ASA에서 VPN 클라이언트에 대한 스플릿 터널링 구성

목차

소개

이 문서에서는 VPN 클라이언트가 Cisco ASA 5500 Series Security Appliance로 터널링하는 동안 인터넷에 액세스할 수 있도록 허용하는 프로세스에 대해 설명합니다.

사전 요구 사항

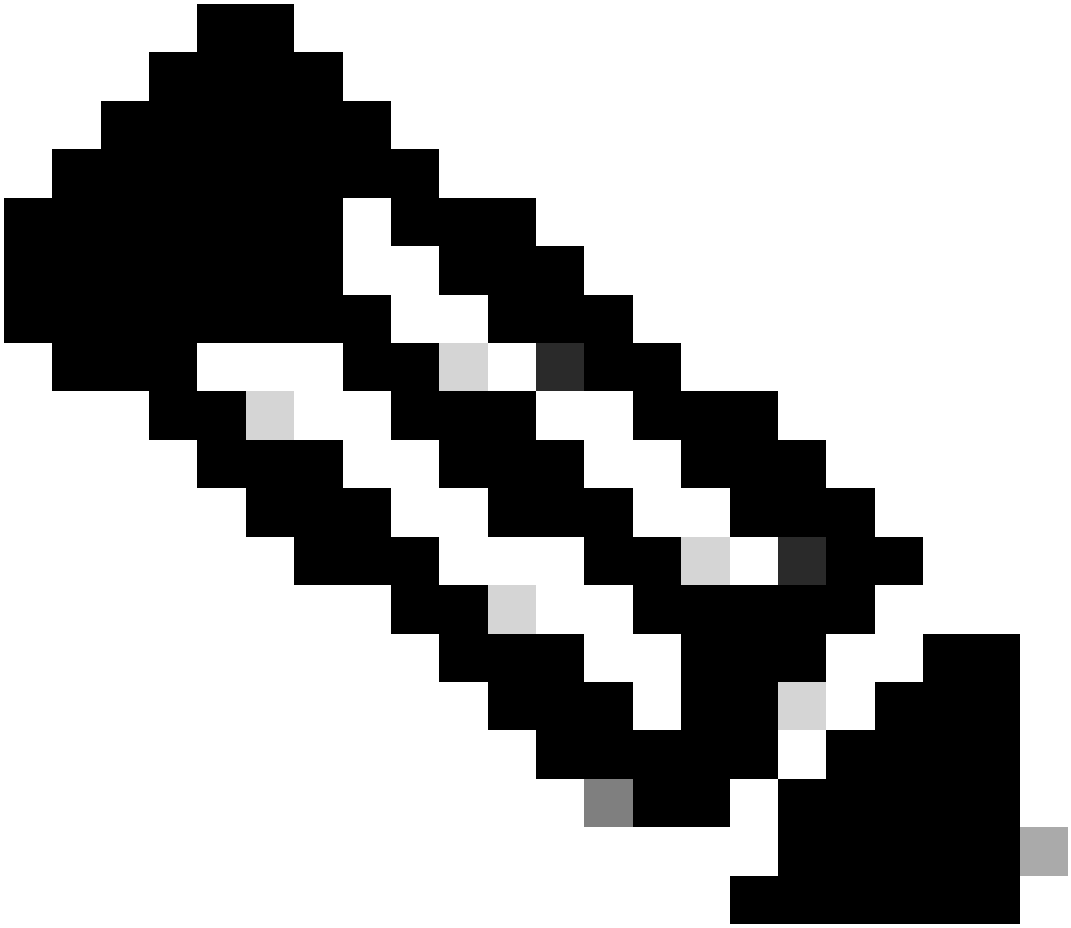
요구 사항

이 문서에서는 작동하는 원격 액세스 VPN 컨피그레이션이 ASA에 이미 있다고 가정합니다. ASDM 컨피그레이션 예를 사용하는 원격 VPN 서버로서 PIX/ASA 7.x가 아직 구성되지 않은 경우 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ASA 5500 Series Security Appliance 소프트웨어 버전 7.x 이상
- Cisco Systems VPN Client 버전 4.0.5
- ASDM(Adaptive Security Device Manager)

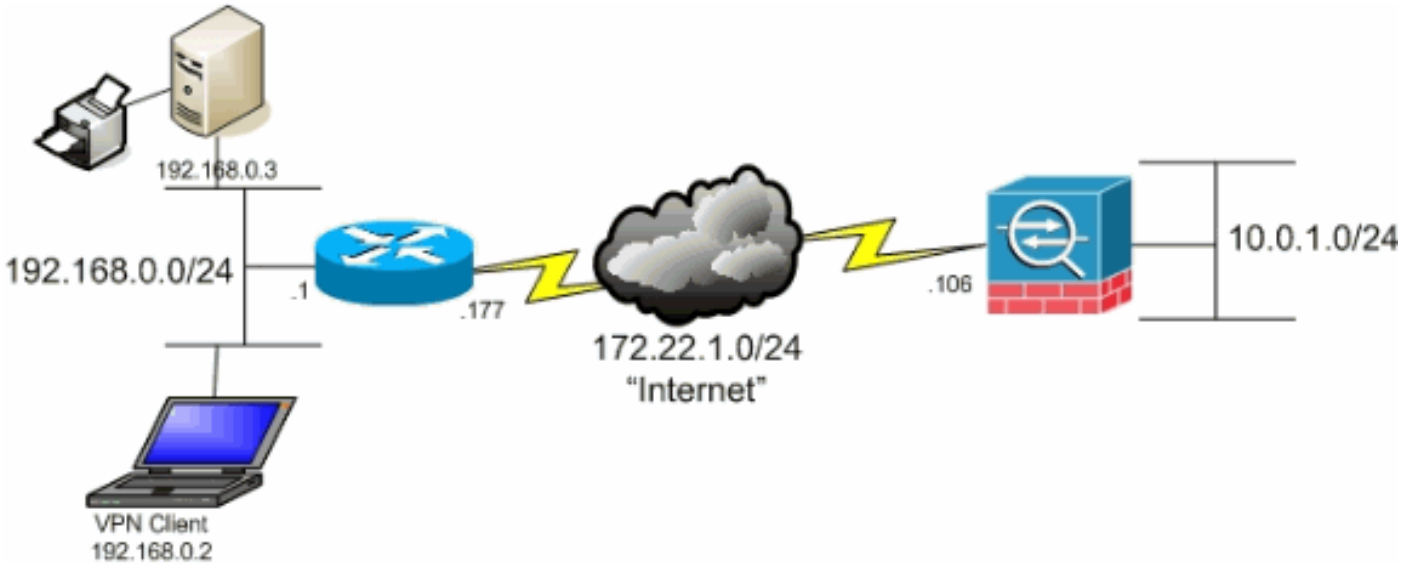


참고: 이 문서에는 Cisco VPN Client 3.x와 호환되는 PIX 6.x CLI 컨피그레이션도 포함되어 있습니다.

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

네트워크 다이어그램

VPN 클라이언트는 일반적인 SOHO 네트워크에 있으며 인터넷을 통해 본사에 연결됩니다.



네트워크 다이어그램

관련 제품

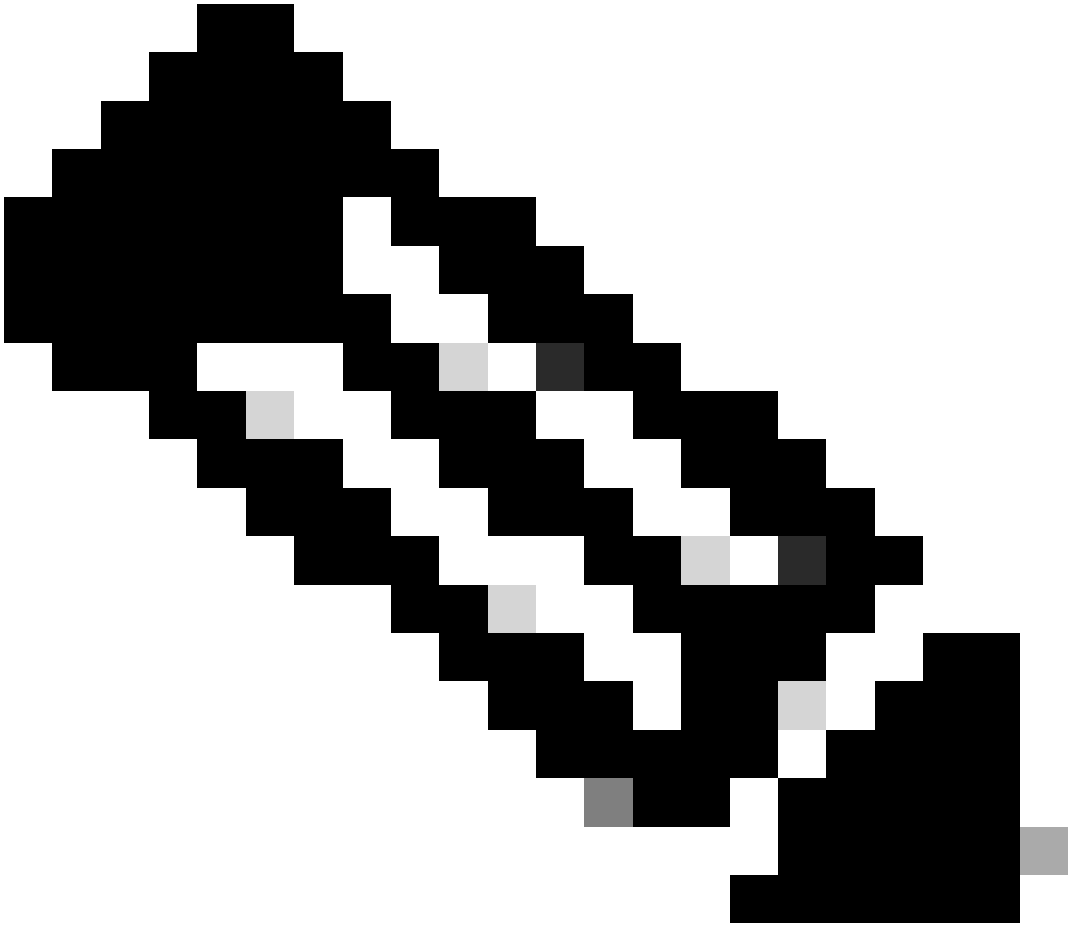
이 컨피그레이션은 Cisco PIX 500 Series Security Appliance Software 버전 7.x에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

이 문서에서는 VPN 클라이언트가 Cisco ASA(Adaptive Security Appliance) 5500 Series Security Appliance로 터널링되는 동안 인터넷에 액세스할 수 있도록 허용하는 방법에 대한 단계별 지침을 제공합니다. 이 컨피그레이션을 통해 VPN 클라이언트는 IPsec을 통해 기업 리소스에 안전하게 액세스하는 동시에 인터넷에 안전하게 액세스할 수 있습니다.



참고: 전체 터널링은 인터넷 및 기업 LAN 모두에 대한 동시 디바이스 액세스를 활성화하지 않으므로 가장 안전한 컨피그레이션으로 간주됩니다. 전체 터널링과 스플릿 터널링이 손상되면 VPN 클라이언트 로컬 LAN 액세스만 허용됩니다. 자세한 내용은 PIX/ASA 7.x: Allow Local LAN Access for VPN Clients 컨피그레이션 예를 참조하십시오.

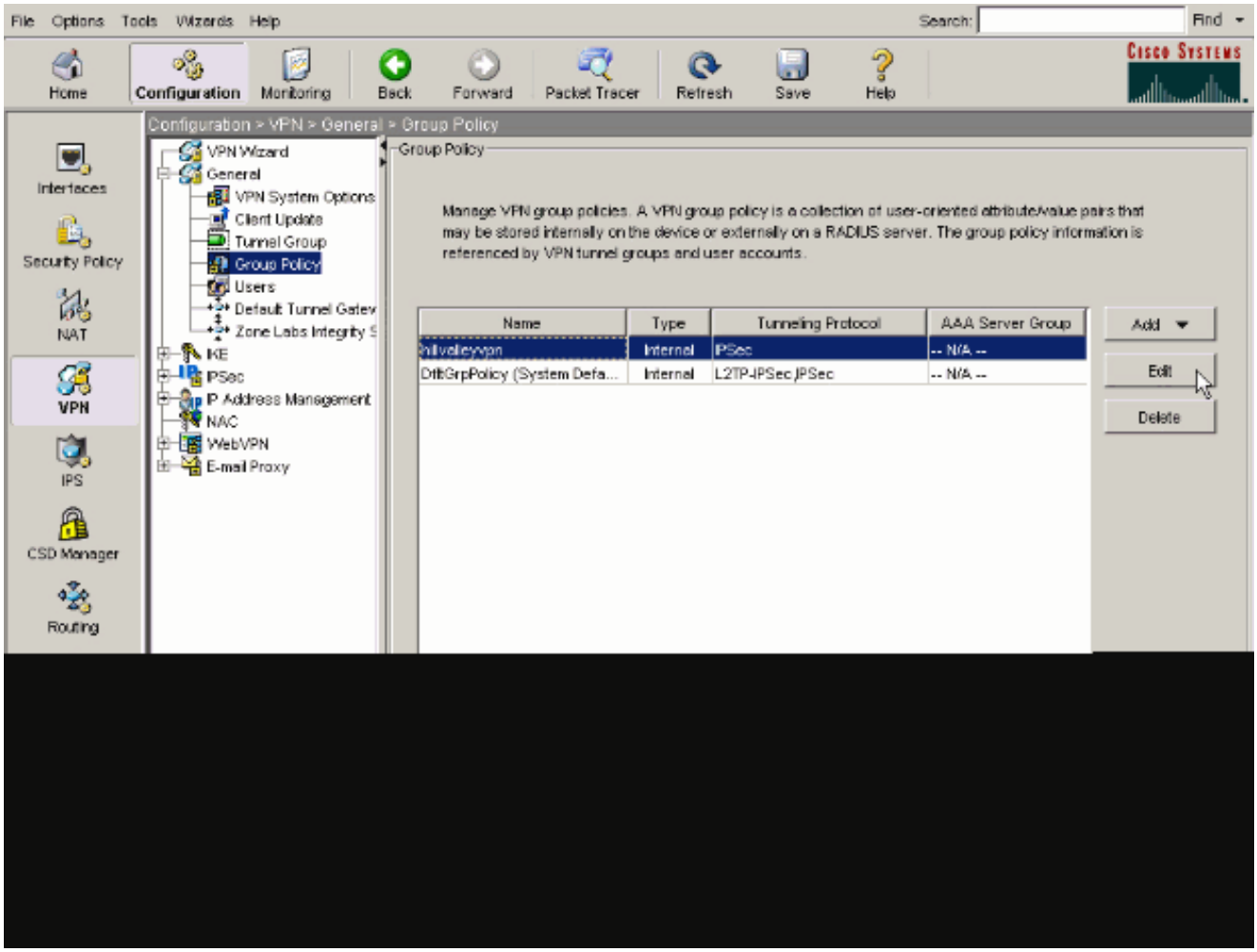
기본 VPN 클라이언트에서 ASA로의 시나리오에서는 VPN 클라이언트의 모든 트래픽이 암호화되어 대상에 관계없이 ASA로 전송됩니다. 컨피그레이션 및 지원되는 사용자 수에 따라 이러한 설정은 대역폭 집약적인 설정이 될 수 있습니다. 스플릿 터널링은 사용자가 터널을 통해 기업 네트워크로 향하는 트래픽만 전송하도록 허용하므로 이 문제를 완화하는 데 도움이 됩니다. 인스턴트 메시징, 이메일 또는 일반 브라우징과 같은 다른 모든 트래픽은 VPN 클라이언트의 로컬 LAN을 통해 인터넷으로 전송됩니다.

