VPN 3000 Concentrator 컨피그레이션의 VPN 클라이언트에 대한 스플릿 터널링 예

목차

소개

이 문서에서는 VPN 클라이언트가 VPN 3000 Series Concentrator로 터널링되는 동안 인터넷에 액세스하는 방법에 대한 단계별 지침을 제공합니다. 이 컨피그레이션을 사용하면 VPN 클라이언트가 IPsec을 통해 기업 리소스에 안전하게 액세스하면서 인터넷에 비보안 액세스를 제공할 수 있습니다 .

참고: 스플릿 터널링을 구성하면 보안 위험이 발생할 수 있습니다. VPN 클라이언트는 인터넷에 대한 보안되지 않은 액세스를 가지고 있으므로 공격자에 의해 보안이 침해될 수 있습니다. 그러면 해당 공격자는 IPsec 터널을 통해 기업 LAN에 액세스할 수 있습니다. 전체 터널링과 스플릿 터널링 간의 절충은 VPN 클라이언트 로컬 LAN 액세스만 허용하는 것일 수 있습니다. 자세한 내용은 VPN 3000 Concentrator 컨피그레이션의 VPN 클라이언트에 대한 로컬 LAN 액세스 허용 예를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에서는 작동 중인 원격 액세스 VPN 컨피그레이션이 VPN Concentrator에 이미 있다고 가정합니다. VPN Client에서 VPN 3000 Concentrator 컨피그레이션(VPN Client에서 VPN 3000 Concentrator 컨피그레이션)이 아직 구성되지 않은 경우 IPsec을 참조하십시오.

사용되는 구성 요소

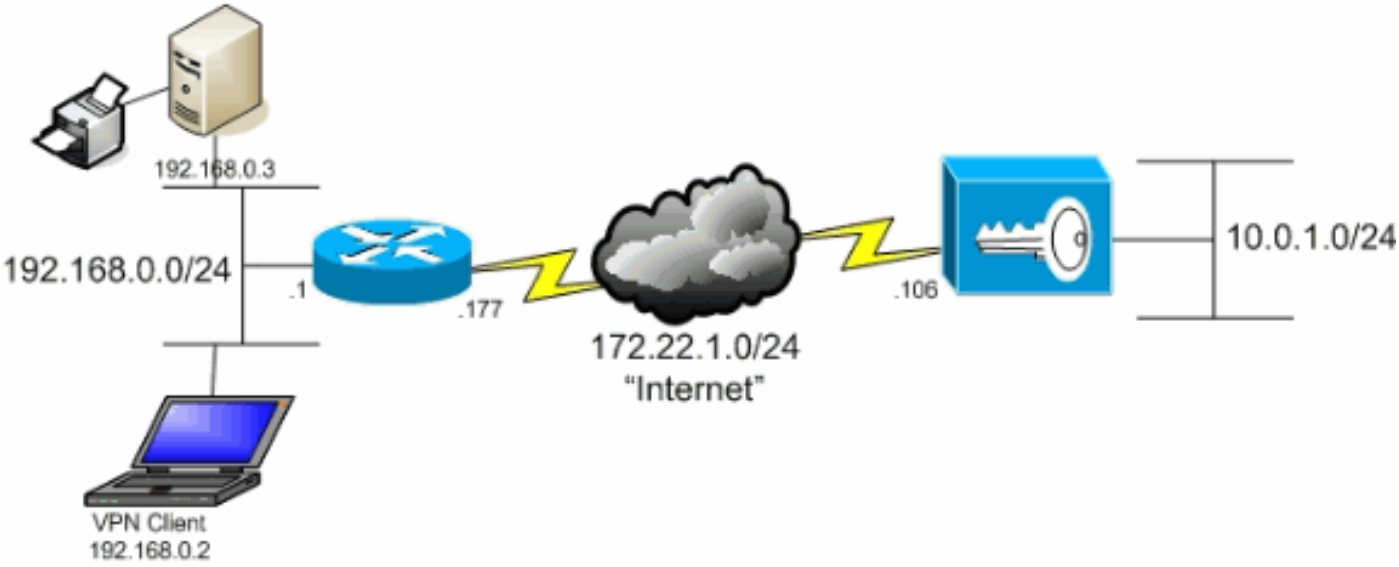
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco VPN 3000 Concentrator Series 소프트웨어 버전 4.7.2.H
- Cisco VPN Client 버전 4.0.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

네트워크 다이어그램

VPN 클라이언트는 일반적인 SOHO 네트워크에 있으며 인터넷을 통해 본사에 연결됩니다.



