VPN 3000集中器上用於VPN客戶端的分割隧道配置示例

目錄

簡介

本文檔提供了有關如何允許VPN客戶端在通過隧道連線到VPN 3000系列集中器時訪問Internet的逐步說明。此配置允許VPN客戶端通過IPsec安全地訪問公司資源，同時提供對Internet的不安全訪問。

注意：配置分割隧道可能會帶來安全風險。因為VPN客戶端擁有對Internet的不安全訪問，所以攻擊者可能會入侵它們。然後，攻擊者可能能夠通過IPsec隧道訪問公司LAN。完全通道和分割通道之間的危害可以只允許使用VPN客戶端本地LAN訪問。有關詳細資訊，請參閱在VPN 3000集中器上允許VPN客戶端本地LAN訪問的配置示例。

必要條件

需求

本文檔假定VPN集中器上已存在有效的遠端訪問VPN配置。如果尚未配置IPsec with VPN Client to VPN 3000集中器配置示例，請參閱。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

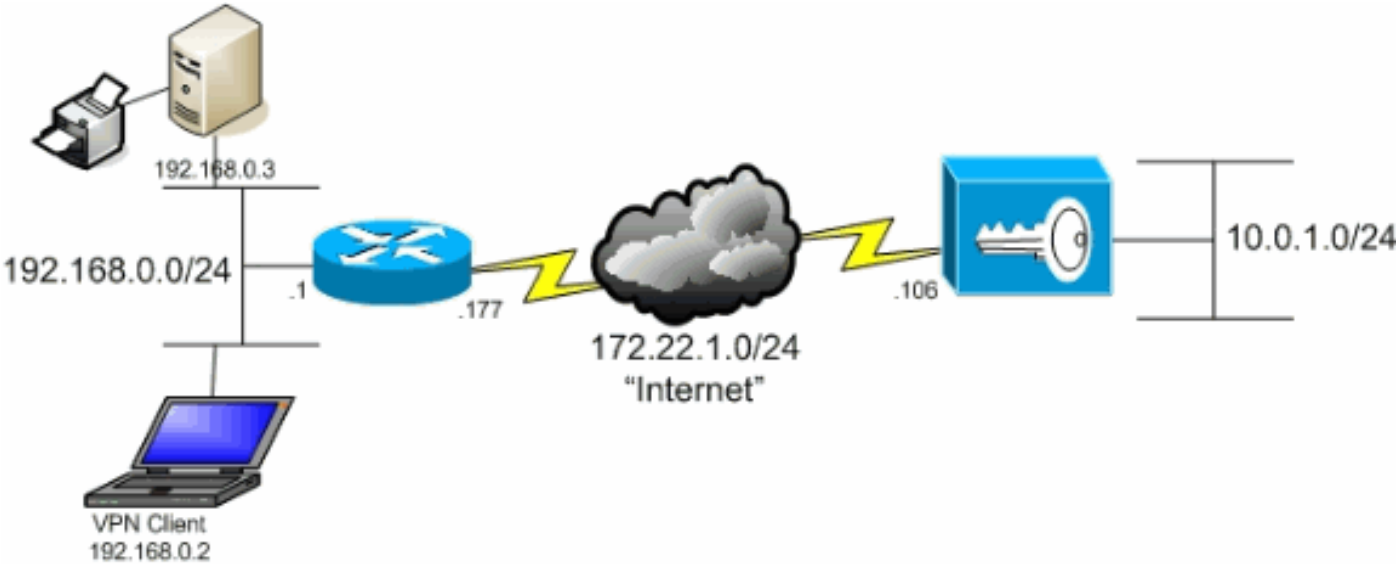
- Cisco VPN 3000 Concentrator系列軟體版本4.7.2.H

