Tunelización dividida para los clientes de VPN en el ejemplo de configuración del Concentrador VPN 3000

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Diagrama de la red
Convenciones
Antecedentes
Configuración de la Tunelización Dividida en el Concentrador VPN
Verificación
Conéctese con el cliente VPN
Ver el registro del cliente VPN
Troubleshoot
Información Relacionada

Introducción

Este documento proporciona instrucciones paso a paso sobre cómo permitir que los clientes VPN accedan a Internet mientras son tunelizados en un Concentrador VPN 3000 Series. Esta configuración concede a los clientes VPN acceso seguro a los recursos corporativos a través de IPsec, mientras que concede acceso no seguro a Internet.

Nota: La tunelización dividida puede suponer un riesgo de seguridad cuando se configura. Como los clientes VPN tienen acceso no seguro a Internet, un atacante puede ponerles en peligro. Ese atacante podría entonces poder acceder a la LAN corporativa a través del túnel IPsec. Un riesgo entre la tunelización completa y la tunelización dividida puede ser permitir solamente el acceso LAN local de los clientes VPN. Refiérase a Ejemplo de Configuración de Permitir Acceso LAN Local para Clientes VPN en el Concentrador VPN 3000 para obtener más información.

Prerequisites

Requirements

Este documento asume que ya existe una configuración de VPN de acceso remoto en funcionamiento en el concentrador VPN. Consulte Ejemplo de Configuración de IPsec con VPN Client a VPN 3000 Concentrator si uno no está configurado todavía.

Componentes Utilizados

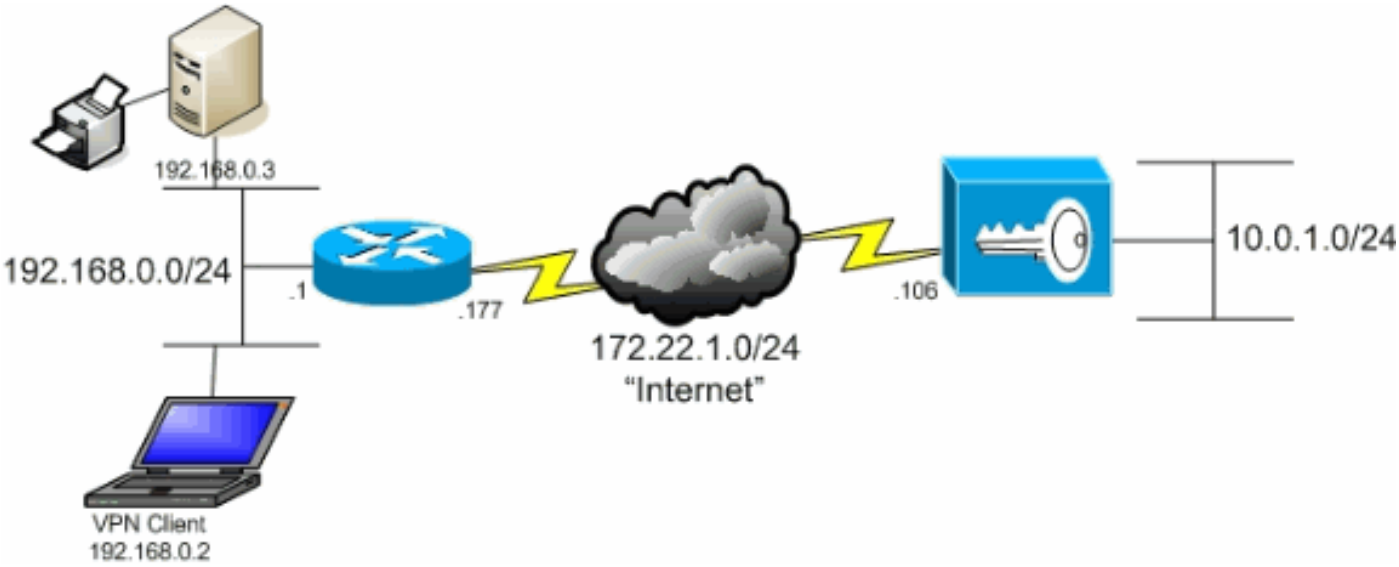
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software Cisco VPN 3000 Concentrator Series versión 4.7.2.H
- Versión 4.0.5 de Cisco VPN Client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

VPN Client se encuentra en una red SOHO típica y se conecta a través de Internet a la oficina principal.



