

PIX/ASA 7.x: Allow Local LAN Access for Cisco VPN Client / SVC Configuration Example

Document ID: 70847

Introduction

Prerequisites

- Requirements
- Components Used
- Network Diagram
- Related Products
- Conventions

Background Information

Configure Local LAN Access for VPN Clients

- Configure the ASA via the ASDM
- Configure the ASA via CLI
- Configure the Cisco VPN Client
- Configure the SSL VPN Client (SVC) / AnyConnect VPN Client

Verify

- Connect with the VPN Client
- View the VPN Client Log
- Test Local LAN Access with Ping

Troubleshoot

- Unable to Print or Browse by Name

Related Information

Introduction

This document provides step-by-step instructions on how to allow Cisco VPN Client to **only** access their local LAN while tunneled into a Cisco ASA 5500 Series Security Appliance or PIX 500 Series Security Appliance. This configuration allows Cisco VPN Clients secure access to corporate resources via IPsec and still gives the client the ability to carry out activities like printing wherever the client is located. If it is permitted, traffic destined for the Internet is still tunneled to the ASA or PIX.

The ASA CLI and ASDM Configuration used in the document can also allow local LAN access for Cisco ANYConnect VPN Client (SVC) while tunneled into a Cisco ASA 5500 Series Security Appliance. This configuration allows SSL VPN Clients secure access to corporate resources through SSL and still gives the client the ability to carry out activities, such as printing, wherever the client is located. If it is permitted, traffic destined for the Internet is still tunneled to the ASA.

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology allows you to connect securely from any location to an internal corporate network, for more information refer to ASA 8.x VPN Access with the AnyConnect SSL VPN Client Configuration Example and .

PIX 500 Series Security Appliance does not support SSL/WEB VPN.

Note: This is not a configuration for split tunneling, where the client has unencrypted access to the Internet while connected to the ASA or PIX. Refer to PIX/ASA 7.x: Allow Split Tunneling for VPN Clients on the ASA Configuration Example for information on how to configure split tunneling on the ASA or PIX.

Prerequisites

Requirements

This document assumes that a working remote access VPN configuration already exists on the ASA or PIX. Refer to PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example for IPsec if one is not already configured.

This document assumes that a functional remote access VPN configuration already exists on the ASA. Refer to ASA 8.x VPN Access with the AnyConnect SSL VPN Client Configuration Example and for SSL if one is not already configured.

Components Used

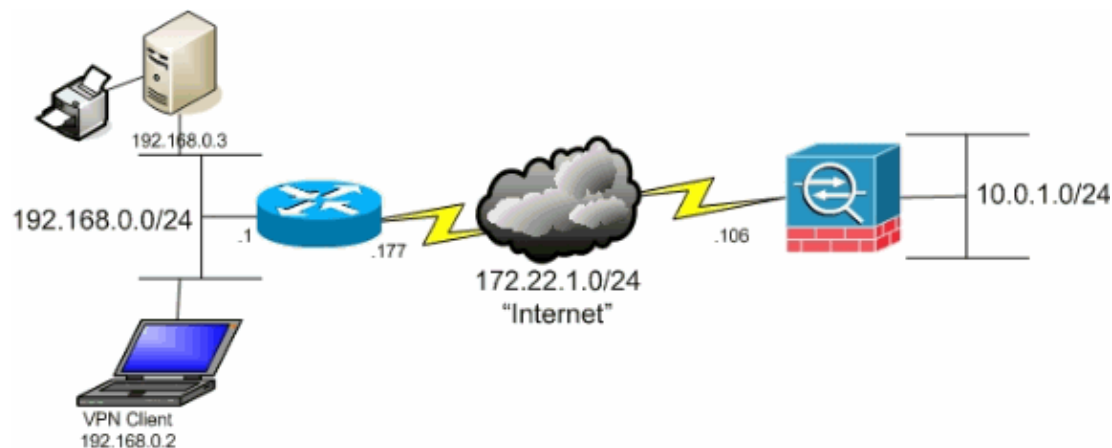
The information in this document is based on these software and hardware versions:

- Cisco ASA 5500 Series Security Appliance version 7.2
- Cisco VPN Client version 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.

Network Diagram

The VPN Client is located on a typical SOHO network and connects across the Internet to the main office.



Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance version 7.x.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Unlike a classic split tunneling scenario in which all Internet traffic is sent unencrypted, when you enable local LAN access for VPN Clients it permits those clients to communicate unencrypted with only devices on the network on which they are located. For example, a VPN Client that is allowed local LAN access while connected to the ASA from home is able to print to its own printer, but not access the Internet without first sending the traffic over the tunnel.

An access list is used in order to allow local LAN access in much the same way that split tunneling is configured on the ASA. However, instead of defining which networks *should be* encrypted, the access list in this case defines which networks *should not be* encrypted. Also, unlike the split tunneling scenario, the actual networks in the list do not need to be known. Instead, the ASA supplies a default network of 0.0.0.0/255.255.255.255 which is understood to mean the local LAN of the VPN Client.

Note: When the VPN Client is connected and configured for local LAN access, you *cannot print or browse by name* on the local LAN. However, you can browse or print by IP address. See the Troubleshooting section of this document for more information as well as workarounds for this situation.

Configure Local LAN Access for VPN Clients

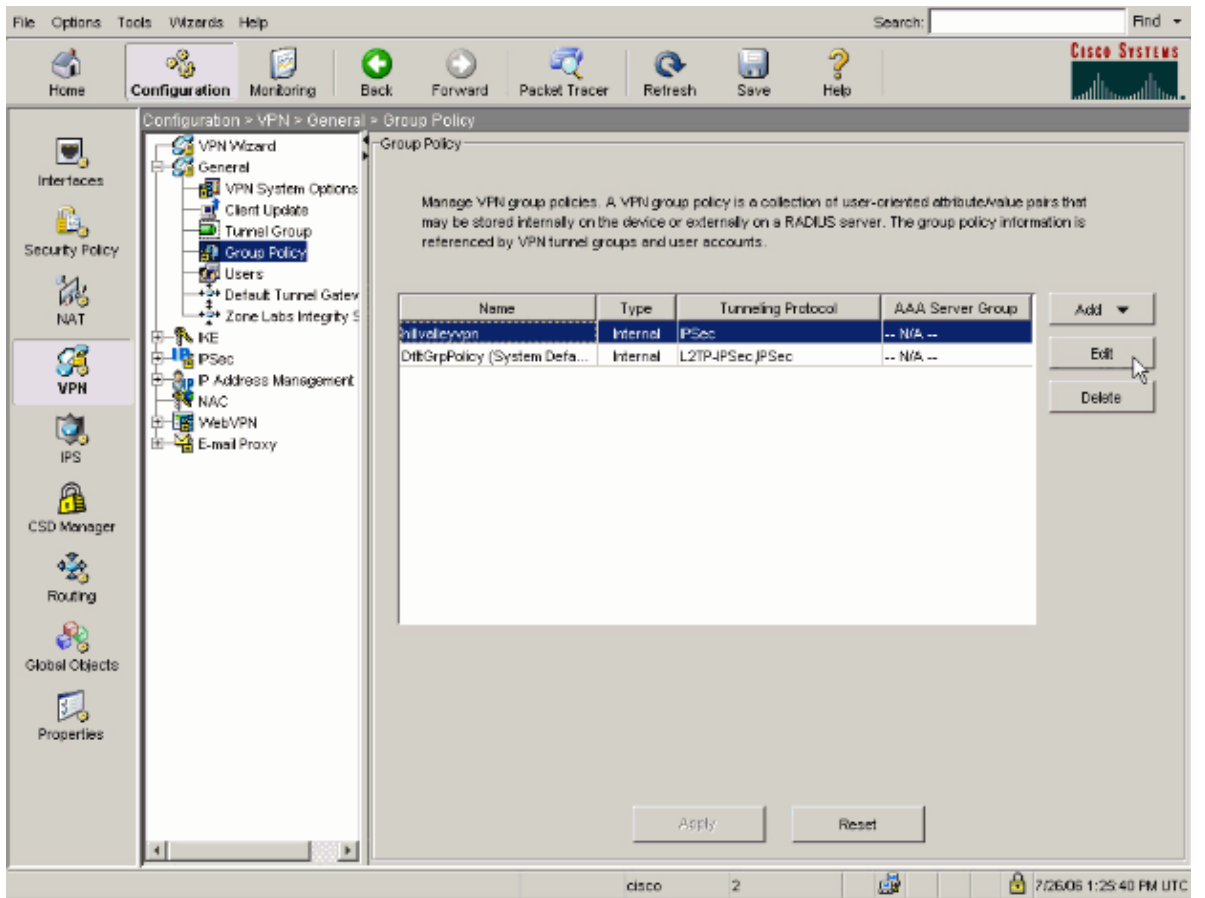
Complete these two tasks in order to allow VPN Clients access to their local LAN while connected to the VPN Concentrator:

- Configure the ASA via the Adaptive Security Device Manager (ASDM) or Configure the ASA via the CLI
- Configure the VPN Client

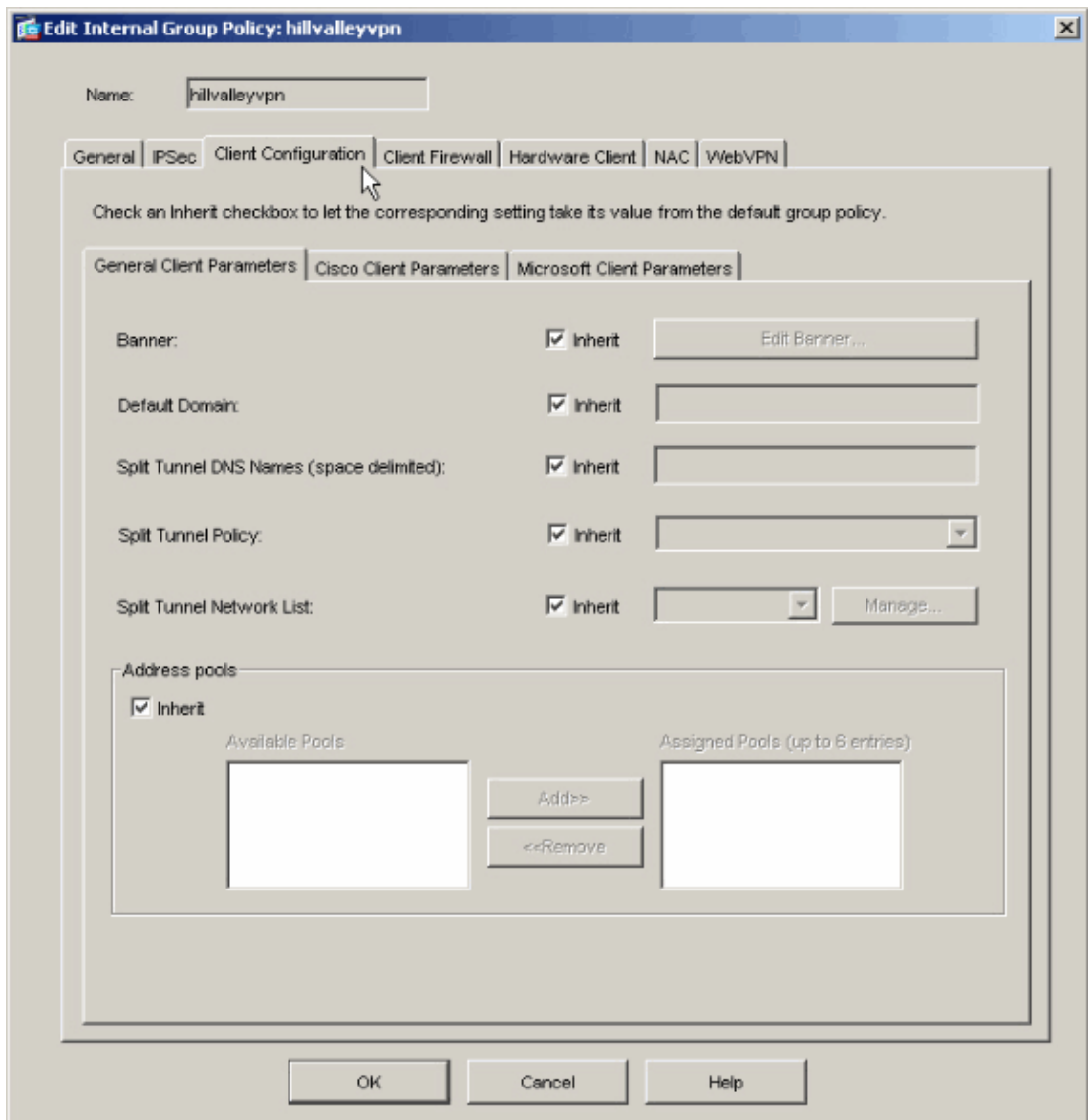
Configure the ASA via the ASDM

Complete these steps in the ASDM to allow VPN Clients to have local LAN access while connected to the ASA:

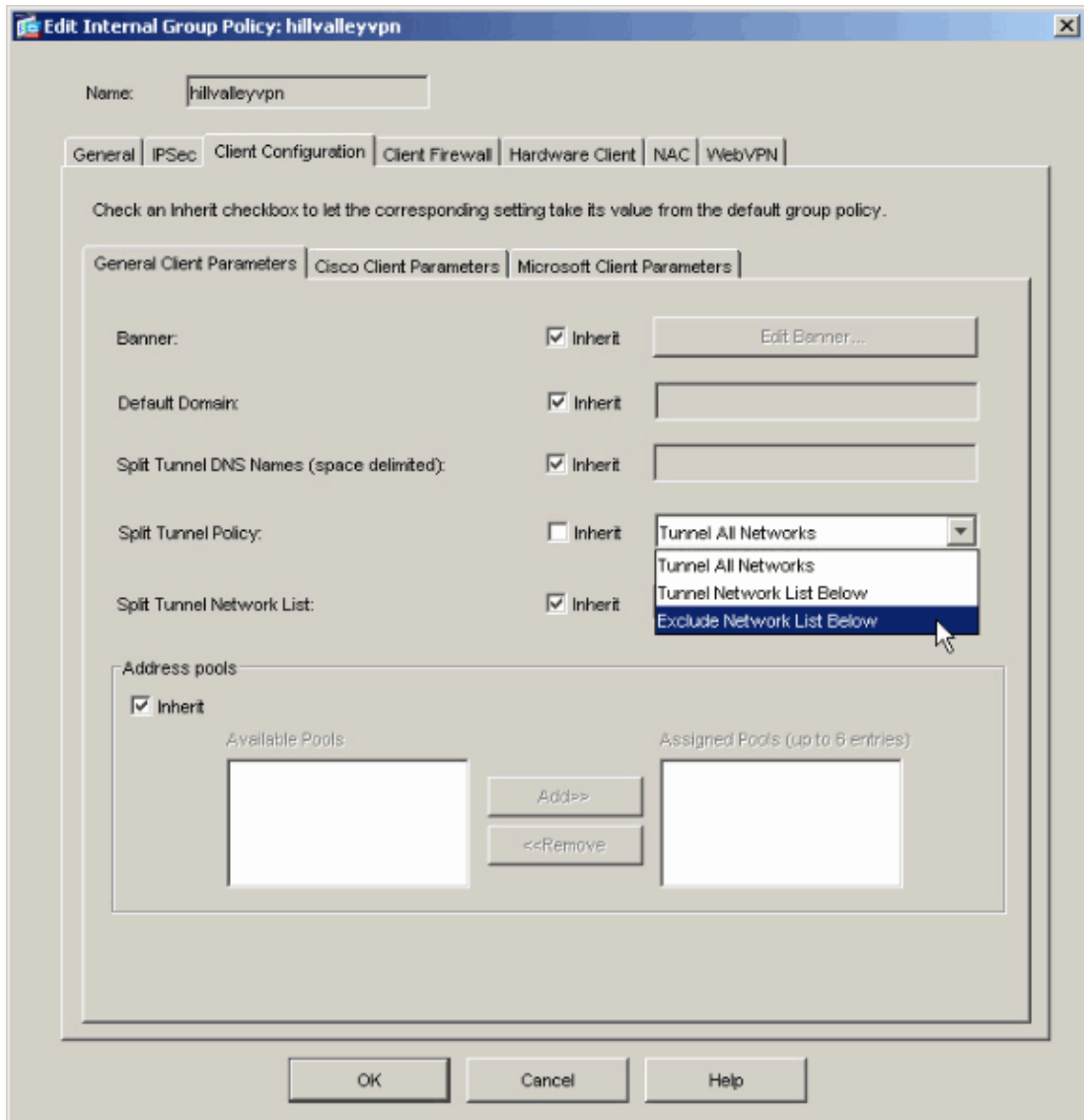
1. Choose **Configuration > VPN > General > Group Policy** and select the Group Policy that you wish to enable local LAN access in. Then click **Edit**.