ASA에서 스플릿 터널링 구성

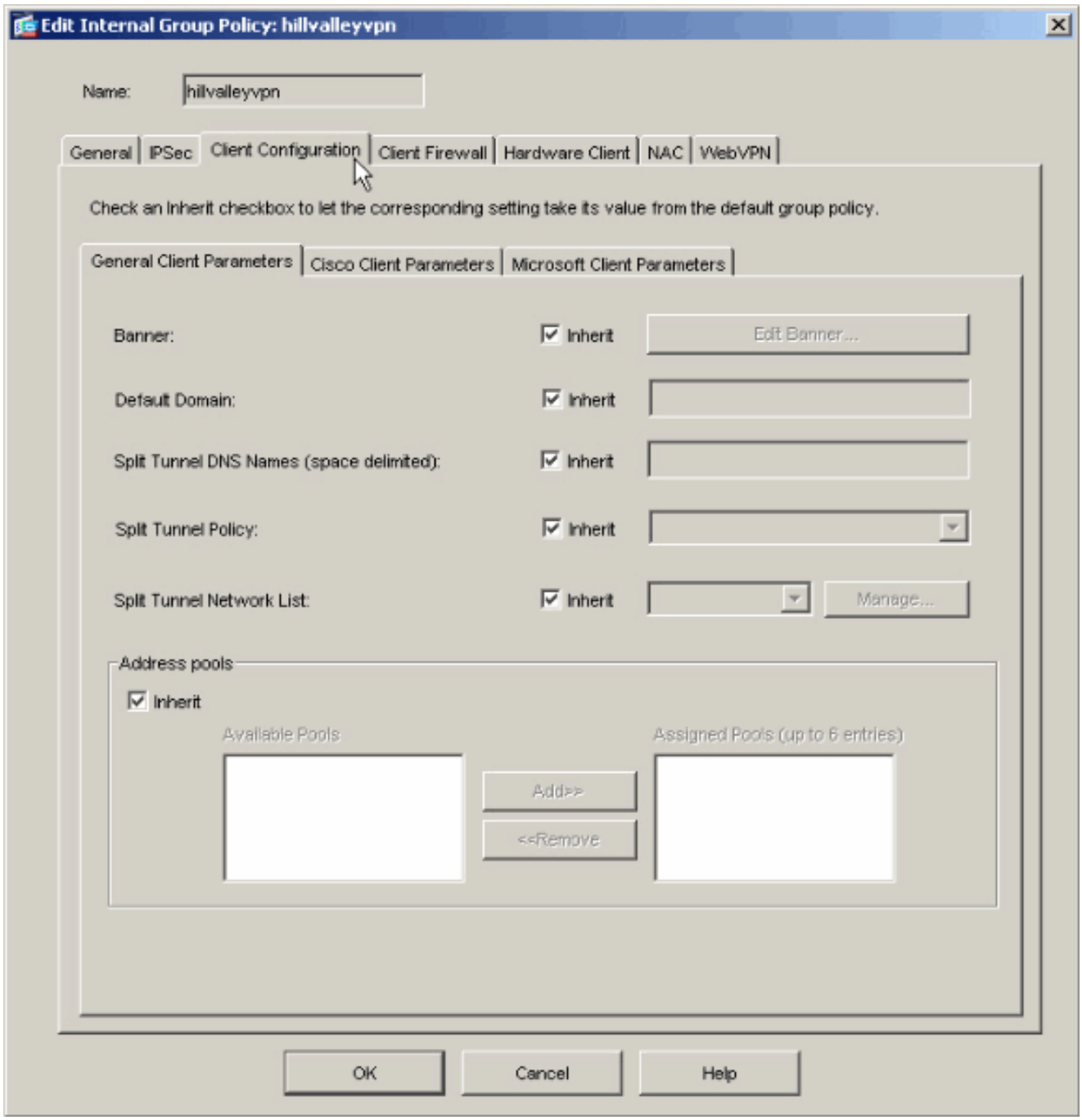
ASDM(Adaptive Security Device Manager) 5.x를 사용하여 ASA 7.x 구성

그룹 내 사용자에 대해 스플릿 터널링을 허용하도록 터널 그룹을 구성하려면 다음 단계를 완료하십시오.

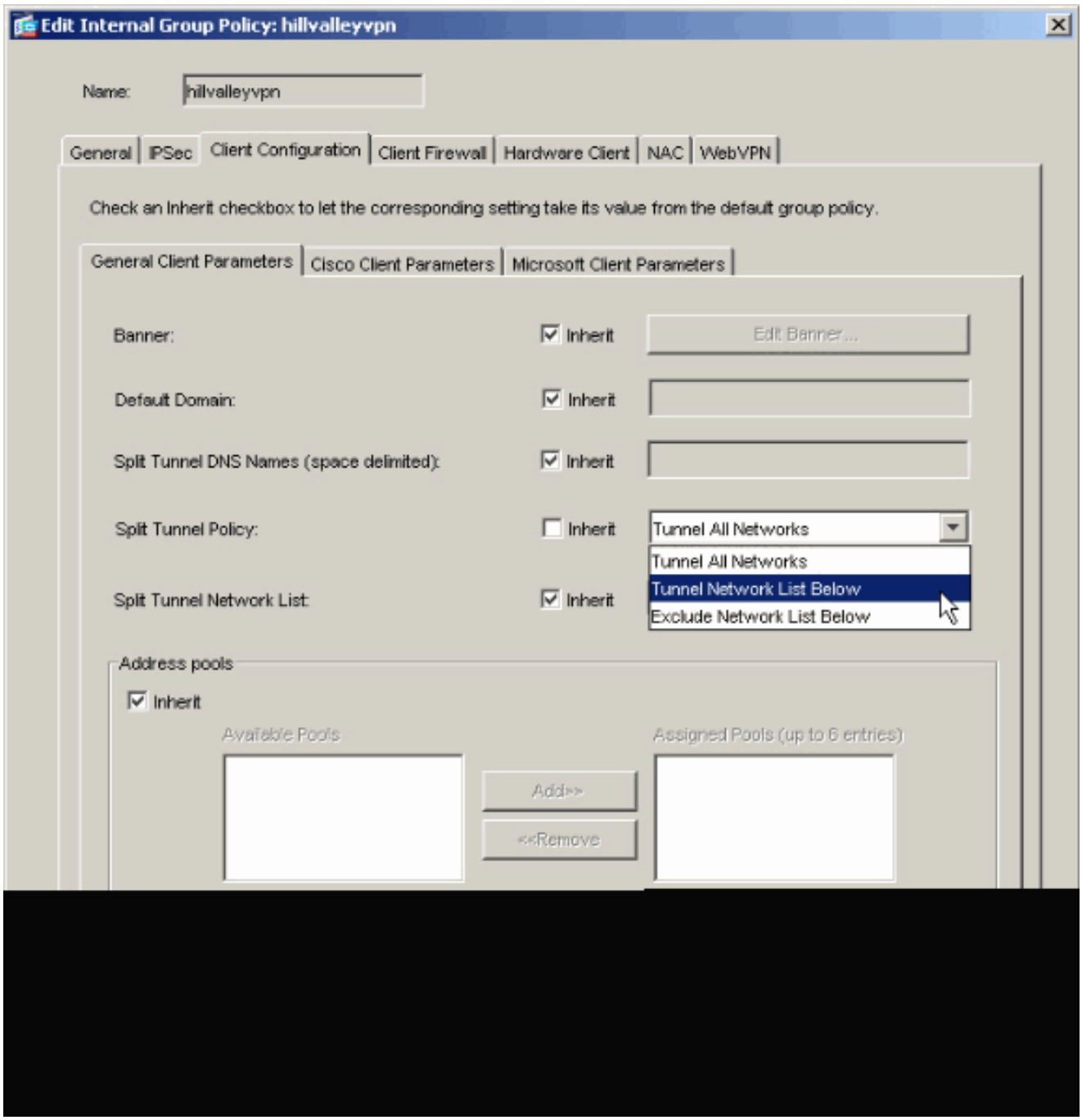
1. Configuration(컨피그레이션) > VPN > General(일반) > Group Policy(그룹 정책)를 선택하고 로컬 LAN 액세스를 활성화하려는 그룹 정책을 선택합니다. 그런 다음 Edit(편집)를 클릭합니다.



2. Client Configuration(클라이언트 구성) 탭으로 이동합니다.

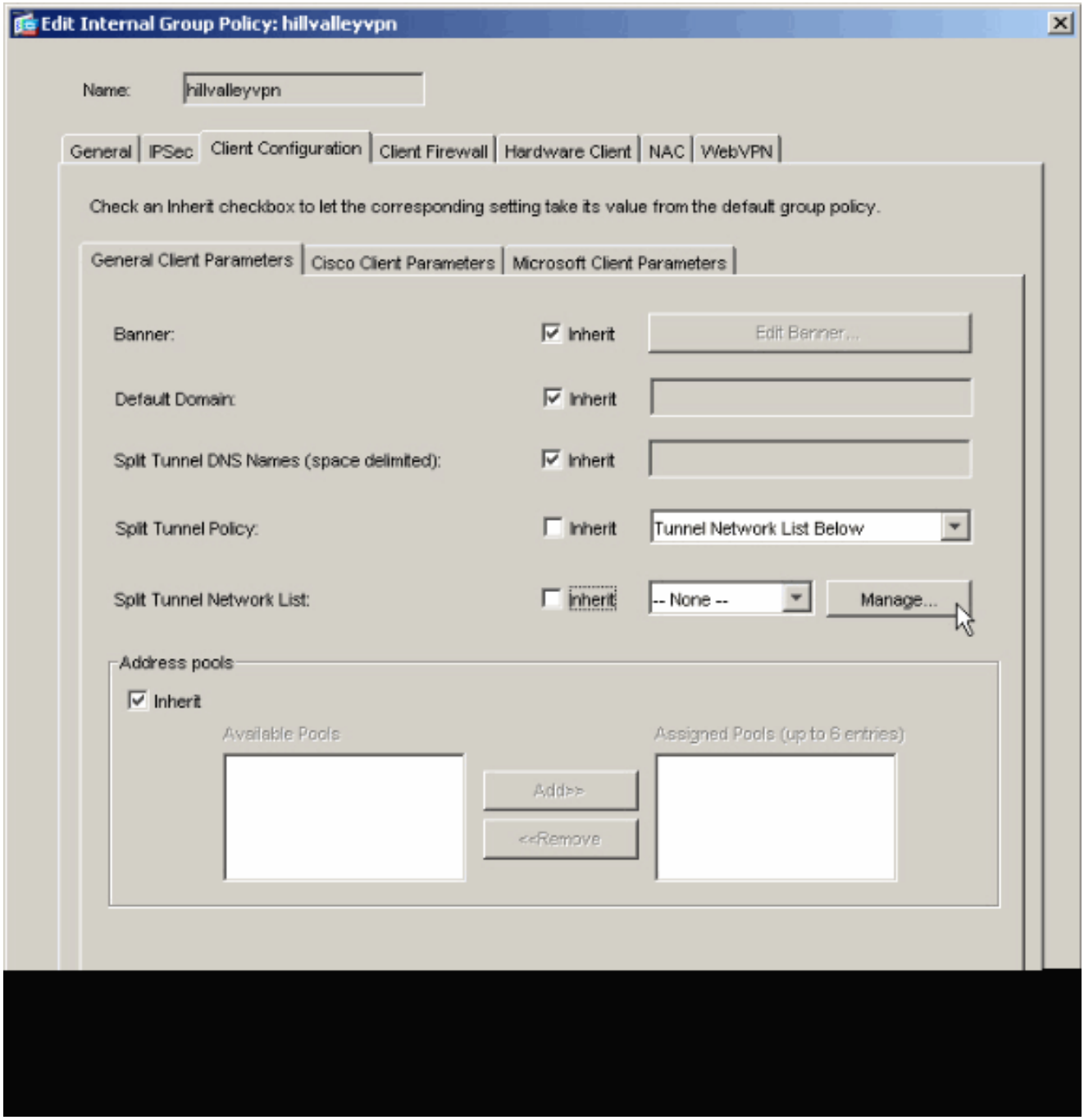


3. Inherit(상속) 상자의 Split Tunnel Policy(스플릿 터널 정책)를 선택 취소하고 Tunnel Network List Below 을 선택합니다.



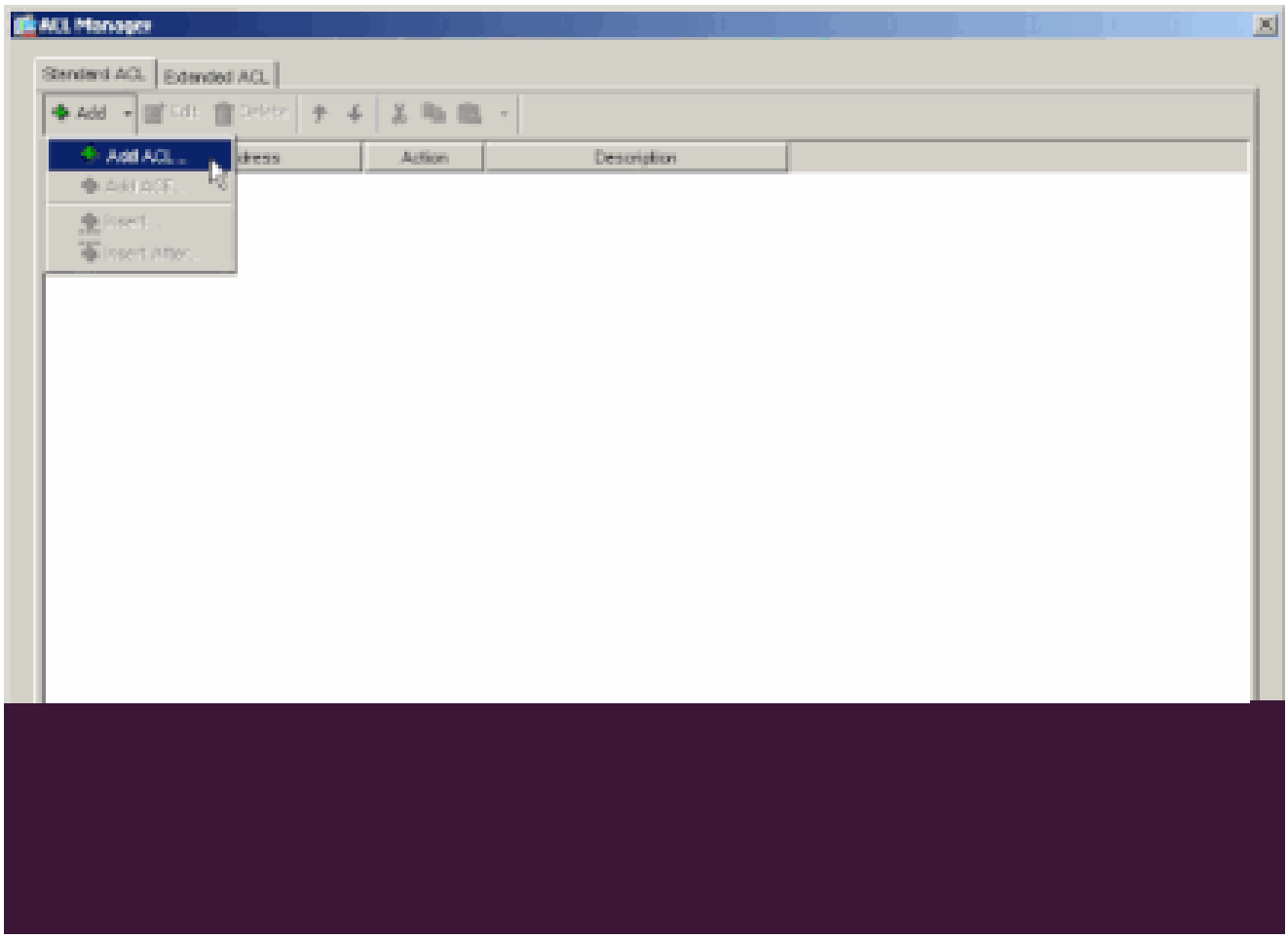
•

ACL Manager를 **시작하려면** Split Tunnel Network List(스플릿 터널 네트워크 목록)의 Inherit(상속) 상자의 선택을 취소한 다음 **Manage(관리)**를 클릭합니다.



