Exemplo de Configuração da Separação de Túneis para Clientes VPN no VPN 3000 Concentrator

Contents

Introduction

Este documento fornece instruções passo a passo sobre como permitir que os Clientes VPN acessem a Internet enquanto são enviados pelo túnel para um VPN 3000 Series Concentrator. Esta configuração fornece aos Clientes VPN acesso seguro aos recursos corporativos através do IPsec, ao passo que gera acesso não protegido à Internet.

Observação: o tunelamento dividido pode potencialmente representar um risco à segurança quando configurado. Como os VPN Clients têm acesso desprotegido à Internet, eles podem ser comprometidos por um invasor. Esse invasor poderá então acessar a LAN corporativa através do túnel IPsec. Um comprometimento entre o tunelamento completo e o tunelamento dividido pode ser permitir apenas o acesso de VPN Clients à LAN local. Consulte Exemplo de Configuração de Permitir Acesso LAN Local para Clientes VPN no VPN 3000 Concentrator para obter mais informações.

Prerequisites

Requirements

Este documento pressupõe que já existe uma configuração de VPN de acesso remoto em funcionamento no VPN Concentrator. Consulte o Exemplo de Configuração de IPsec com VPN

Client para VPN 3000 Concentrator se um ainda não estiver configurado.

Componentes Utilizados

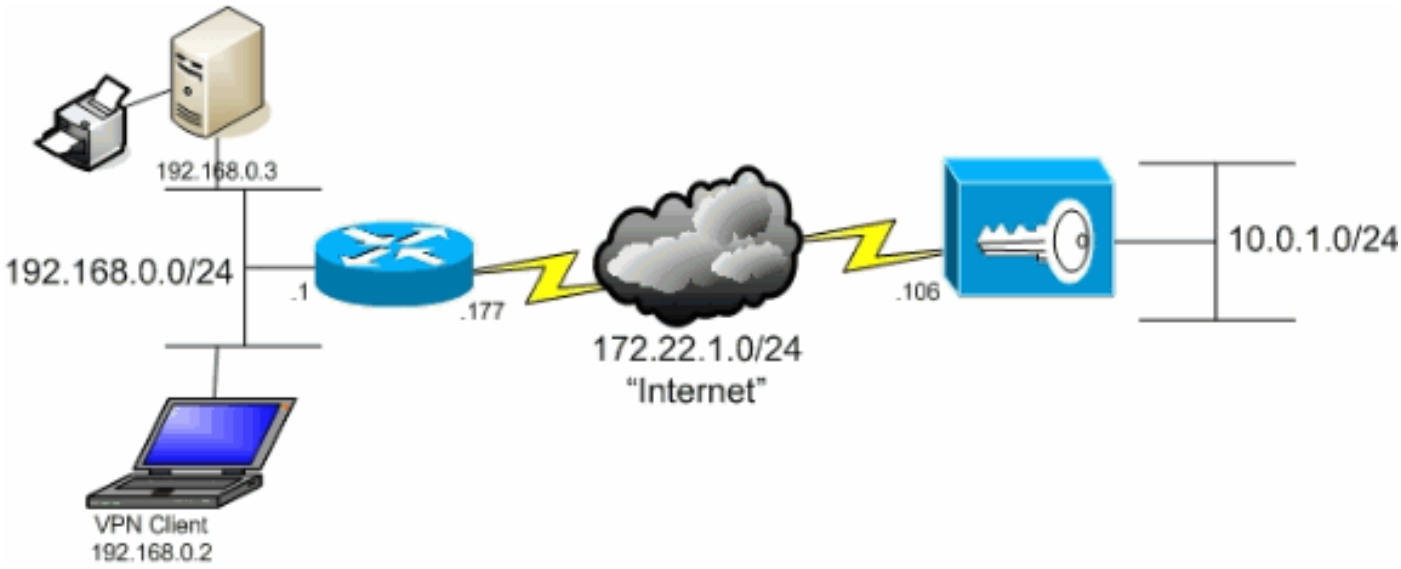
As informações neste documento são baseadas nestas versões de software e hardware:

- Software Cisco VPN 3000 Concentrator Series versão 4.7.2.H
- Cisco VPN Client versão 4.0.5

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 Rede

O VPN Client está localizado em uma rede SOHO típica e se conecta através da Internet ao escritório principal.



Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

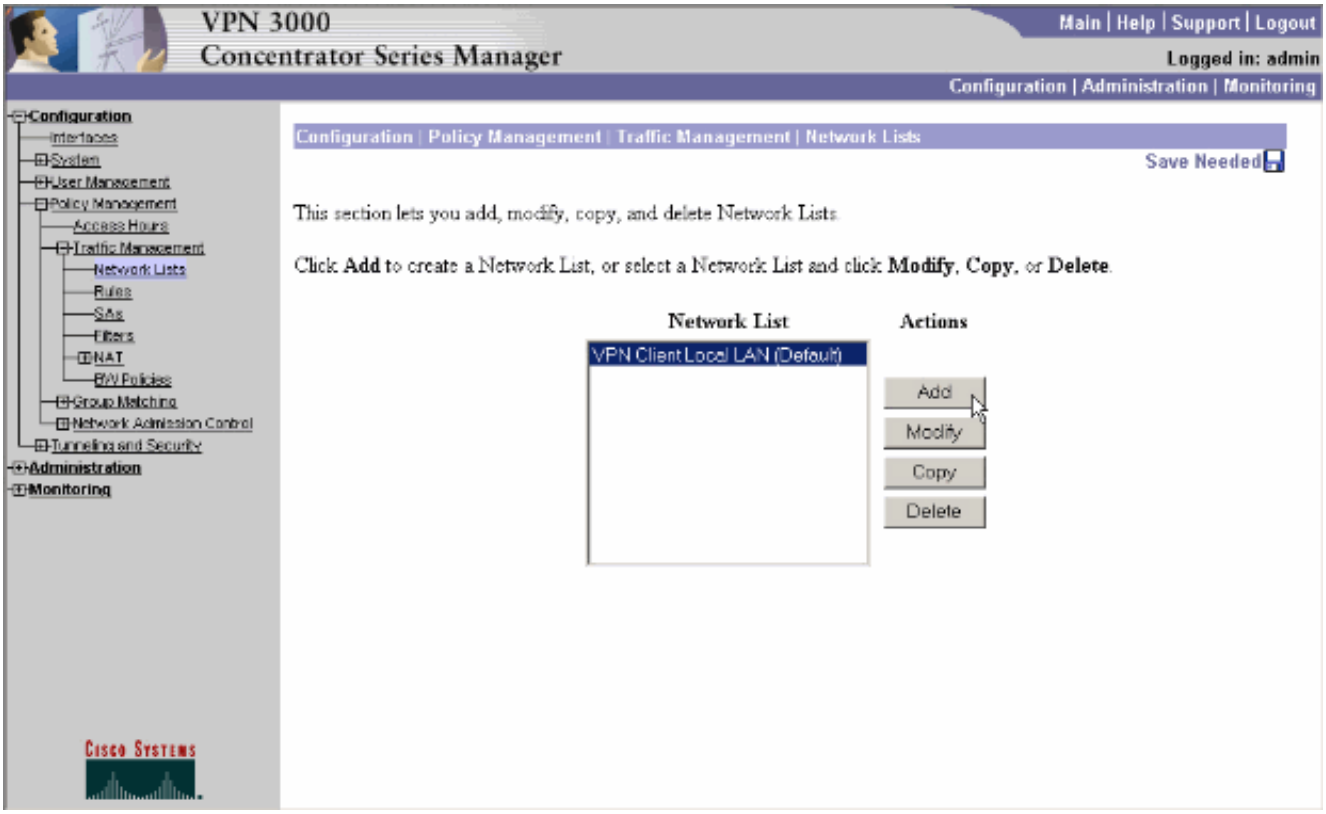
Informações de Apoio

Em um cenário de VPN Client to VPN Concentrator básico, todo o tráfego do VPN Client é criptografado e enviado ao VPN Concentrator independentemente do destino. Com base na sua configuração e no número de usuários suportados, essa configuração pode se tornar uma largura de banda intensa. O tunelamento dividido pode funcionar para aliviar esse problema, permitindo que os usuários enviem apenas o tráfego destinado à rede corporativa através do túnel. Todo o tráfego restante, como IM, e-mail ou navegação casual, é enviado para a Internet através da LAN local do VPN Client.

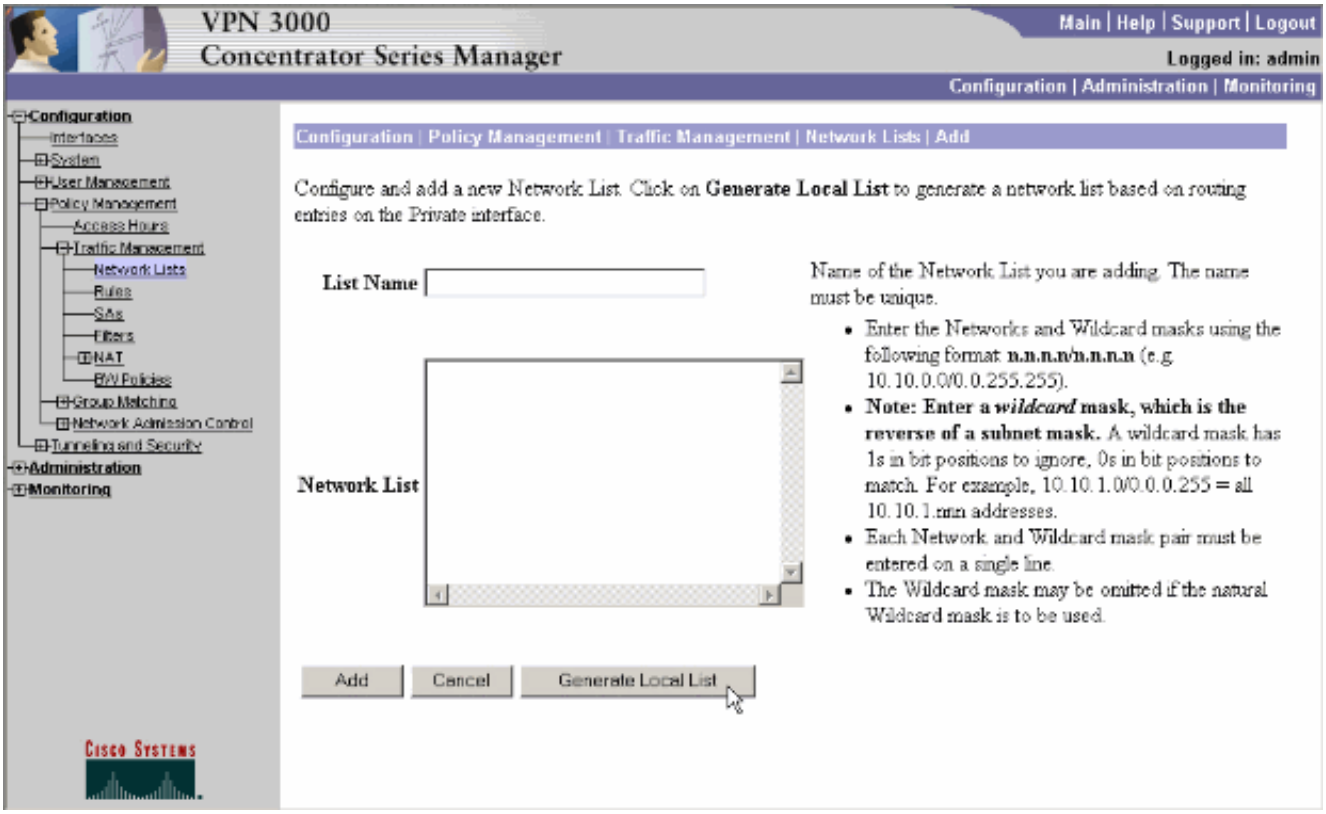
Configurar o tunelamento dividido no VPN Concentrator