Convenciones

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

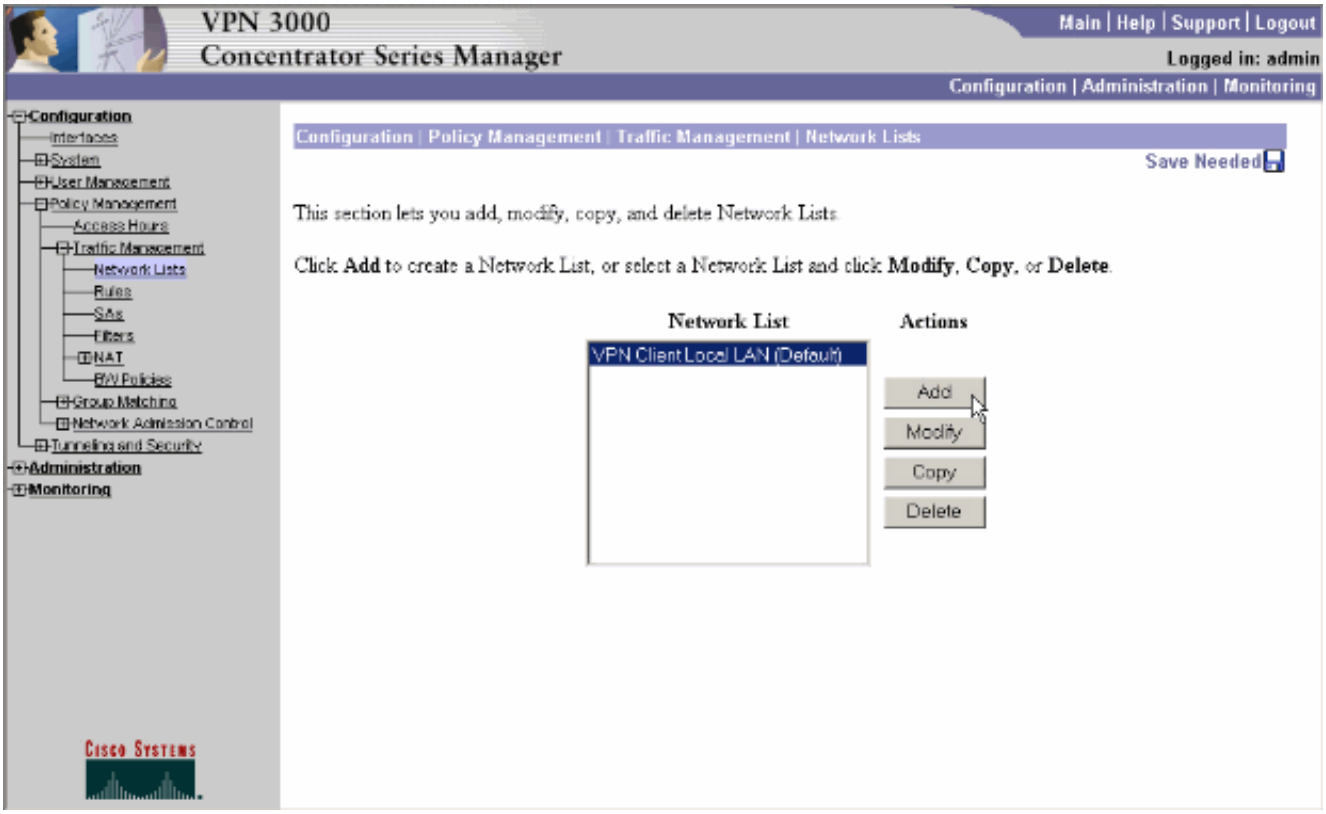
Antecedentes

En un escenario básico de VPN Client a VPN Concentrator, todo el tráfico del VPN Client se cifra y se envía al VPN Concentrator sin importar el destino. En función de su configuración y del número de usuarios admitidos, dicha configuración puede requerir un gran ancho de banda. La tunelización dividida puede ayudar a aliviar este problema al permitir que los usuarios envíen sólo el tráfico destinado a la red corporativa a través del túnel. El resto del tráfico como IM, correo electrónico o navegación casual se envía a Internet a través de la LAN local del VPN Client.

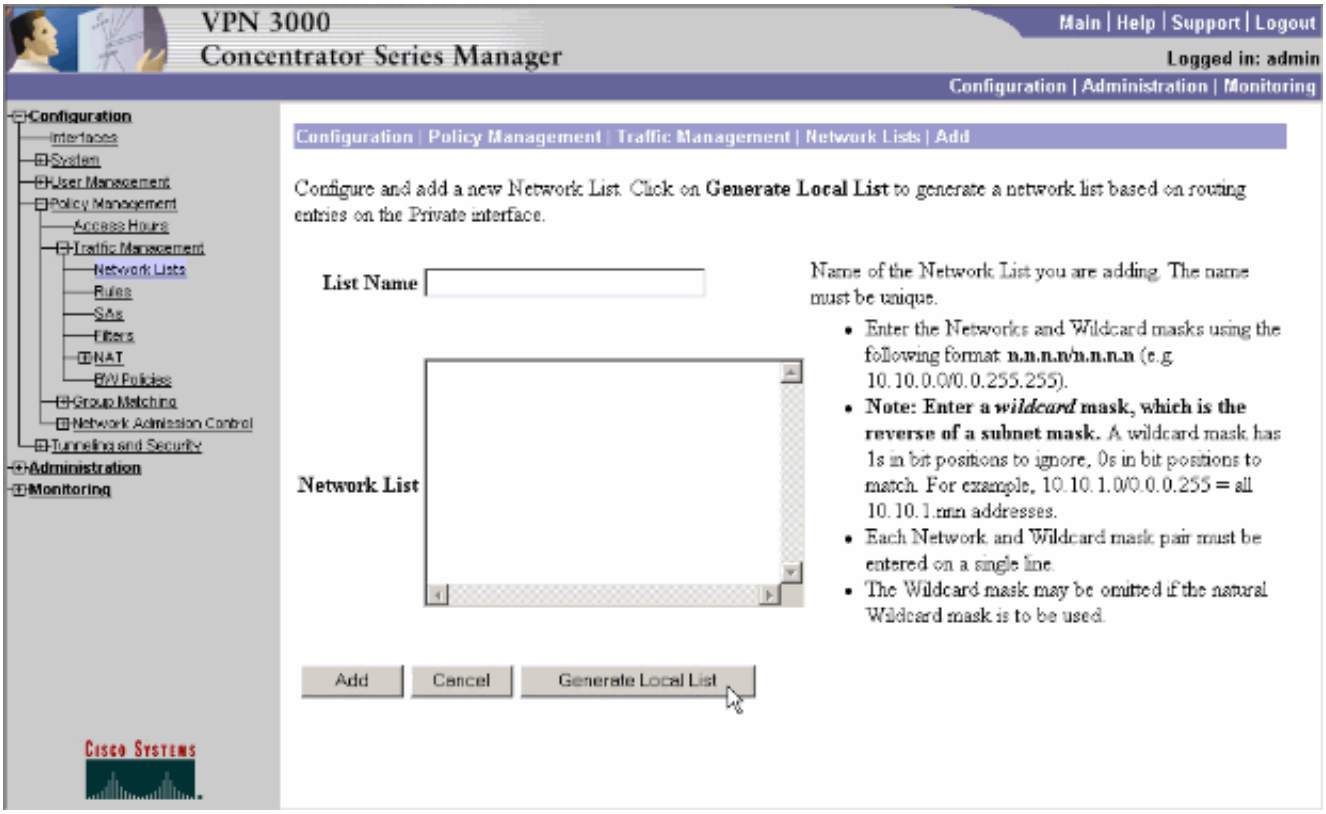
Configuración de la Tunelización Dividida en el Concentrador VPN