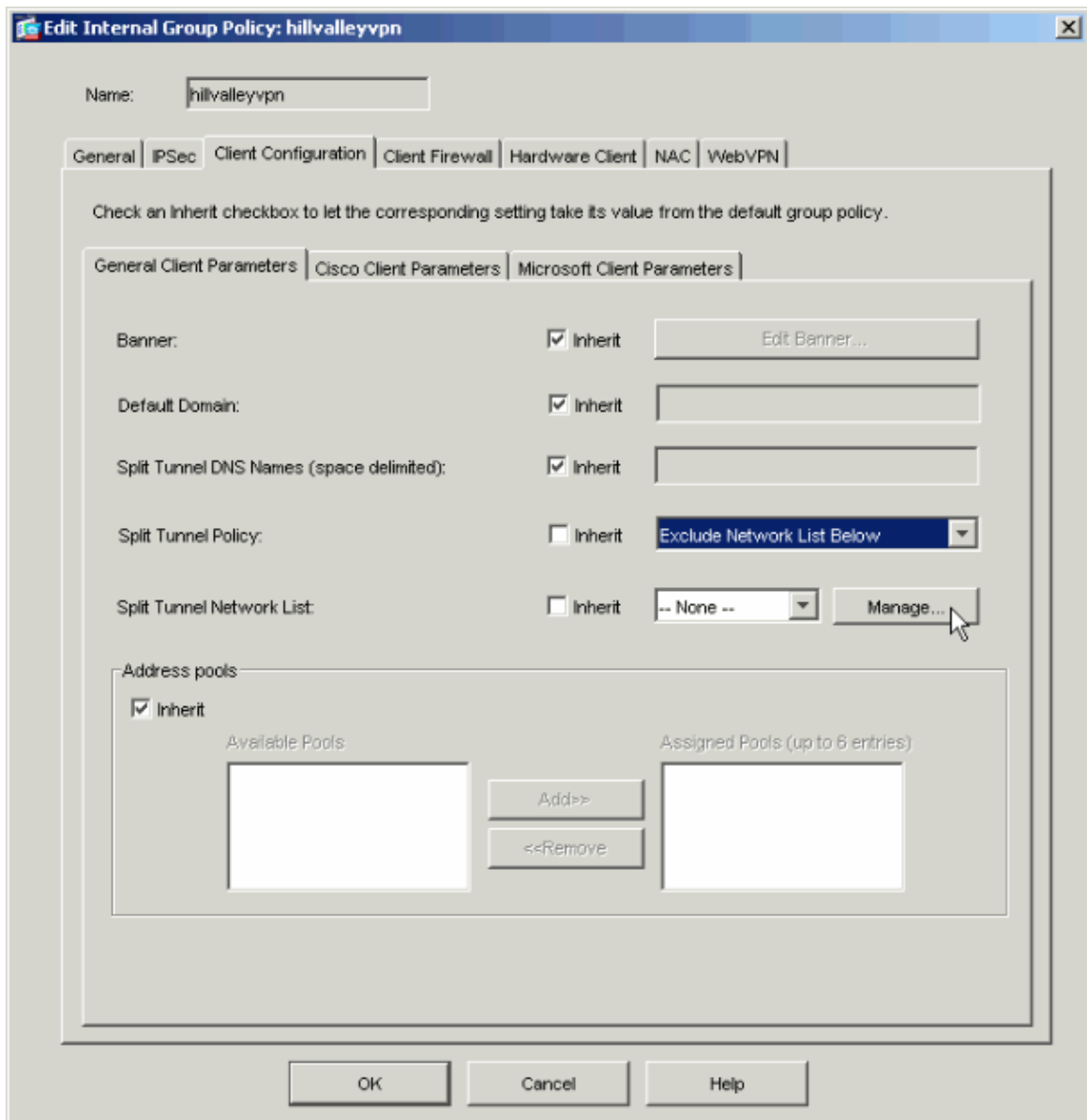
2. Choose the **Client Configuration** tab.



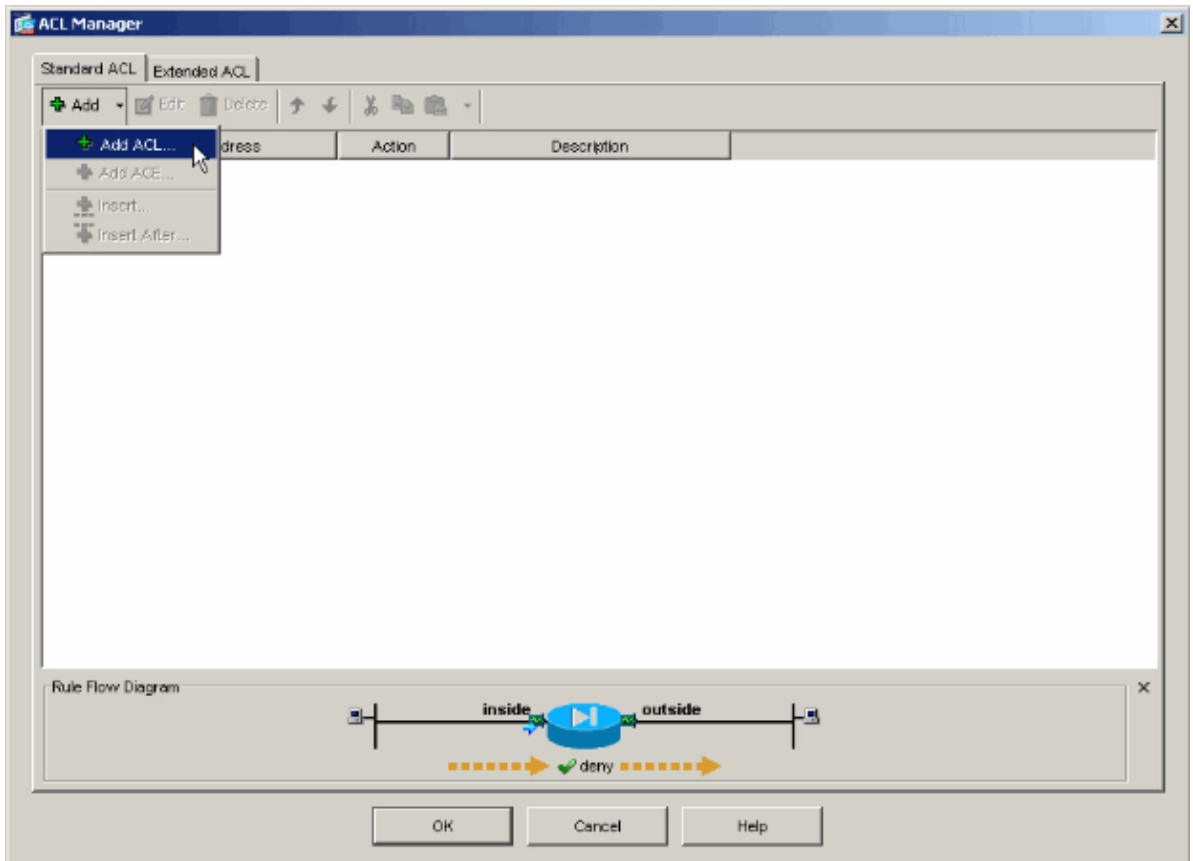
3. Uncheck the **Inherit** box for Split Tunnel Policy and chose **Exclude Network List Below**.