Conclua estes passos para configurar seu grupo de túneis para permitir o tunelamento dividido para usuários no grupo. Primeiro, crie uma lista de rede. Essa lista define as redes de destino para as quais o VPN Client envia tráfego criptografado. Quando a lista for criada, adicione a lista à política de tunelamento dividido do grupo de túneis do cliente.

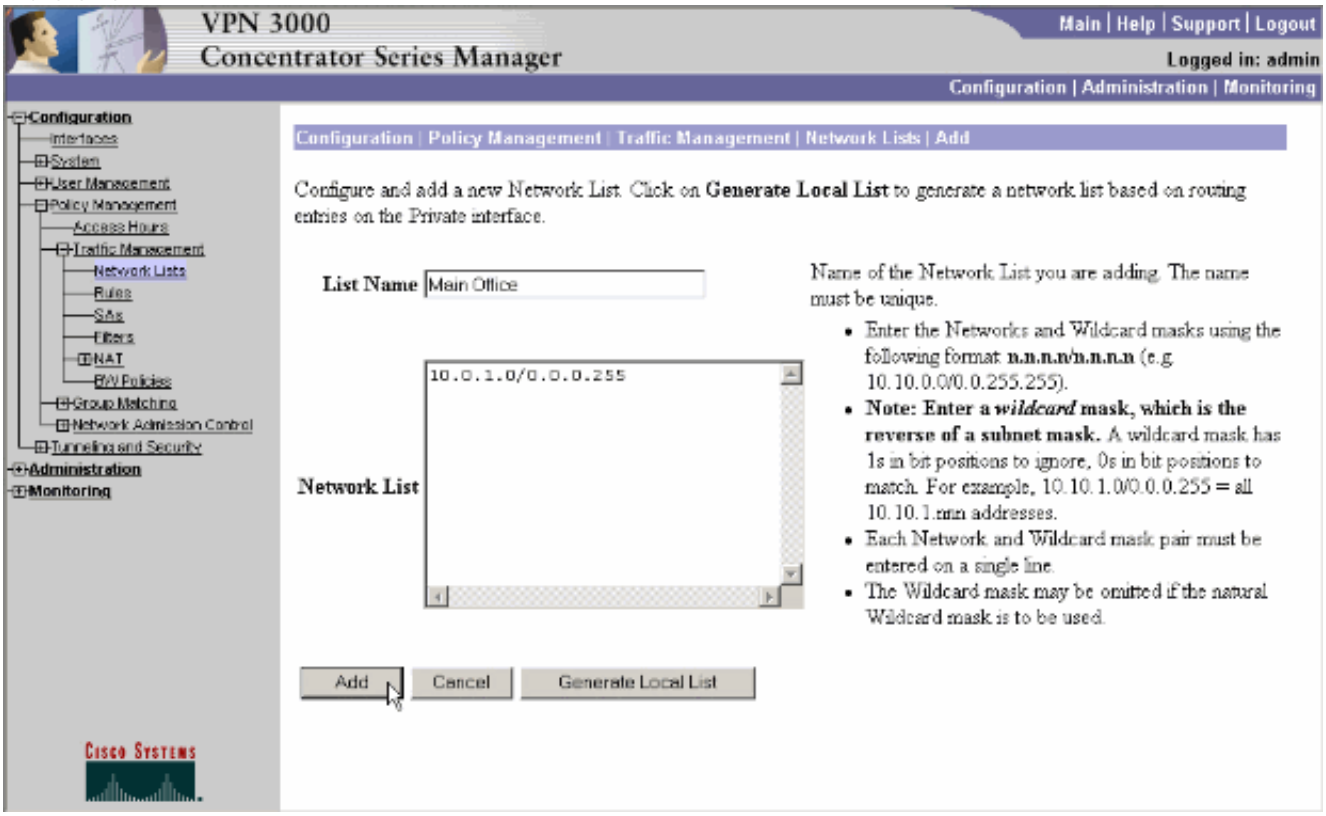
1. Escolha **Configuration > Policy Management > Traffic Management > Network Lists** e clique em
Add.



2. Essa lista define as redes de destino para as quais o VPN Client envia tráfego criptografado. Insira essas redes manualmente ou clique em **Gerar lista local** para criar uma lista com base em entradas de roteamento na interface privada do VPN Concentrator.Neste exemplo, a lista foi criada
automaticamente.