- Cisco VPN使用者端版本4.0.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

VPN客戶端位於典型的SOHO網路上，通過Internet連線到總部。



慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

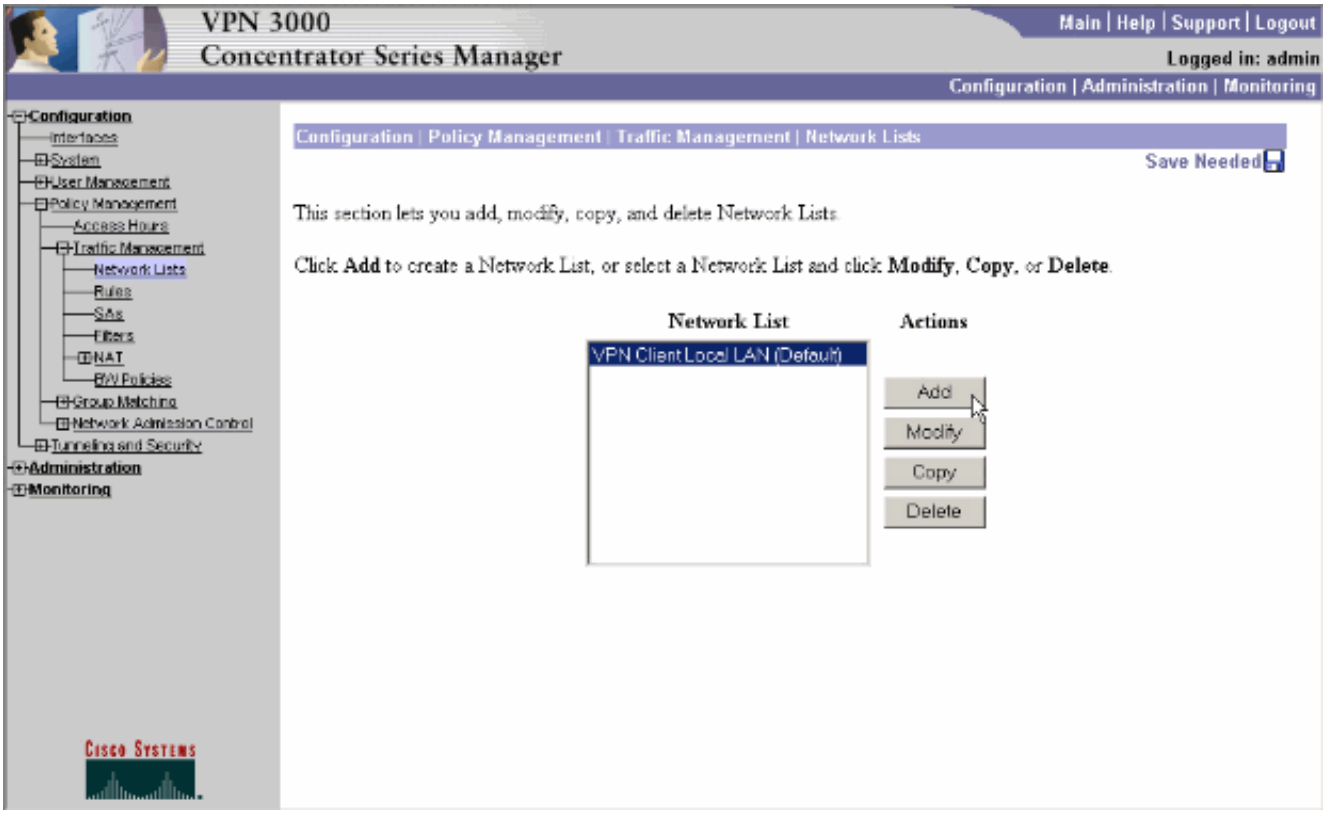
背景資訊

在基本VPN客戶端到VPN集中器場景中，無論目的地是什麼，來自VPN客戶端的所有流量都會被加密並傳送到VPN集中器。根據您的配置和支援的使用者數量，此類設定可能會佔用大量頻寬。分割通道可以透過允許使用者透過通道僅傳送目的地為公司網路的流量來緩解此問題。所有其他流量（例如IM、電子郵件或隨意瀏覽）均通過VPN客戶端的本地LAN傳送到網際網路。