Complete estos pasos para configurar su grupo de túnel para permitir la tunelización dividida para los usuarios del grupo. En primer lugar, cree una lista de red. Esta lista define las redes de destino a las que el cliente VPN envía tráfico cifrado. Una vez creada la lista, agregue la lista a la política de tunelización dividida del grupo de túnel del cliente.

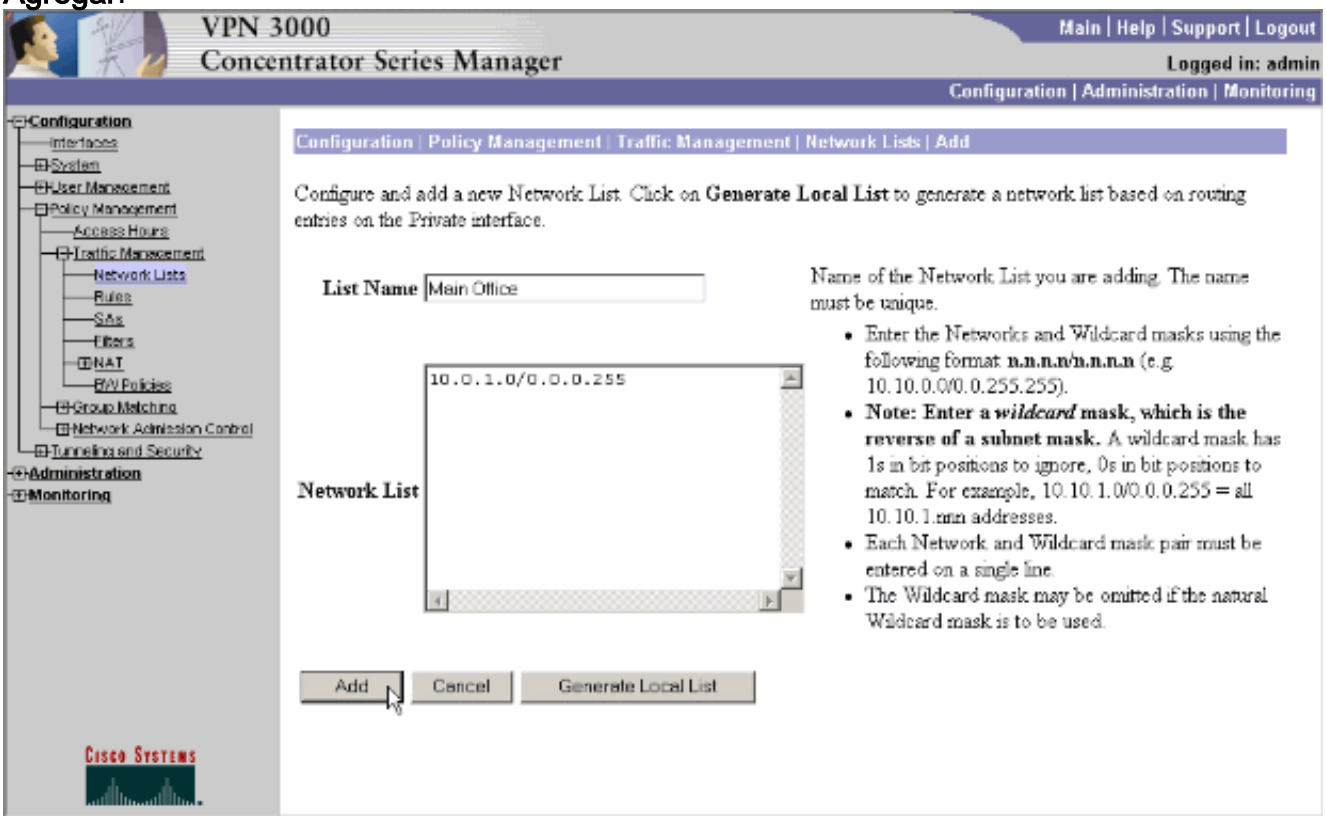
1. Elija **Configuration > Policy Management > Traffic Management > Network Lists** y haga clic en
Add.



2. Esta lista define las redes de destino a las que el cliente VPN envía tráfico cifrado. Ingrese estas redes manualmente o haga clic en **Generar lista local** para crear una lista basada en las entradas de ruteo en la interfaz privada del concentrador VPN.En este ejemplo, la lista se creó
automáticamente.