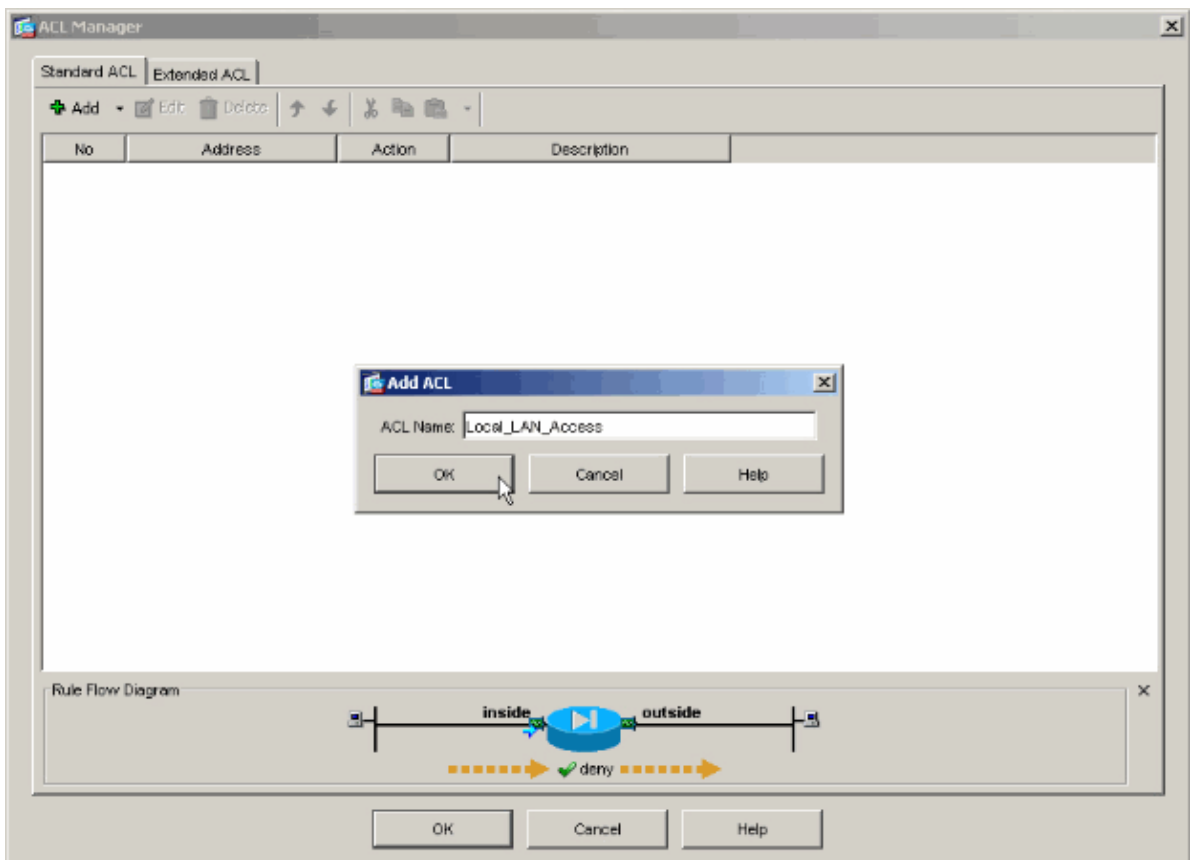
4. Uncheck the **Inherit** box for Split Tunnel Network List and then click **Manage** in order to launch the ACL Manager.



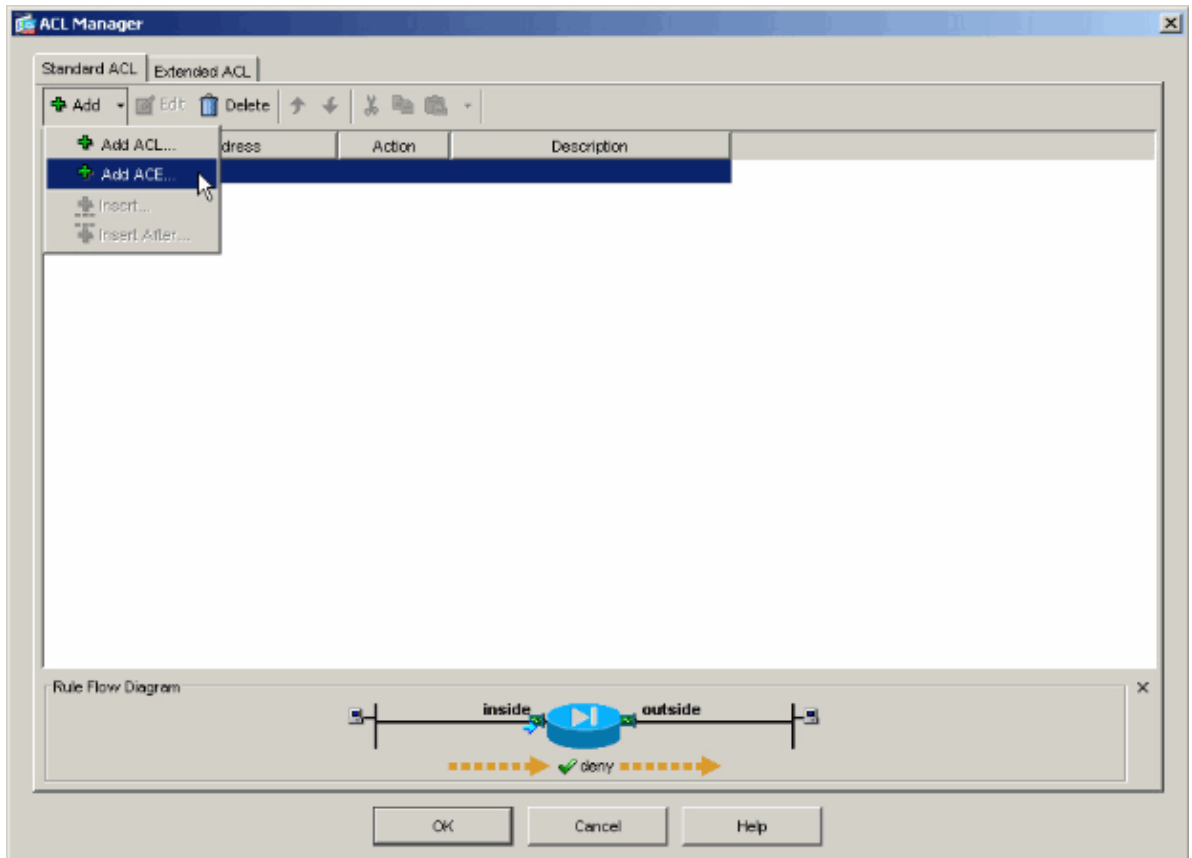
5. Within the ACL Manager choose **Add > Add ACL...** in order to create a new access list.



