VPN 3000 集中器上针对 VPN Client 使用分割隧道的配置示例

目录

简介

本文档提供有关如何允许 VPN 客户端在通过隧道技术进入 VPN 3000 系列集中器时访问互联网的分步说明。此配置允许 VPN 客户端在无法安全访问 Internet 时通过 IPsec 安全地访问公司资源。

注意：配置分割隧道时，可能会带来安全风险。由于 VPN 客户端不安全地访问 Internet，因此可能会受到攻击者的安全威胁。然后，该攻击者可以通过 IPSec 隧道访问公司 LAN。可以在完全隧道和分割隧道之间进行折衷，以允许 VPN 客户端仅访问本地 LAN。有关更多信息，请参阅允许 VPN 客户端在 VPN 3000 集中器上进行本地 LAN 访问的配置示例。

先决条件

要求

本文档假定 VPN 集中器上已存在有效的远程访问 VPN 配置。如果尚未配置 IPsec，请参阅 VPN 客户端与 VPN 3000 集中器之间的 IPsec 配置示例。

使用的组件

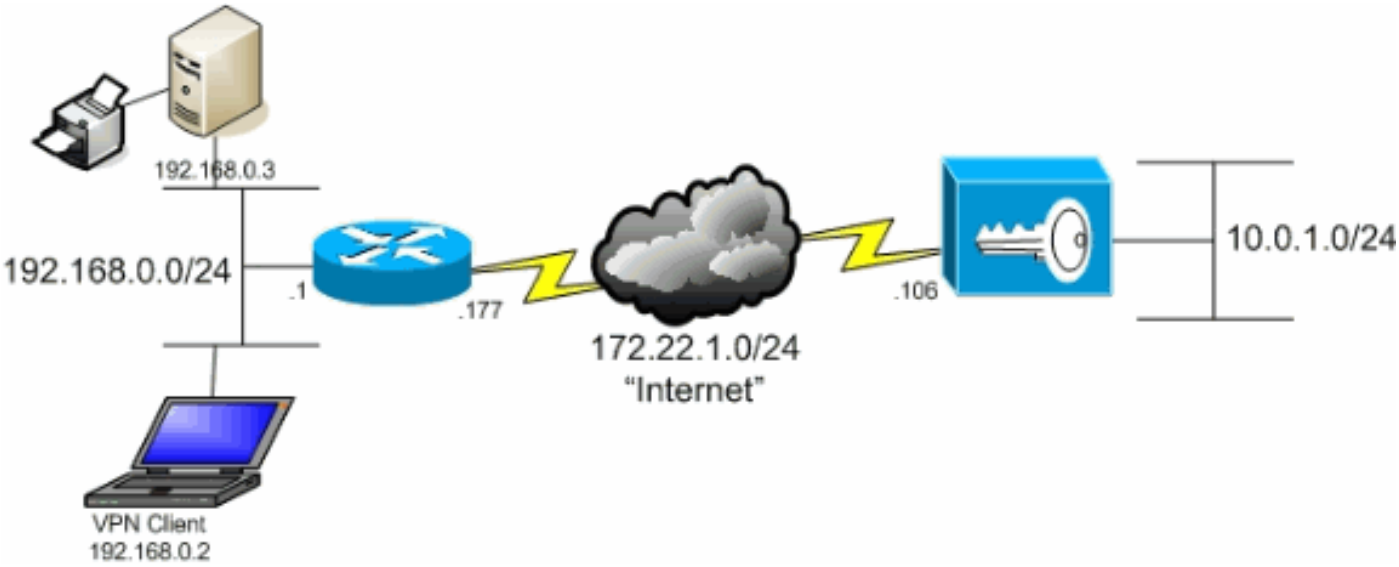