표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

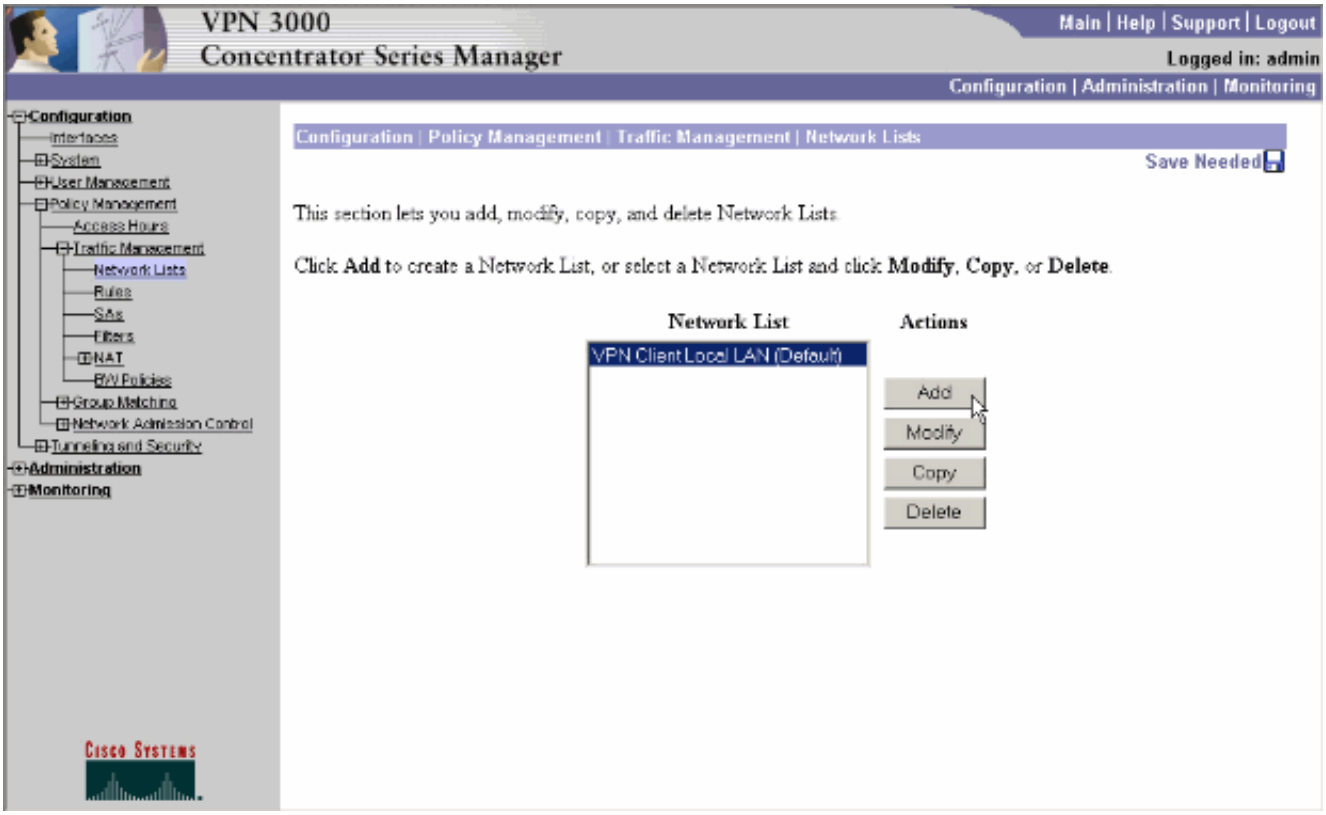
기본 VPN Client to VPN Concentrator 시나리오에서는 VPN 클라이언트의 모든 트래픽이 암호화되어 목적지의 종류에 상관없이 VPN Concentrator로 전송됩니다. 컨피그레이션 및 지원되는 사용자 수에 따라 이러한 설정은 대역폭 집약적인 설정이 될 수 있습니다. 스플릿 터널링은 사용자가 터널을 통해 기업 네트워크로 향하는 트래픽만 전송하도록 허용하여 이 문제를 완화하도록 할 수 있습니다. IM, 이메일 또는 일반 브라우징과 같은 다른 모든 트래픽은 VPN 클라이언트의 로컬 LAN을 통해 인터넷으로 전송됩니다.

VPN Concentrator에서 스플릿 터널링 구성

그룹의 사용자에 대해 스플릿 터널링을 허용하도록 터널 그룹을 구성하려면 다음 단계를 완료합니다. 먼저 네트워크 목록을 생성합니다. 이 목록은 VPN 클라이언트가 암호화된 트래픽을 전송하는 대상 네트워크를 정의합니다. 목록이 생성되면 클라이언트 터널 그룹의 스플릿 터널링 정책에 목록을 추가합니다.

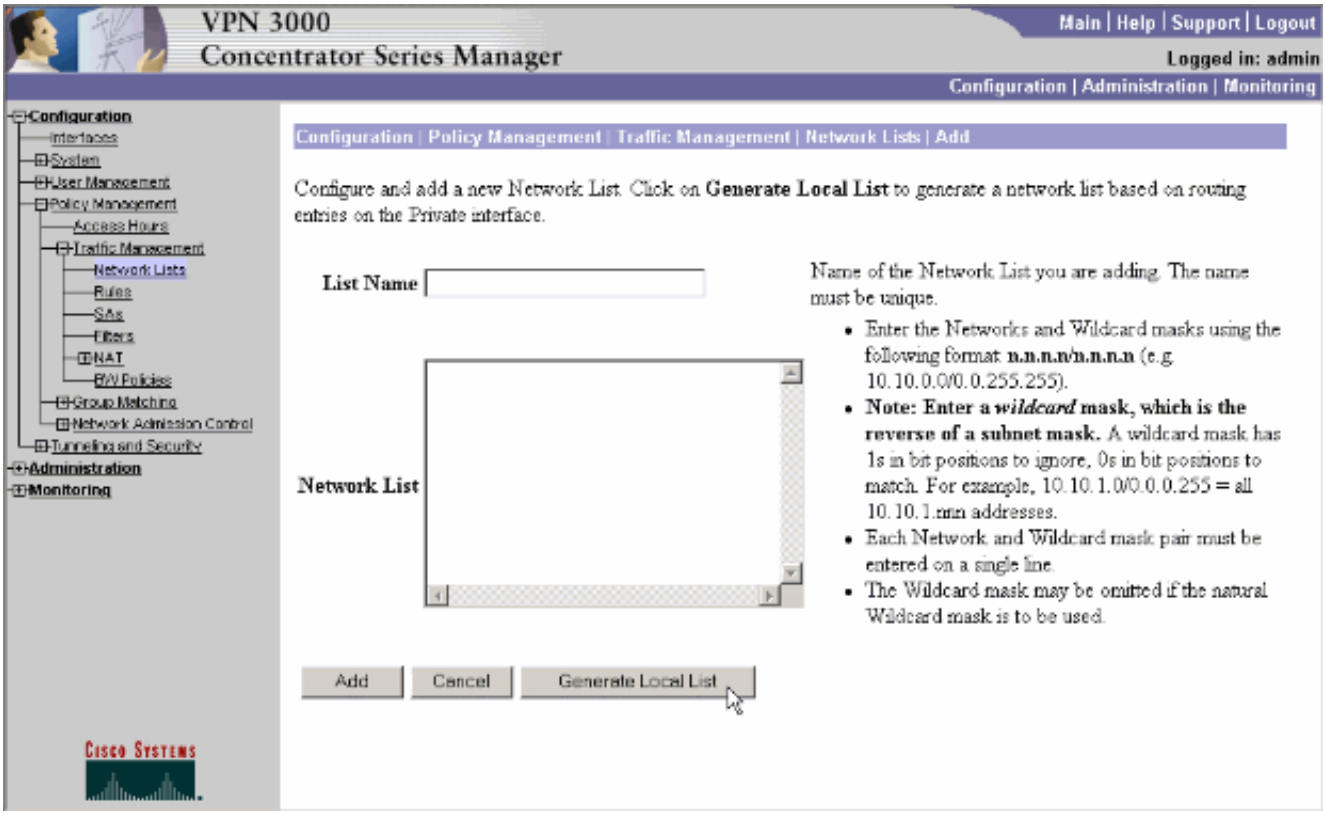
1. Configuration **> Policy Management > Traffic Management > Network Lists를 선택하고 Add를 클릭합니다**