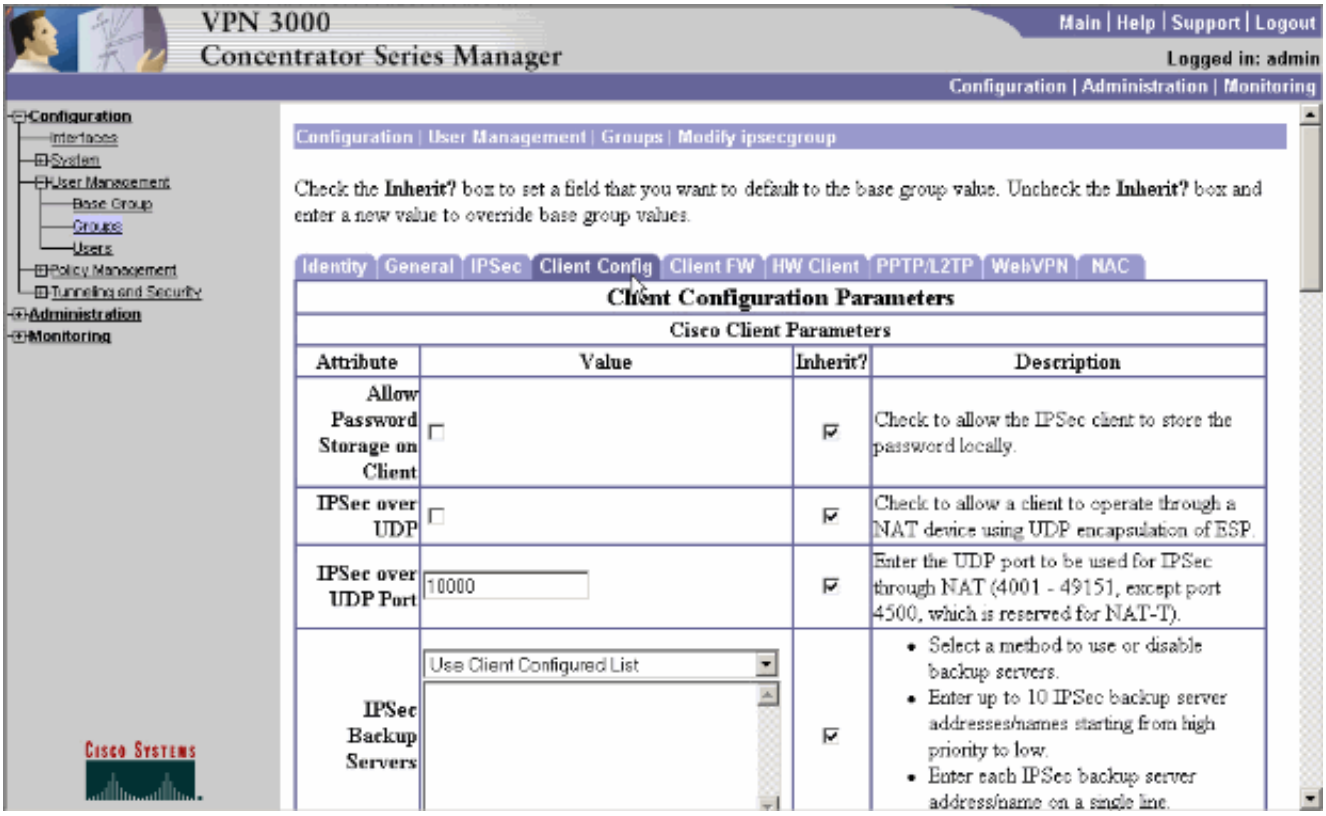


3. Una vez creada o rellenada, proporcione un nombre para la lista y haga clic en **Agregar**.

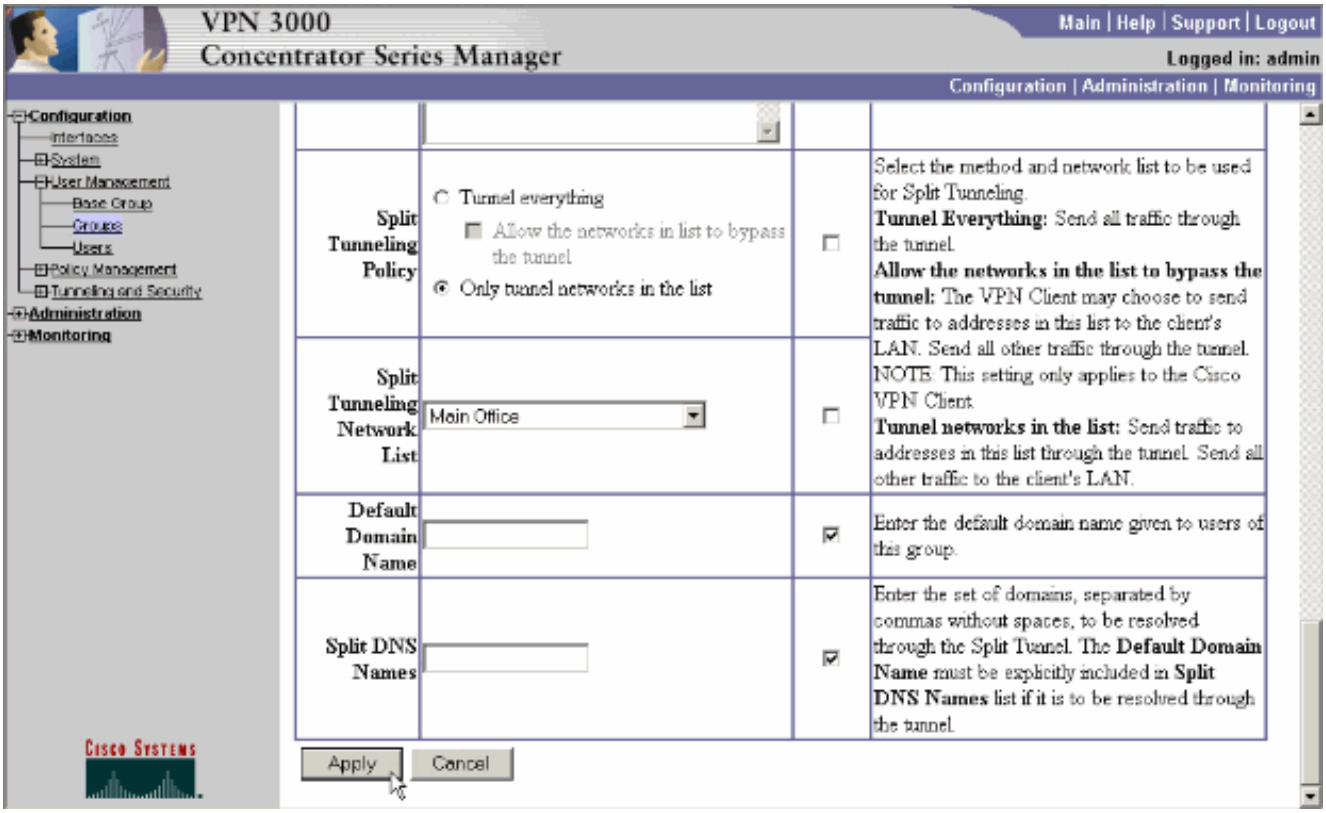


4. Una vez creada la lista de red, asígnala a un grupo de túnel. Elija **Configuration > User Management > Groups**, seleccione el grupo que desea cambiar y haga clic en **Modify Group**.

5. Vaya a la ficha Configuración de cliente del grupo que ha elegido modificar.