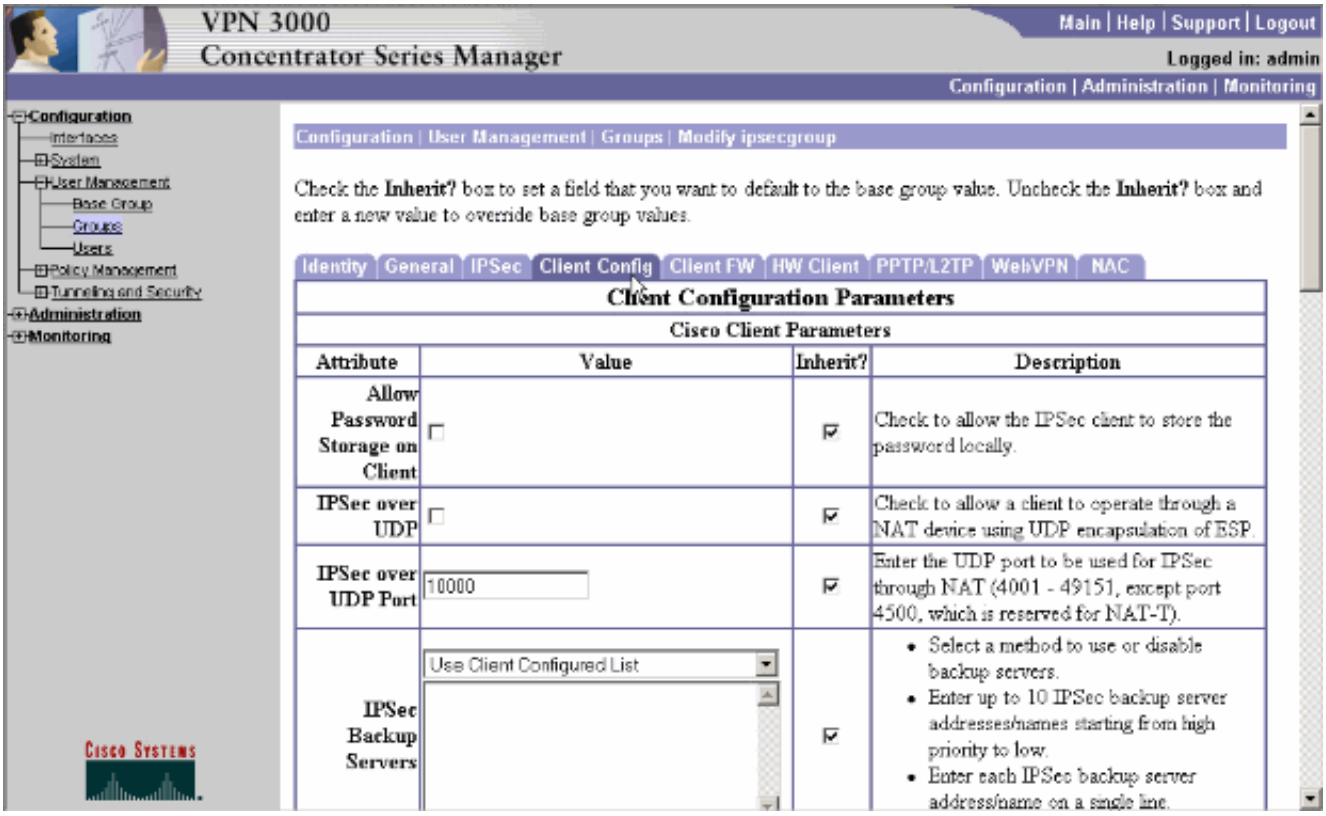


3. Depois de criada ou preenchida, forneça um nome para a lista e clique em **Adicionar**.

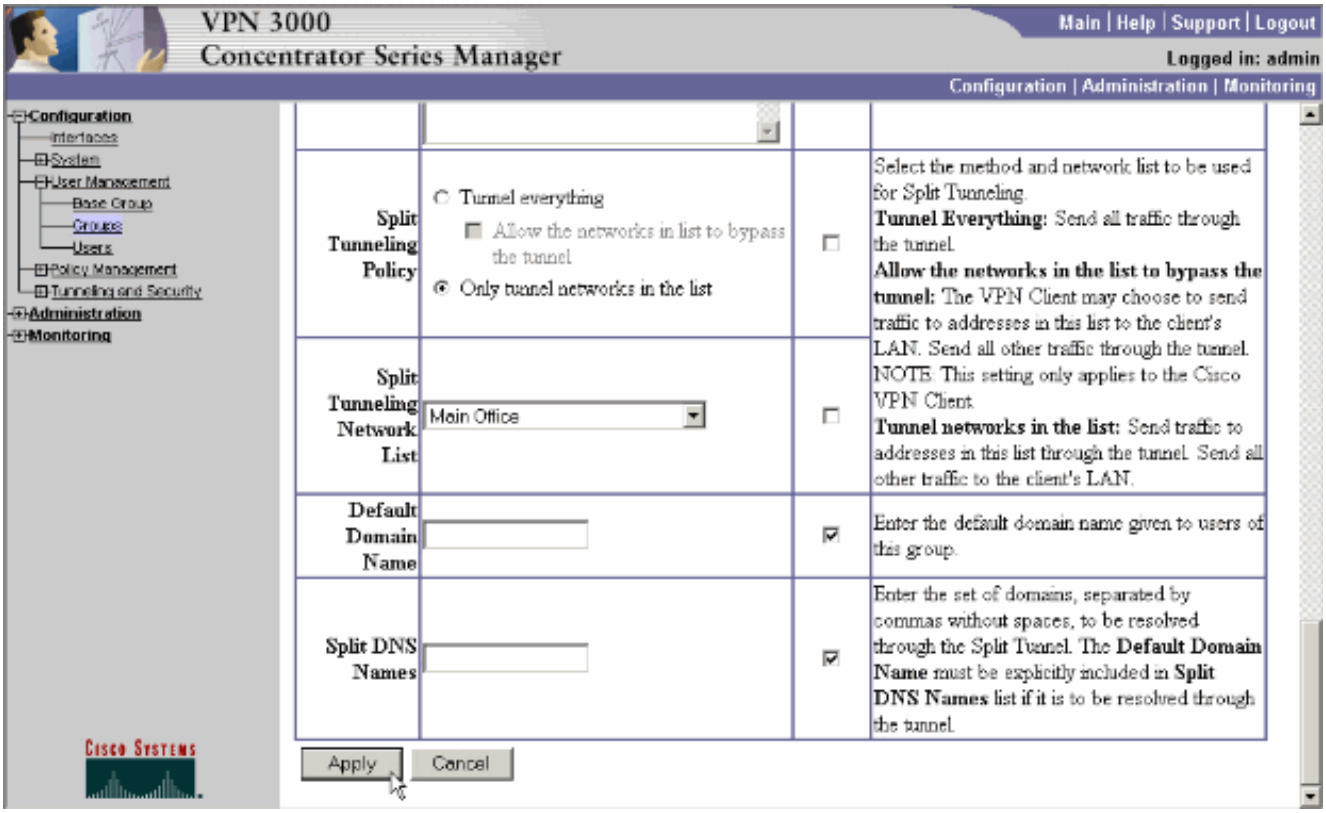


4. Depois de criar a lista de rede, atribua-a a um grupo de túneis. Escolha **Configuration > User Management > Groups**, selecione o grupo que deseja alterar e clique em **Modify Group**.

5. Vá até a guia Client Config do grupo que você escolheu modificar.