.



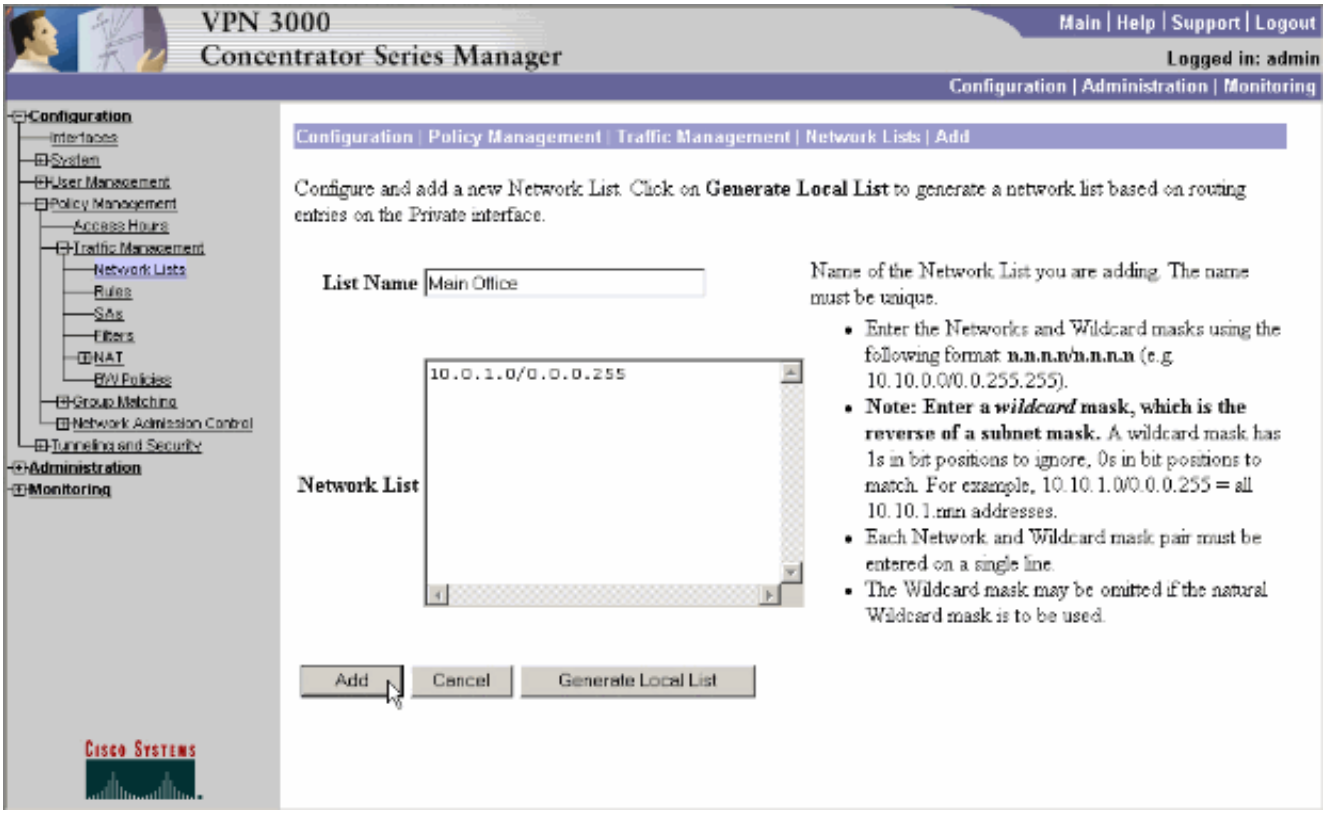
2. 이 목록은 VPN 클라이언트가 암호화된 트래픽을 전송하는 대상 네트워크를 정의합니다. 이러한 네트워크를 수동으로 입력하거나 **Generate Local List(로컬 목록 생성)**를 클릭하여 VPN Concentrator의 프라이빗 인터페이스에서 라우팅 항목을 기반으로 목록을 생성합니다.이 예에서는 목록이 자동으로 생성되었습니다

.