6. Desplácese hasta las secciones Dividir la Política de Tunelización y Dividir la Lista de Red de Tunelización y haga clic en **Sólo redes de túnel en la lista**.
7. Elija la lista creada anteriormente en la lista desplegable. En este caso, es la **Oficina Principal**. ¿La Herencia? las casillas de verificación se vacían automáticamente en ambos casos.



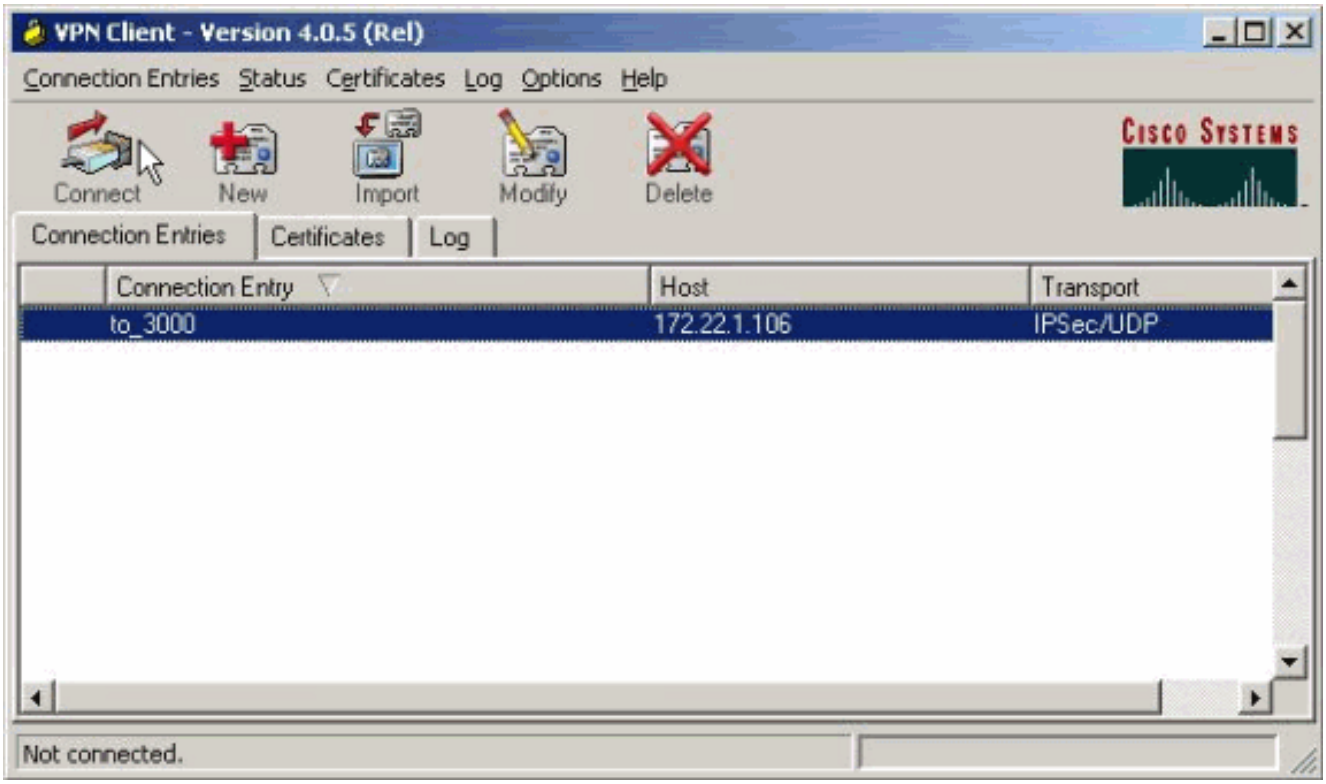
8. Haga clic en **Aplicar** cuando haya terminado.