6. Provide a name for the ACL and click **OK**.

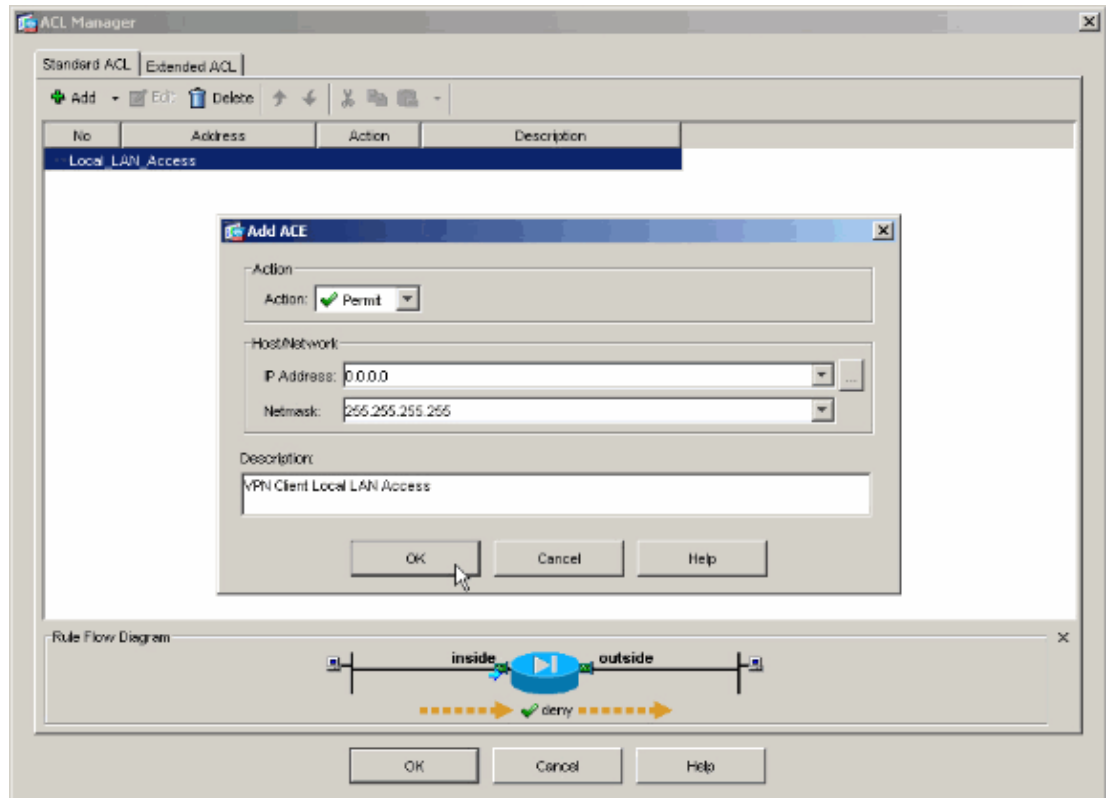


7. Once the ACL is created, choose **Add > Add ACE...** in order to add an Access Control Entry (ACE).

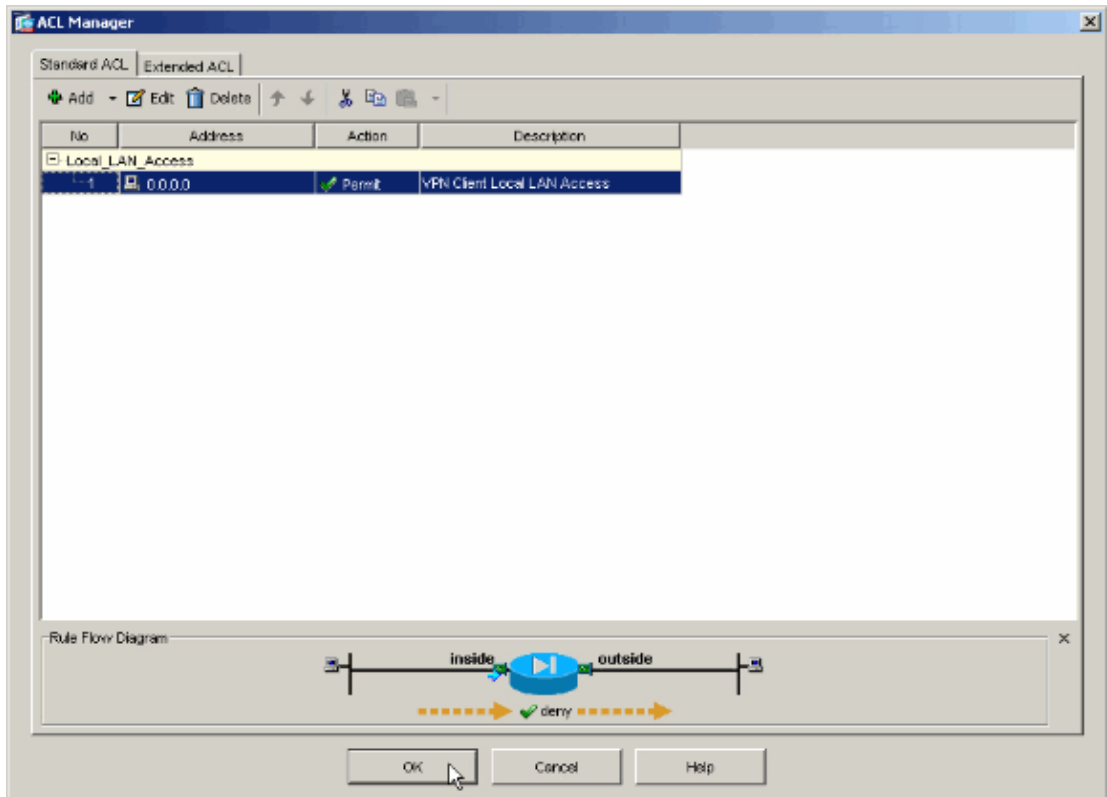


8. Define the ACE that corresponds to the local LAN of the client.

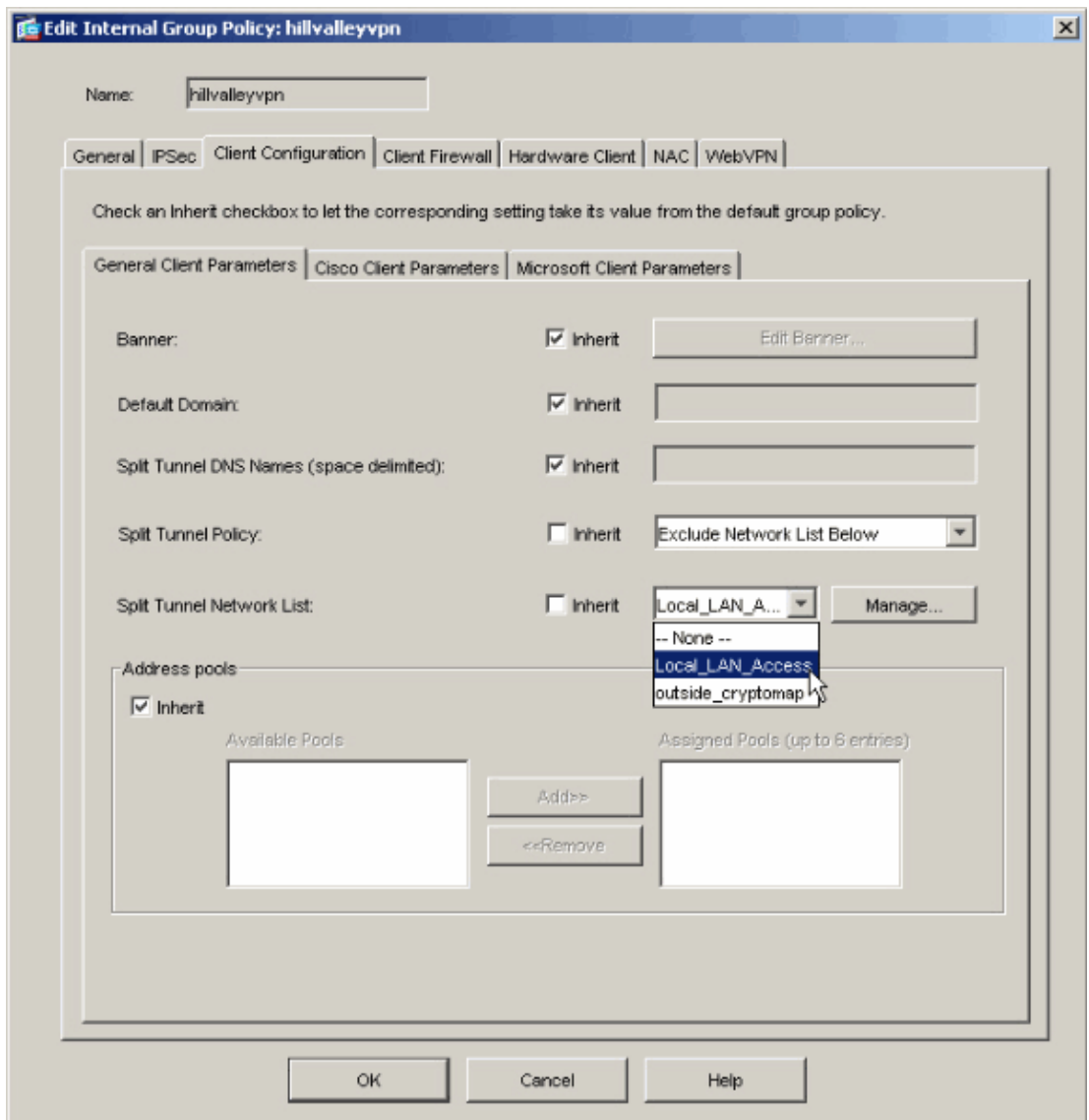
- a. Choose **Permit**.
- b. Choose an IP Address of **0.0.0.0**
- c. Choose a Netmask of **255.255.255.255**.
- d. (*Optional*) Provide a description.
- e. Click **OK**.