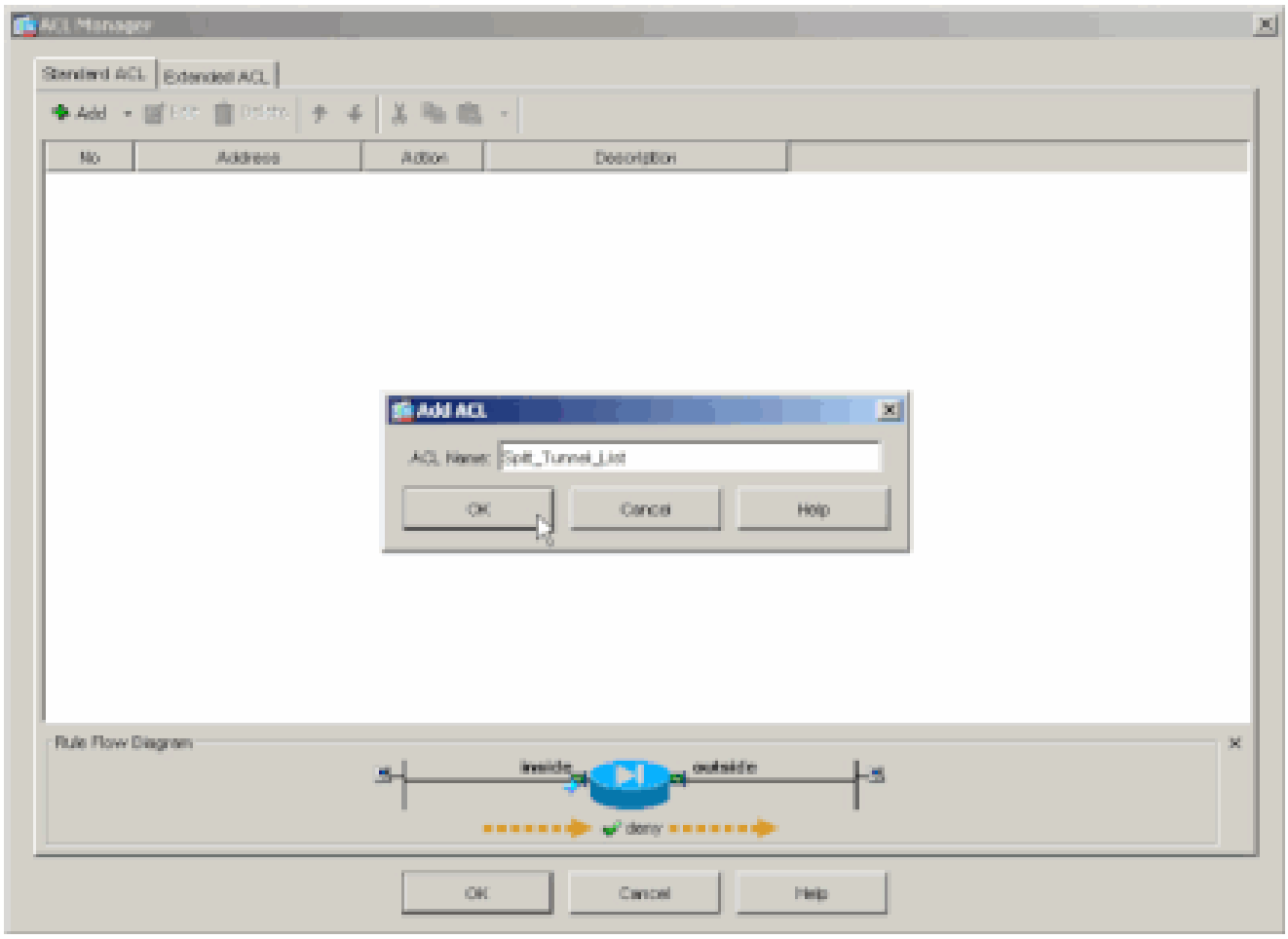
•

새 액세스 목록을 생성하려면 ACL Manager에서 **Add(추가) > Add ACL...**(ACL 추가...)을 선택합니다.



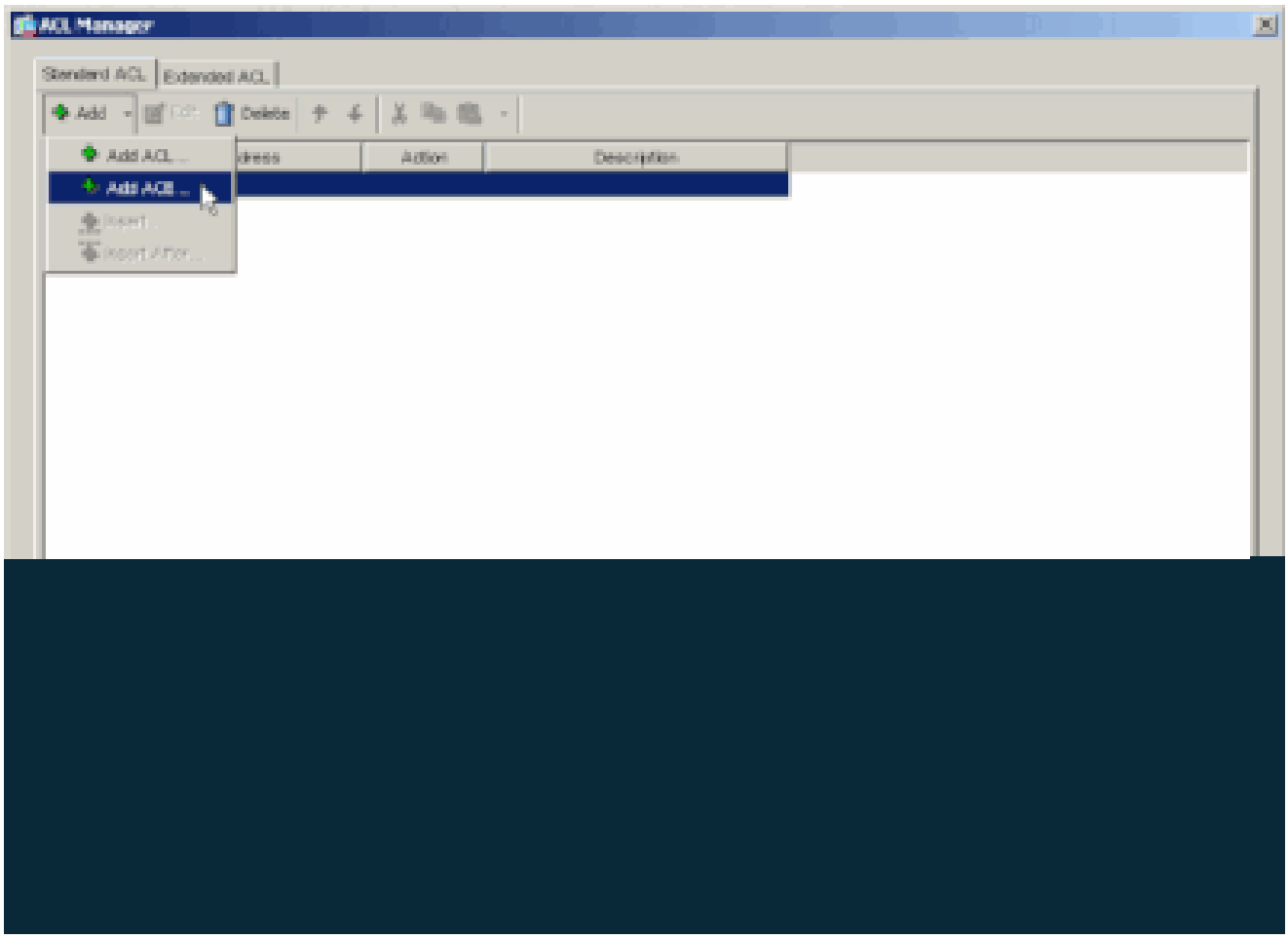
•

ACL의 이름을 입력하고 **OK**(확인)를 클릭합니다.



•

ACL이 생성되면 Add(추가) > **Add ACE(ACE 추가)**를 선택합니다. .ACE(Access Control Entry)를 추가합니다.



-

ASA 뒤의 LAN에 해당하는 ACE를 정의합니다. 이 경우 네트워크는 10.0.1.0/24입니다.

a.

Permit(허용)을 선택합니다.

b.

10.0.1.0의 IP 주소 선택

c.

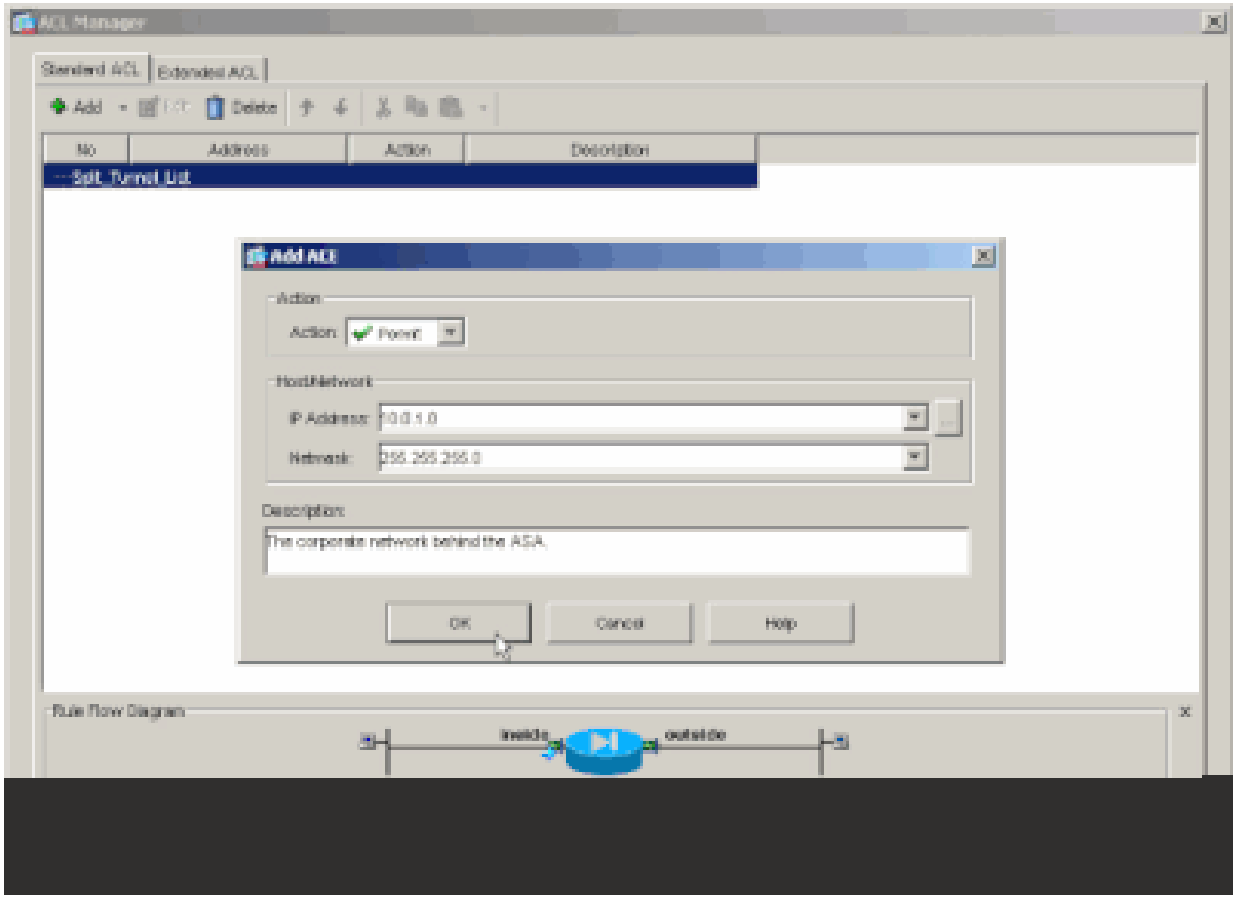
255.255.255.0의 넷마스크를 **선택합니다**.

d.

*(*선택 사항)설명을 제공합니다.

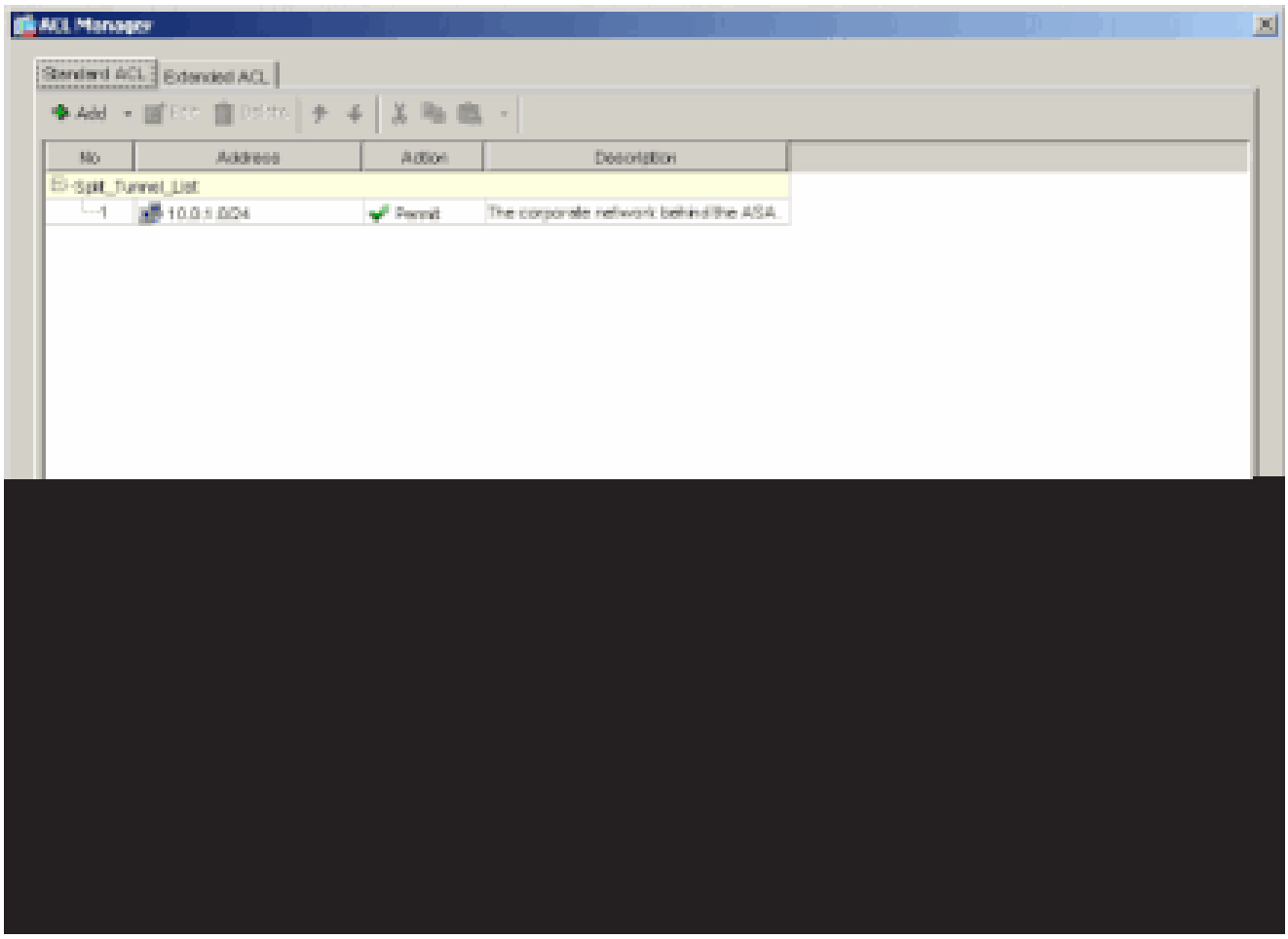
e.

> 확인을 **클릭합니다**.