Verificación

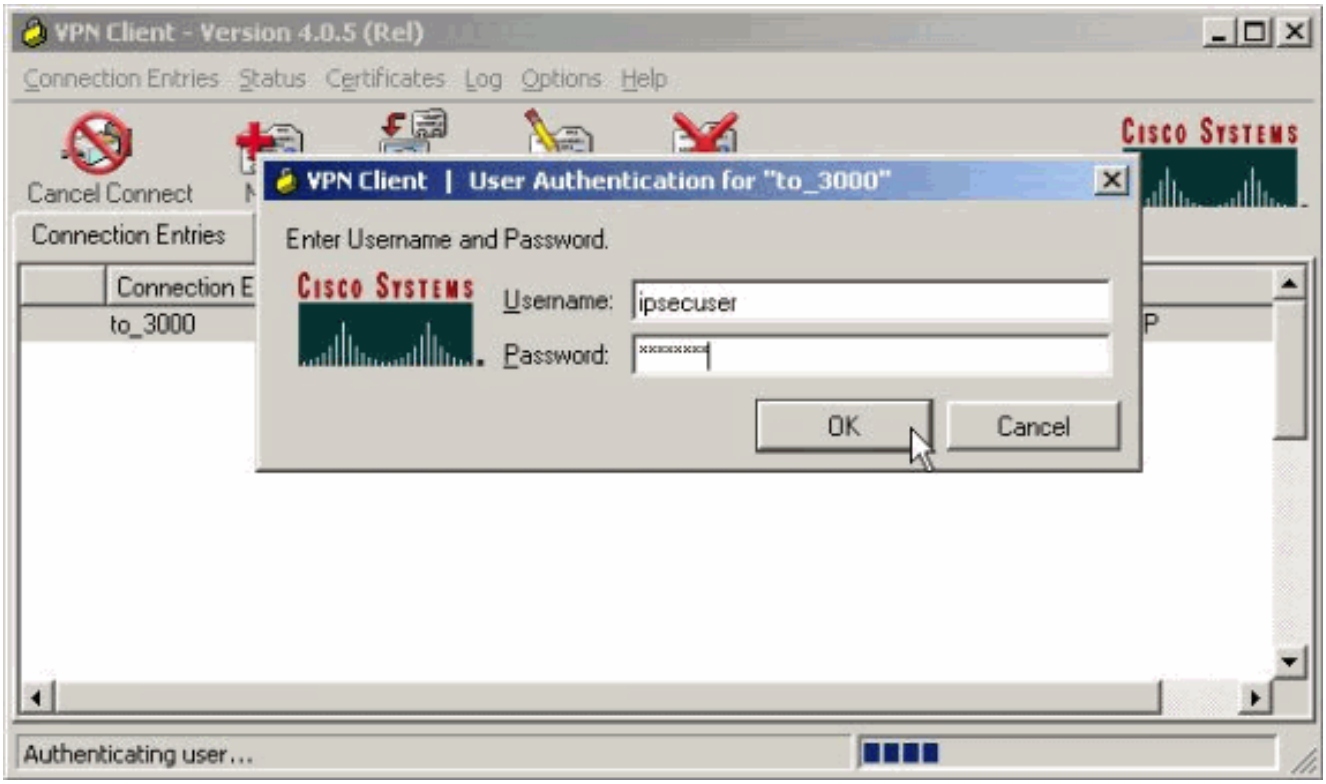
Conéctese con el cliente VPN

Conecte su VPN Client al VPN Concentrator para verificar su configuración.

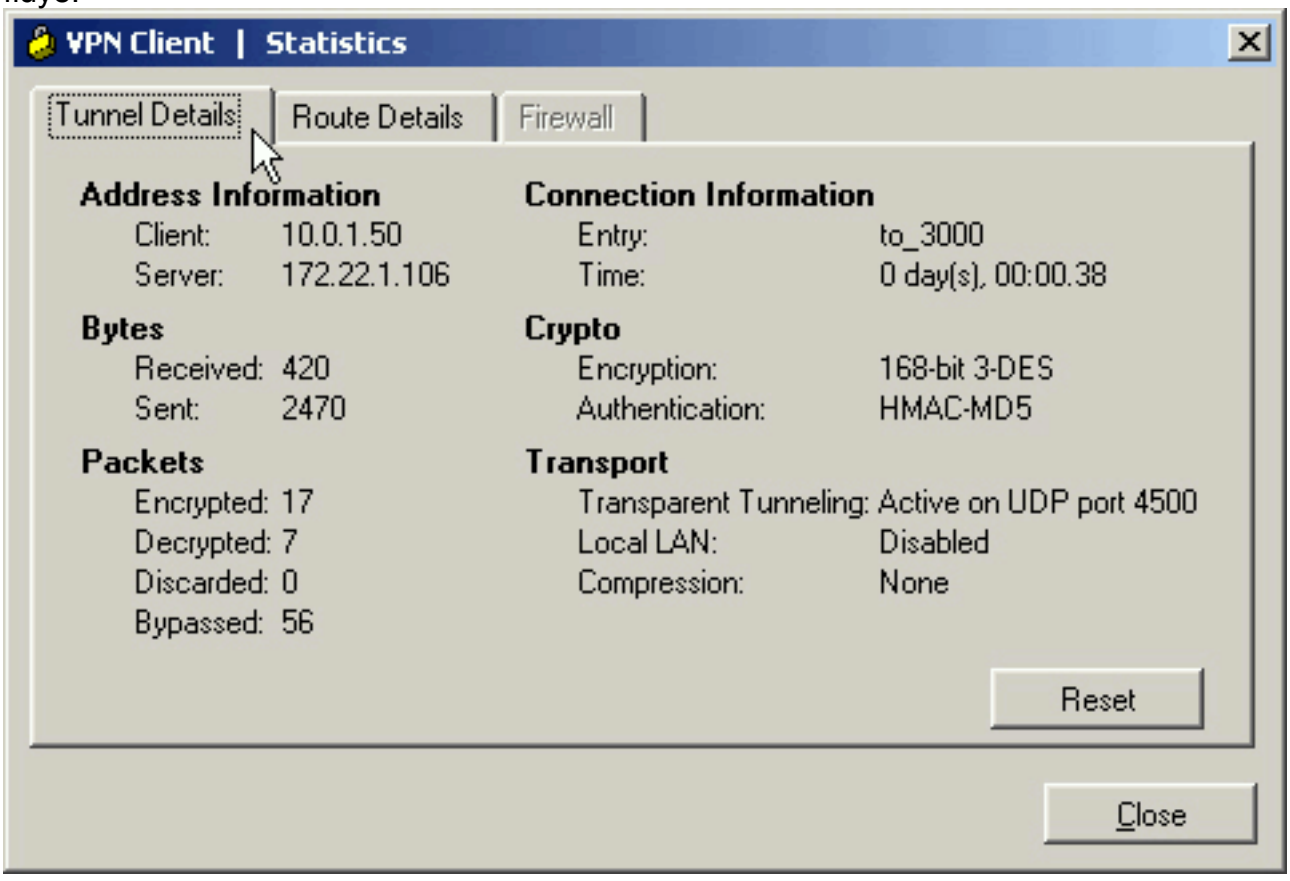
1. Elija la entrada de conexión de la lista y haga clic en **Conectar**.