本文档中的信息基于以下软件和硬件版本：

- Cisco VPN 3000 集中器系列软件版本 4.7.2.H
- Cisco VPN 客户端 4.0.5 版

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

网络图

VPN 客户端位于典型的 SOHO 网络中，并通过 Internet 连接到总部。



规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

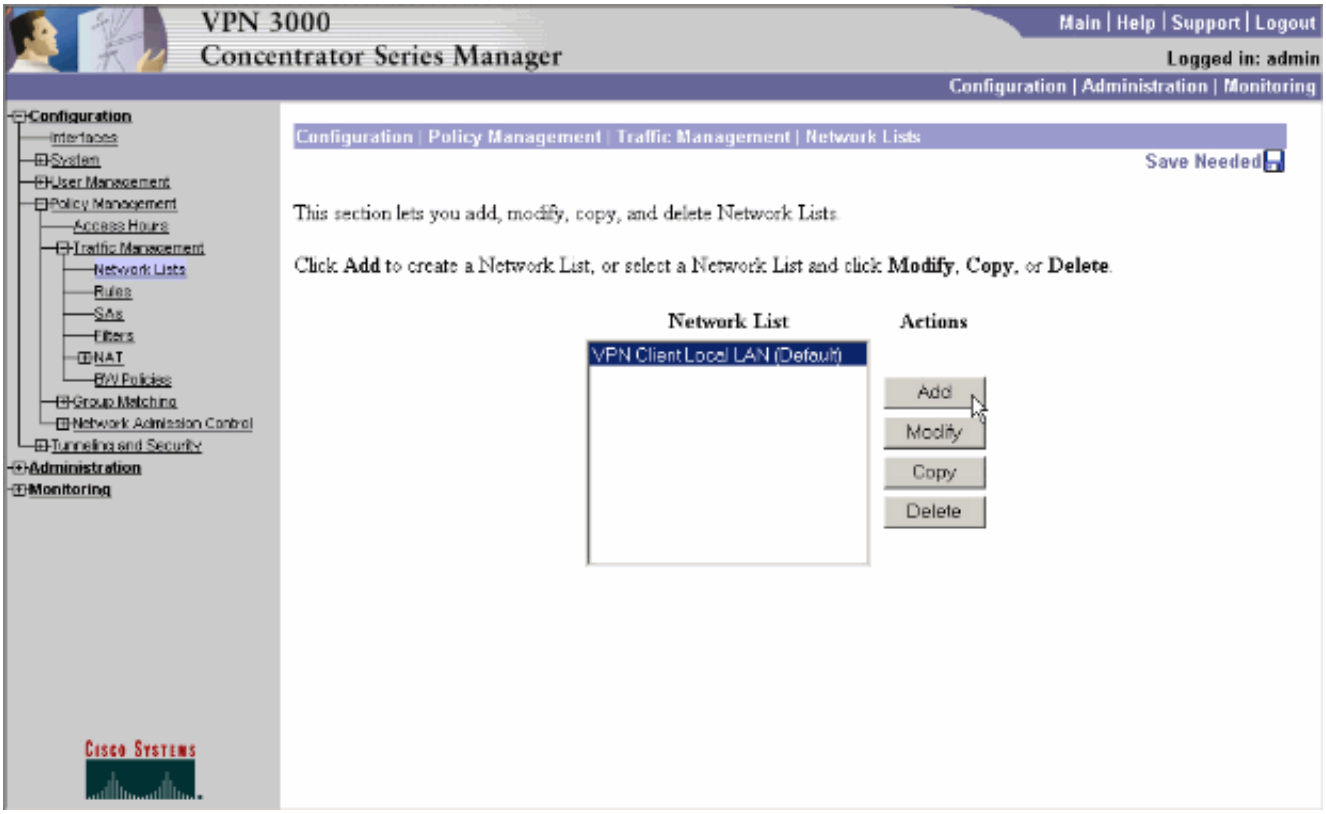
背景信息

在 VPN 客户端至 VPN 集中器的基本场景中，VPN 客户端的所有流量将加密并发送至 VPN 集中器，不论目标为何。根据您的配置和支持的用户数量，此设置可变为带宽密集型设置。分割隧道可通过允许用户在隧道上只发送去往企业网络的流量来缓解此问题。所有其他流量（例如 IM、邮件或随意浏览）将通过 VPN 客户端的本地 LAN 发送至互联网。