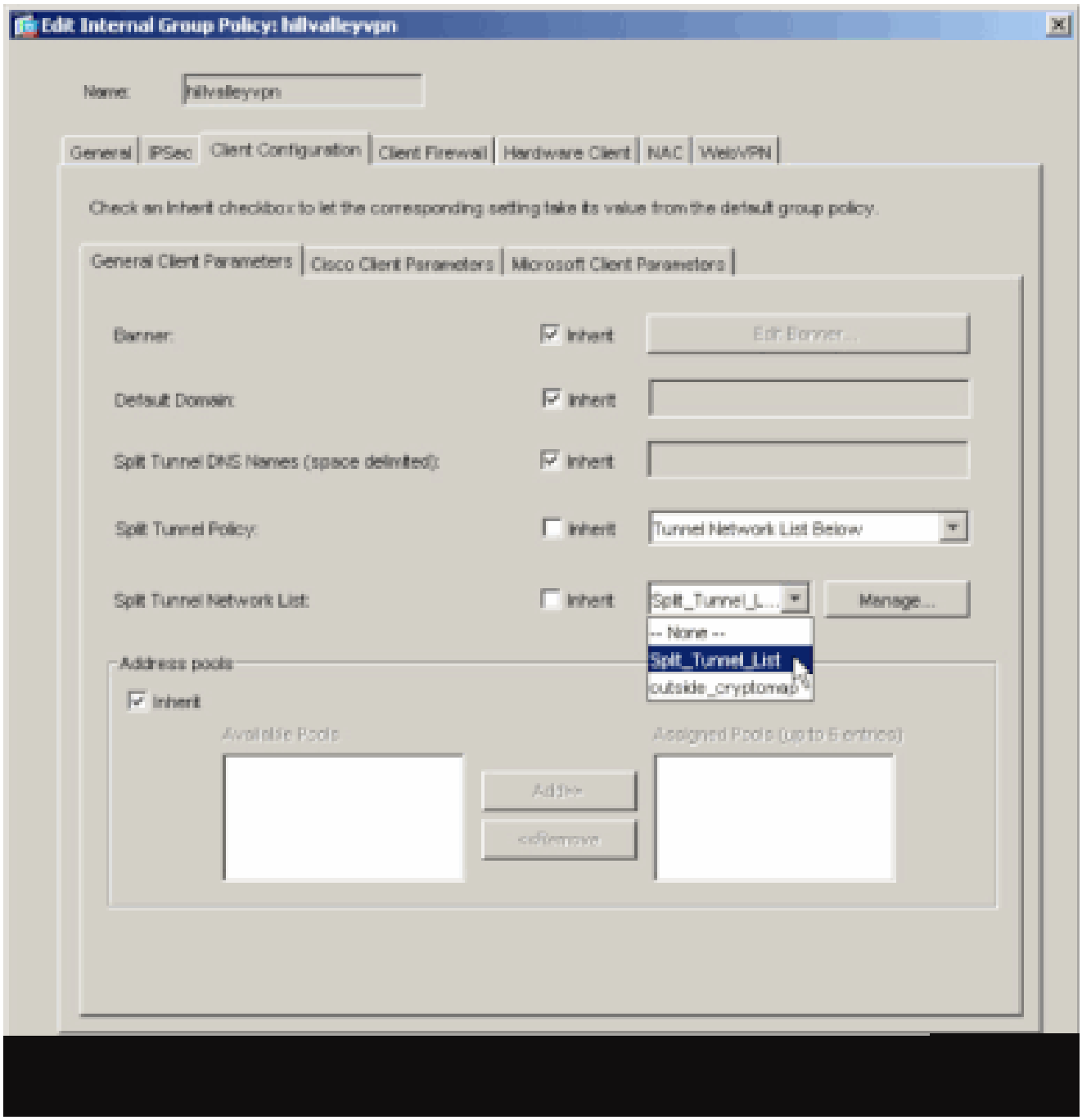
•

ACL **관리자**를 종료하려면 OK를 클릭합니다.



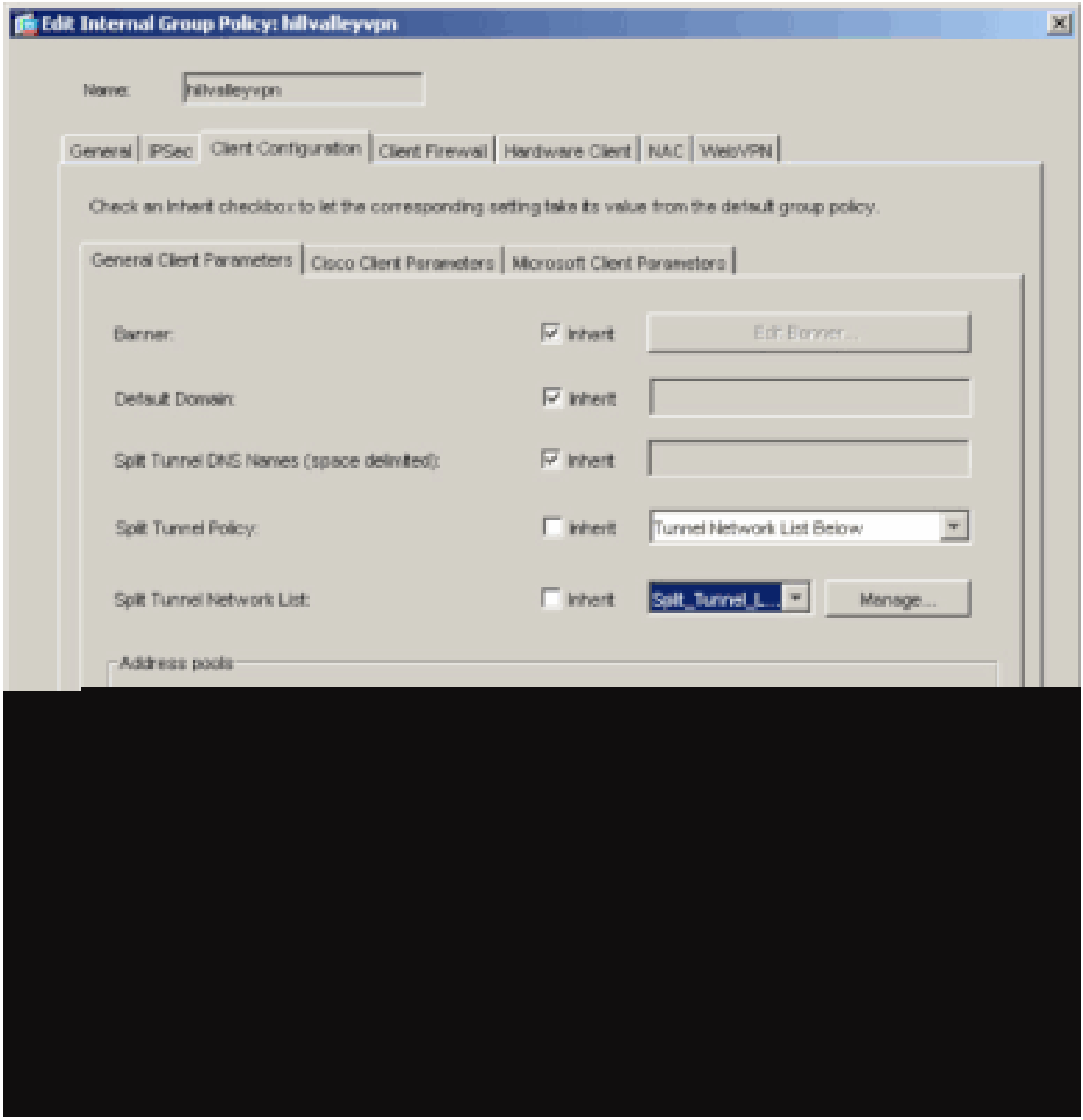
•

방금 생성한 ACL이 스플릿 터널 네트워크 목록에 대해 선택되었는지 확인합니다.



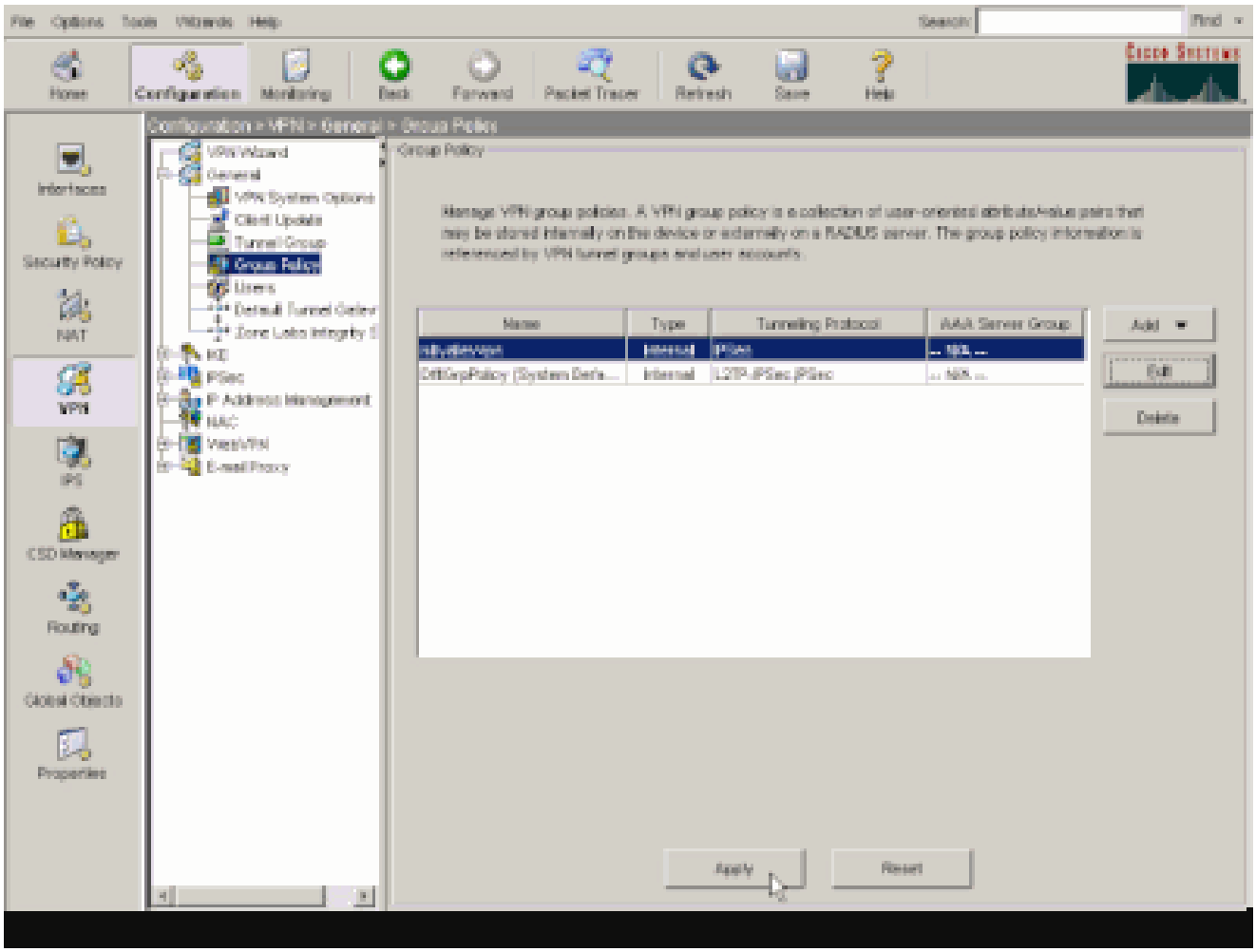
•

OK(**확인**)를 클릭하여 그룹 정책 컨피그레이션으로 돌아갑니다.



•

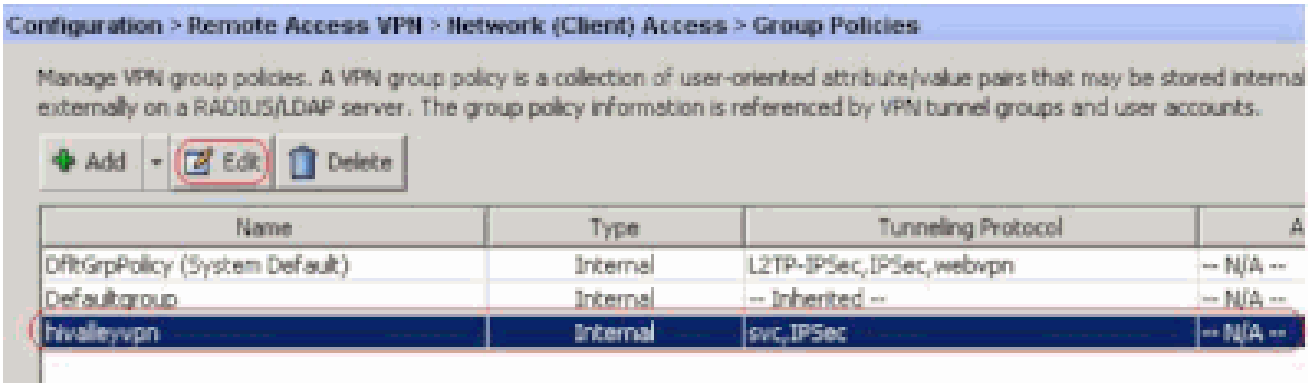
Apply(**적용**)를 클릭한 **다음 Send**(필요한 경우)(보내기)를 클릭하여 ASA에 명령을 보냅니다.



ASDM 6.x로 ASA 8.x 구성

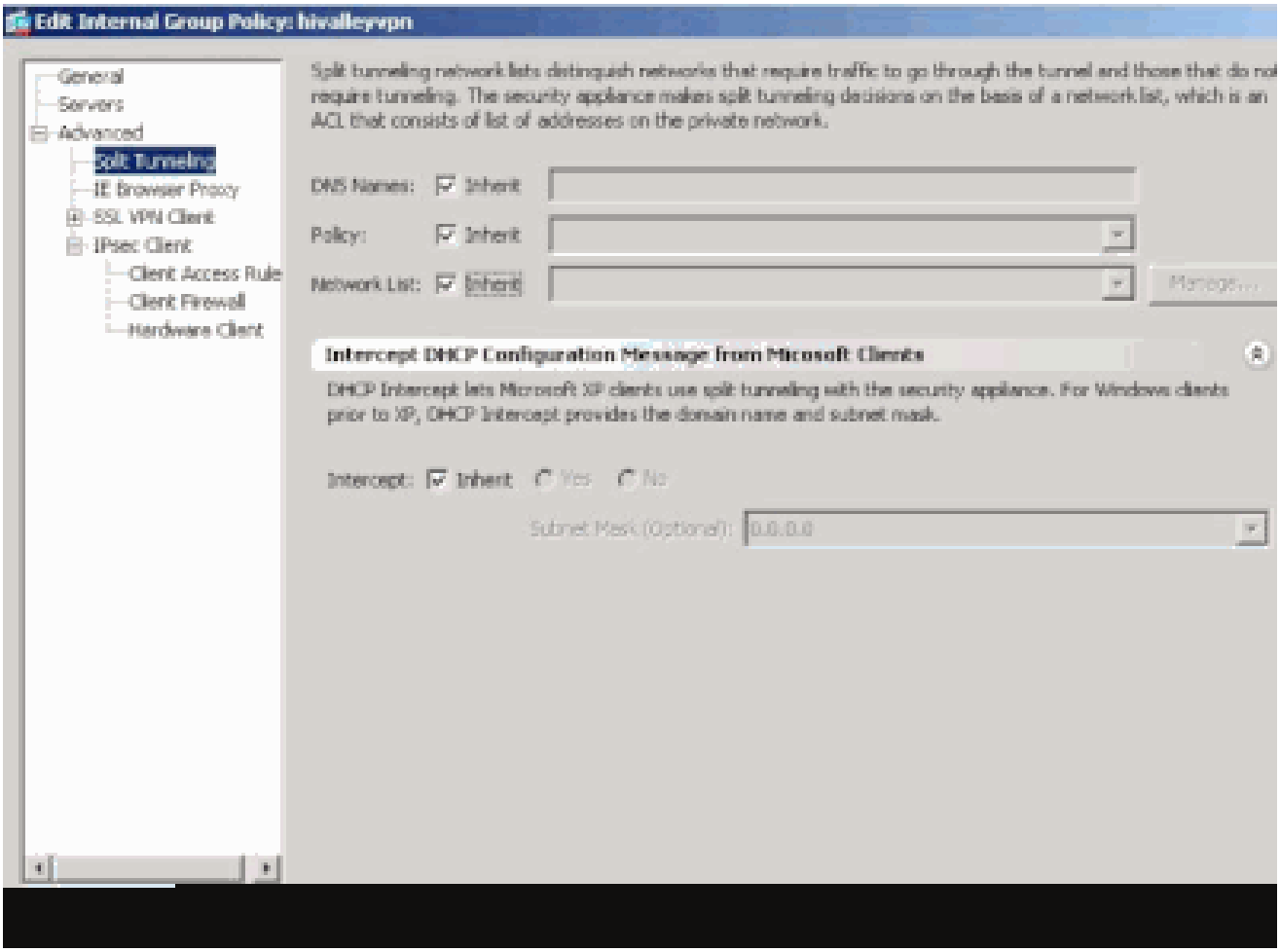
그룹 내 사용자에 대해 스플릿 터널링을 허용하도록 터널 그룹을 구성하려면 다음 단계를 완료하십시오.