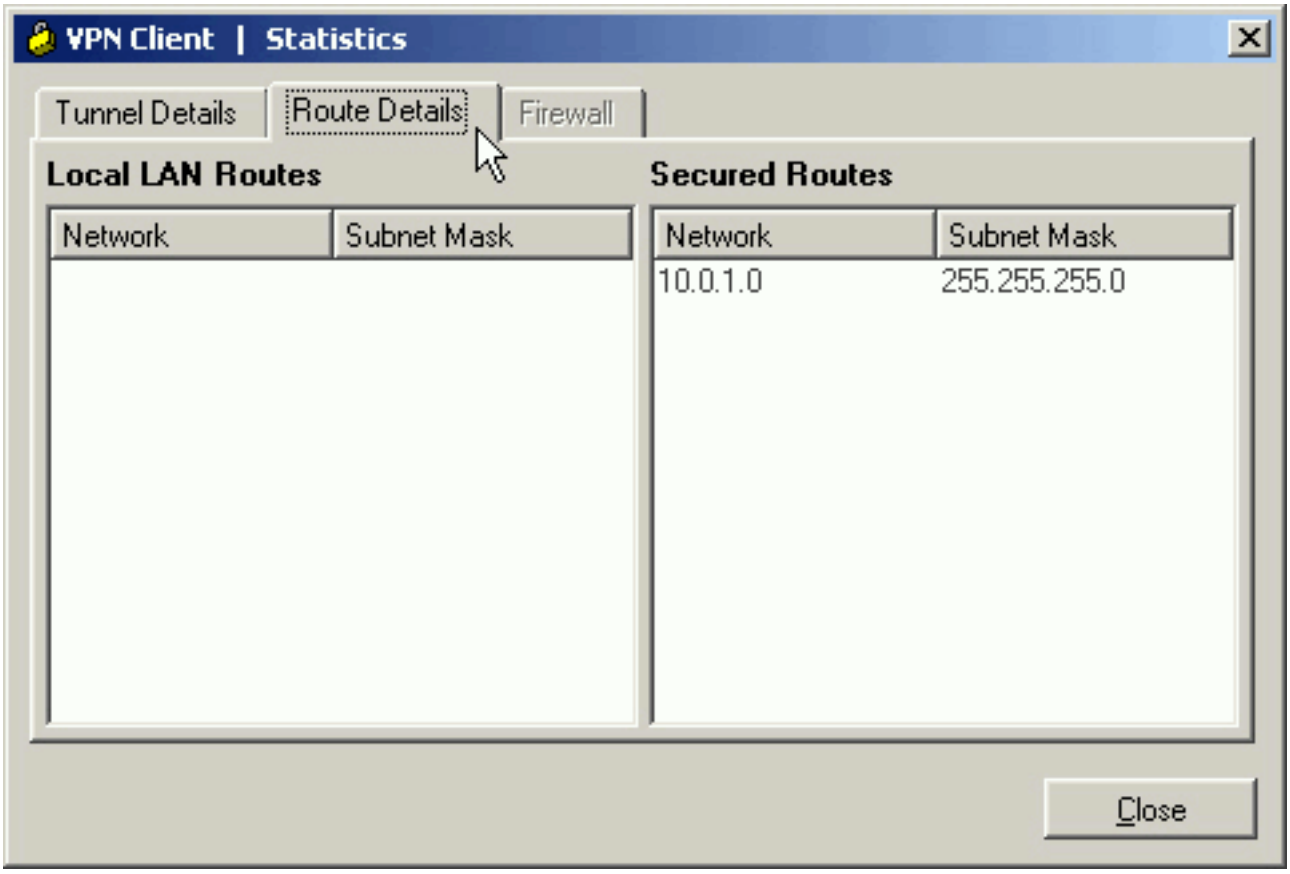
2. Introduzca sus credenciales.



3. Elija **Estado > Estadísticas...** para mostrar la ventana Detalles del túnel donde puede inspeccionar los detalles del túnel y ver el tráfico que fluye.