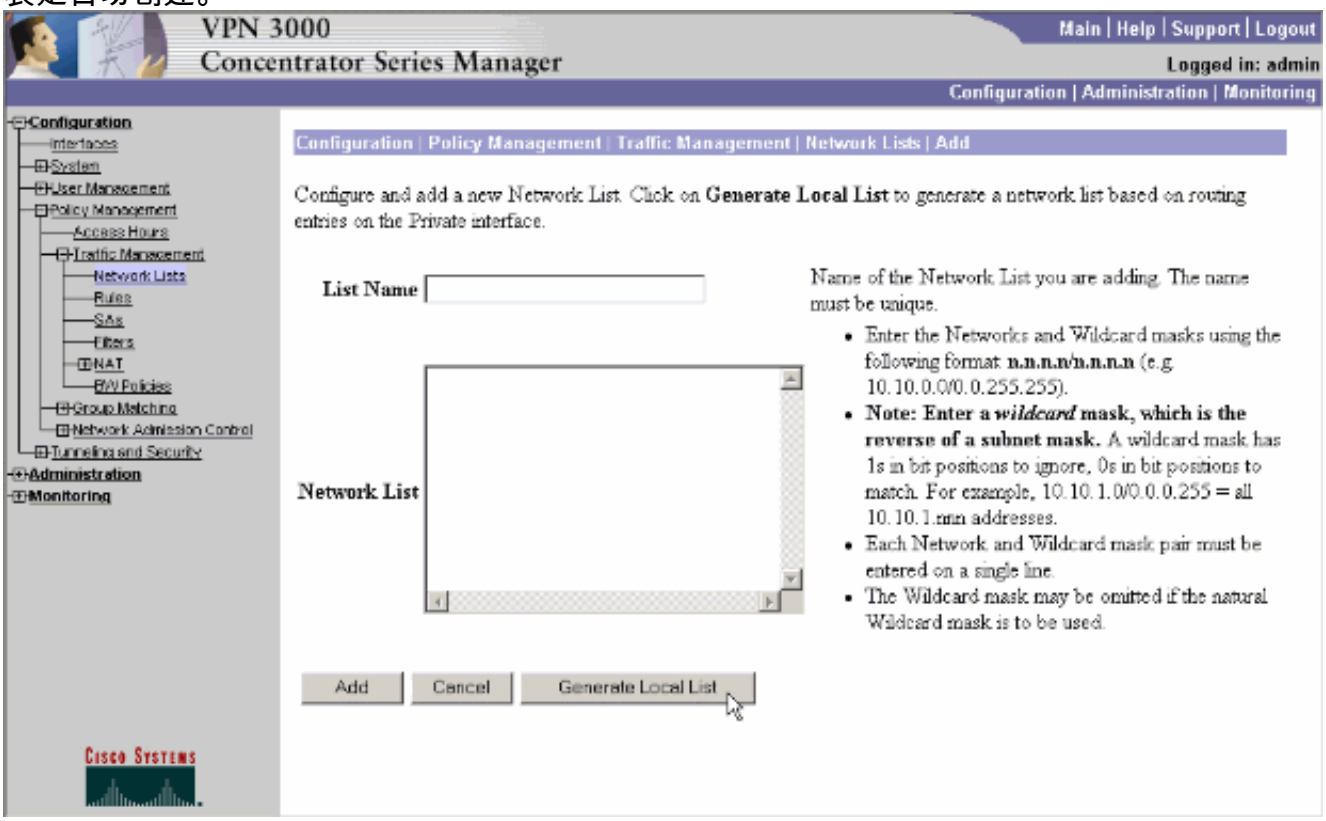
在 VPN 集中器上配置分割隧道

完成以下步骤来配置隧道组，以便允许为组中的用户配置分割隧道。首先创建一个网络列表。此列表定义了 VPN 客户端要向其发送加密流量的目标网络。创建列表后，将列表添加到客户端隧道组的分割隧道策略。

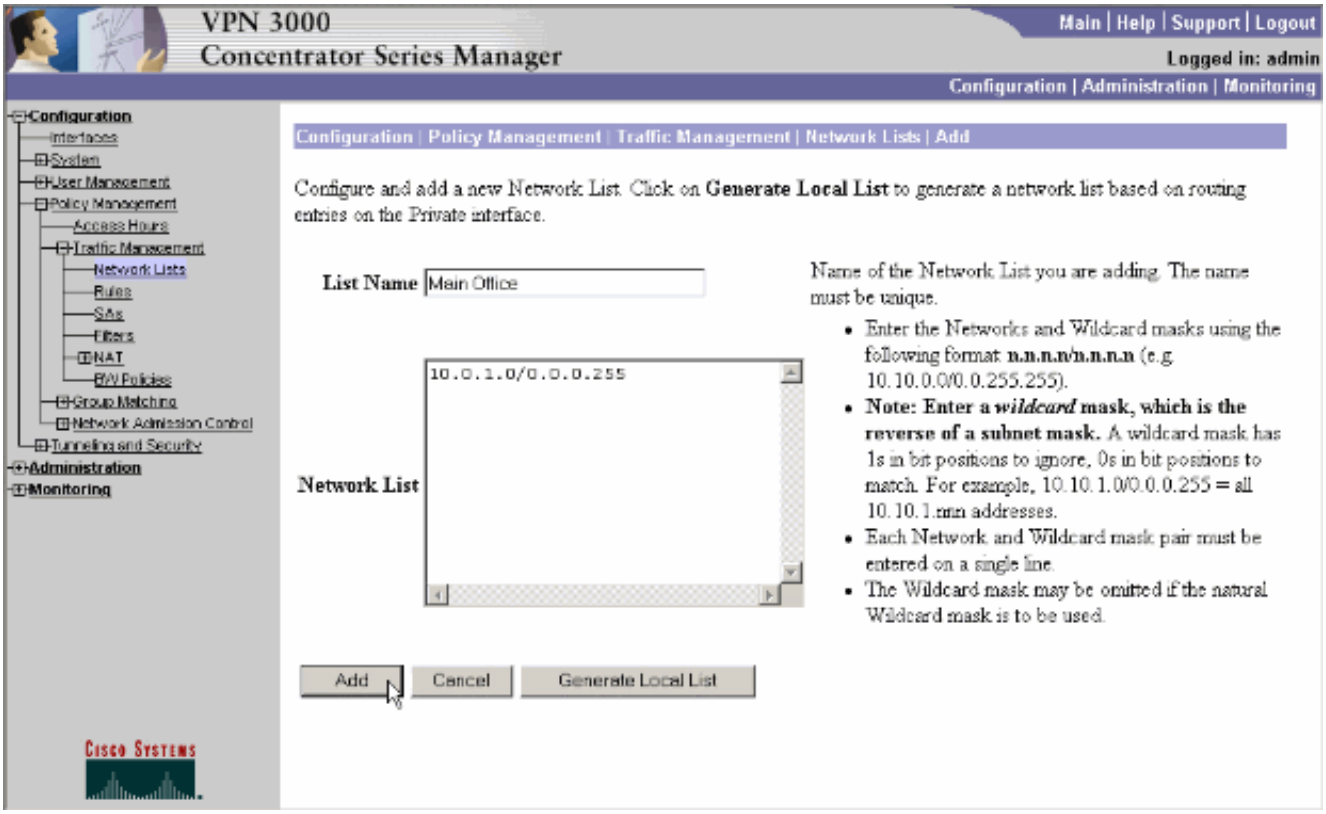
1. 选择 **Configuration > Policy Management > Traffic Management > Network Lists** 并点击 **Add**。



2. 此列表定义了 VPN 客户端要向其发送加密流量的目标网络。手动输入这些网络，或点击 **Generate Local List 以根据 VPN 集中器的专用接口的路由条目创建一个列表。**在本例中，列表是自动创建。