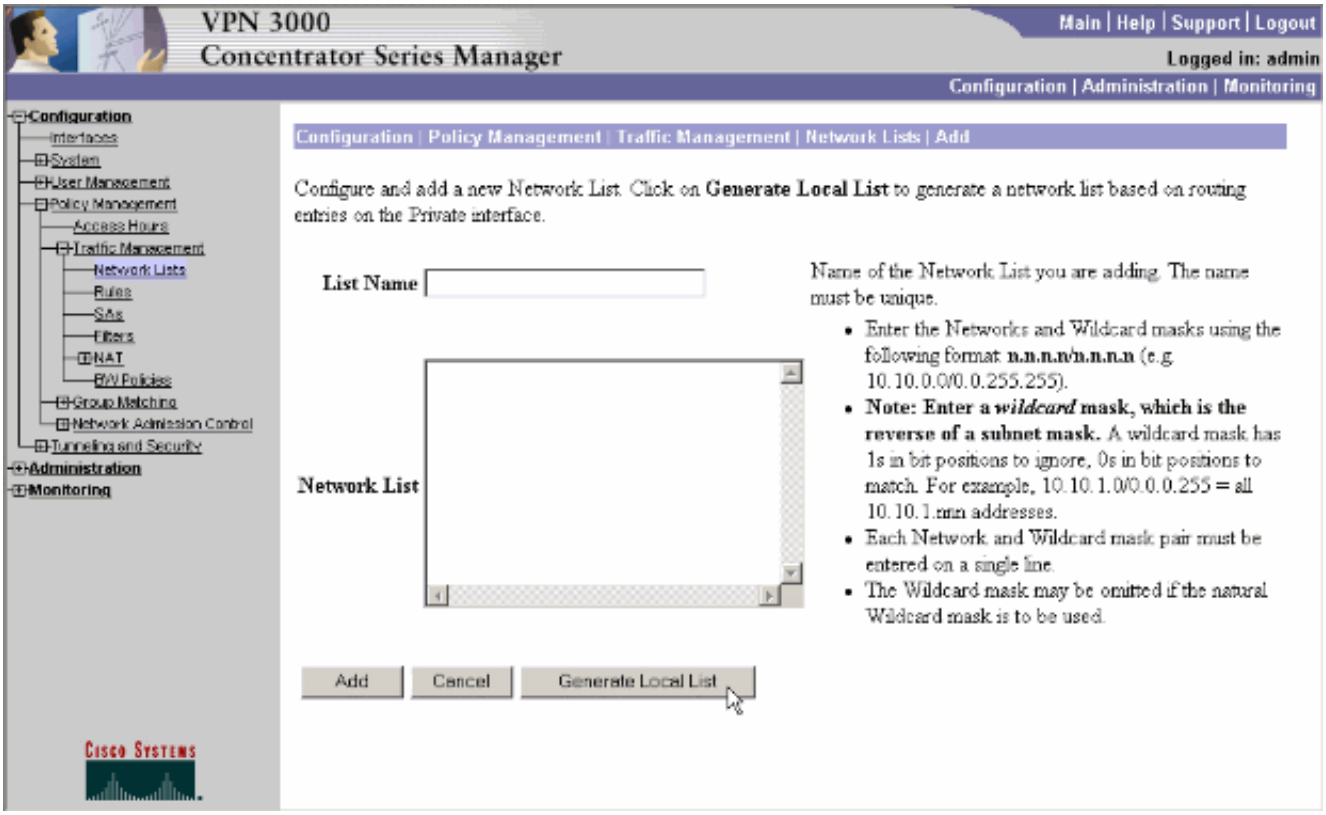
在VPN集中器上配置拆分隧道

完成這些步驟，將通道組配置為允許組內使用者使用分割通道。首先建立網路清單。此清單定義VPN客戶端向其傳送加密流量的目標網路。建立該清單後，將該清單新增到客戶端隧道組的拆分隧道策略中。

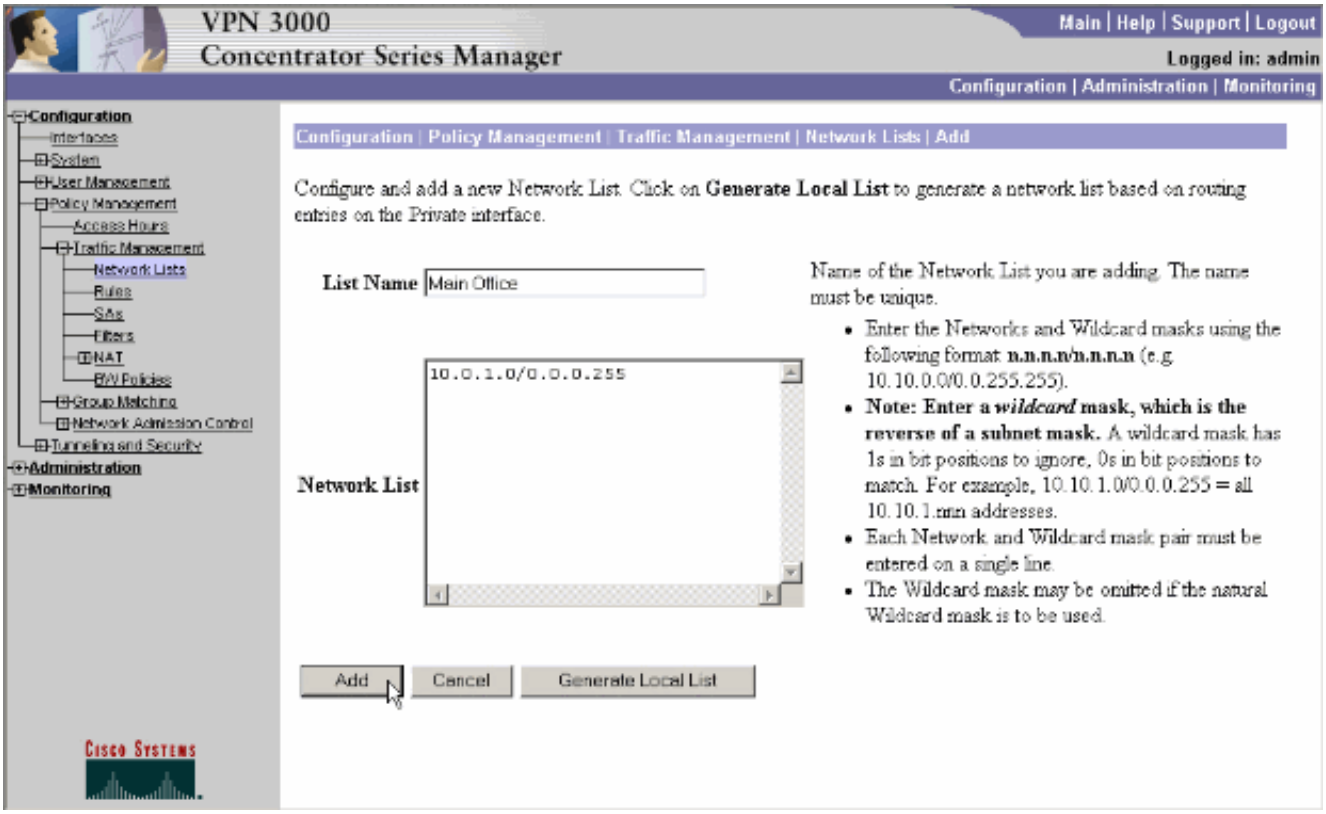
1. 選擇**Configuration > Policy Management > Traffic Management > Network Lists**，然後點選**Add**。



2. 此清單定義VPN客戶端向其傳送加密流量的目標網路。手動輸入這些網路，或按一下**Generate Local List**以根據VPN集中器專用介面上的路由條目建立清單。在此示例中，清單是自動建立的。