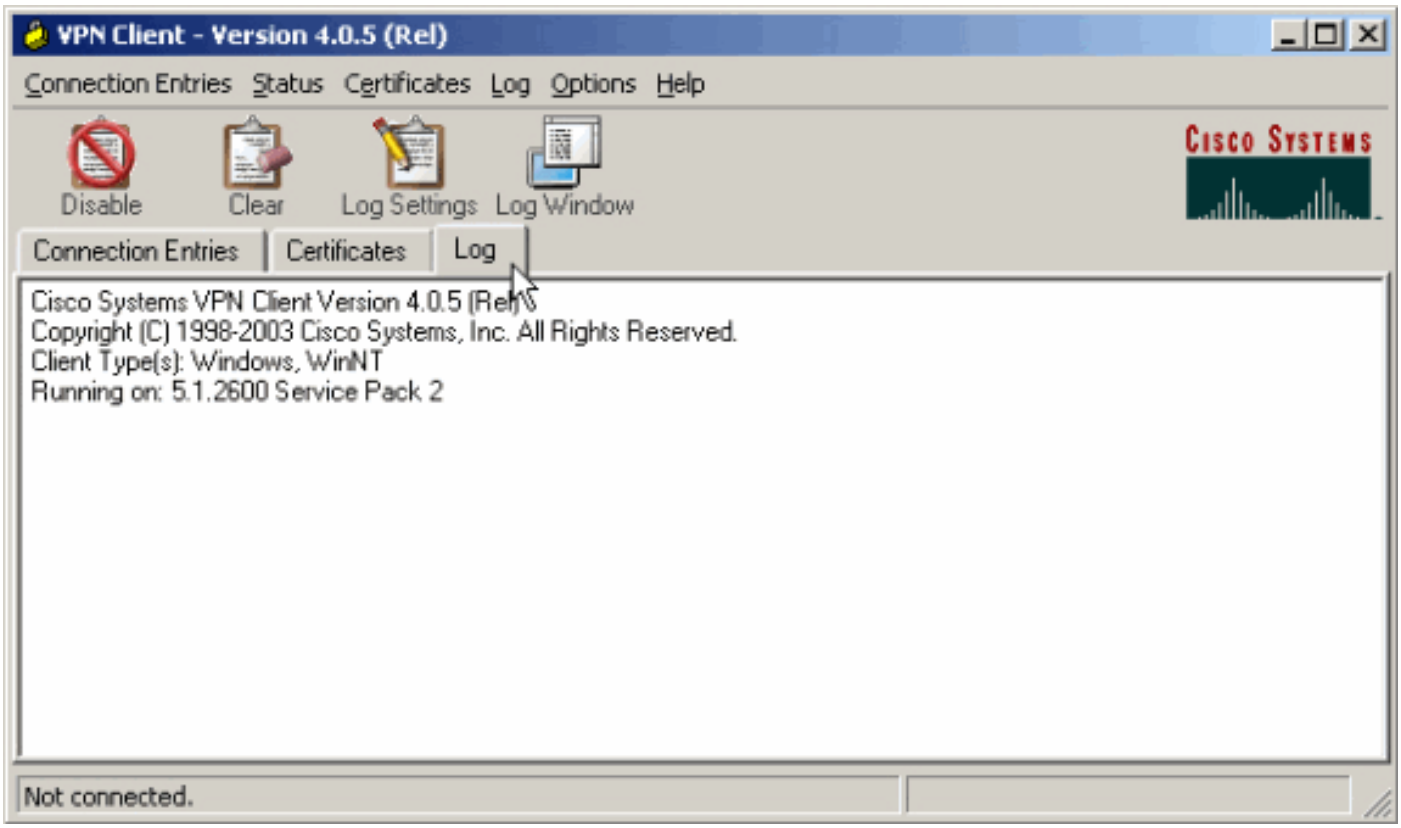


4. Vaya a la ficha Route Details para ver a qué redes envía el cliente VPN tráfico cifrado. En este ejemplo, VPN Client se comunica de forma segura con 10.0.1.0/24 mientras que el resto del tráfico se envía sin cifrar a Internet.



Ver el registro del cliente VPN

Cuando examina el registro de VPN Client, puede determinar si el parámetro que permite la tunelización dividida está configurado o no. Vaya a la ficha Log (Registro) en VPN Client para ver el registro. Haga clic en **Log Settings** para ajustar lo que está registrado. En este ejemplo, IKE e IPsec se establecen en **3- Alto** mientras que todos los demás elementos de registro se establecen en **1 - Bajo**.



```
Cisco Systems VPN Client Version 4.0.5 (Rel)
Copyright (C) 1998-2003 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Windows, WinNT
Running on: 5.1.2600 Service Pack 2

1      14:21:43.106  07/21/06  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 172.22.1.106.

!--- Output is supressed. 28 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005D Client sending a
firewall request to concentrator 29 14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall
Policy: Product=Cisco Systems Integrated Client, Capability= (Centralized Protection Policy). 30
14:21:55.151 07/21/06 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Intrusion
Prevention Security Agent, Capability= (Are you There?). 31 14:21:55.171 07/21/06 Sev=Info/4
IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.106 32 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 172.22.1.106 33 14:21:56.114
07/21/06 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
172.22.1.106 34 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50 35 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0 36 14:21:56.114
07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value =
0x00000000 !--- Split tunneling is configured. 37 14:21:56.114 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets), value
= 0x00000001 38 14:21:56.114 07/21/06 Sev=Info/5 IKE/0x6300000F SPLIT_NET #1 subnet = 10.0.1.0
mask = 255.255.255.0 protocol = 0 src port = 0 dest port=0 39 14:21:56.124 07/21/06 Sev=Info/5
IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 40
14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION,
value = Cisco Systems, Inc./VPN 3000 Concentrator Version 4.7.2.H built by vmurphy on Jun 29
2006 20:21:56 41 14:21:56.124 07/21/06 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute =
Received and using NAT-T port number , value = 0x00001194 !--- Output is supressed.
```

Troubleshoot

Refiérase a Ejemplo de Configuración de IPsec con VPN Client to VPN 3000 Concentrator - Troubleshooting para obtener información general sobre la solución de problemas de esta configuración.

Información Relacionada

- Ejemplo de Configuración de IPsec con VPN Client to VPN 3000 Concentrator
- Cisco VPN 3000 Series Concentrators
- Cliente de Cisco VPN
- Soporte Técnico y Documentación - Cisco Systems