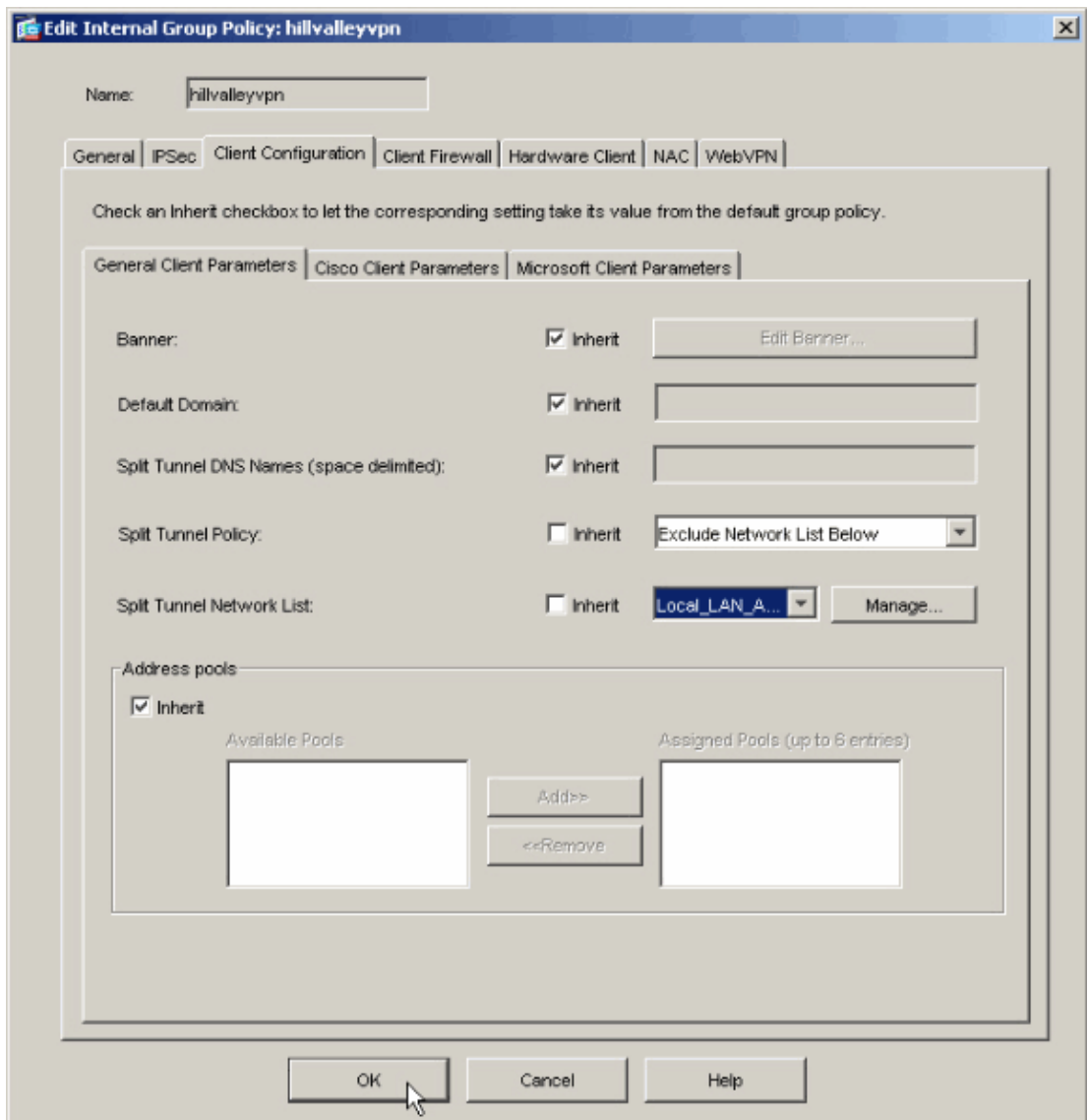
9. Click **OK** in order to exit the ACL Manager.



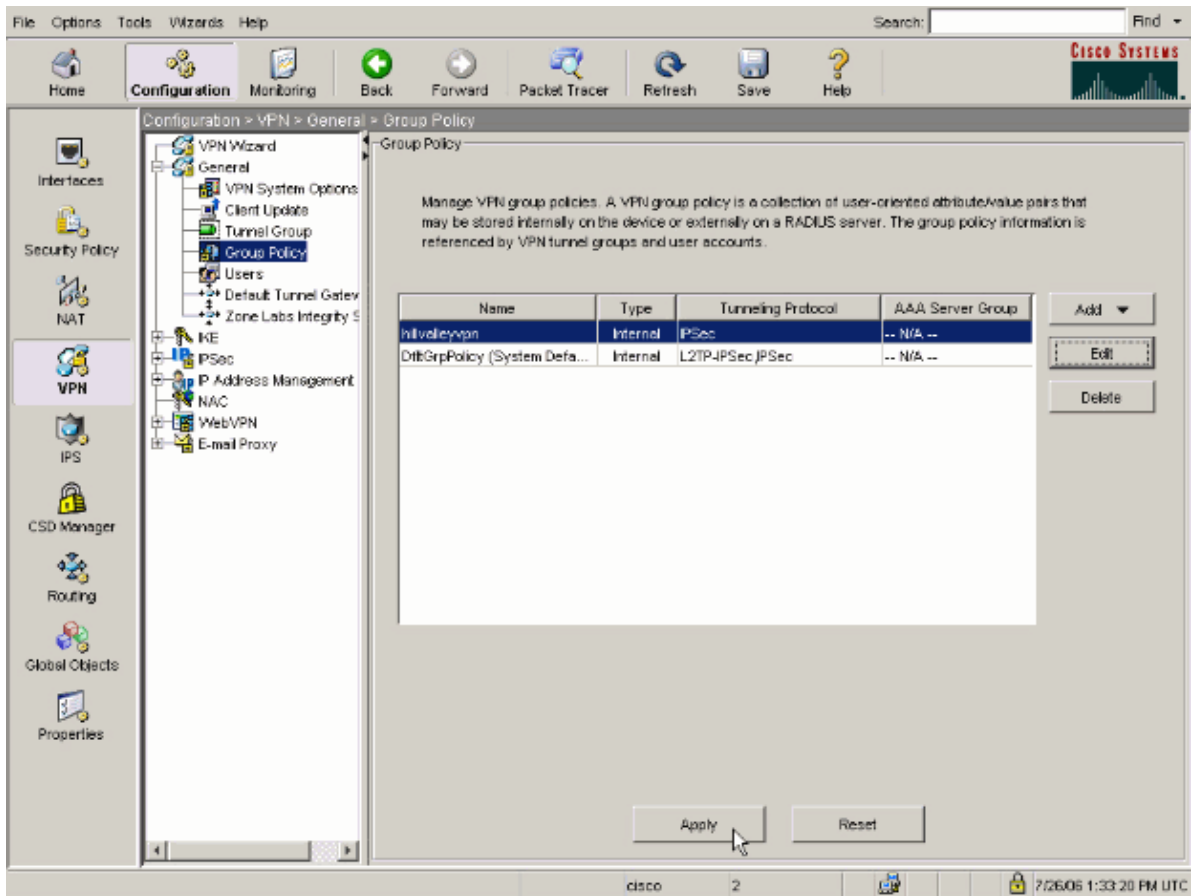
10. Be sure that the ACL you just created is selected for Split Tunnel Network List.



11. Click **OK** in order to return to the Group Policy configuration.



12. Click **Apply** and then **Send** (if required) in order to send the commands to the ASA.



Configure the ASA via CLI

Rather than use the ASDM, you can complete these steps in the ASA CLI in order to allow VPN Clients to have local LAN access while connected to the ASA:

1. Enter configuration mode.

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#
```

2. Create the access list to allow local LAN access.

```
ciscoasa(config)#access-list Local_LAN_Access remark VPN Client Local LAN Access
ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0
```

3. Enter Group Policy configuration mode for the policy that you wish to modify.

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

4. Specify the split tunnel policy. In this case the policy is **excludespecified**.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

5. Specify the split tunnel access list. In this case, the list is **Local_LAN_Access**.

