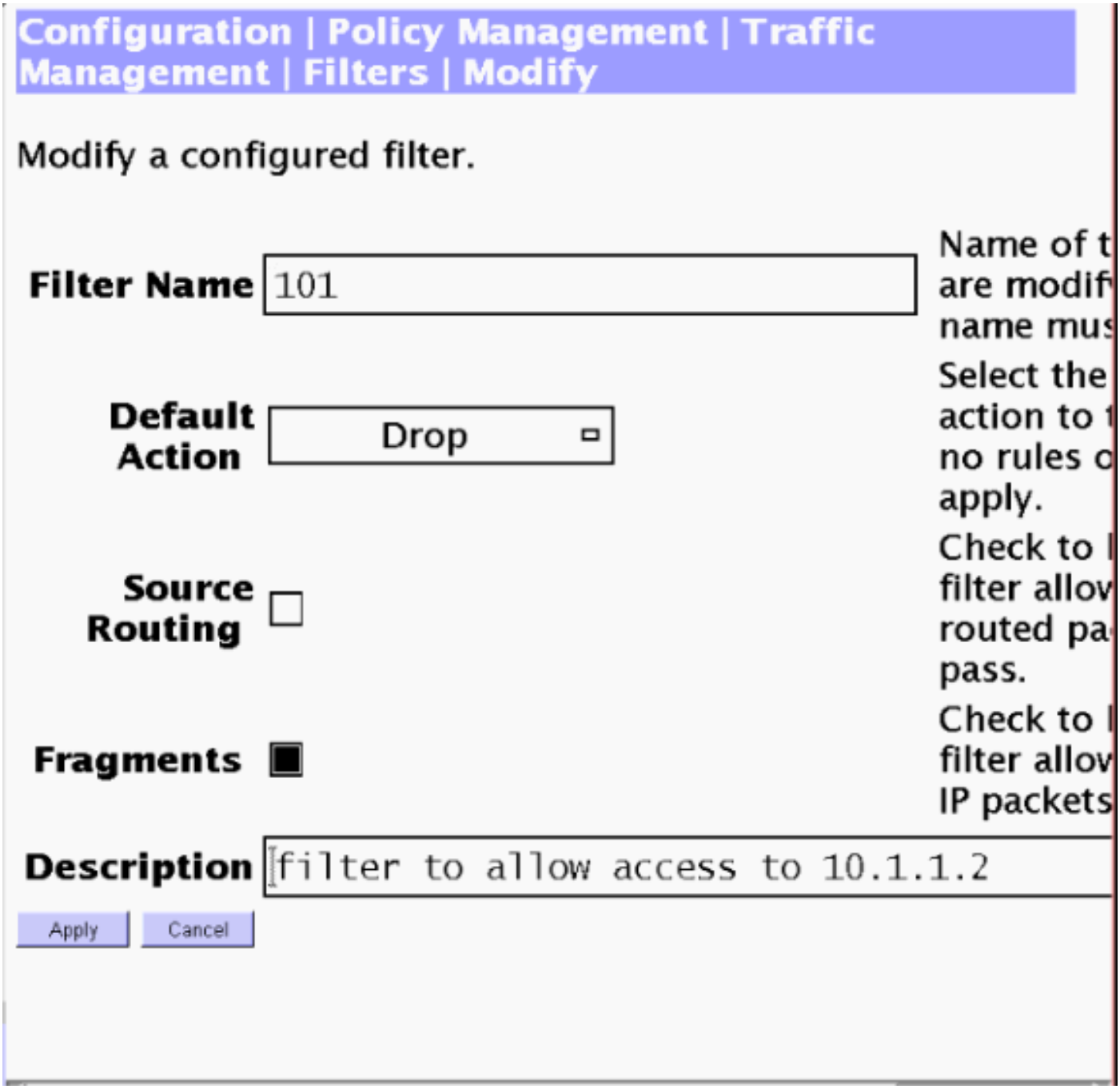
Del 3.6 y posteriores del código del concentrador VPN, usted puede filtrar tráfico para cada túnel del IPSec VPN del LAN a LAN. Por ejemplo, si usted construye un túnel de LAN a LAN a otro concentrador VPN con el direccionamiento 172.16.1.1, y quiera permitir el acceso de 10.1.1.2 del host al túnel mientras que usted niega el resto del tráfico, usted puede aplicar el **filter_with_2_rules** cuando usted elige el **Configuration (Configuración) > System (Sistema) > Tunneling Protocols (Protocolos de tunelización) > IPSec > LAN-to-LAN (LAN a LAN) > Modify (Modificar)** y selecciona el **filter_with_2_rules** bajo el **filtro**.