6. Role para baixo até as seções Split Tunneling Policy e Split Tunneling Network List e clique em **Only tunnel networks na lista**.
7. Escolha a lista criada anteriormente na lista suspensa. Neste caso, é o **escritório central**. O Herdar? as caixas de seleção são automaticamente esvaziadas em ambos os casos.



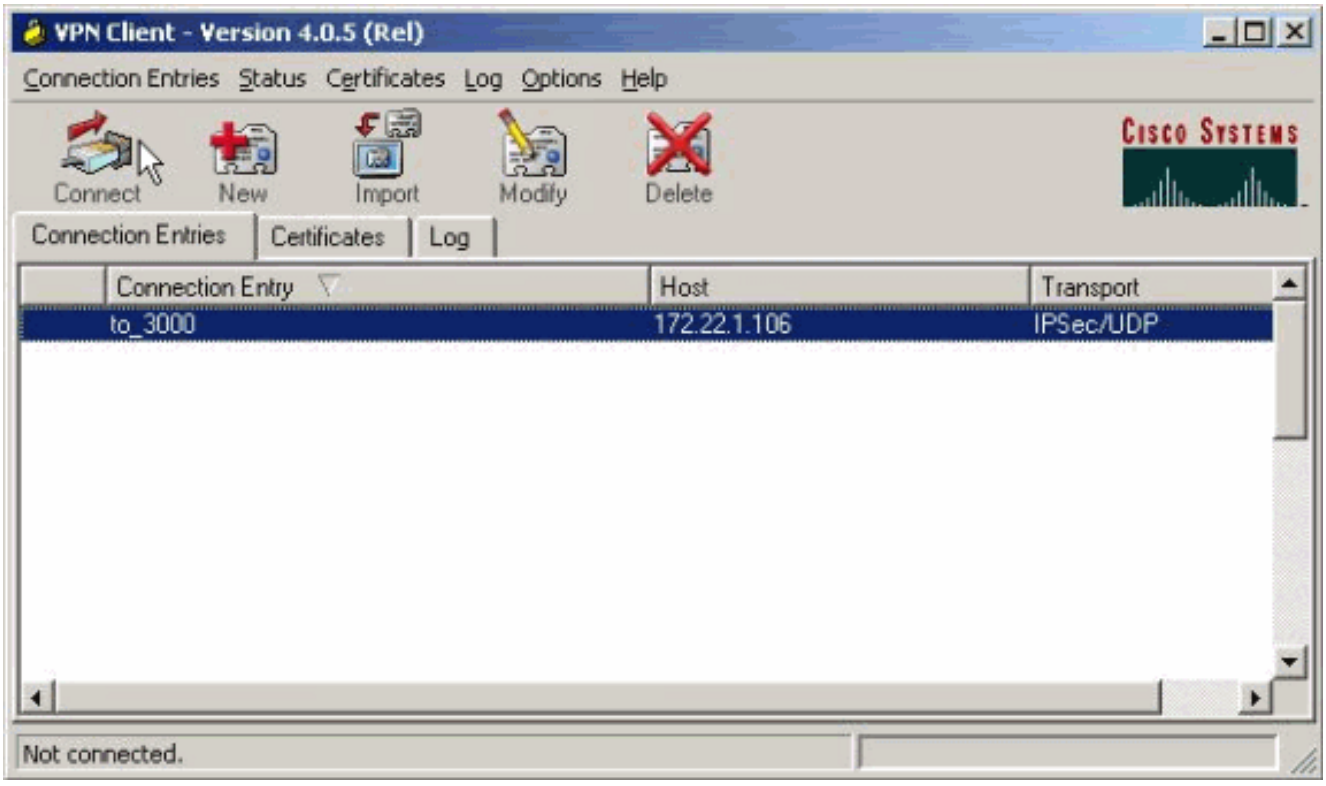
8. Clique em **Apply** quando terminar.