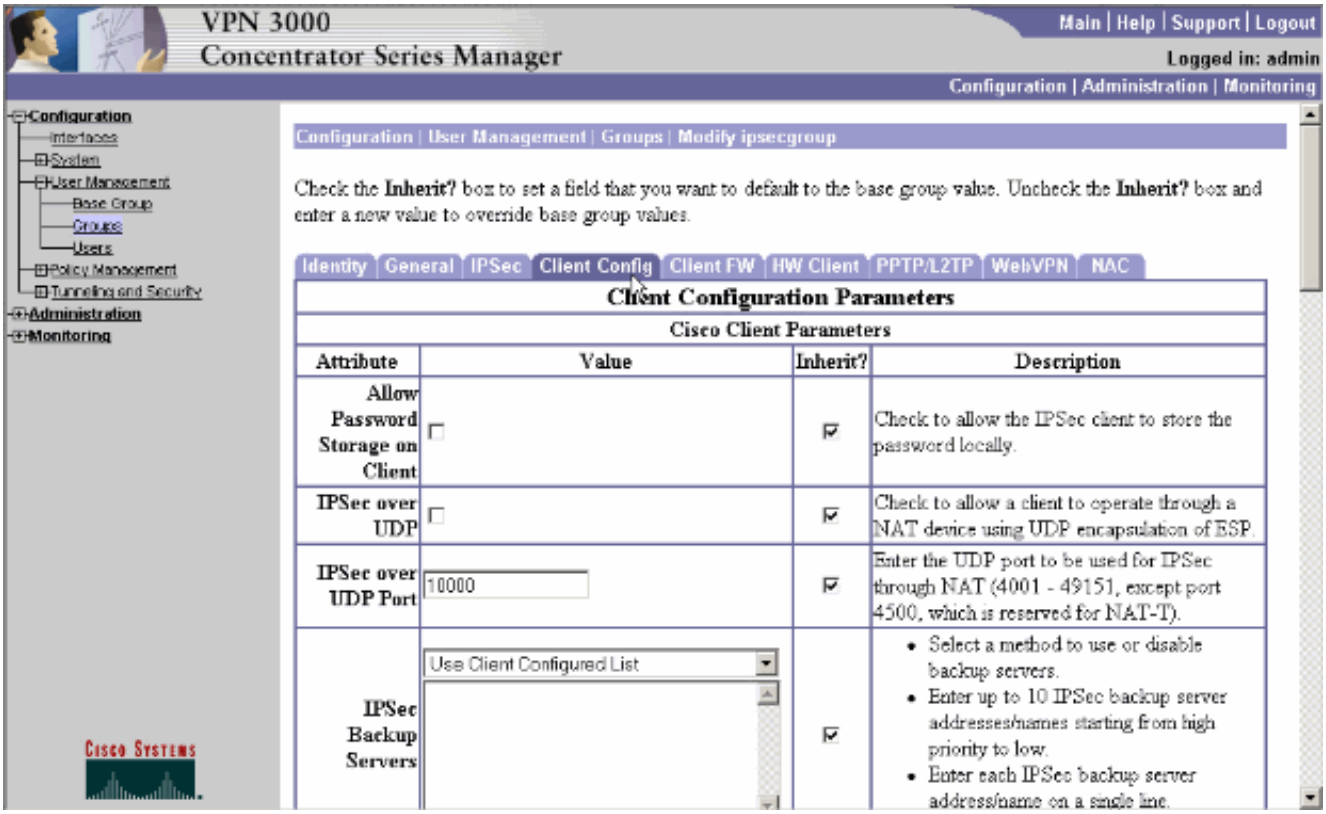


3. 建立或填充清單後，為清單提供一個名稱，然後按一下**Add**。

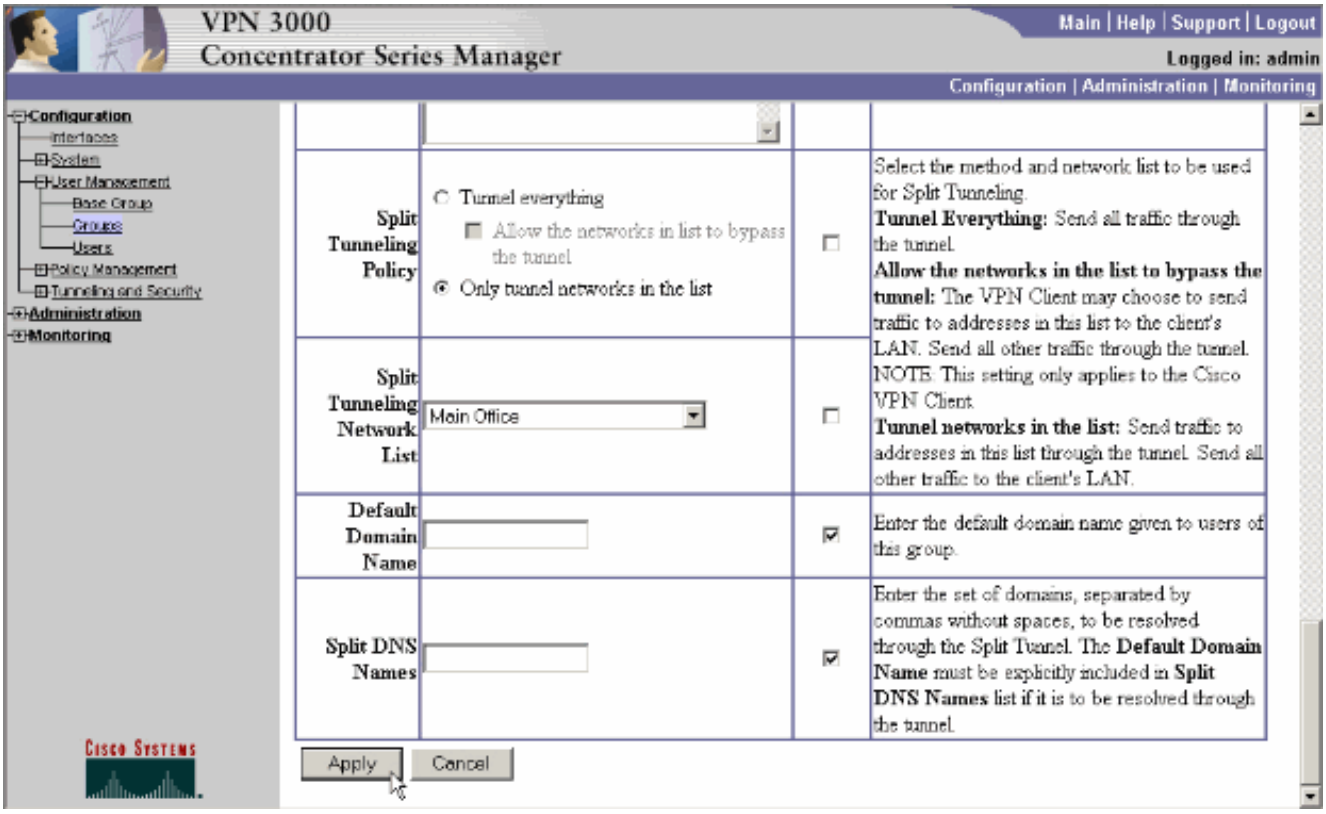


4. 建立網路清單後，將其分配給隧道組。選擇**Configuration > User Management > Groups**，選擇要更改的組，然後按一下**Modify Group**。

5. 轉到已選擇修改的組的Client Config（客戶端配置）頁籤。



6. 向下滾動到Split Tunneling Policy和Split Tunneling Network List部分，然後按一下清單**中的Only tunnel networks**。
7. 從下拉選單中選擇之前建立的清單。本例中為**總部**。繼承者？兩種情況下覈取方塊均自動清空。