Configuración de VPN 3000 – Asignación de filtro de RADIUS

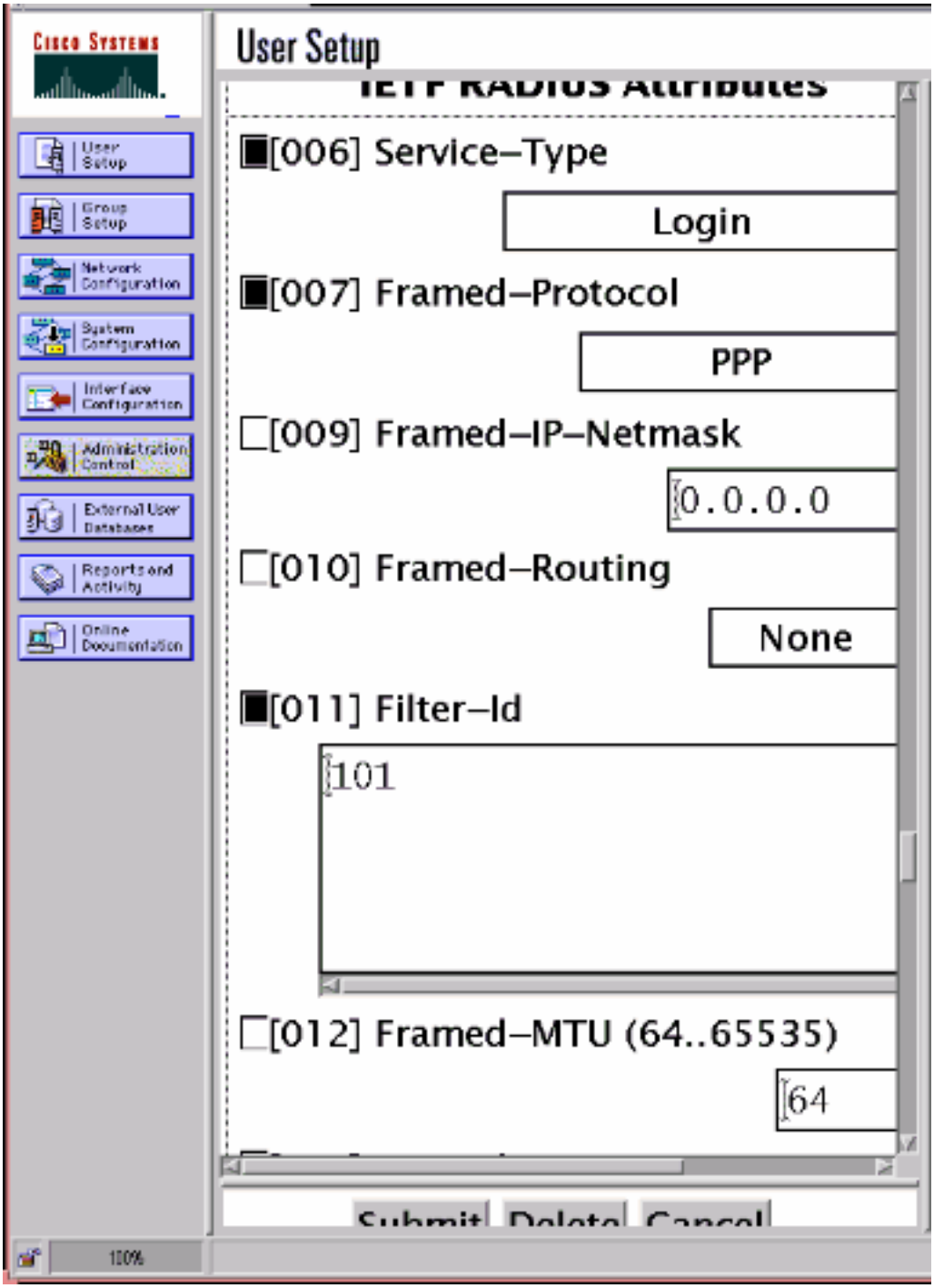
Es también posible definir un filtro en el concentrador VPN y entonces pasar abajo del número de filtro de un servidor de RADIUS (en los términos RADIUS, el atributo 11 es id del filtro), para cuando autentican al usuario en el servidor de RADIUS, asociar el id del filtro a esa conexión. En este ejemplo, la suposición es que la autenticación de RADIUS para los usuarios del concentrador VPN es ya operativa y solamente el id del filtro debe ser agregado.

Defina el filtro en el concentrador VPN como en el ejemplo anterior:



Configuración del servidor CSNT - Asignación de filtro de RADIUS

Atributo 11 de la configuración, id del filtro en el servidor del Cisco Secure NT a ser **101**:



Depuración – Asignación de filtro RADIUS

Si el AUTHDECODE (gravedad 1-13) está encendido en el concentrador VPN, el registro muestra que el servidor del Cisco Secure NT envía abajo del access-list 101 en el atributo 11 (0x0B):

```
207 01/24/2001 11:27:58.100 SEV=13 AUTHDECODE/0 RPT=228
0000: 020C002B 768825C5 C29E439F 4C8A727A     ...+v.%...C.L.rz
0010: EA7606C5 06060000 00020706 00000001     .v..............
0020: 0B053130 310806FF FFFFFF                   ..101......
```

Verificación

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

Troubleshooting

Para los propósitos de Troubleshooting solamente, usted puede girar el debugging del filtro cuando usted elige el **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases)** y agrega la clase **FILTERDBG** con la **gravedad para registrar = 13**. En las reglas, cambie la acción predeterminada de delantero (o del descenso) **para remitir y para registrar** (o caer y registro). Cuando el registro de acontecimientos se extrae en el **Monitoring (Monitoreo) > Event Log (Registro de evento)**, debe mostrar las entradas por ejemplo:

```
221 12/21/2000 14:20:17.190 SEV=9 FILTERDBG/1 RPT=62
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8

222 12/21/2000 14:20:18.690 SEV=9 FILTERDBG/1 RPT=63
Deny In: intf 1038, ICMP, Src 10.99.99.1, Dest 10.1.1.3, Type 8
```

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Preguntas frecuentes concentradoras VPN 3000
- Soporte a RADIUS
- Soporte del Cisco VPN 3000 Concentrator
- Soporte del Cliente Cisco VPN 3000
- Soporte del Cisco Secure ACS for Windows
- Request For Comments (RFC)
- Soporte Técnico y Documentación - Cisco Systems