Verificar

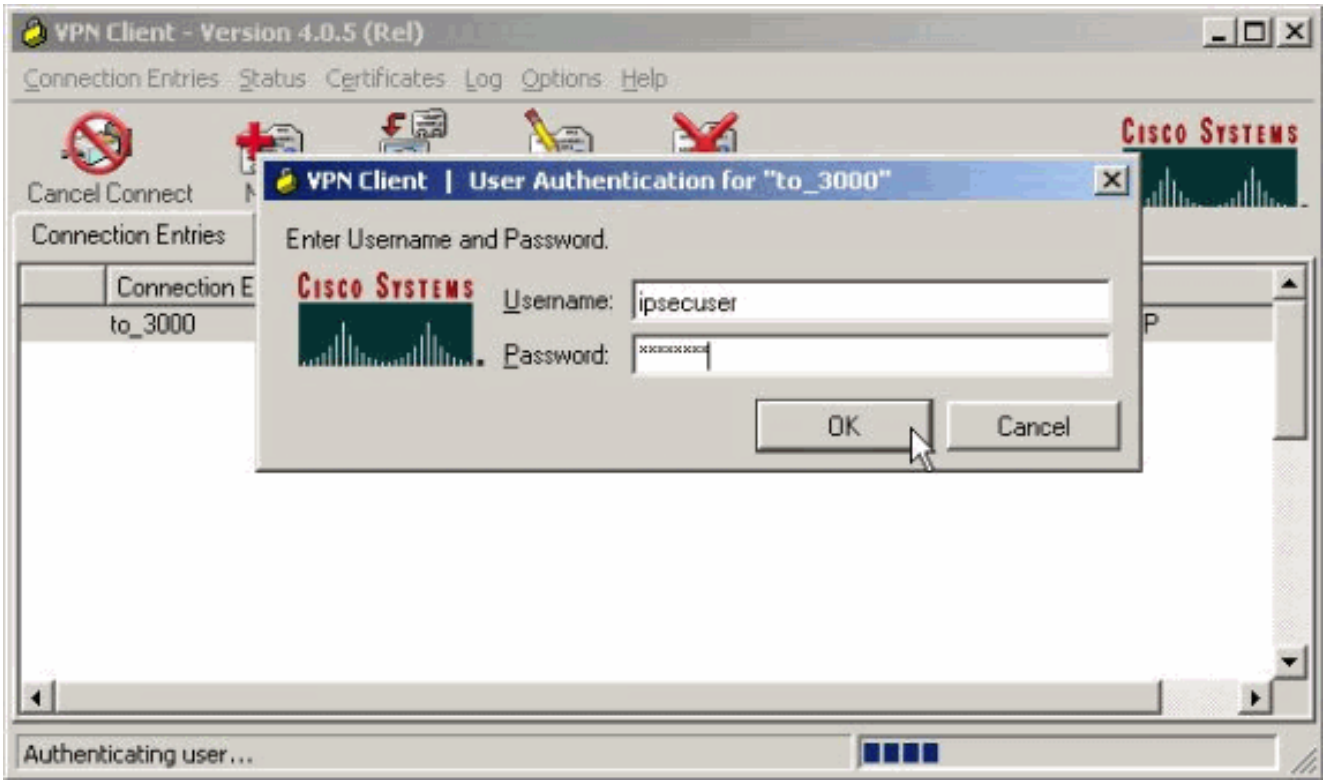
Conexão com o Cliente VPN

Conecte seu VPN Client ao VPN Concentrator para verificar sua configuração.