- Configuration**(구성) > Remote Access VPN(원격 액세스 VPN) > Network (Client) Access(네트워크(클라이언트) 액세스) > Group Policies(그룹 정책)**를 선택하고 로컬 LAN 액세스를 활성화할 그룹 정책을 선택합니다. 그런 다음 Edit(수정)**를 클릭합니다**.



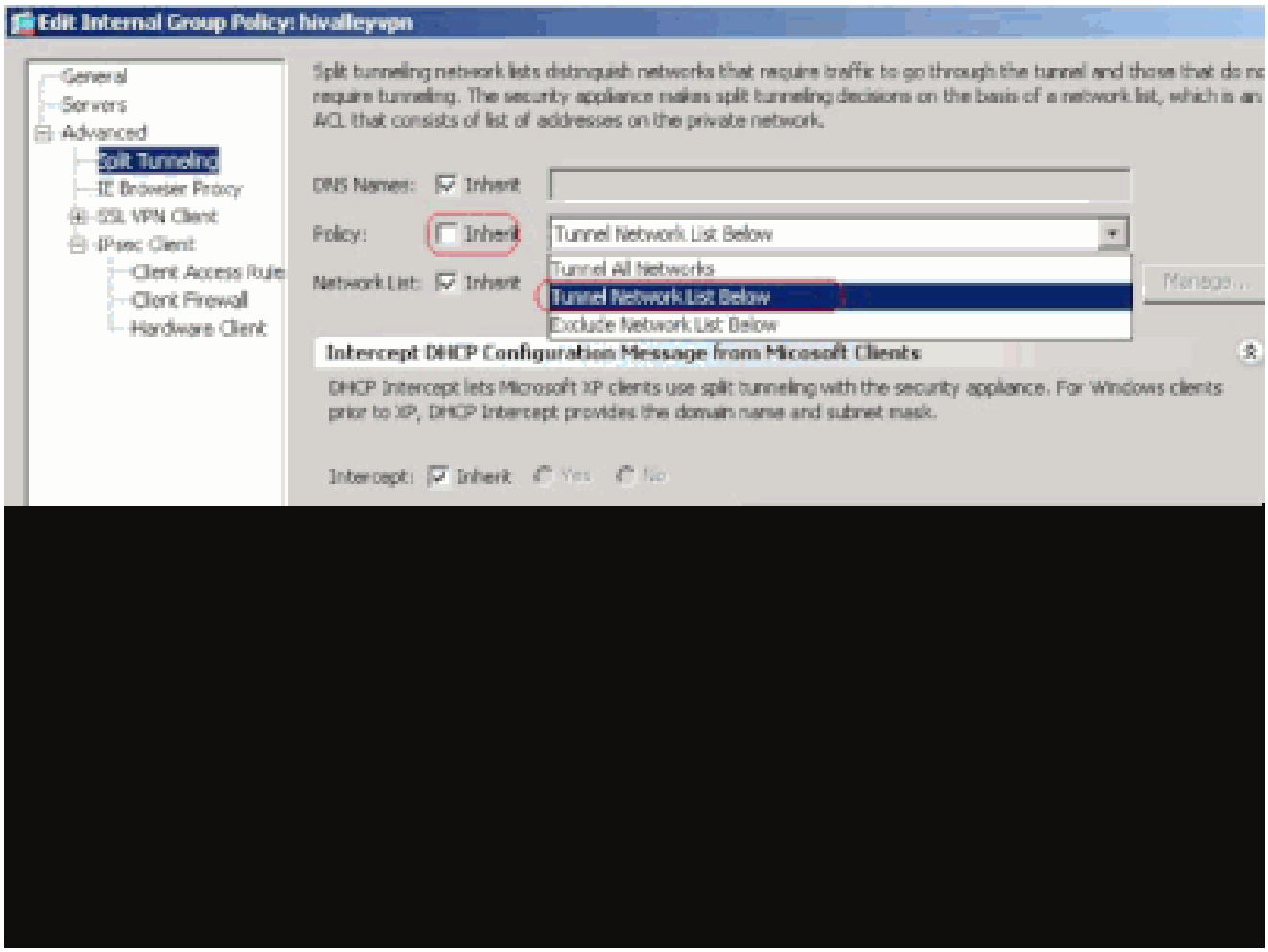
-

스플릿 터널링을 **클릭합니다**.



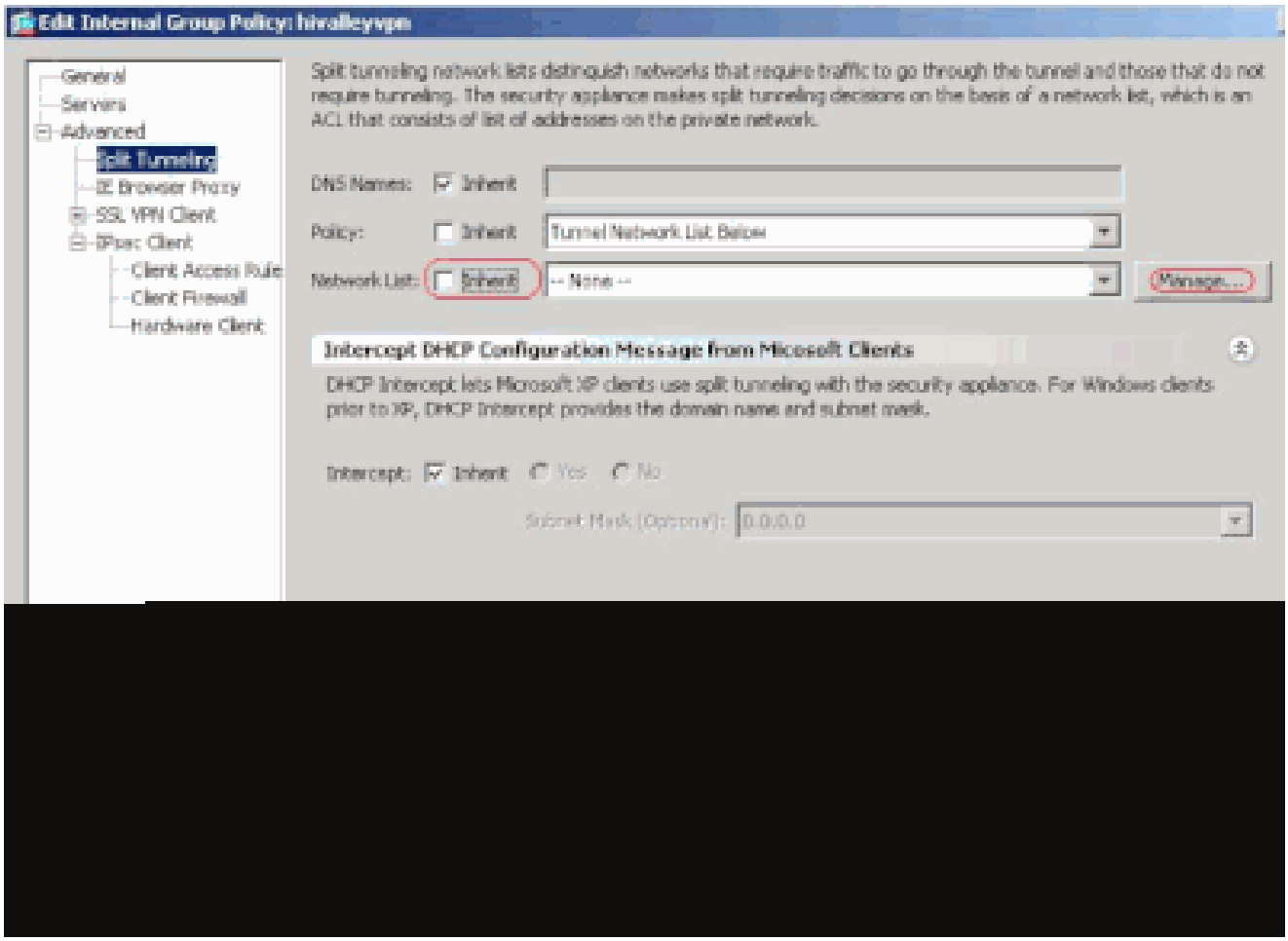
-

스플릿 터널 **정책**에 대한 Inherit(상속) 상자의 선택을 취소하고 Tunnel **Network List Below(아래 터널 네트워크 목록)를 선택합니다**.



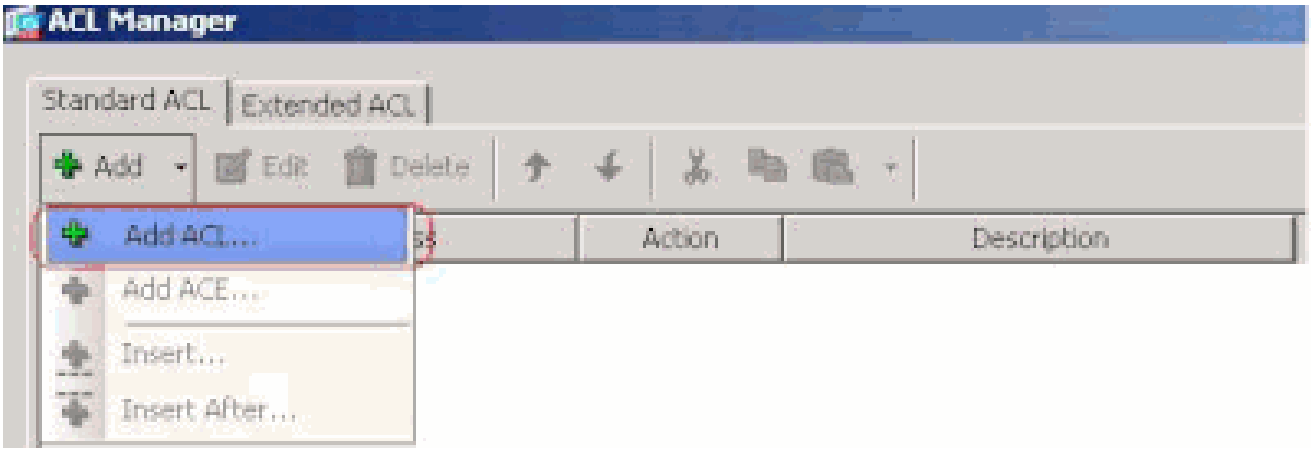
•

ACL Manager를 **시작하려면** Split Tunnel Network List(스플릿 터널 네트워크 목록)의 Inherit(상속) 상자를 선택 취소한 다음 **Manage(관리)**를 클릭합니다.



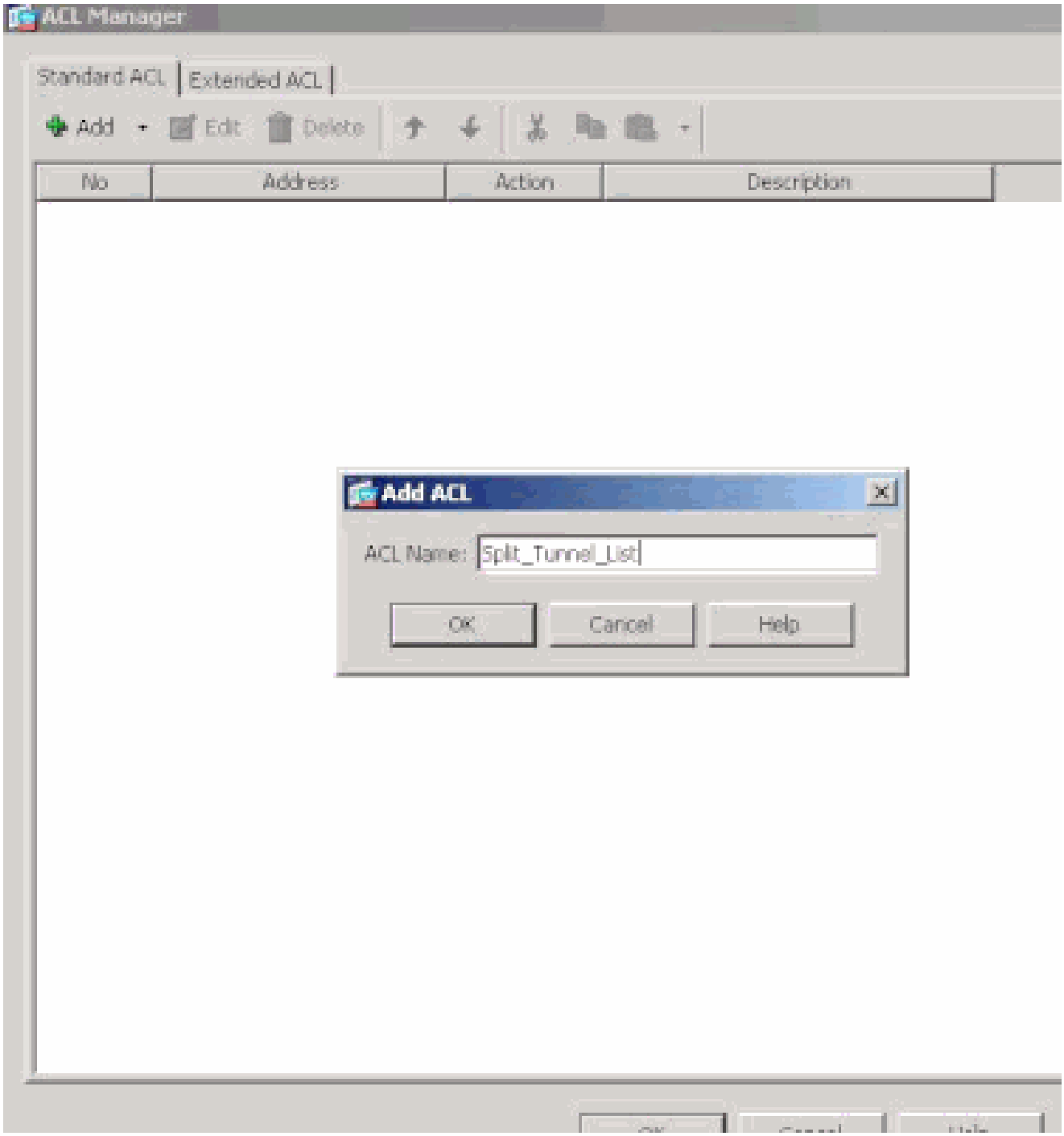
•

새 액세스 목록을 생성하려면 ACL Manager에서 **Add(추가) > Add ACL...**(ACL 추가...)을 선택합니다.