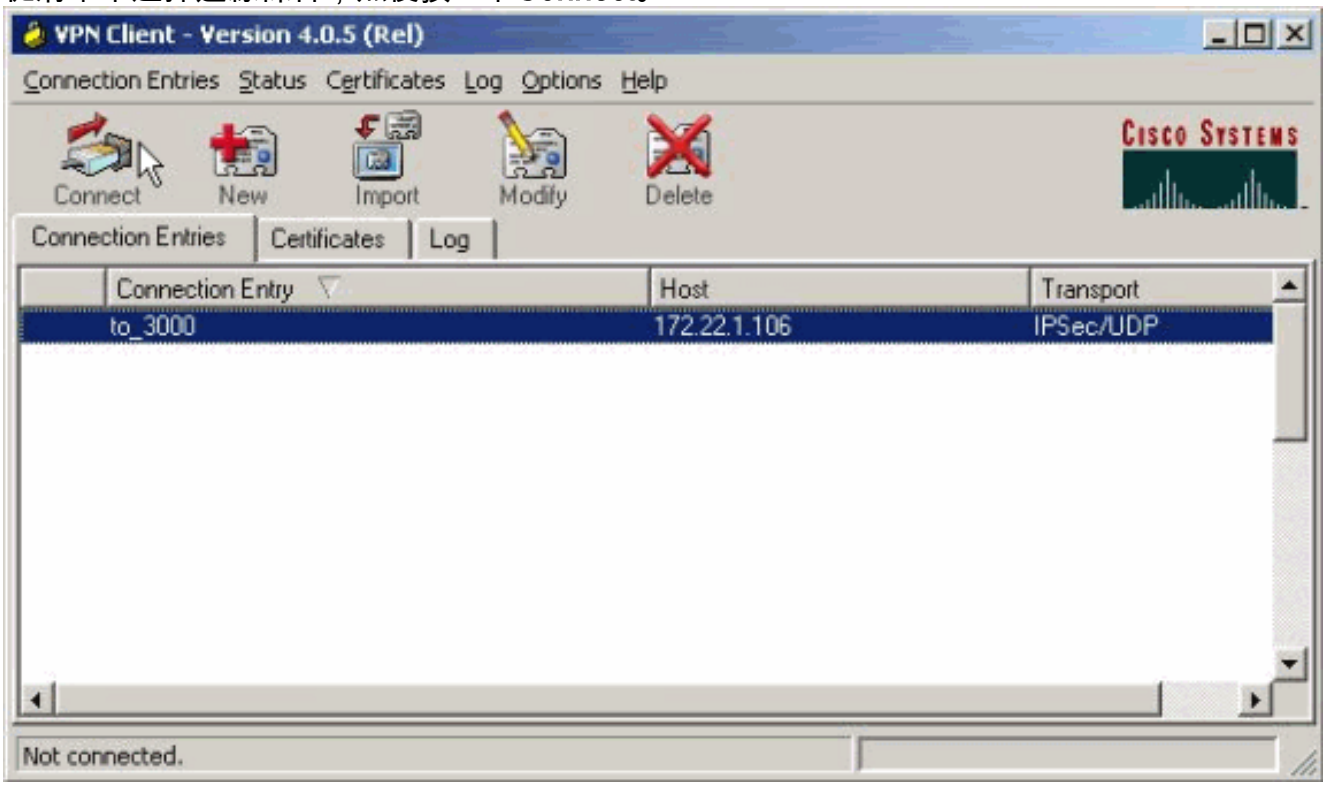
8. 完成後按一下**Apply**。

驗證

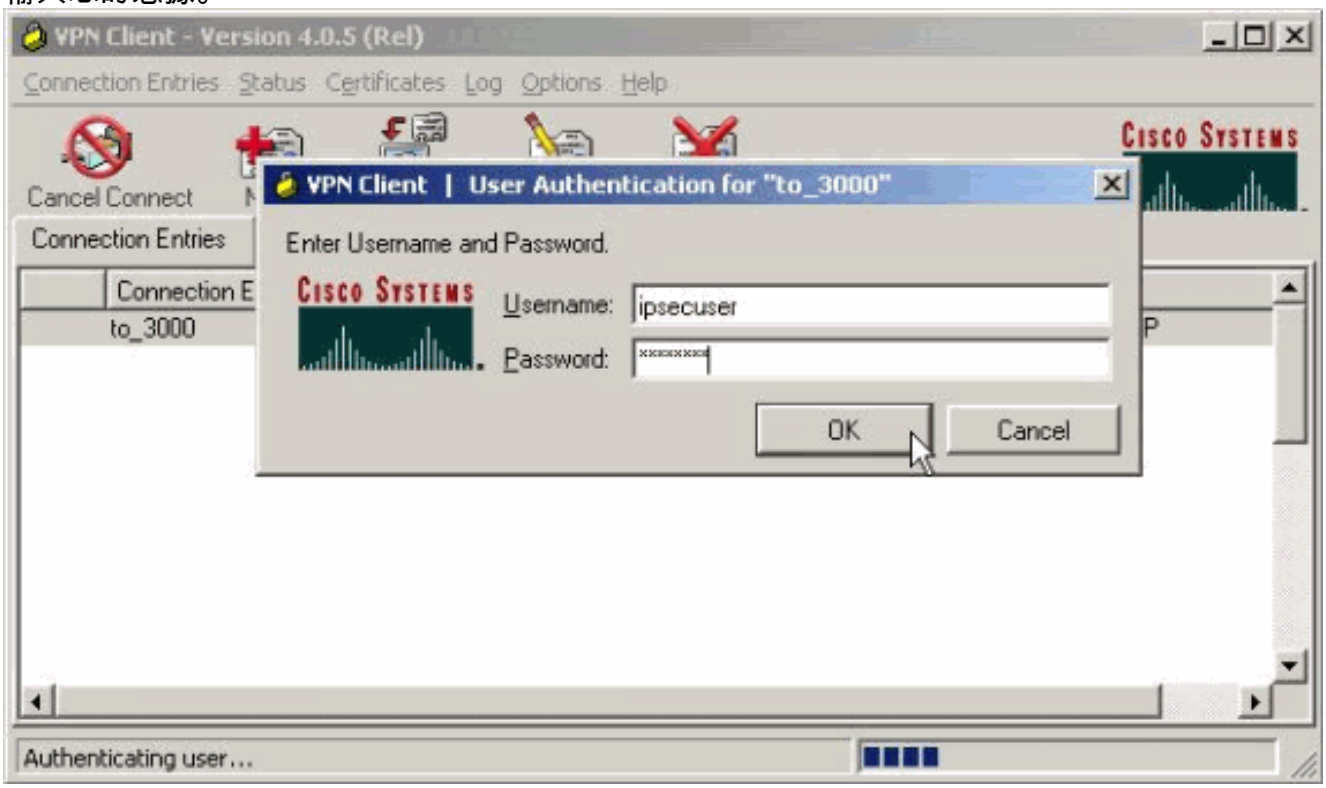
連線VPN客戶端

將VPN客戶端連線到VPN集中器以驗證您的配置。

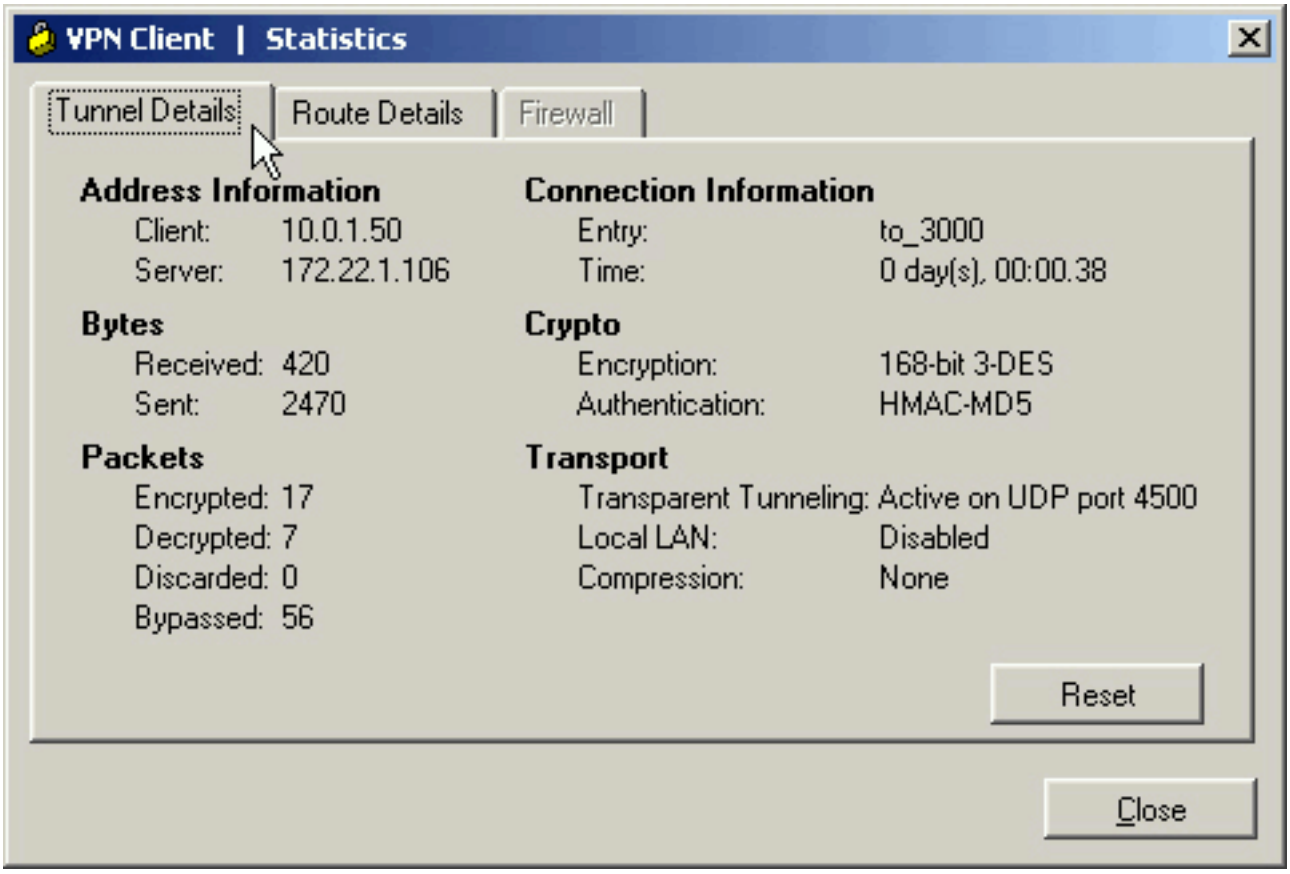
1. 從清單中選擇連線條目，然後按一下**Connect**。