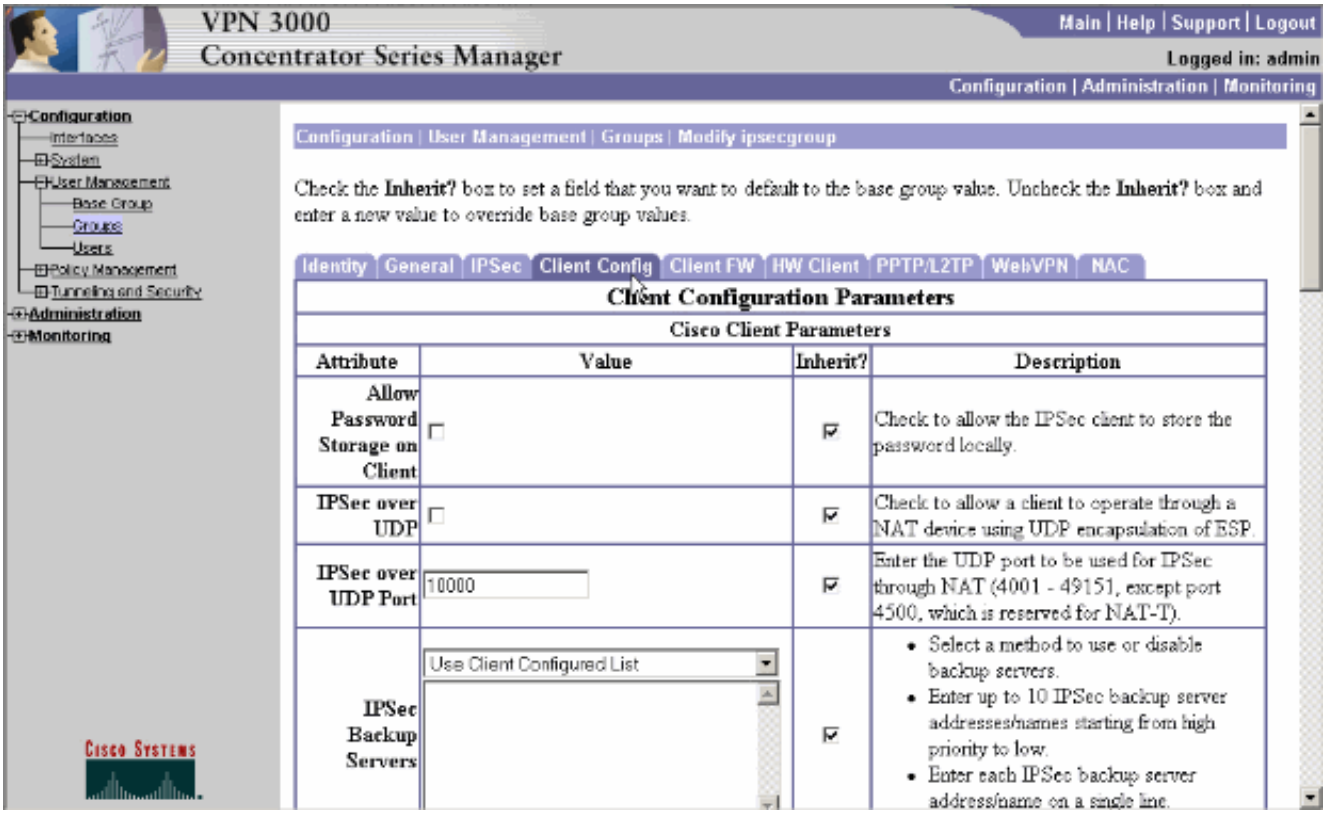


3. 创建或填充列表后，为列表提供一个名称并点击 **Add**。

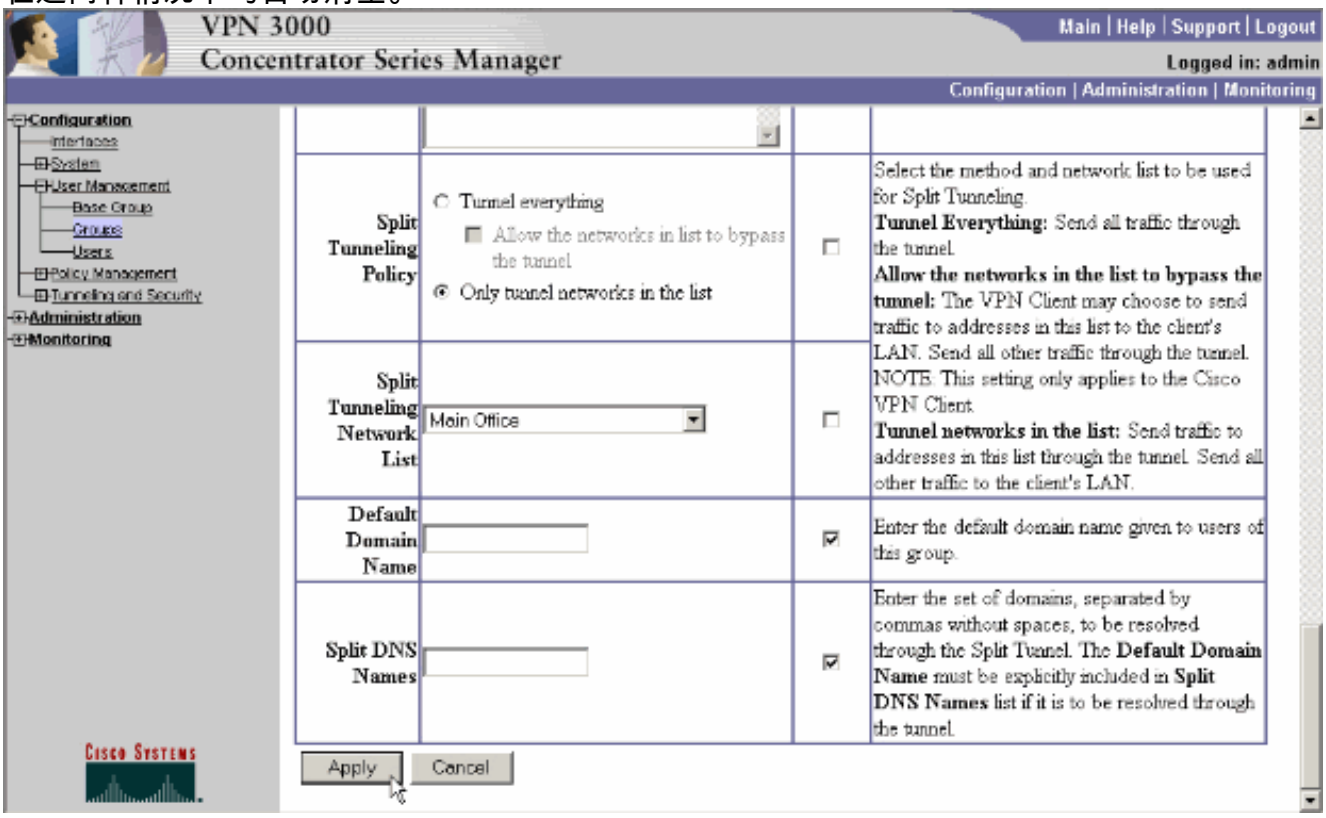


4. 创建网络列表后，将其分配到隧道组。选择 **Configuration > User Management > Groups**，然后选择您希望更改的组，然后再单击 **Modify Group**。

5. 移至已选择要修改的组的 Client Config 选项卡。



6. 向下滚动至 Split Tunneling Policy 和 Split Tunneling Network List 部分并点击**列表中的 Only tunnel networks**。
7. 从下拉列表中选择此前创建的列表。在本例中，选择的列表为 **Main Office**。“Inherit?”复选框在这两种情况下均自动清空。