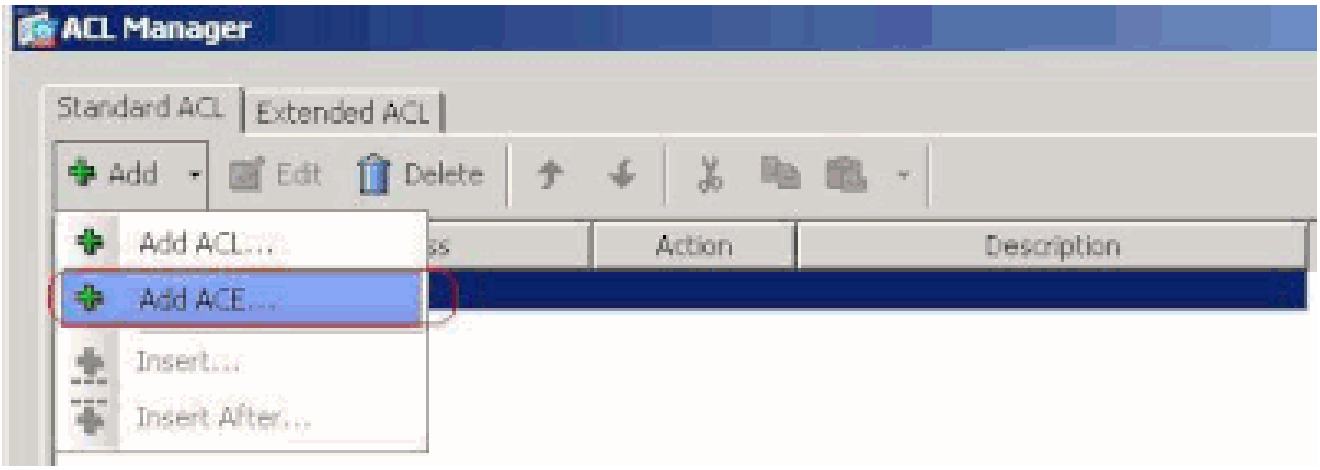
•

ACL의 이름을 입력하고 **OK(확인)**를 클릭합니다.



•

ACL이 생성되면 ACE(Access Control Entry)를 추가하려면 Add(**추가**) > **Add** ACE(ACE 추가)...를 선택합니다.



-

ASA 뒤의 LAN에 해당하는 ACE를 정의합니다. 이 경우 네트워크는 10.0.1.0/24입니다.

a.

Permit(**허용)** 라디오 버튼을 클릭합니다.

b.

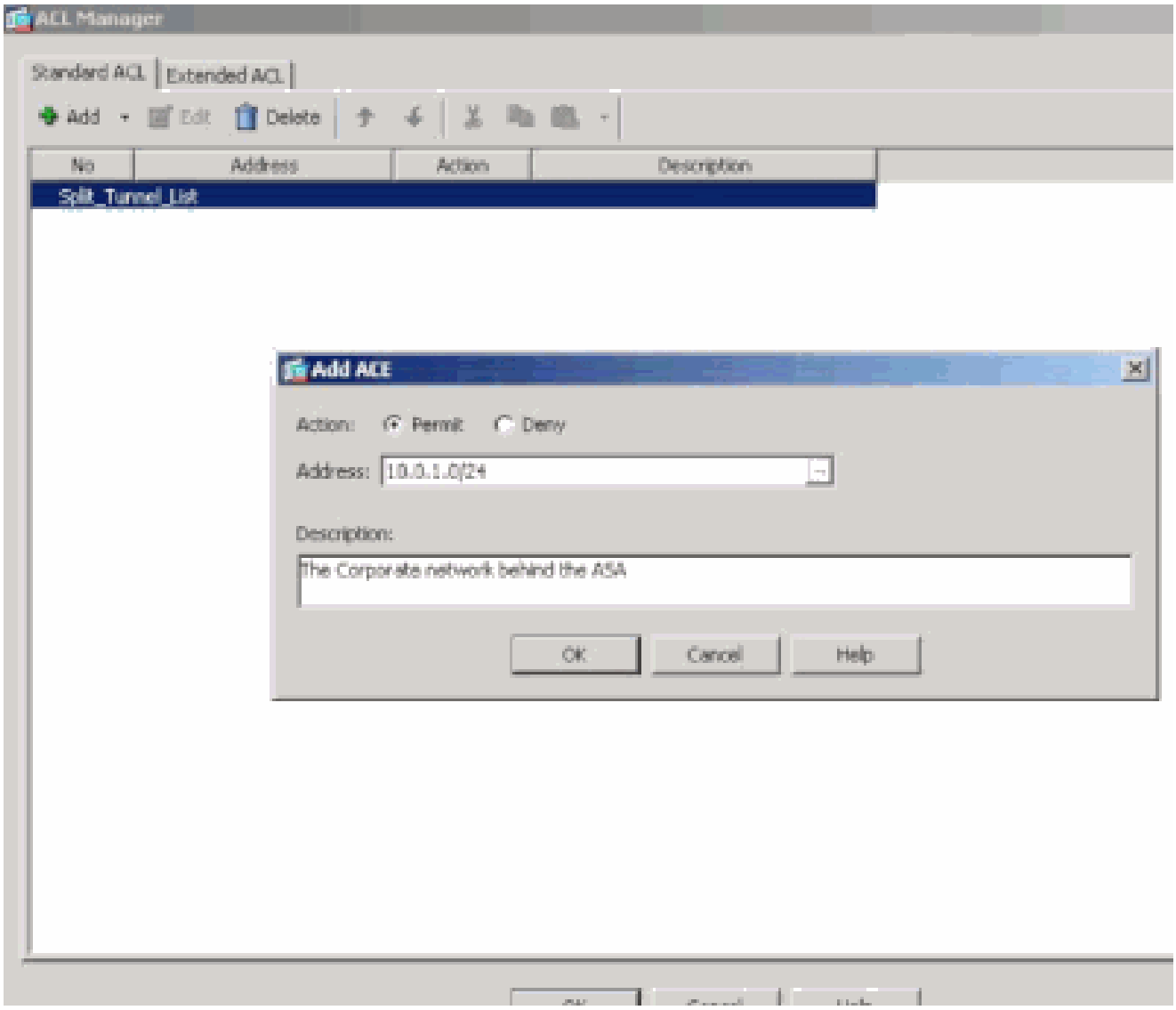
마스크 **10.**0.1.0/24의 네트워크 주소를 **선택합니다**.

c.

(선택 사항) 설명을 제공합니다.

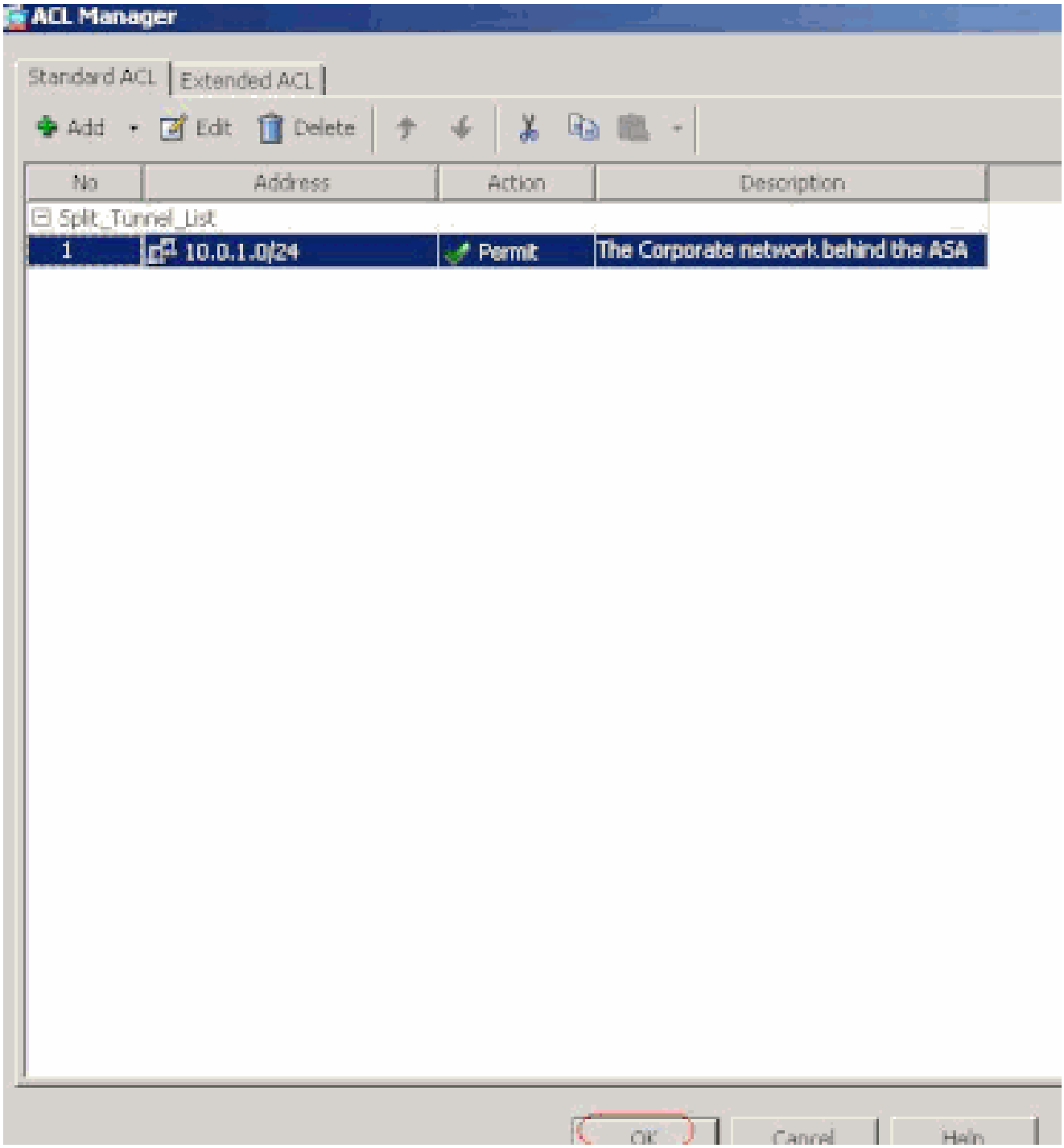
d.

OK(확인)를 클릭합니다.



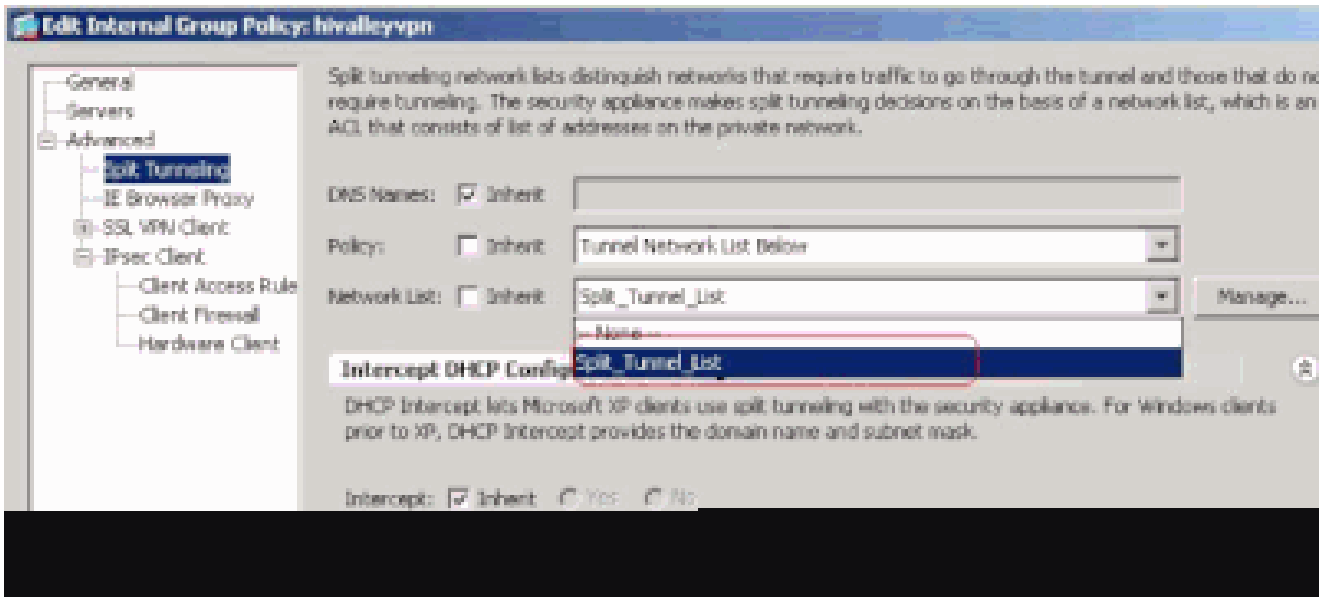
•

ACL **Manager**를 종료하려면 OK를 클릭합니다.



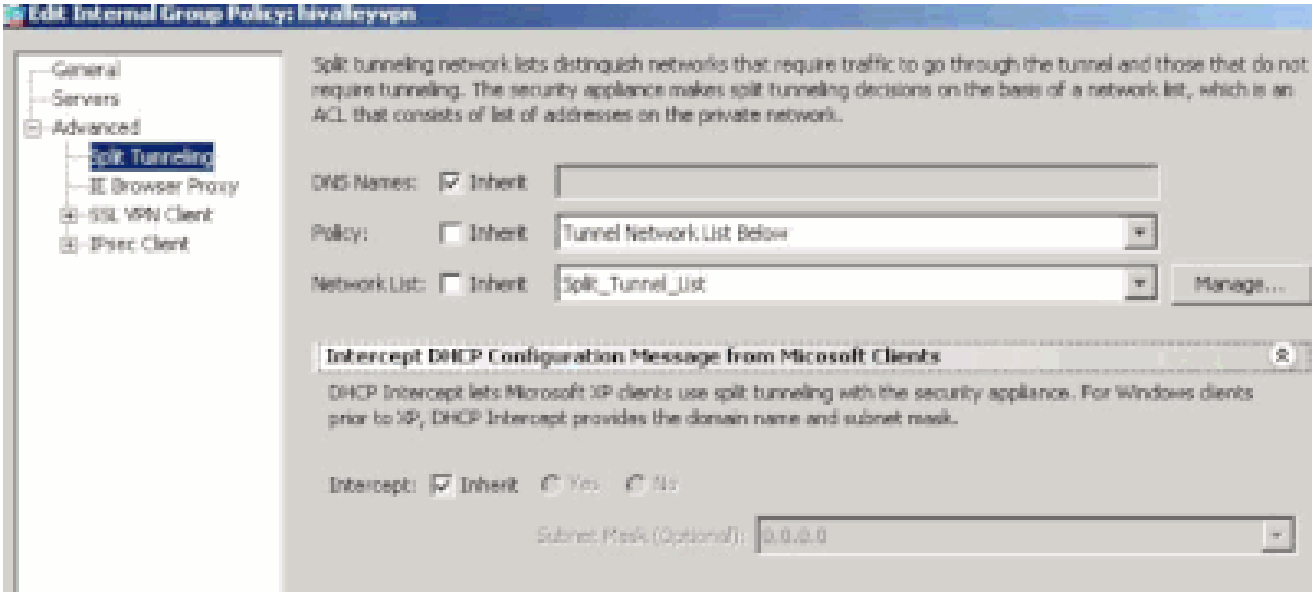
•

방금 생성한 ACL이 스플릿 터널 네트워크 목록에 대해 선택되었는지 확인합니다.