3. 생성되거나 채워지면 목록의 이름을 입력하고 Add(추가)를 **클릭합니다**

.

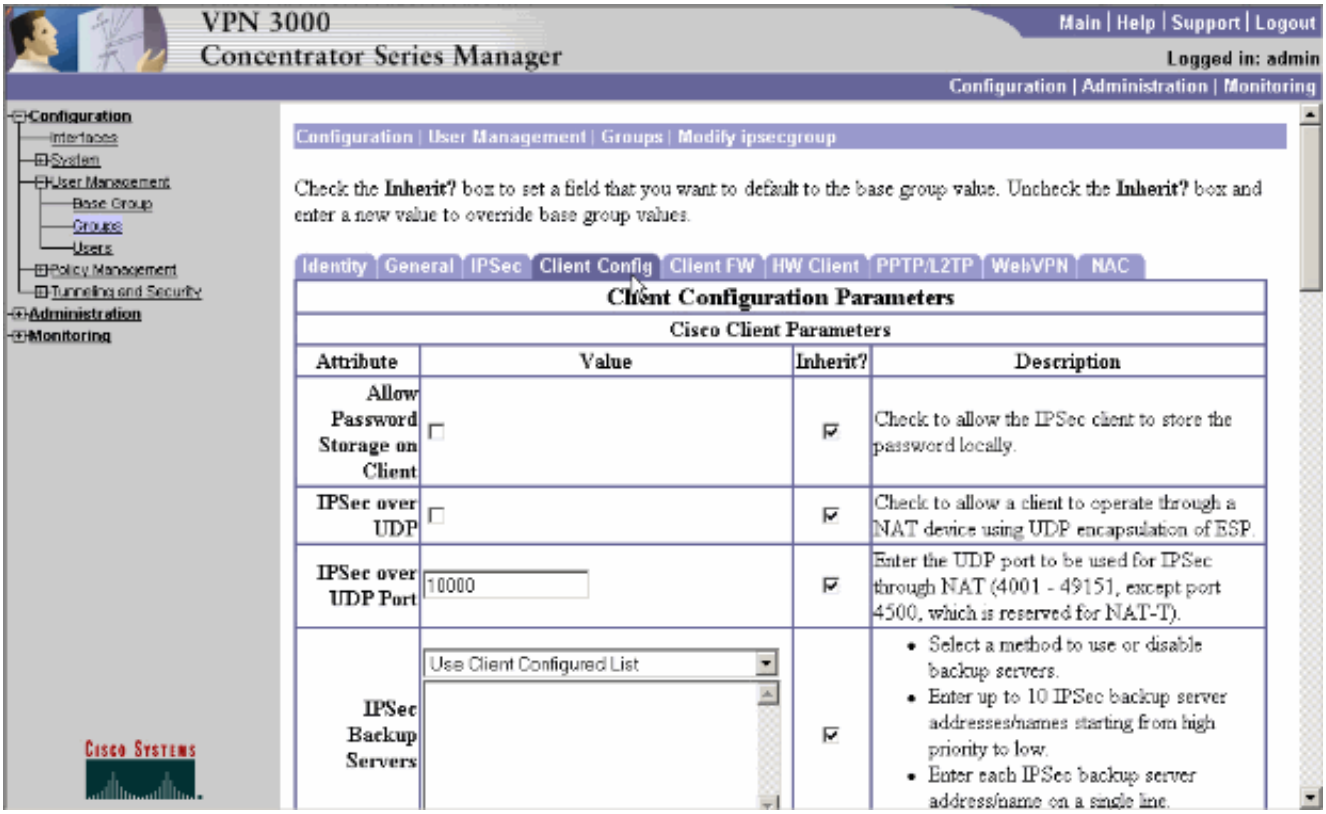


4. 네트워크 목록을 생성한 후 터널 그룹에 할당합니다. Configuration **> User Management > Groups**를 선택하고 변경할 그룹을 선택한 다음 **Modify Group**을 클릭합니다

.