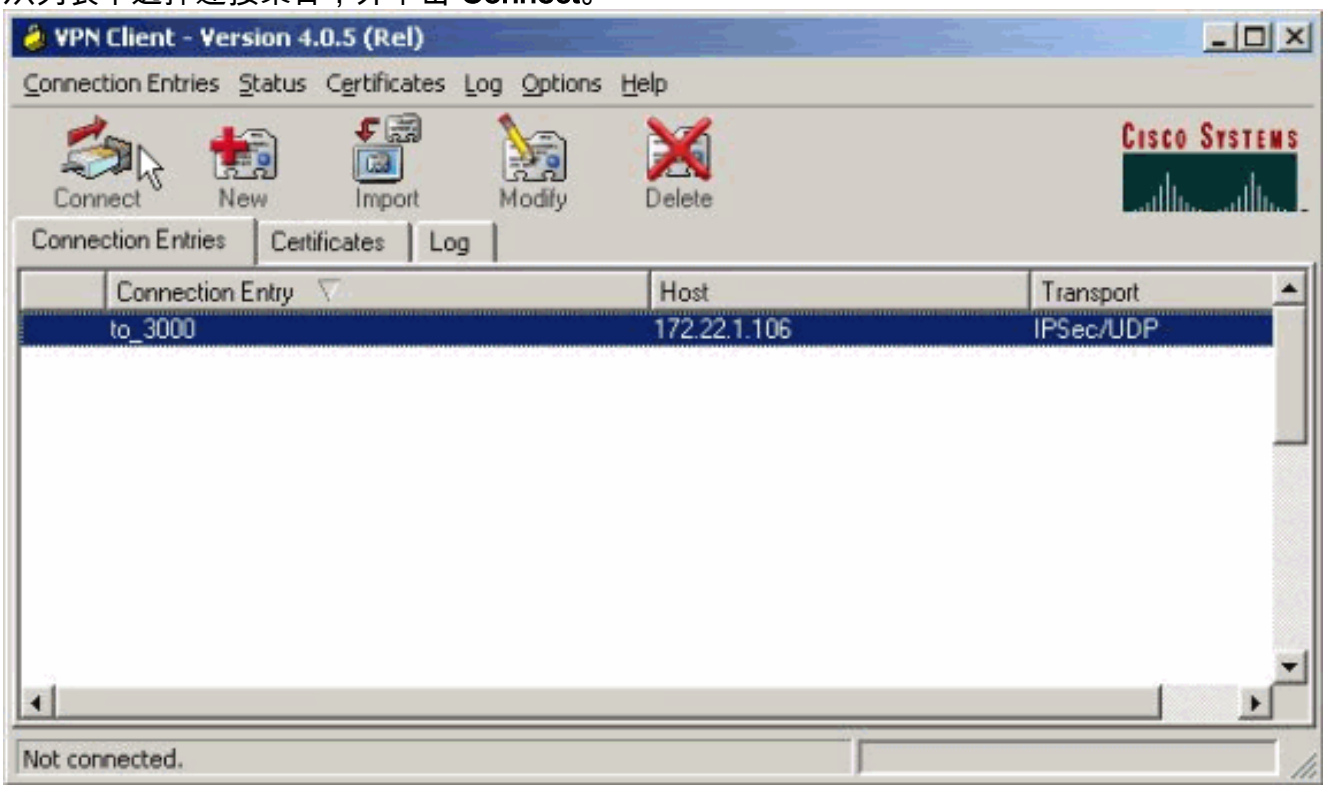
8. 完成后，请单击 **Apply**。

验证

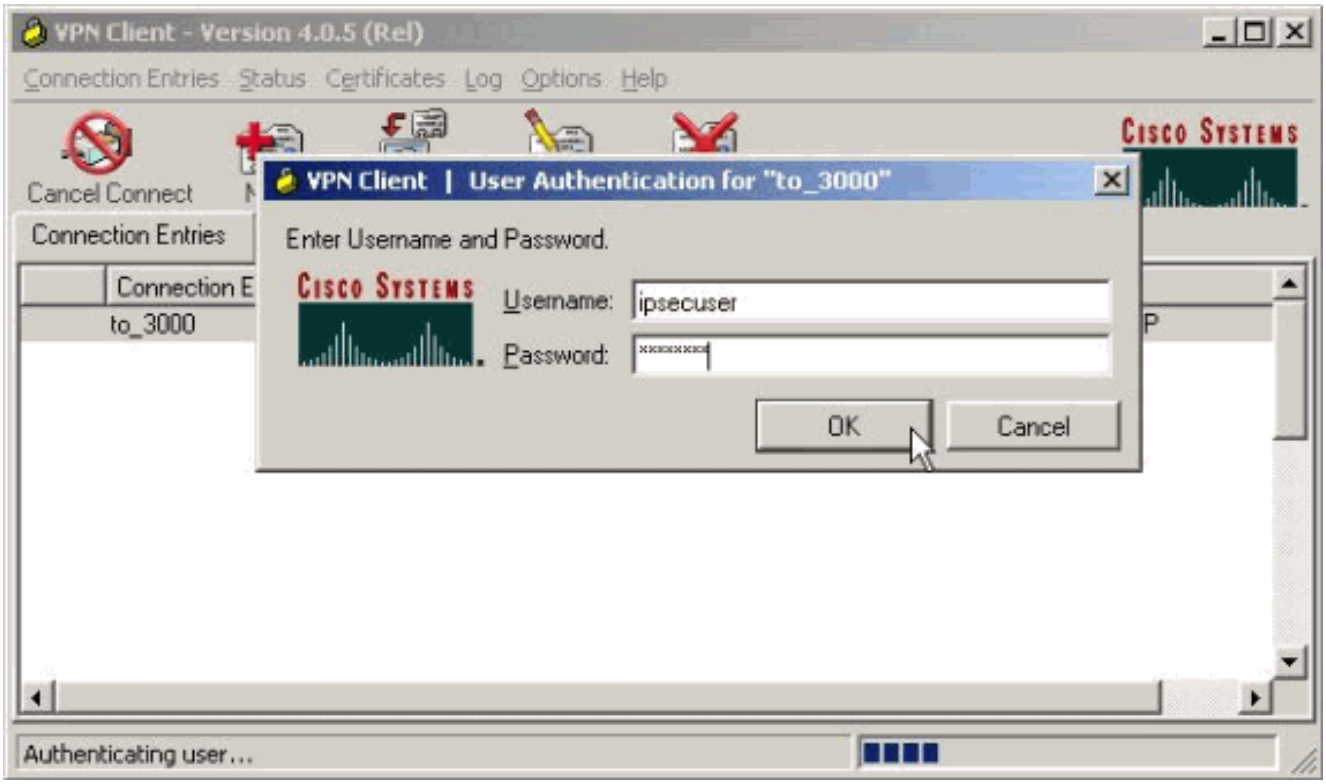
连接 VPN 客户端

将 VPN 客户端连接到 VPN 集中器，以便验证配置。

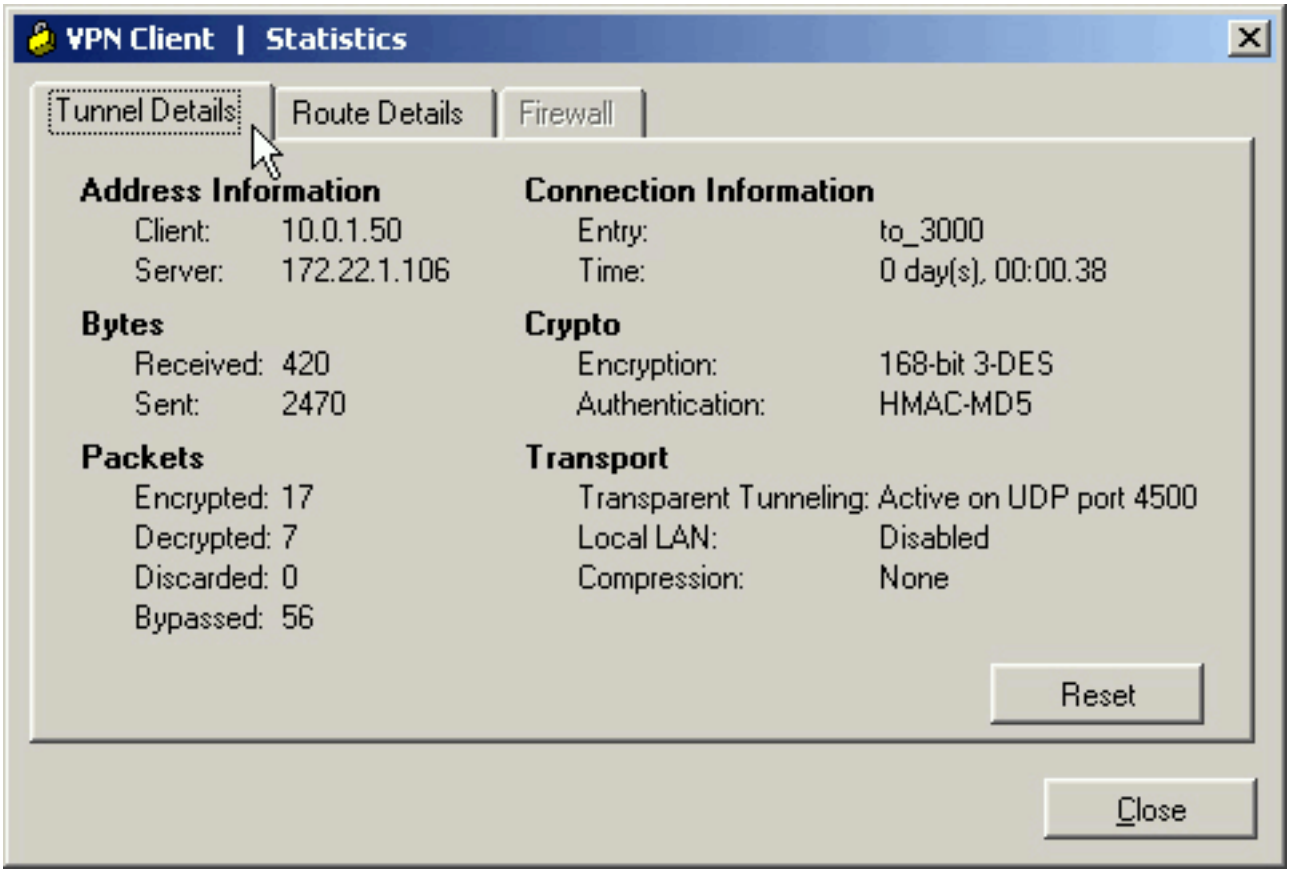
1. 从列表中选择连接条目，并单击 **Connect**。