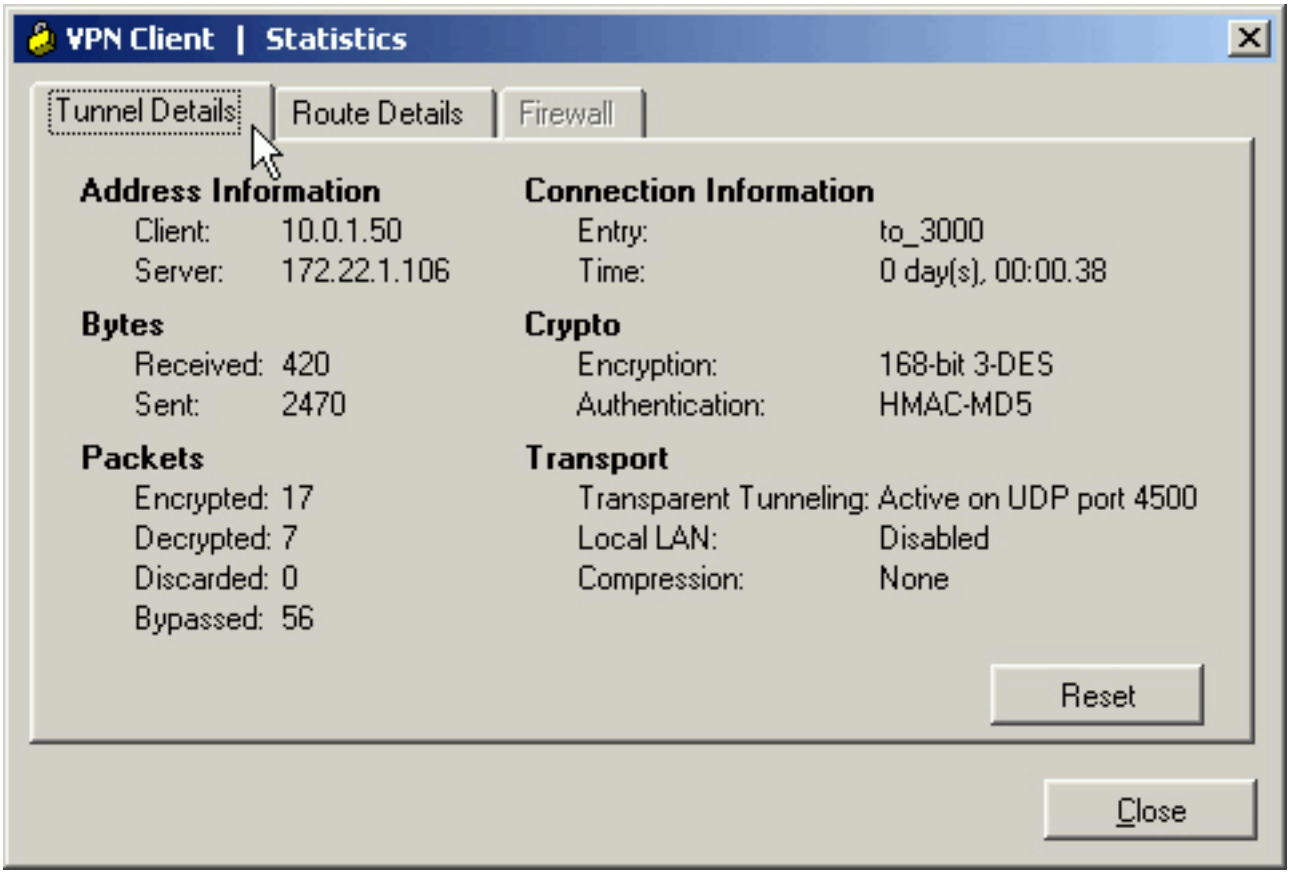
1. Selecione sua entrada de conexão da lista e clique em **Connect**.



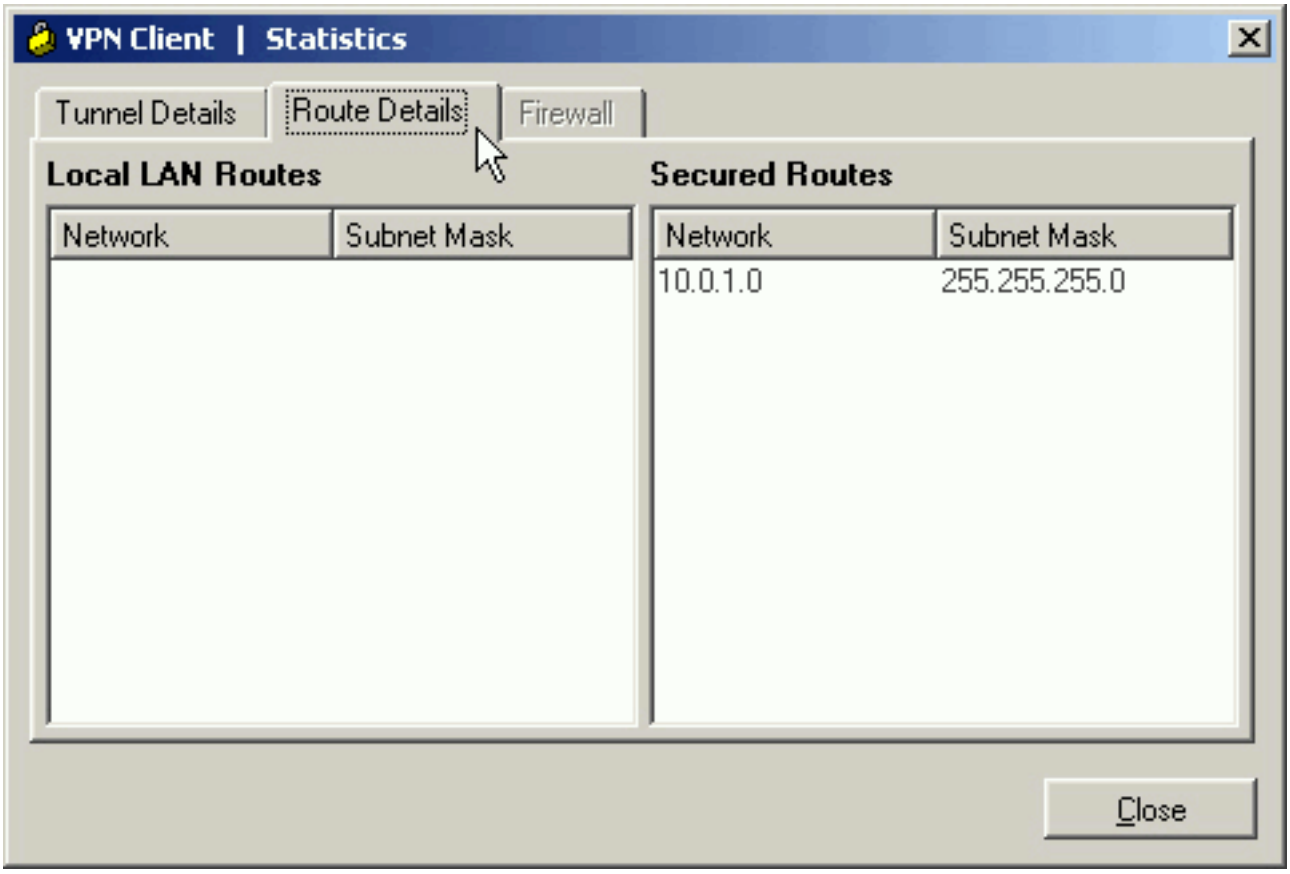
2. Digite suas credenciais.