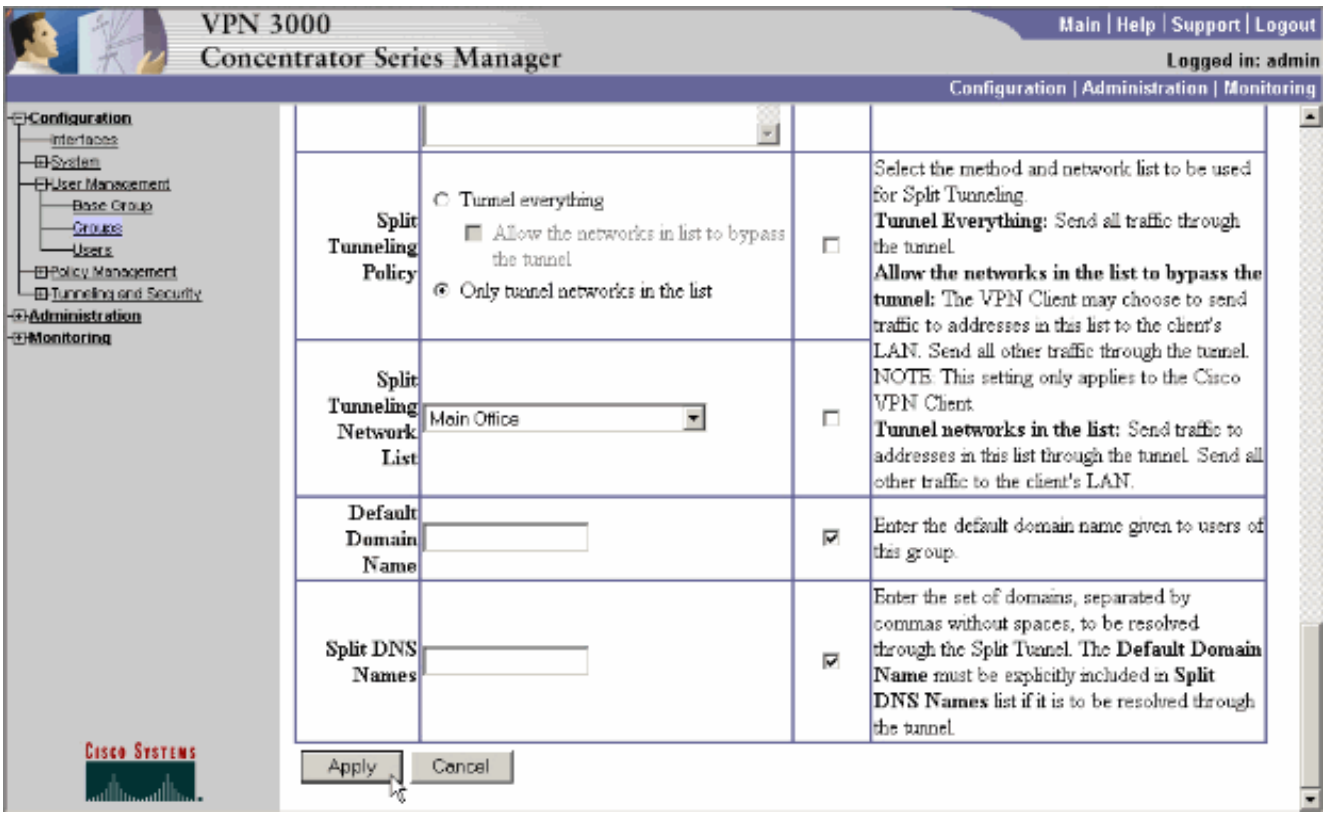
5. 수정하도록 선택한 그룹의 Client Config 탭으로 이동합니다

.



6. 아래로 스크롤하여 Split Tunneling Policy and Split Tunneling Network List(스플릿 터널링 정책 및 스플릿 터널링 네트워크 목록) 섹션으로 이동하고 **목록에서 Only tunnel networks(터널링만)를** 클릭합니다.
7. 드롭다운에서 앞서 생성한 목록을 선택합니다. 이 경우에는 **본사입니다**. 상속? 두 경우 모두 확인란이 자동으로 비워집니다

.



8. 완료되면 **적용**을 클릭합니다.

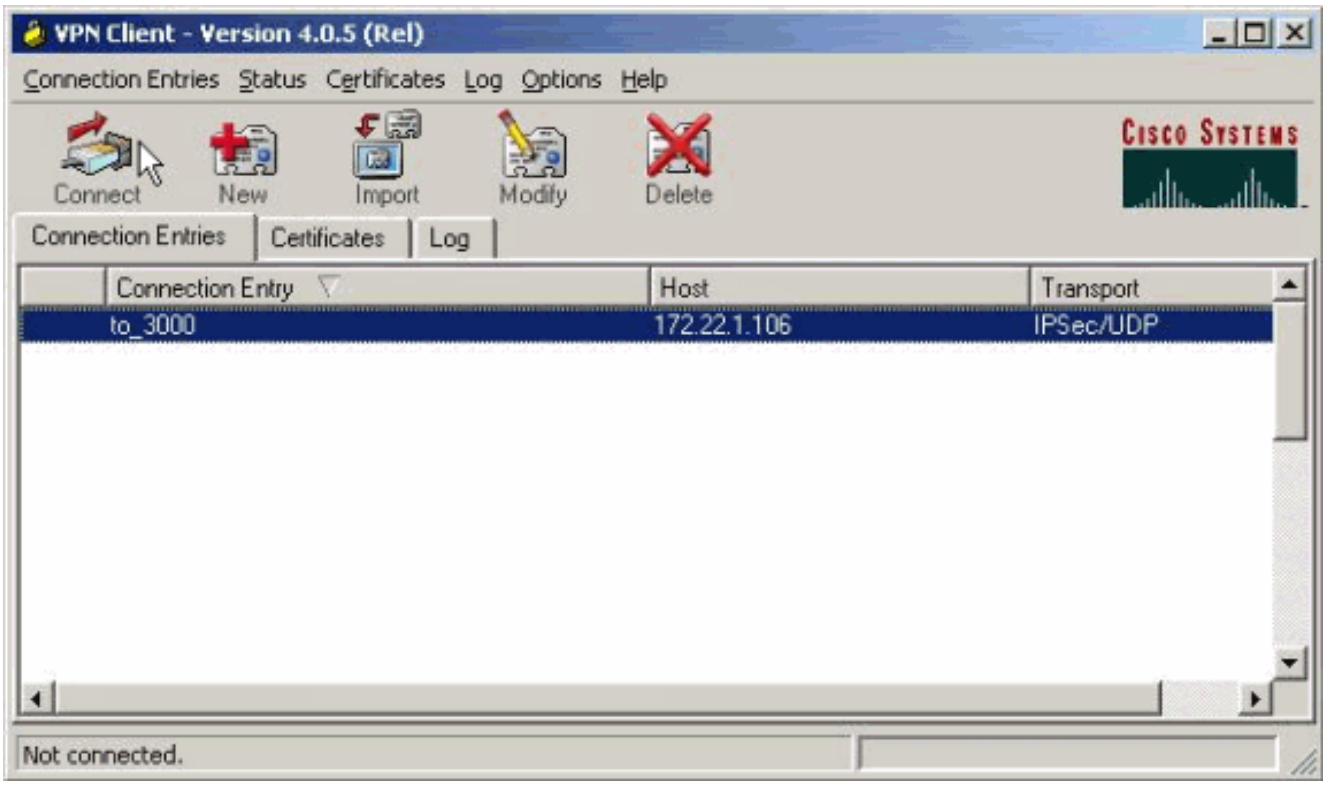
다음을 확인합니다.