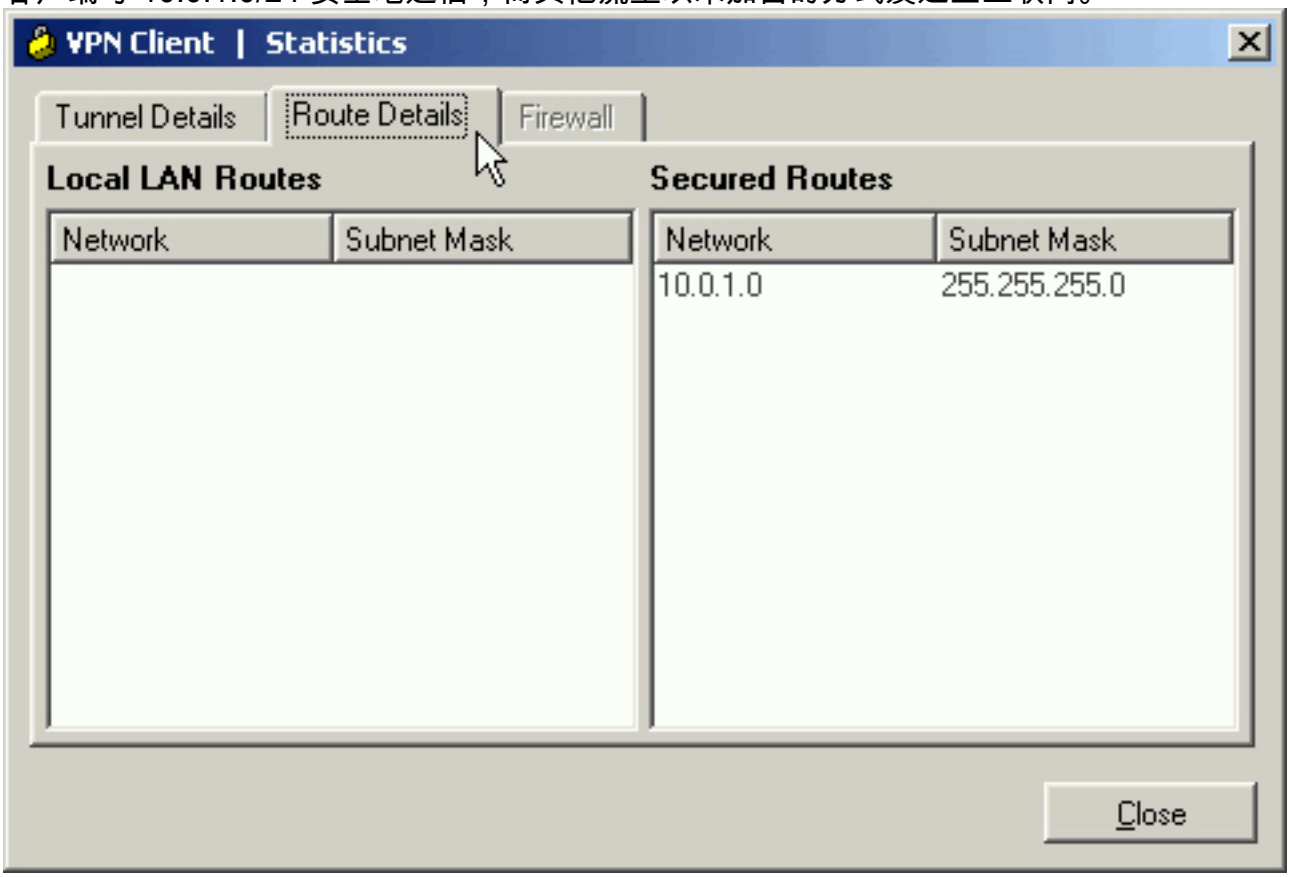
2. 输入您的凭证。



3. 选择 **Status > Statistics... 以便显示 Tunnel Details 窗口，您可以在此窗口中检查隧道特定信息并查看数据流。**



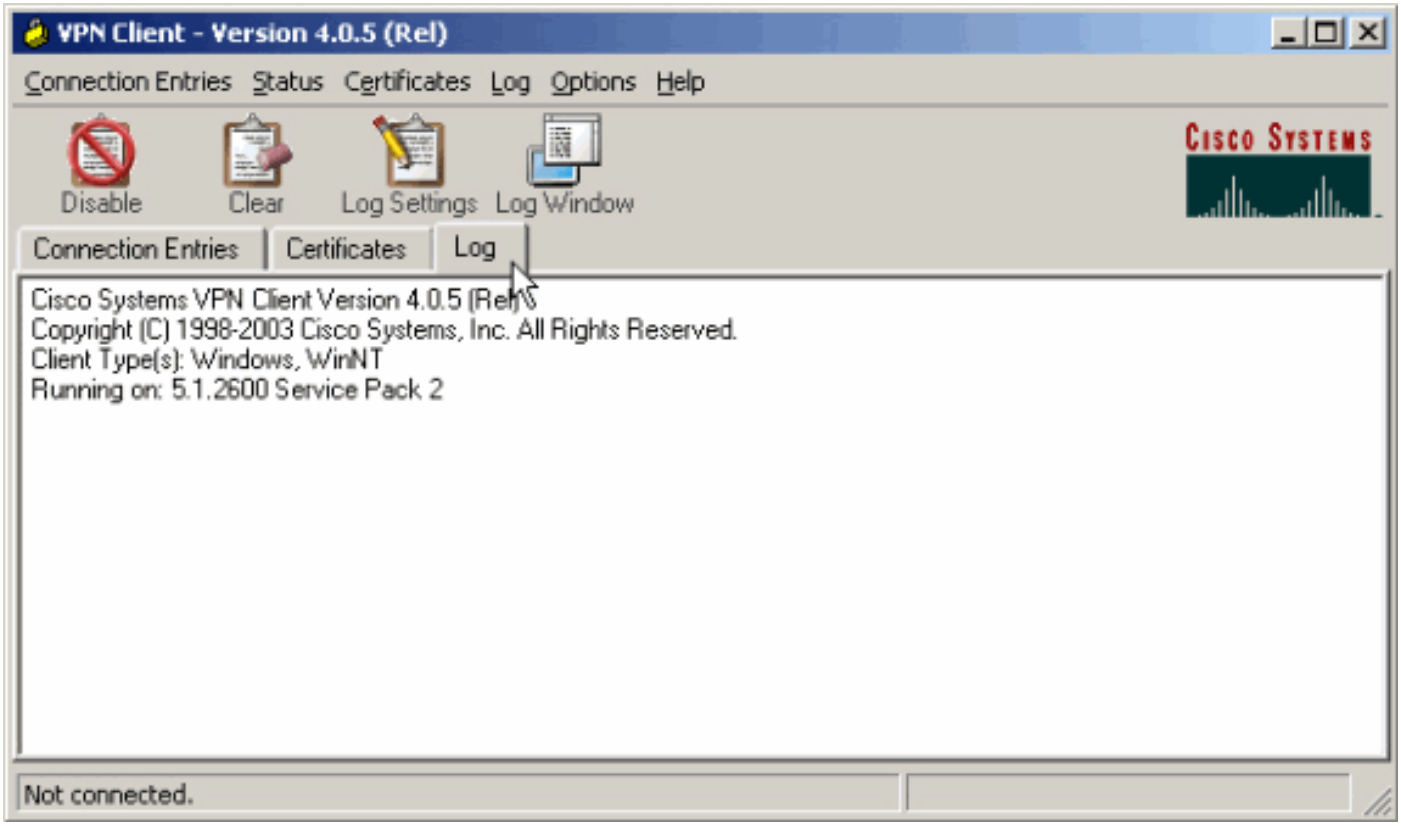
4. 移至 Route Details 选项卡以查看 VPN 客户端要向其发送加密流量的网络。在本例中，VPN 客户端与 10.0.1.0/24 安全地通信，而其他流量以未加密的方式发送至互联网。



查看 VPN 客户端日志

当您检查 VPN 客户端日志时，您可以确定是否设置允许分割隧道的参数。移至 VPN 客户端中的 Log 选项卡以查看日志。点击 **Log Settings 以调整记录的内容。**在本示例中，IKE 和 IPsec 设置为

3 - High，而所有其他日志元素均设置为 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.
```

故障排除

有关对此配置进行故障排除的一般信息，请参阅使用 VPN 客户端的 IPsec 到 VPN 3000 集中器的

配置示例 - 故障排除。

相关信息

- 使用 VPN 客户端的 IPsec 到 VPN 3000 集中器的配置示例
- Cisco VPN 3000 系列集中器
- Cisco VPN 客户端
- 技术支持和文档 - Cisco Systems