```
ciscoasa(config-group-policy)#split-tunnel-network-list value Local_LAN_Access
```

6. Issue this command:

```
ciscoasa(config)#tunnel-group hillvalleyvpn general-attributes
```

7. Associate the group policy with the tunnel group

```
ciscoasa(config-tunnel-ipsec)# default-group-policy hillvalleyvpn
```

8. Exit the two configuration modes.

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

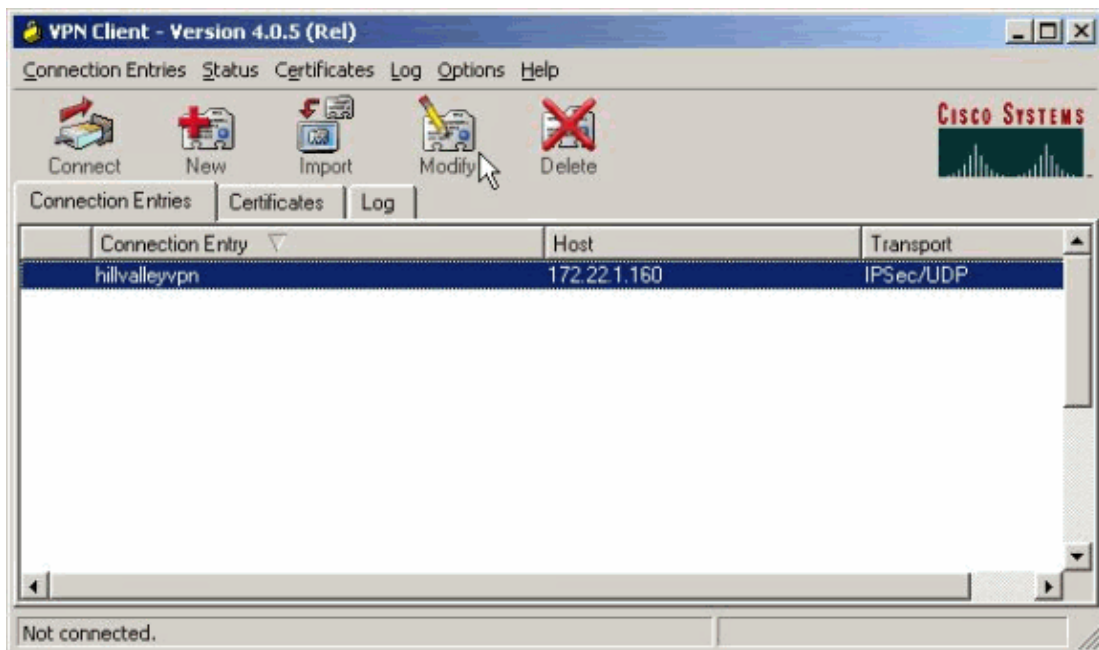
9. Save the configuration to non-volatile RAM (NVRAM) and press **Enter** when prompted to specify the source filename.