VPN 클라이언트와 연결

컨피그레이션을 확인하려면 VPN 클라이언트를 VPN Concentrator에 연결합니다.

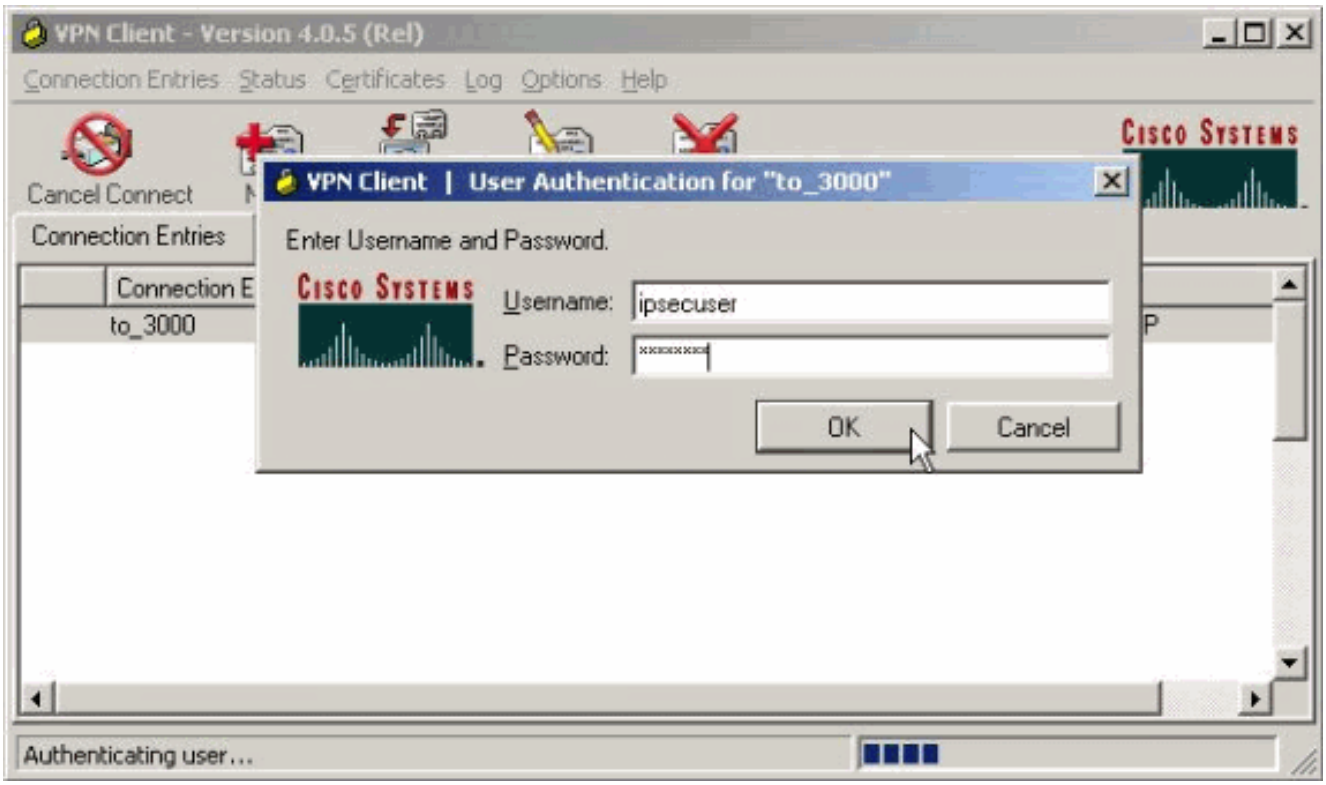
1. 목록에서 연결 항목을 선택하고 **연결**을 클릭합니다

.