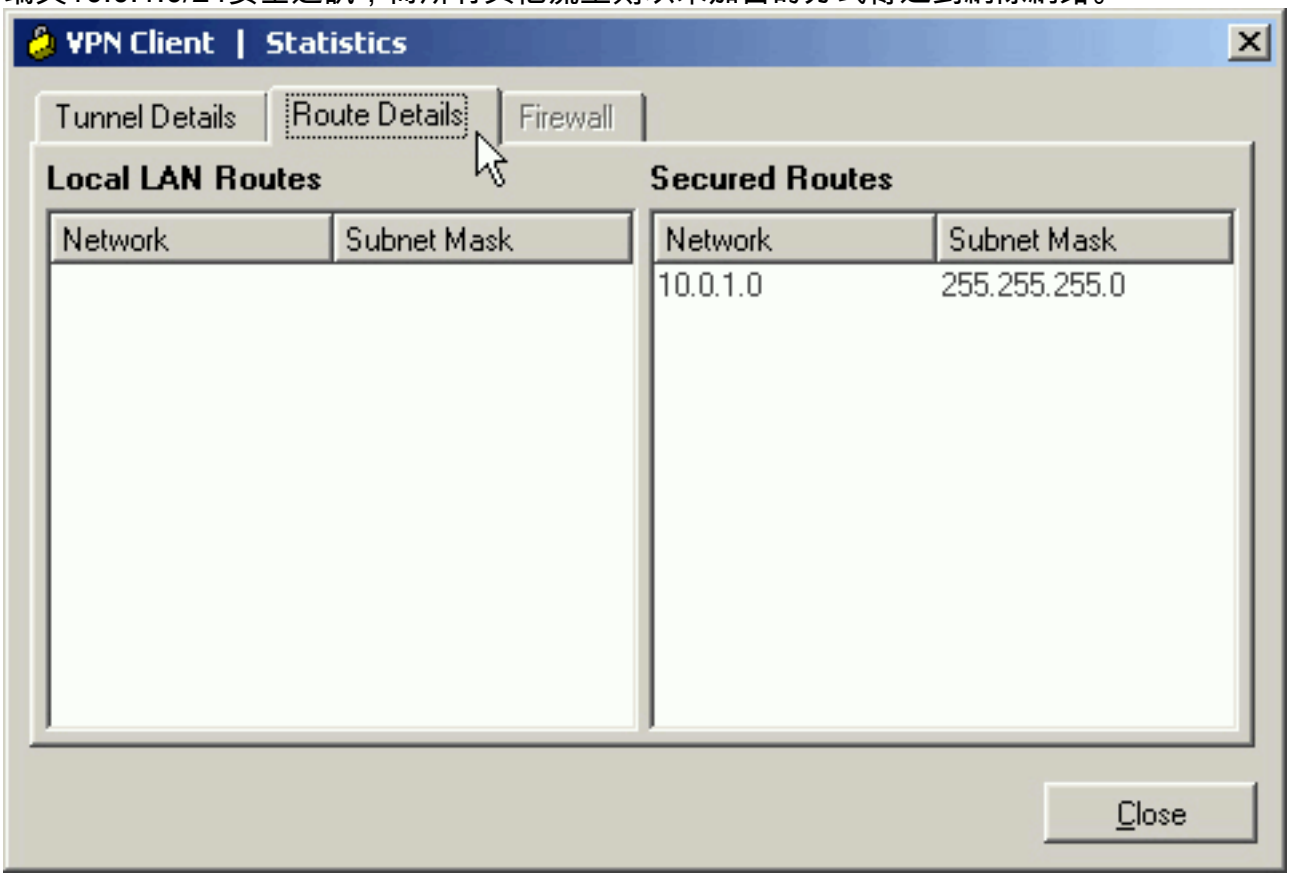
2. 輸入您的憑據。



3. 選擇**Status > Statistics...**以顯示「Tunnel Details」視窗，您可以在此視窗中檢查隧道的詳細資訊並檢視流量流。



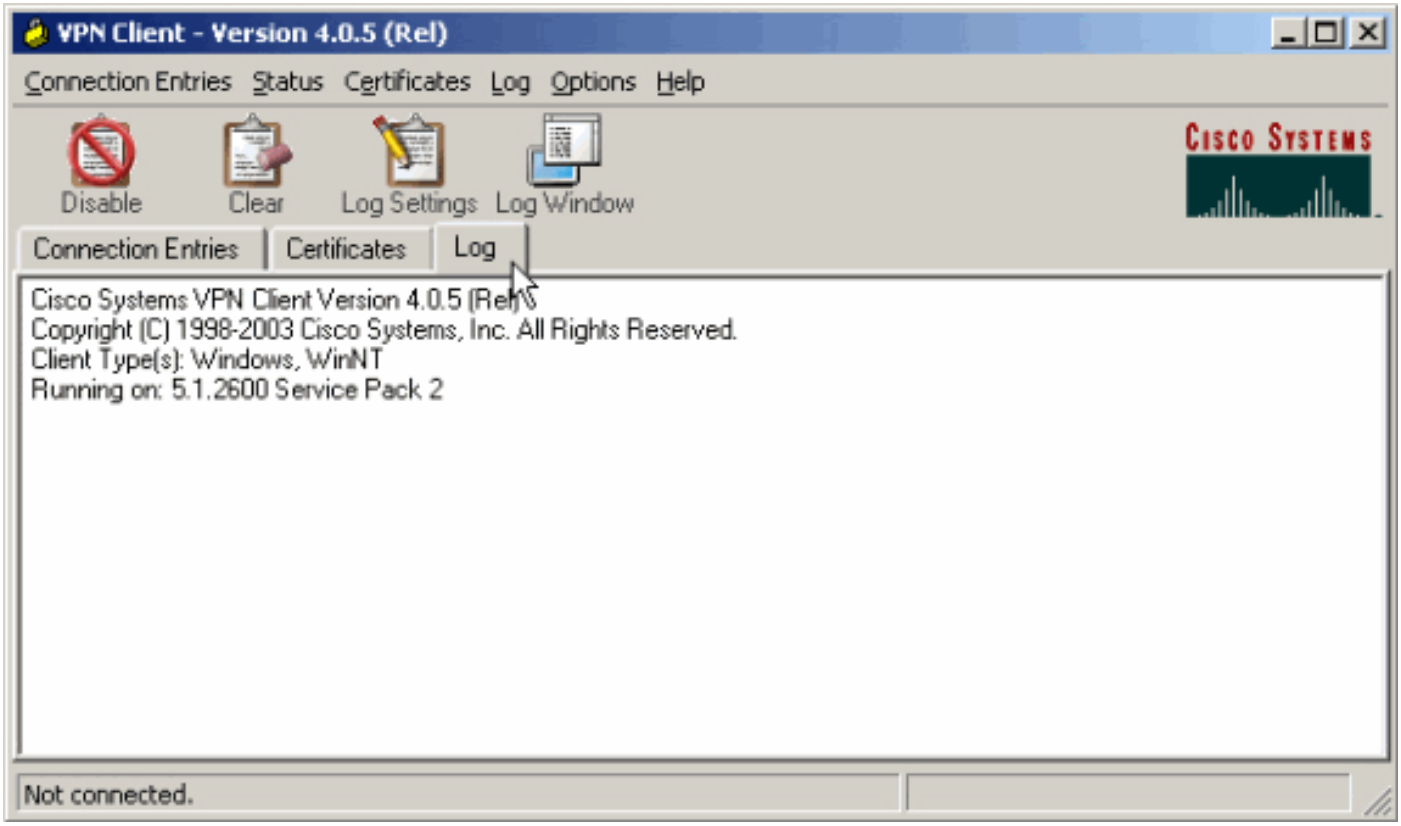
4. 轉到Route Details頁籤以檢視VPN客戶端將加密流量傳送到哪些網路。在此示例中，VPN客戶端與10.0.1.0/24安全通訊，而所有其他流量則以未加密的方式傳送到網際網路。



檢視VPN客戶端日誌

當您檢查VPN客戶端日誌時，可以確定是否設定了允許分割隧道的引數。轉到VPN Client中的Log頁籤以檢視日誌。按一下「**Log Settings**」以調整記錄的內容。在本示例中，IKE和IPsec設定為

3 — 高，而所有其他日誌元素設定為1 — 低。




```
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.
```

疑難排解

請參閱IPsec with VPN Client to VPN 3000 Concentrator配置示例 — 故障排除，瞭解有關此配置故

障排除的一般資訊。

相關資訊

- IPsec with VPN Client to VPN 3000 Concentrator配置示例
- Cisco VPN 3000系列集中器
- Cisco VPN使用者端
- 技術支援與文件 - Cisco Systems