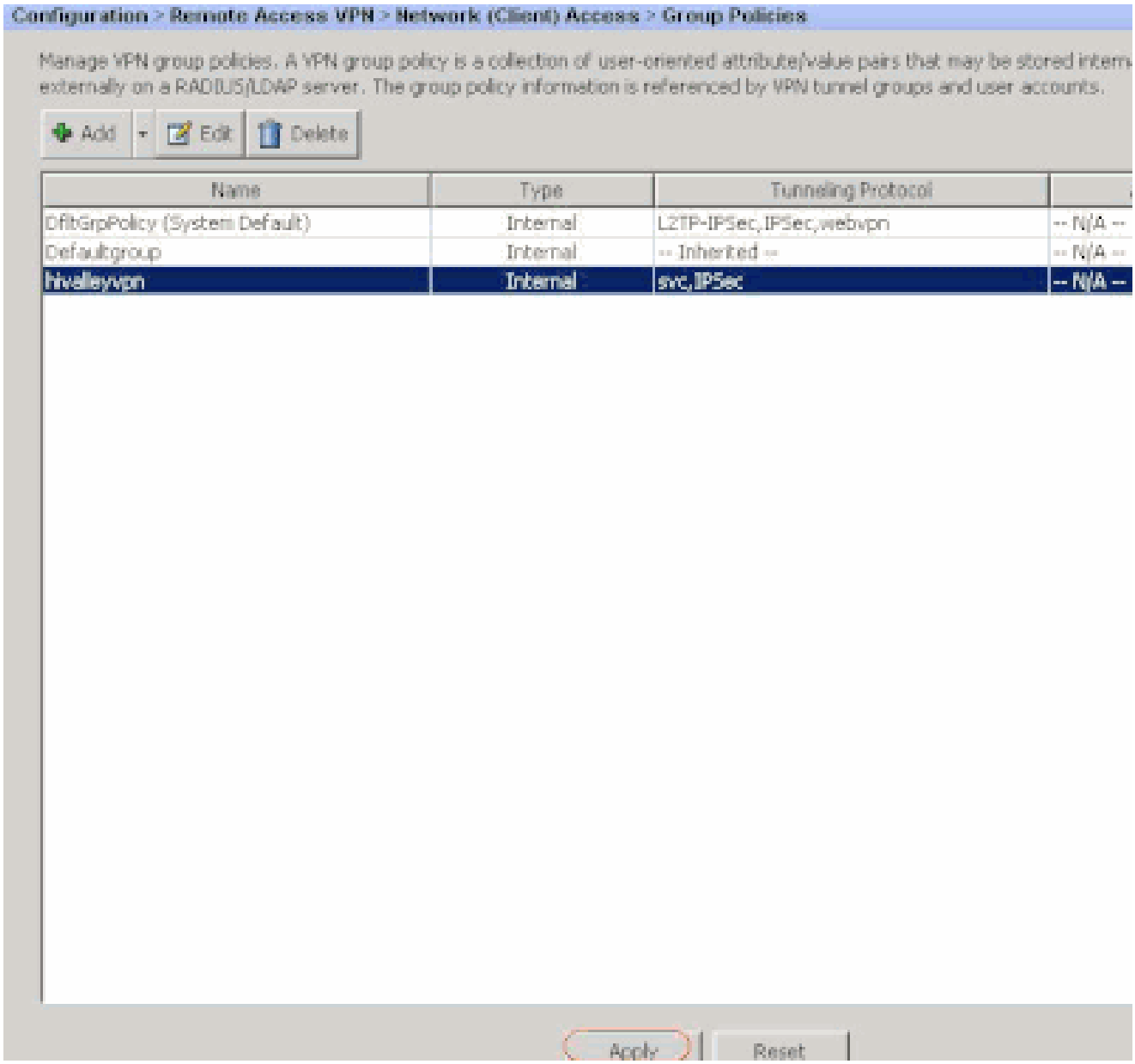
•

OK(**확인**)를 클릭하여 그룹 정책 컨피그레이션으로 돌아갑니다.



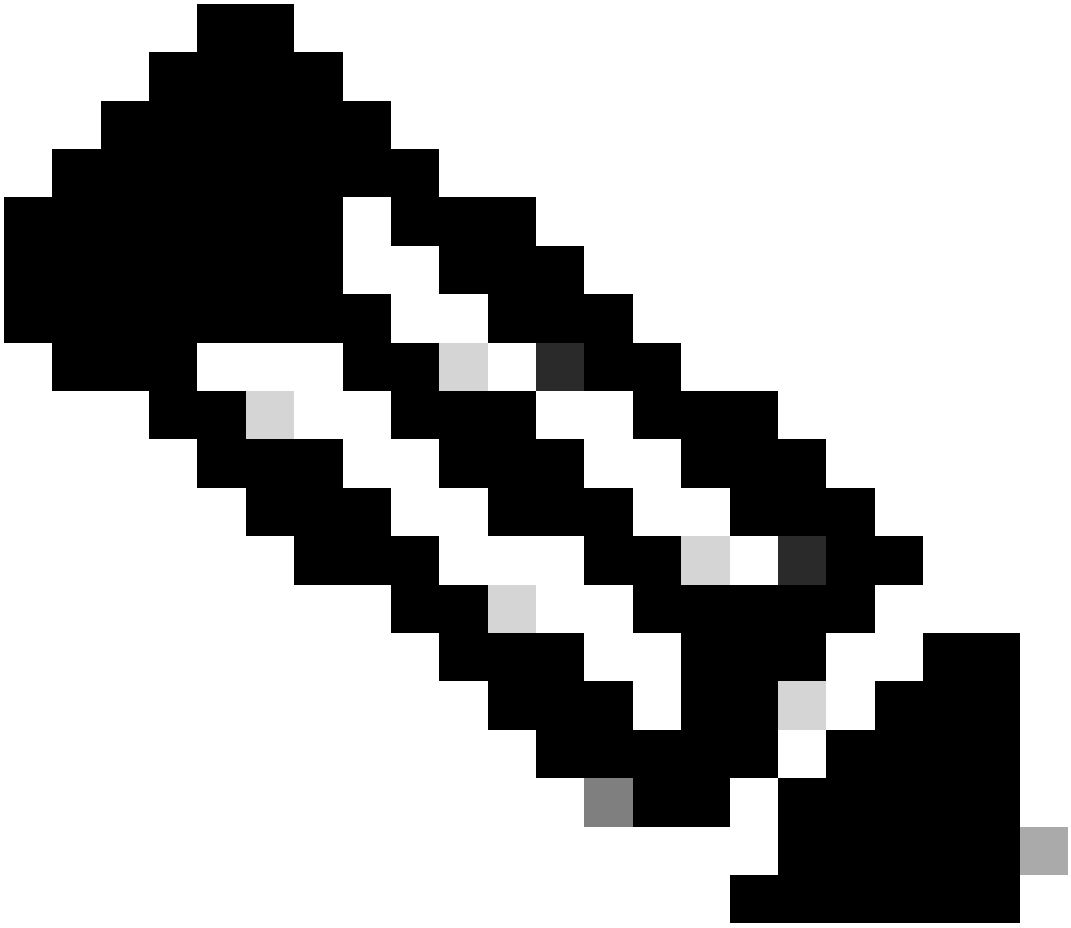
•

Apply(**적용**)를 클릭한 **다음 Send**(필요한 경우)(보내기)를 클릭하여 ASA에 명령을 보냅니다.



CLI를 통해 ASA 7.x 이상 구성

ASDM을 사용하지 않고 ASA에서 스플릿 터널링을 허용하기 위해 ASA CLI에서 다음 단계를 완료할 수 있습니다.



참고: CLI 스플릿 터널링 컨피그레이션은 ASA 7.x 및 8.x 모두에서 동일합니다.

-

컨피그레이션 모드로 들어갑니다.

```
<#root>

ciscoasa>
```

enable

Password: ********
ciscoasa#

configure terminal

ciscoasa(config)#

- ASA 뒤에 있는 네트워크를 정의하는 액세스 목록을 생성합니다.

<#root>

ciscoasa(config)#

access-list Split_Tunnel_List remark The corporate network behind the ASA.

ciscoasa(config)#

access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0

- 수정하려는 정책에 대해 그룹 정책 컨피그레이션 모드로 들어갑니다.

<#root>

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

```
ciscoasa(config-group-policy)#
```

- 스플릿 터널 정책을 지정합니다. 이 경우 정책은 tunnelspecified**입니다**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

- 스플릿 터널 액세스 목록을 지정합니다. 이 경우 목록은 Split_**Tunnel_List입니다**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

- 다음 명령을 실행합니다.

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

- 그룹 정책을 터널 그룹과 연결

<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

- 두 가지 컨피그레이션 모드를 종료합니다.

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

```
 exit


ciscoasa#
```

- 컨피그레이션을 비휘발성 RAM(NVRAM)에 저장하고 소스 파일 **이름**을 지정하라는 메시지가 나타나면 Enter 키를 누릅니다.

```
    <#root>

ciscoasa#


 copy running-config startup-config



Source filename [running-config]?
Cryptochecksum: 93bb3217 0f60bfa4 c36bbb29 75cf714a

3847 bytes copied in 3.470 secs (1282 bytes/sec)
ciscoasa#
```

CLI를 통해 PIX 6.x 구성

다음 단계를 완료하십시오.

- PIX 뒤에 있는 네트워크를 정의하는 액세스 목록을 생성합니다.