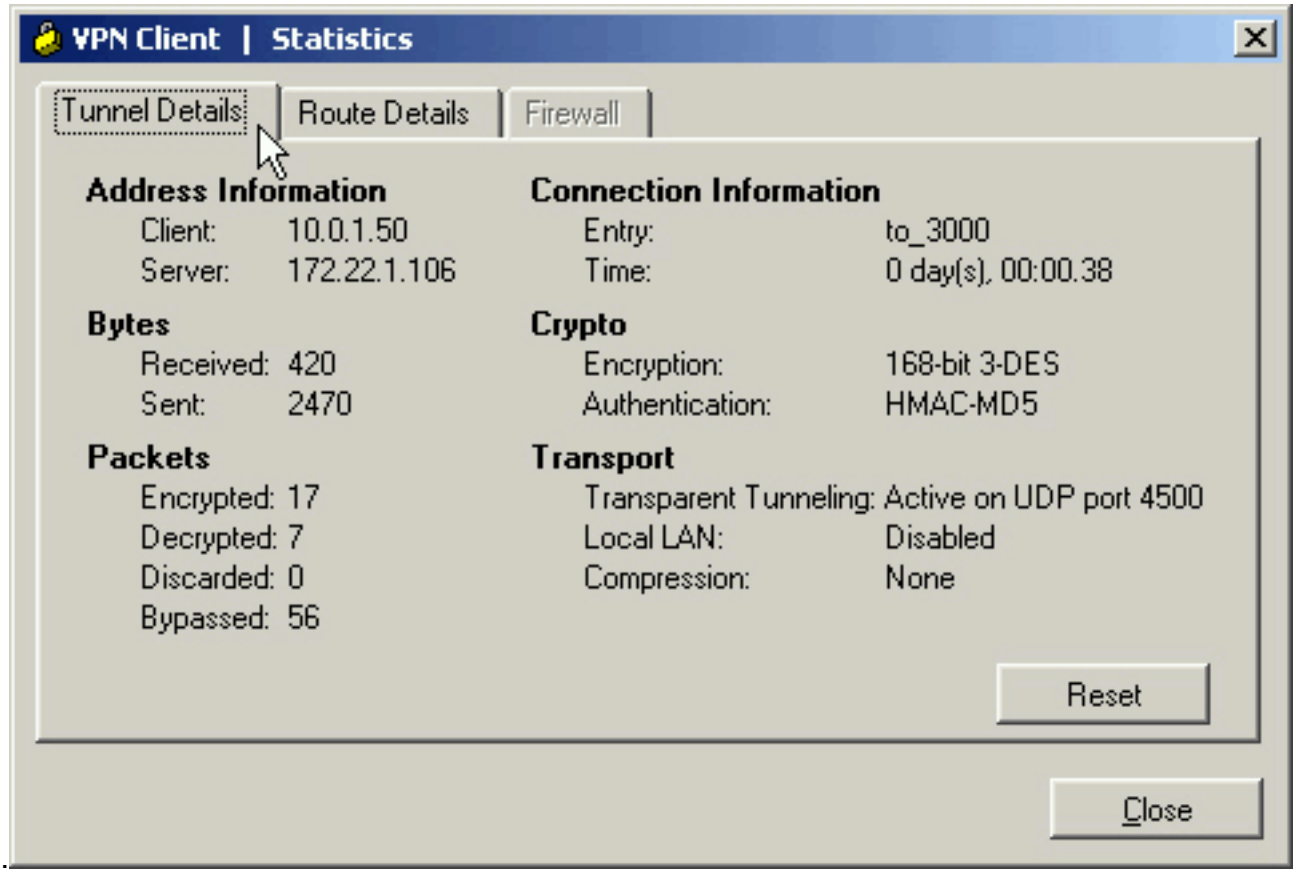


2. 자격 증명을 입력합니다

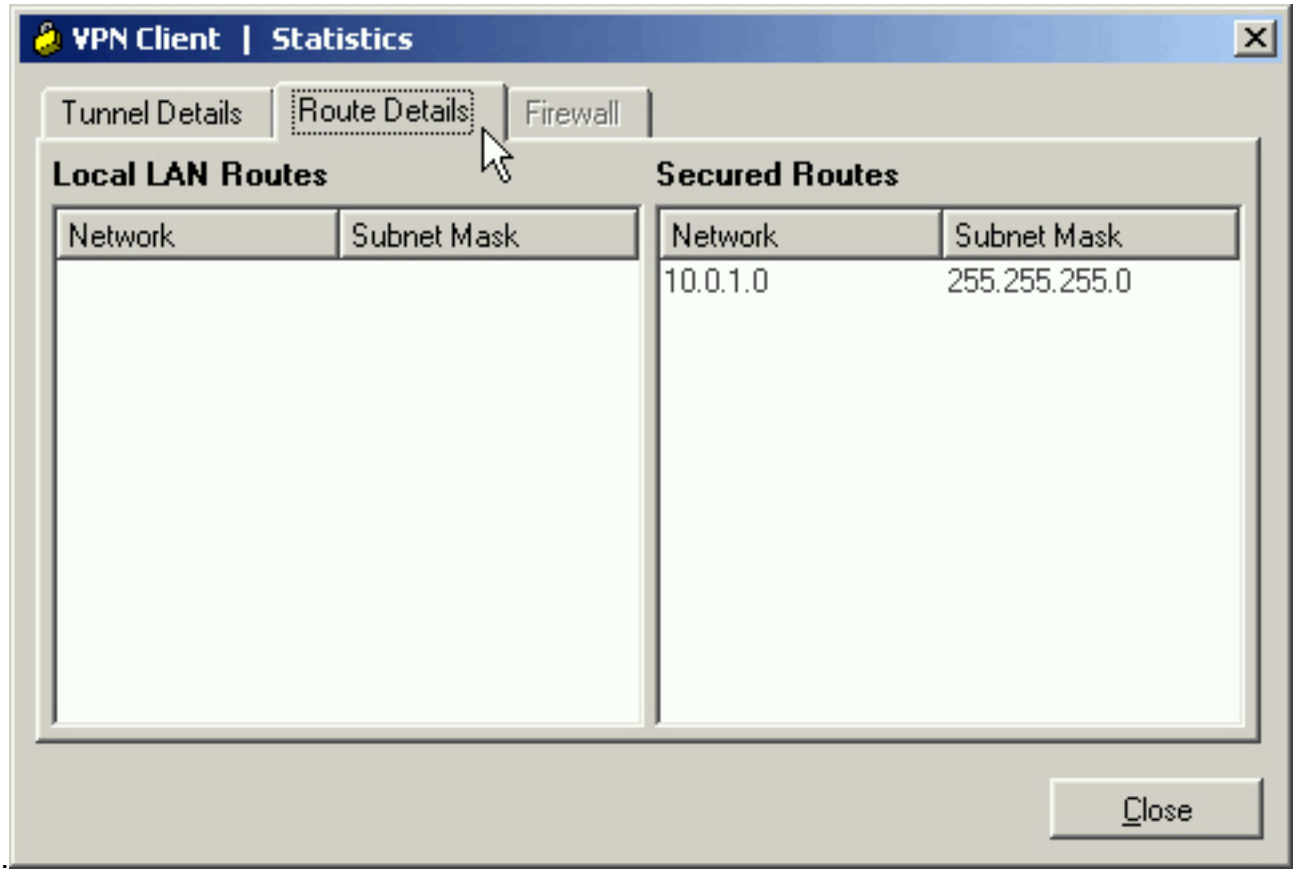
.