```
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#
```

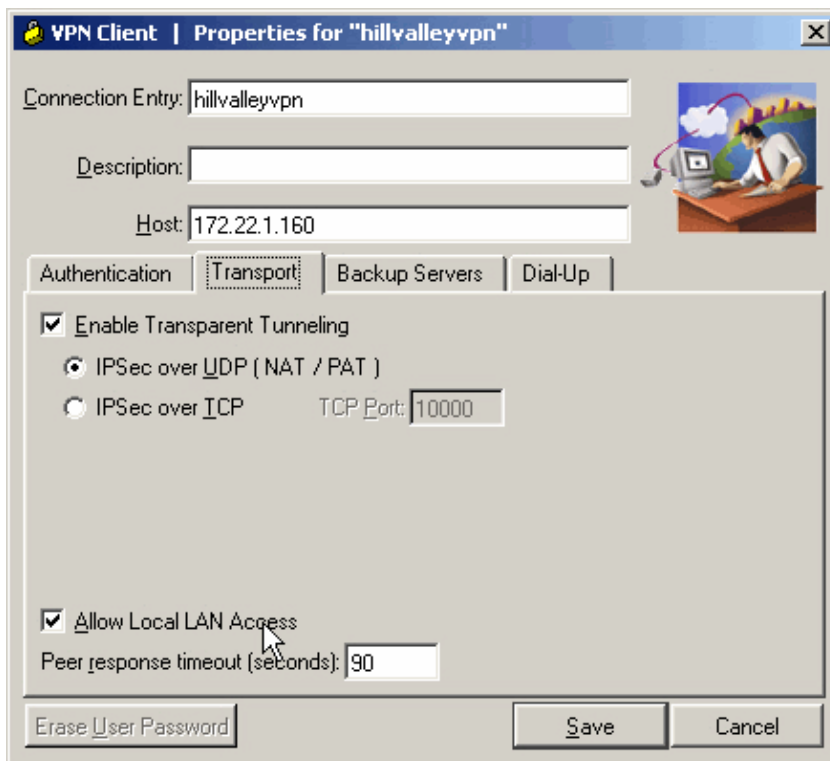
Configure the Cisco VPN Client

Complete these steps in the VPN Client in order to allow the client to have local LAN access while connected to the ASA.

1. Choose your existing connection entry and click **Modify**.



2. Go to the Transport tab and check **Allow Local LAN Access**. Click **Save** when you are done.



Configure the SSL VPN Client (SVC) / AnyConnect VPN Client

In order to configure the SSL VPN Client, refer to the Establish the SSL VPN Connection with SVC section of ASA 8.x : Allow Split Tunneling for AnyConnect VPN Client on the ASA Configuration Example.

Verify

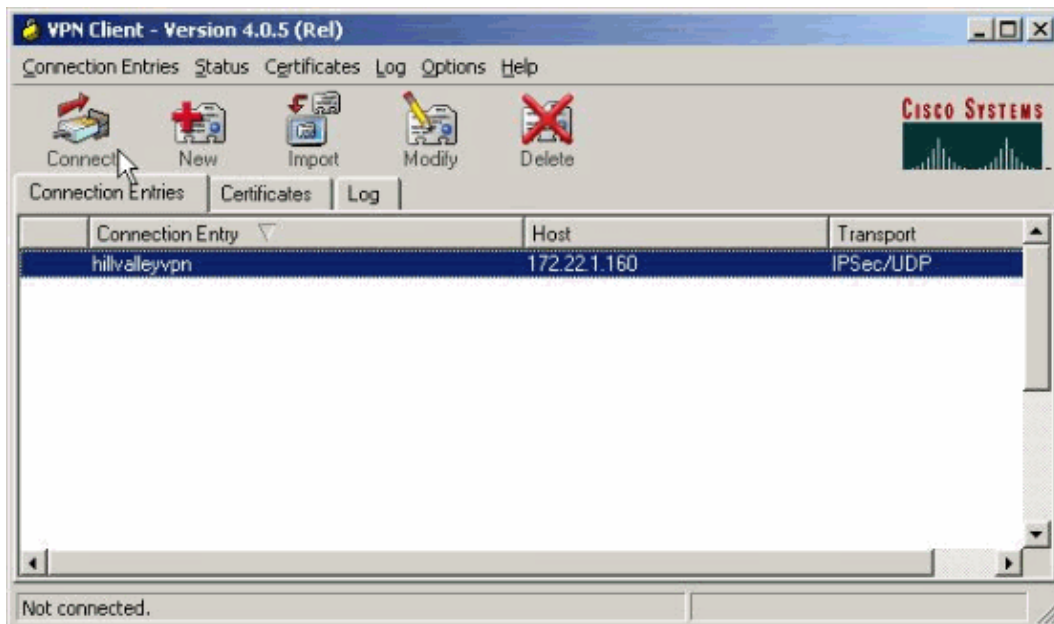
Follow the steps in these sections in order to verify your configuration.

- Connect with the VPN Client
- View the VPN Client Log
- Test Local LAN Access with Ping

Connect with the VPN Client

Connect your VPN Client to the VPN Concentrator in order to verify your configuration.

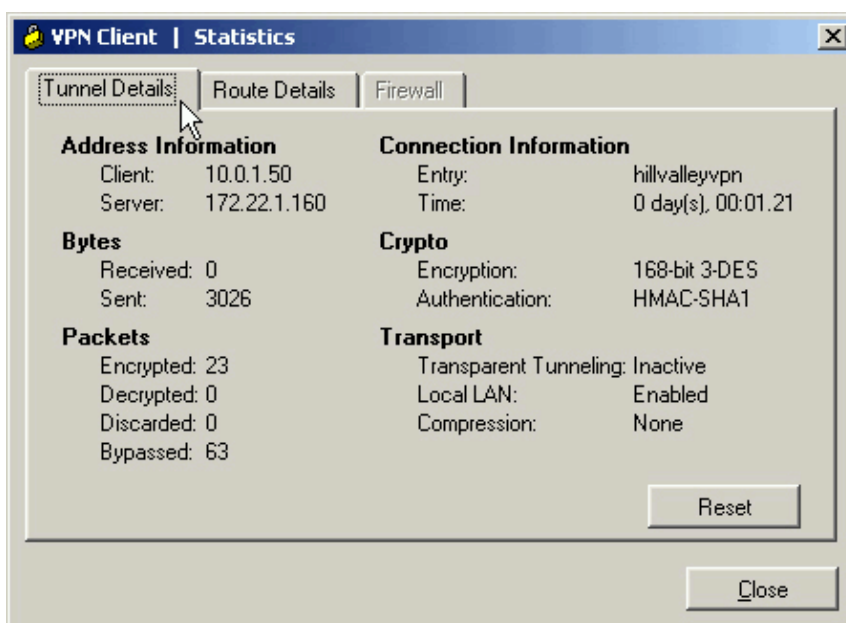
1. Choose your connection entry from the list and click **Connect**.



2. Enter your credentials.

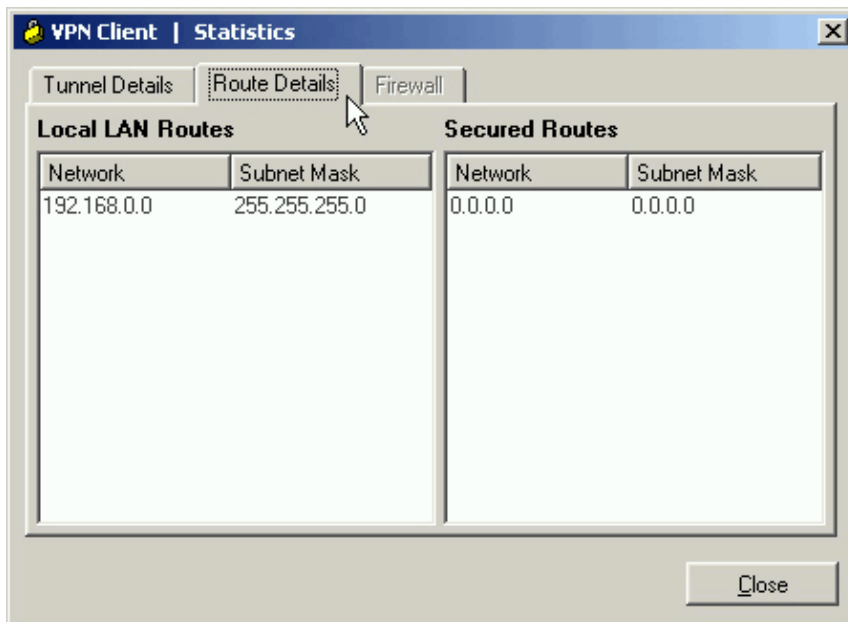


3. Choose **Status > Statistics...** in order to display the Tunnel Details window where you can inspect the particulars of the tunnel and see traffic flowing. You can also see that Local LAN is enabled in the Transport section.



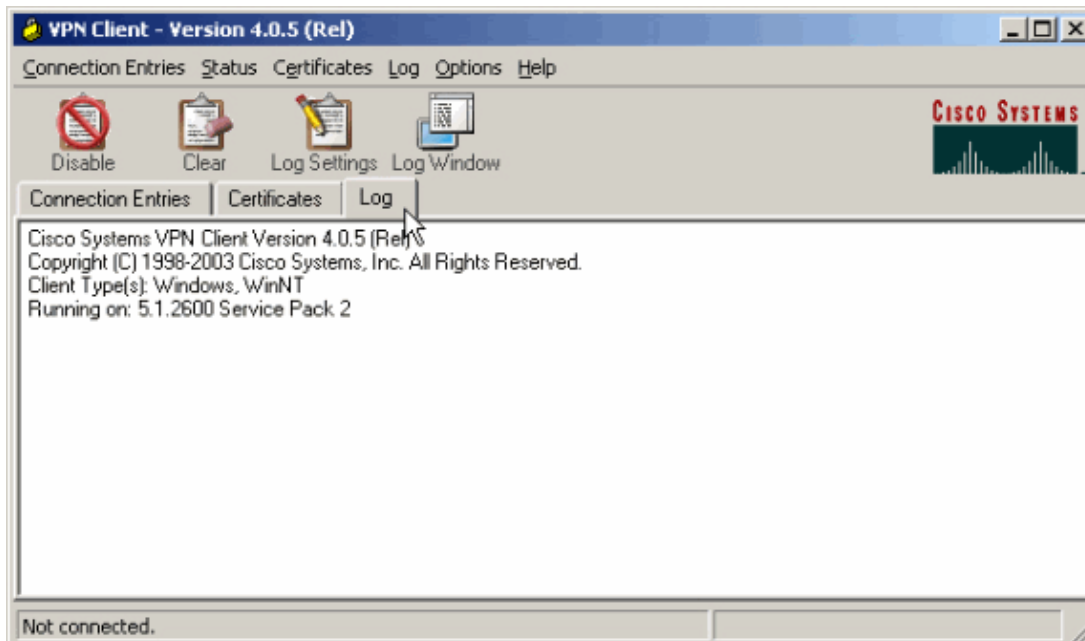
4. Go to the Route Details tab in order to see the routes to which the VPN Client still has local access.

In this example, the VPN Client is allowed local LAN access to 192.168.0.0/24 while all other traffic is encrypted and sent across the tunnel.



View the VPN Client Log

When you examine the VPN Client log, you can determine whether or not the parameter that allows local LAN access is set. In order to view the log, go to the Log tab in the VPN Client. Then click on **Log Settings** in order to adjust what is logged. In this example, IKE is set to **3– High** while all other log elements are set to **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      14:20:09.532 07/27/06 Sev=Info/6      IKE/0x6300003B
Attempting to establish a connection with 172.22.1.160.
```

!--- Output is suppressed

```

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

!--- Local LAN access is permitted and the local LAN is defined.

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

30      14:20:14.238  07/27/06  Sev=Info/5      IKE/0x6300000F
LOCAL_NET #1
      subnet = 192.168.0.0
      mask = 255.255.255.0
      protocol = 0
      src port = 0
      dest port=0

!--- Output is suppressed.

```

Test Local LAN Access with Ping

An additional way to test that the VPN Client still has local LAN access while tunneled to the VPN Concentrator is to use the **ping** command at the Windows command line. The local LAN of the VPN Client is 192.168.0.0/24 and another host is present on the network with an IP address of 192.168.0.3.

```

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
```

Troubleshoot

Unable to Print or Browse by Name

When the VPN Client is connected and configured for local LAN access, you *cannot print or browse by name* on the local LAN. There are two options available in order to work around this situation:

- Browse or print by IP address.
 - ◆ In order to browse, instead of using the syntax `\\sharename`, use the syntax `\\x.x.x.x` where `x.x.x.x` is the IP address of the host computer.
 - ◆ In order to print, change the properties for the network printer to use an IP address instead of a name. For example, instead of the syntax `\\sharename\printername`, use `\\x.x.x.x\printername`, where `x.x.x.x` is an IP address.
- Create or modify the VPN Client LMHOSTS file. An LMHOSTS file on a Windows PC allows you to create static mappings between hostnames and IP addresses. For example, an LMHOSTS file might look like this:

```
192.168.0.3 SERVER1
192.168.0.4 SERVER2
192.168.0.5 SERVER3
```

In Windows XP Professional Edition, the LMHOSTS file is located in `%SystemRoot%\System32\Drivers\Etc`. Refer to your Microsoft documentation or Microsoft KB Article 314108 for more information.

Related Information

- [PIX/ASA 7.x as a Remote VPN Server using ASDM Configuration Example](#)
- [SSL VPN Client \(SVC\) on IOS with SDM Configuration Example](#)
- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 25, 2008

Document ID: 70847