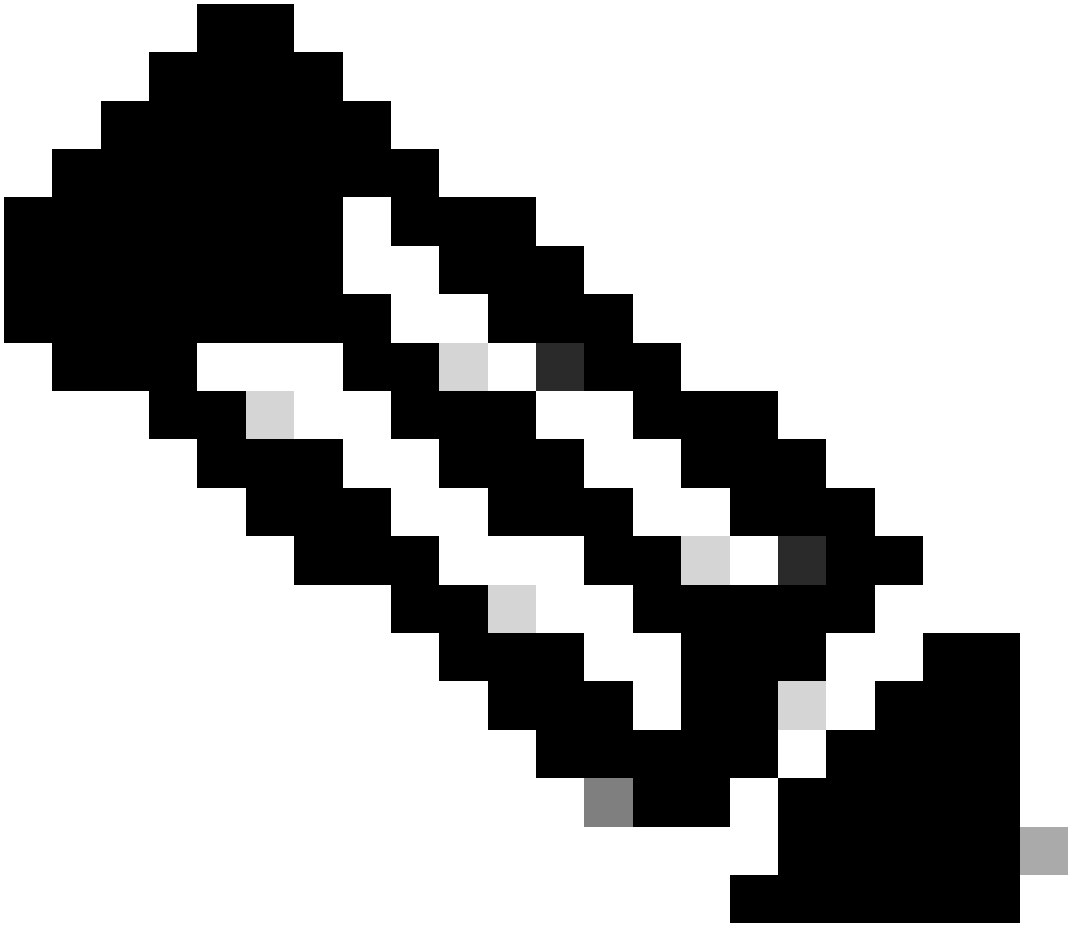
```
    <#root>


 PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- 다음과 같이 vpn 그룹 **vpn3000**을 생성하고 분할 터널 ACL을 지정합니다.

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



참고: PIX 6.x의 원격 액세스 VPN 컨피그레이션에 대한 자세한 내용은 Cisco Secure PIX Firewall 6.x 및 Cisco VPN Client 3.5 for Windows with Microsoft Windows 2000 and 2003 IAS RADIUS Authentication을 참조하십시오.

다음을 확인합니다.

컨피그레이션을 확인하려면 이 섹션의 단계를 완료하십시오.

- VPN 클라이언트에 연결

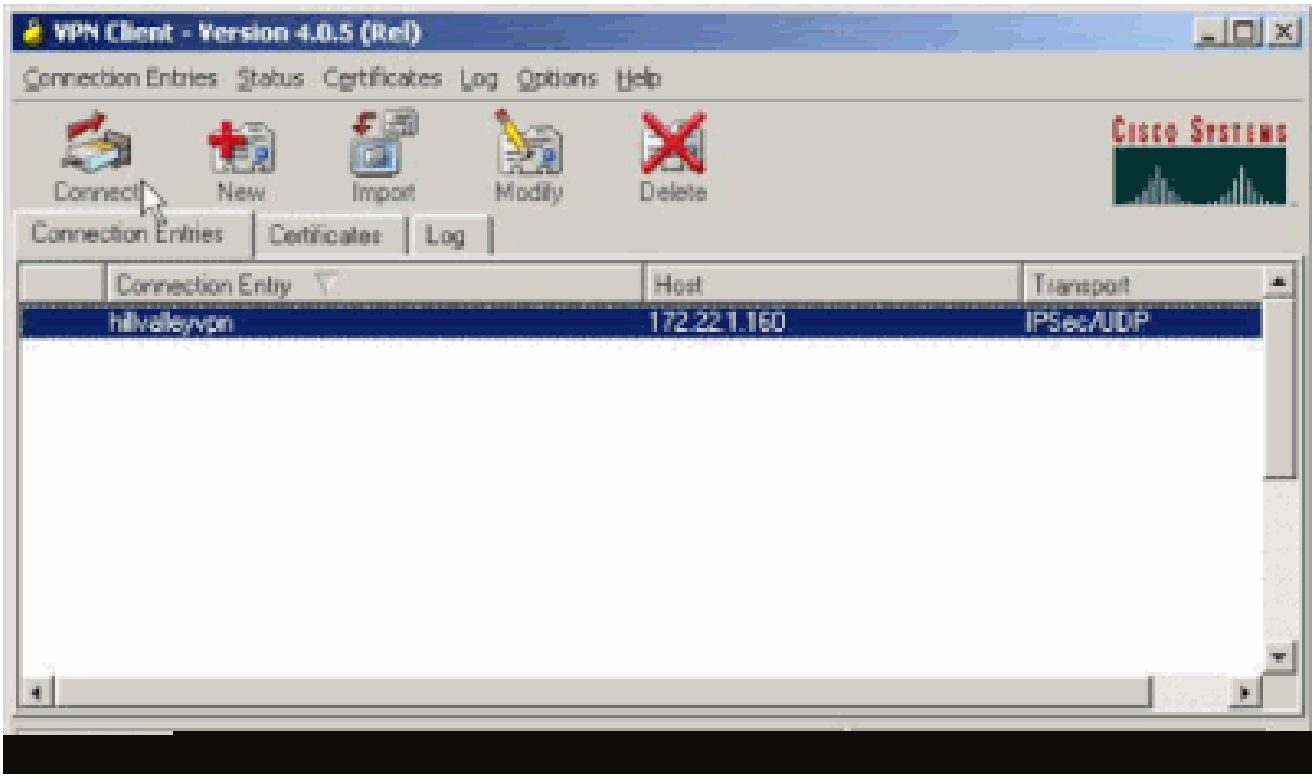
- VPN 클라이언트 로그 보기

- Ping으로 로컬 LAN 액세스 테스트

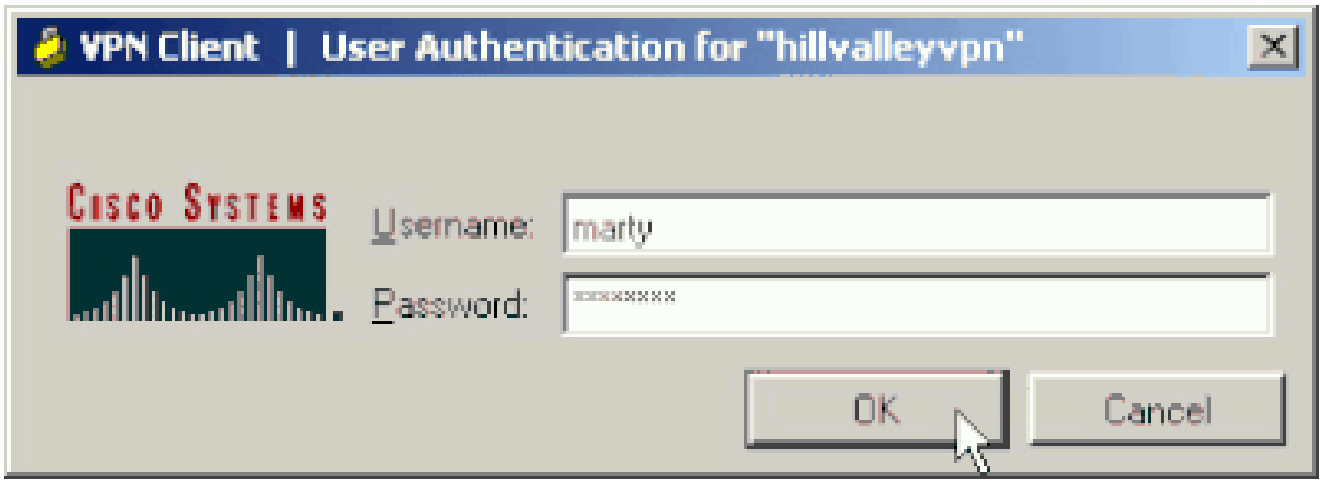
VPN 클라이언트에 연결

컨피그레이션을 확인하기 위해 VPN 클라이언트를 VPN Concentrator에 연결합니다.

- 목록에서 연결 항목을 선택하고 연결을 **클릭합니다**.

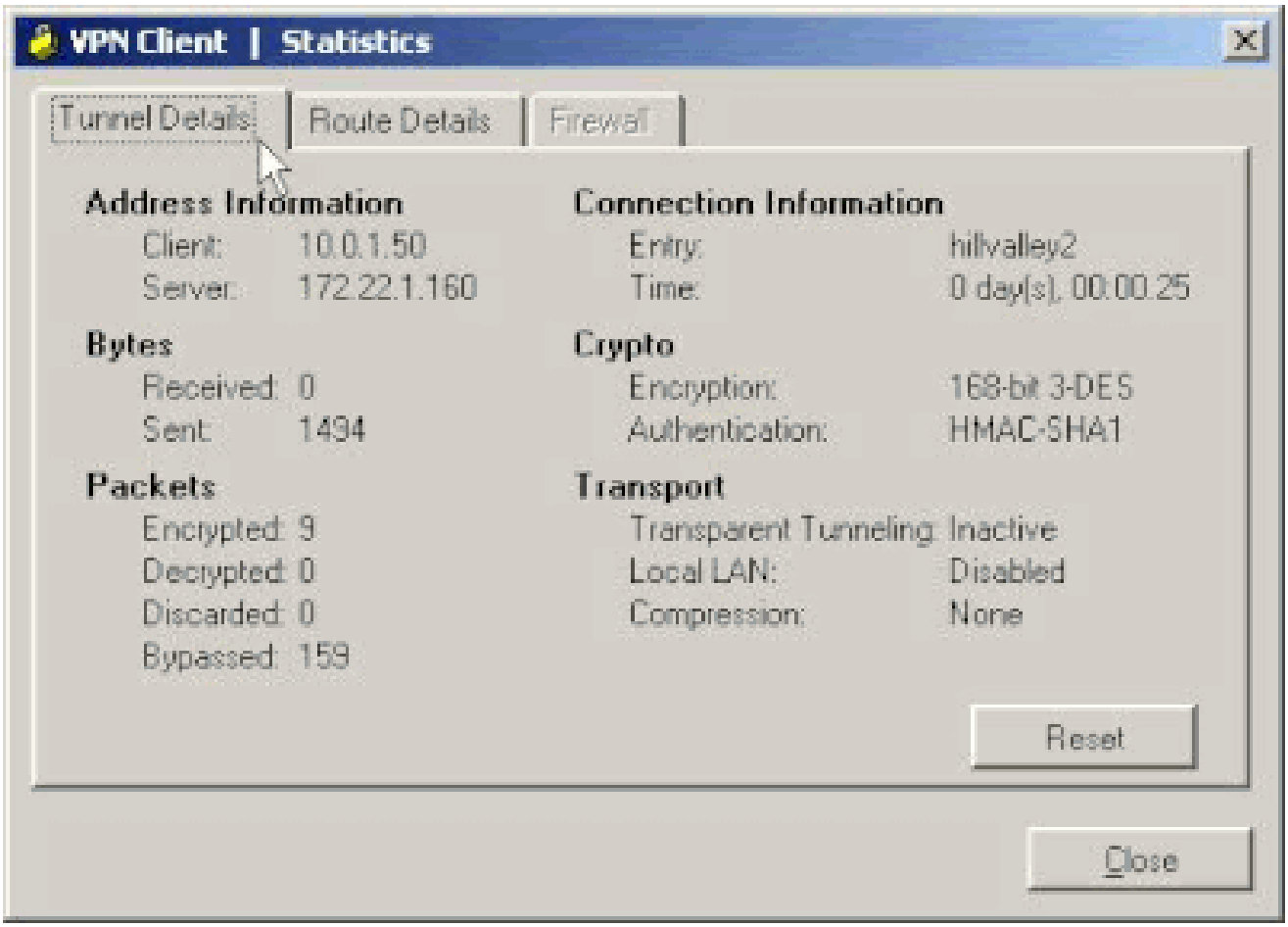


- 자격 증명을 입력합니다.



-

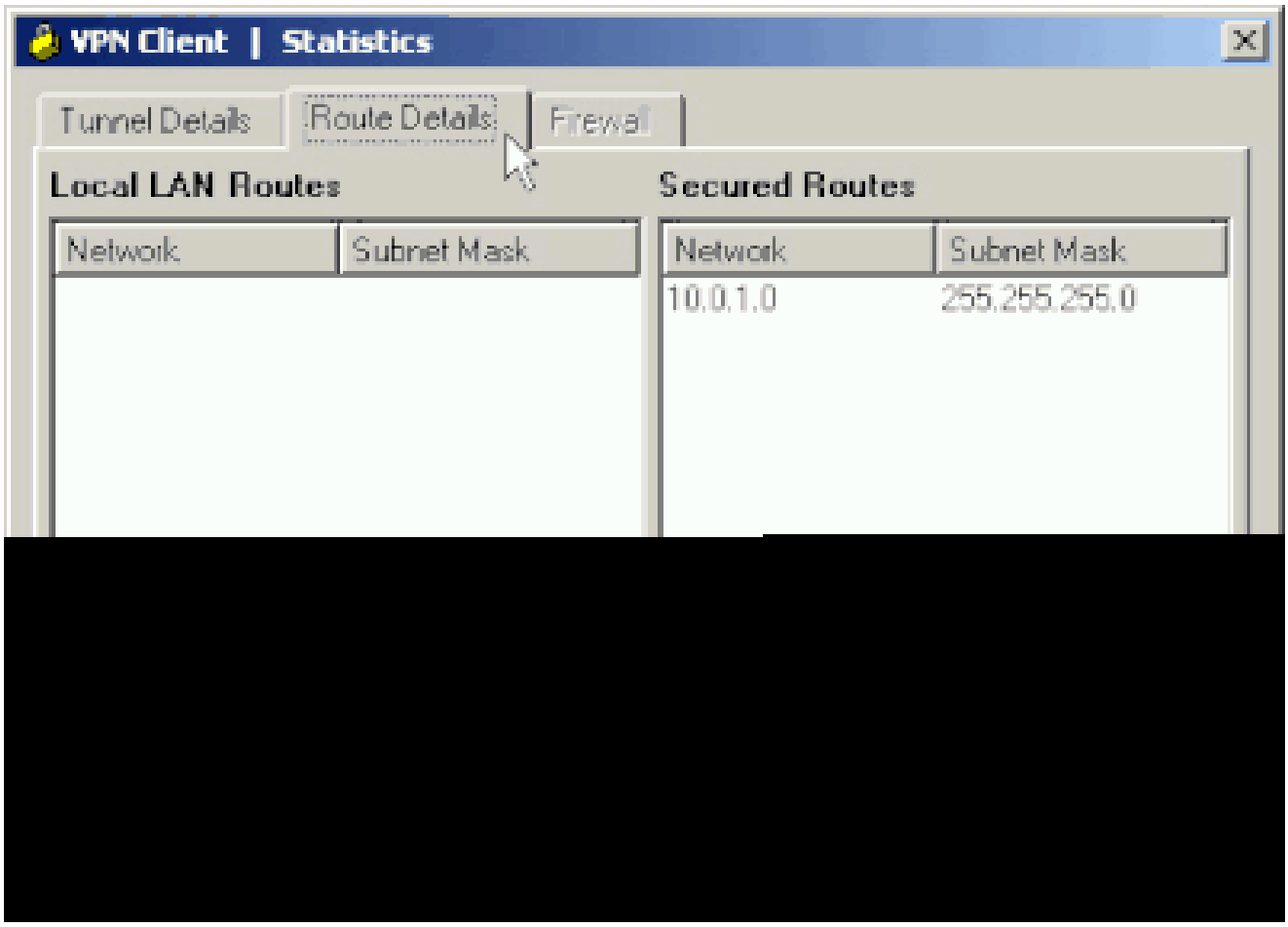
터널**의 세부 사항**을 검사하고 트래픽 흐름을 확인할 수 있는 Tunnel Details(터널 세부 정보) 창을 표시하려면 Status(상태) > Statistics...를 선택합니다.



-

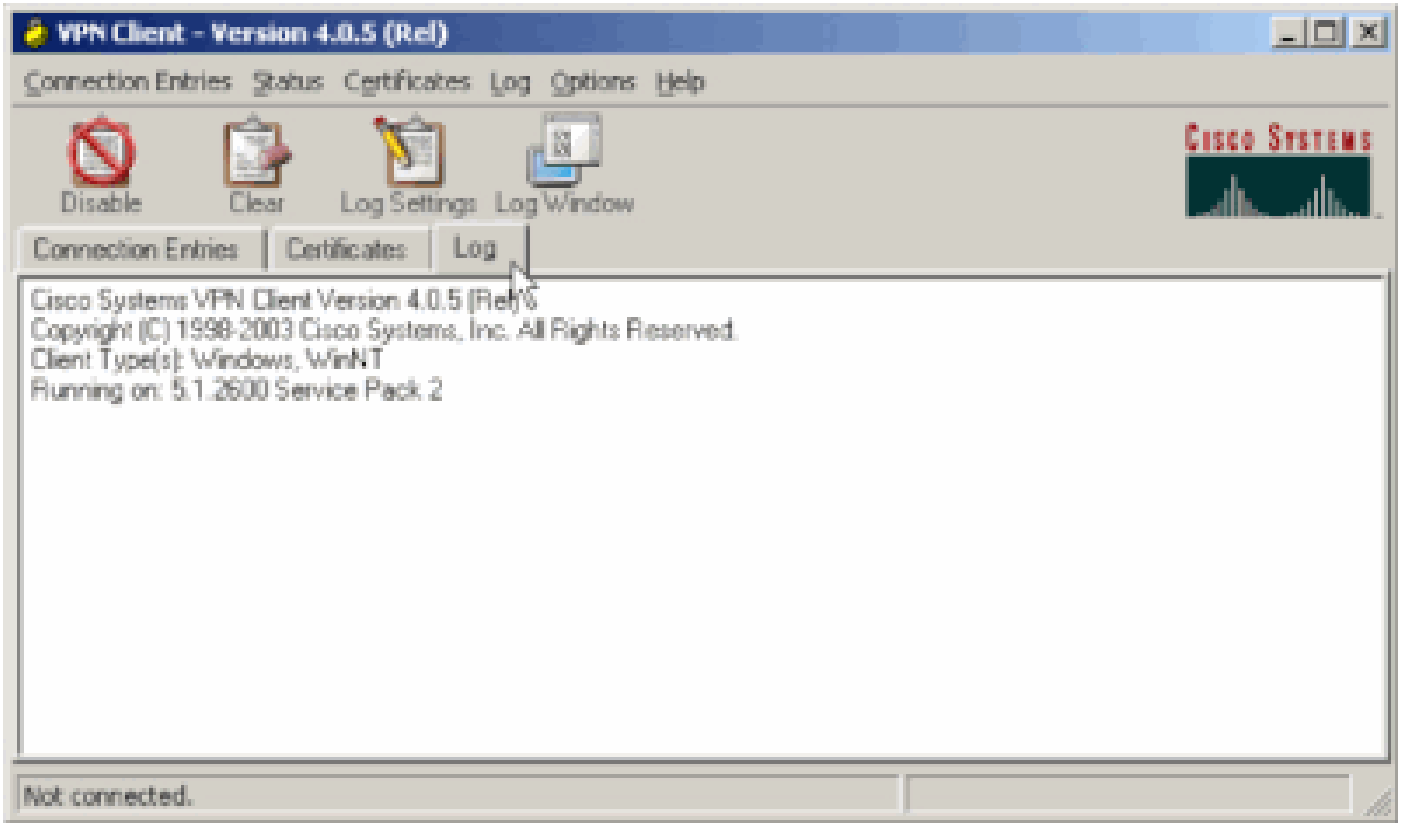
Route Details(경로 세부사항) 탭으로 이동하여 VPN Client가 ASA로 보호하는 경로를 확인합니다.

이 예에서 VPN 클라이언트는 10.0.1.0/24에 대한 액세스를 보호하는 반면 다른 모든 트래픽은 암호화되지 않으며 터널을 통해 전송되지 않습니다.



VPN 클라이언트 로그 보기

VPN 클라이언트 로그를 검토할 때 스플릿 터널링을 지정하는 매개변수를 설정할지 여부를 결정할 수 있습니다. 로그를 보려면 VPN 클라이언트의 Log(로그) 탭으로 이동합니다. 그런 다음 **Log Settings(로그 설정)**를 클릭하여 로깅된 항목을 조정합니다. 이 예에서는 IKE가 **3 - High**로 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      14:20:09.532  07/27/06  Sev=Info/6    IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.


!--- Output is supressed


18     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005D
Client sending a firewall request to concentrator

19     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005C
Firewall Policy: Product=Cisco Systems Integrated Client,
Capability= (Centralized Protection Policy).

20     14:20:14.188  07/27/06  Sev=Info/5    IKE/0x6300005C
Firewall Policy: Product=Cisco Intrusion Prevention Security Agent,
Capability= (Are you There?).

21     14:20:14.208  07/27/06  Sev=Info/4    IKE/0x63000013
SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 172.22.1.160

22     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300002F
Received ISAKMP packet: peer = 172.22.1.160

23     14:20:14.208  07/27/06  Sev=Info/4    IKE/0x63000014
RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 172.22.1.160

24     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x63000010
```

```
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 10.0.1.50

25     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x63000010
MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NETMASK: , value = 255.255.255.0

26     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000

27     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000

28     14:20:14.208  07/27/06  Sev=Info/5    IKE/0x6300000E
MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems,
Inc ASA5510 Version 7.2(1) built by root on Wed 31-May-06 14:45

!--- Split tunneling is permitted and the remote LAN is defined.

29     14:20:14.238  07/27/06  Sev=Info/5    IKE/0x6300000D
MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SPLIT_INCLUDE (# of split_nets),
value = 0x00000001

30     14:20:14.238  07/27/06  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

!--- Output is supressed.
```

Ping으로 로컬 LAN 액세스 테스트

ASA로 터널링되는 동안 VPN 클라이언트가 스플릿 터널링에 대해 구성되었는지 테스트하는 추가 방법은 Windows 명령줄에서 **ping** 명령을 사용하는 것입니다. VPN 클라이언트의 로컬 LAN은 192.168.0.0/24이며 IP 주소가 192.168.0.3인 다른 호스트가 네트워크에 있습니다.

```
  <#root>

C:\>

 ping 192.168.0.3

Pinging 192.168.0.3 with 32 bytes of data:
```

```
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255
Reply from 192.168.0.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

문제 해결

스플릿 터널 ACL의 항목 수 제한

스플릿 터널에 사용되는 ACL의 항목 수에 제한이 있습니다. 만족스러운 기능을 위해 50-60개 이상의 ACE 항목을 사용하지 않는 것이 좋습니다. IP 주소 범위를 포함하도록 서브넷 지정 기능을 구현하는 것이 좋습니다.

관련 정보

- **ASDM을 사용하는 원격 VPN 서버로서의 PIX/ASA 7.x 컨피그레이션 예**
- **Cisco ASA 5500 Series Adaptive Security Appliance**
- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.