3. Escolha **Status > Estatísticas...** para exibir a janela Detalhes do túnel onde você pode inspecionar os detalhes do túnel e ver o tráfego fluindo.

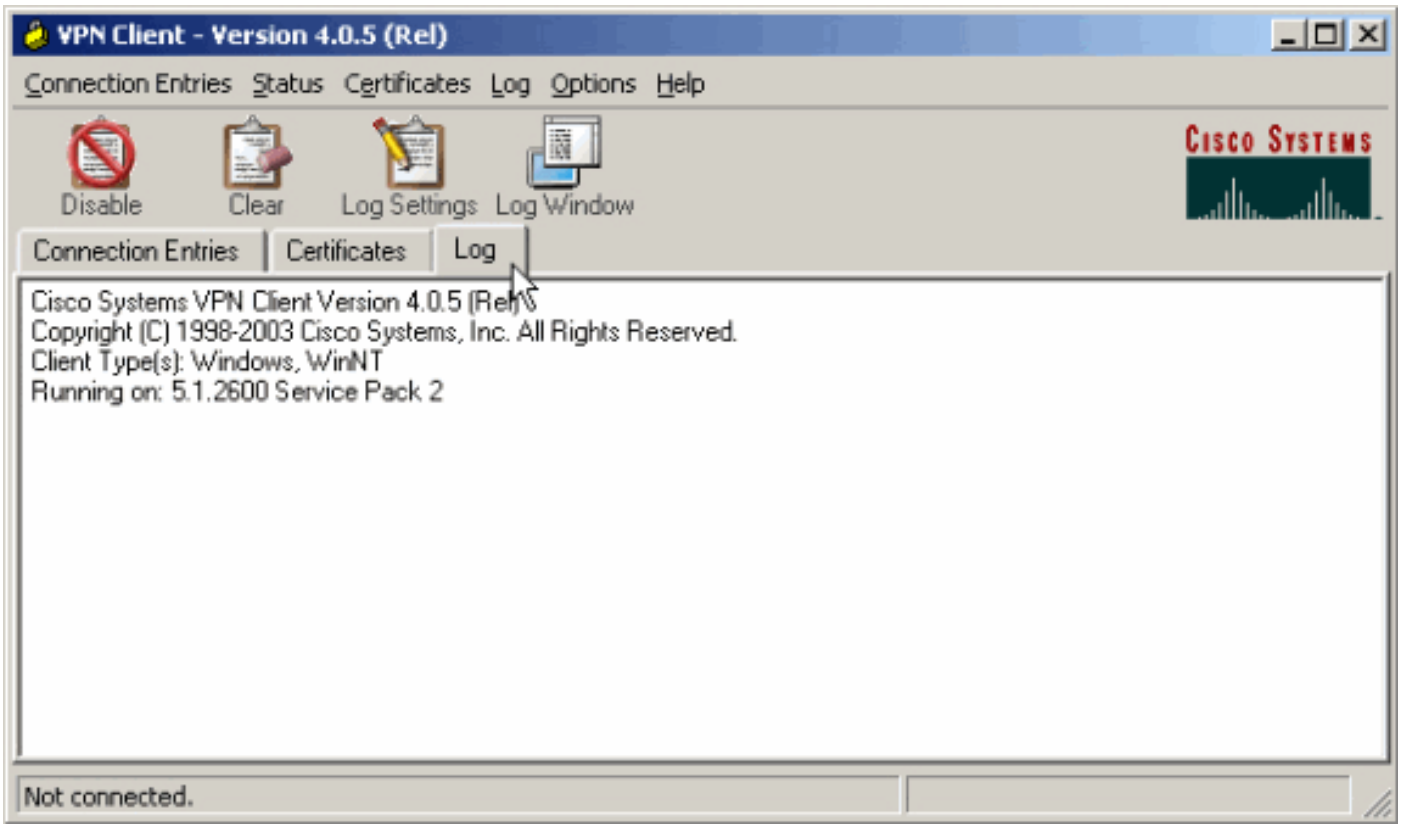


4. Vá até a guia Route Details (Detalhes da rota) para ver para quais redes o VPN Client envia tráfego criptografado. Neste exemplo, o VPN Client se comunica com segurança com 10.0.1.0/24 enquanto todo o tráfego restante é enviado sem criptografia para a Internet.



Exibir o log do cliente VPN

Ao examinar o log do VPN Client, você pode determinar se o parâmetro que permite o tunelamento dividido está definido ou não. Acesse a guia Log no VPN Client para visualizar o log. Clique em **Configurações de log** para ajustar o que está registrado. Neste exemplo, IKE e IPsec são definidos como **3- High** enquanto todos os outros elementos de log são definidos como **1 - Low**.



```
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

Consulte Exemplo de Configuração de IPsec com VPN Client para VPN 3000 Concentrator - Troubleshooting para obter informações gerais sobre Troubleshooting desta configuração.

Informações Relacionadas

- Exemplo de configuração de IPsec com VPN Client para VPN 3000 Concentrator
- Cisco VPN 3000 Series Concentrators
- Cisco VPN Client
- Suporte Técnico e Documentação - Cisco Systems