3. Status > **Statistics..**를 선택하여 터널 세부 정보를 검사하고 트래픽 흐름을 확인할 수 있는 Tunnel Details 창을 표시합니다



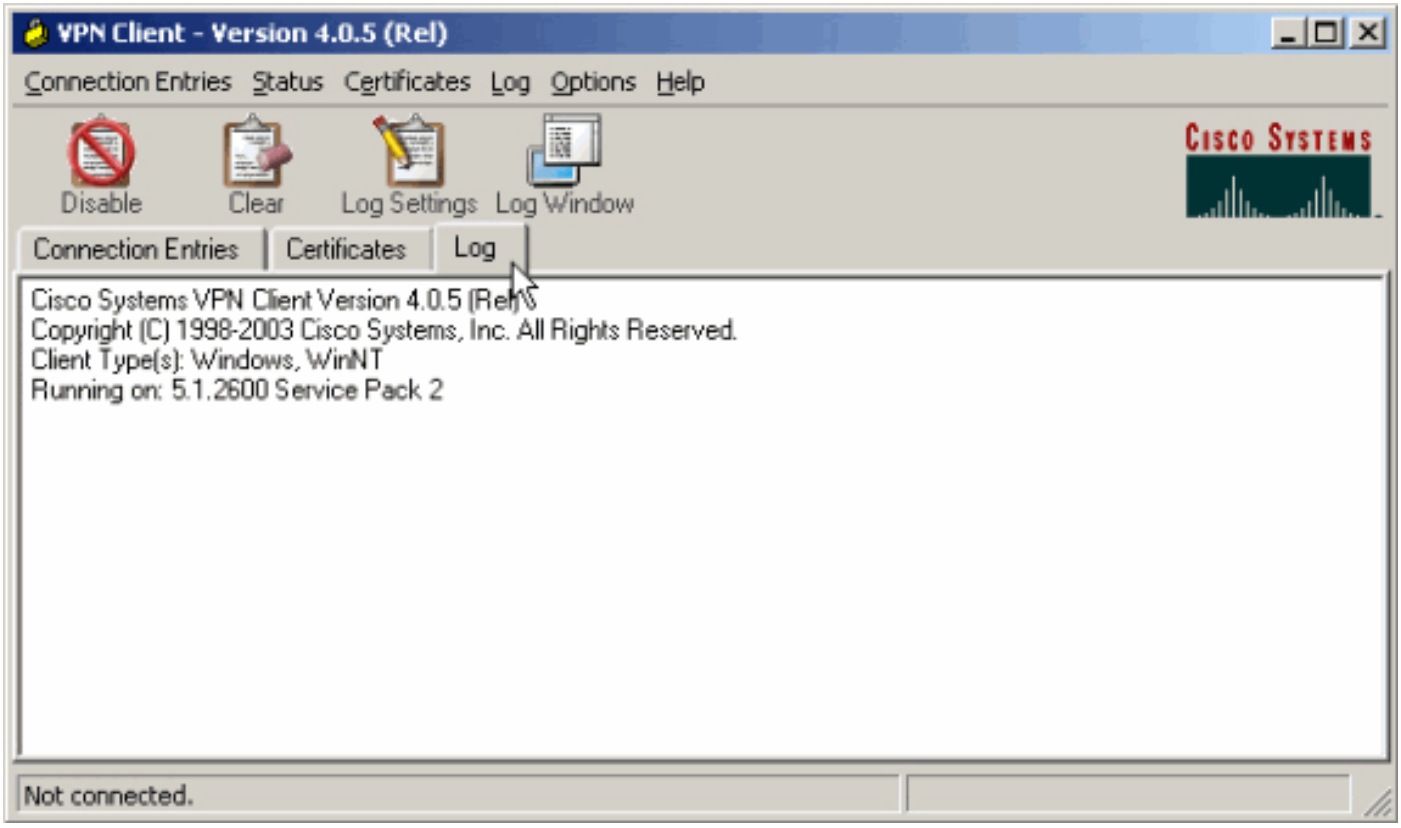
4. Route Details(경로 세부사항) 탭으로 이동하여 VPN 클라이언트에서 암호화된 트래픽을 전송하는 네트워크를 확인합니다. 이 예에서 VPN 클라이언트는 10.0.1.0/24과 안전하게 통신하지만 다른 모든 트래픽은 암호화되지 않은 상태로 인터넷에 전송됩니다



VPN 클라이언트 로그 보기

VPN 클라이언트 로그를 검사할 때 스플릿 터널링을 허용하는 매개변수가 설정되었는지 여부를 결

정할 수 있습니다. 로그를 보려면 VPN Client의 Log(로그) 탭으로 이동합니다. 로그 **설정**을 클릭하여 로깅된 항목을 조정합니다. 이 예에서 IKE 및 IPsec은 **3- High로** 설정되고 다른 모든 로그 요소는 **1 - Low로** 설정됩니다.




```
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.
```

문제 해결

이 컨피그레이션 트러블슈팅에 대한 일반적인 정보는 IPsec with VPN Client to VPN 3000 Concentrator Configuration Example - Troubleshooting(VPN 클라이언트에서 VPN 300 Concentrator 컨피그레이션으로 IPsec을 참조하십시오.

관련 정보

- VPN Client to VPN 3000 Concentrator 컨피그레이션의 IPsec 예
- Cisco VPN 3000 Series Concentrator
- Cisco VPN 클라이언트
- 기술 지원 및 문서 – Cisco Systems