Configure AnyConnect Client Access to Local LAN

Contents

Introduction

This document describes how to allow the Cisco AnyConnect Secure Mobility Client to access the local LAN while connected to a Cisco ASA.

Prerequisites

Requirements

This document assumes that a functional remote access VPN configuration already exists on the Cisco Adaptive Security Appliance (ASA).

Refer to CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17 for configuration assistance if needed.

Components Used

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

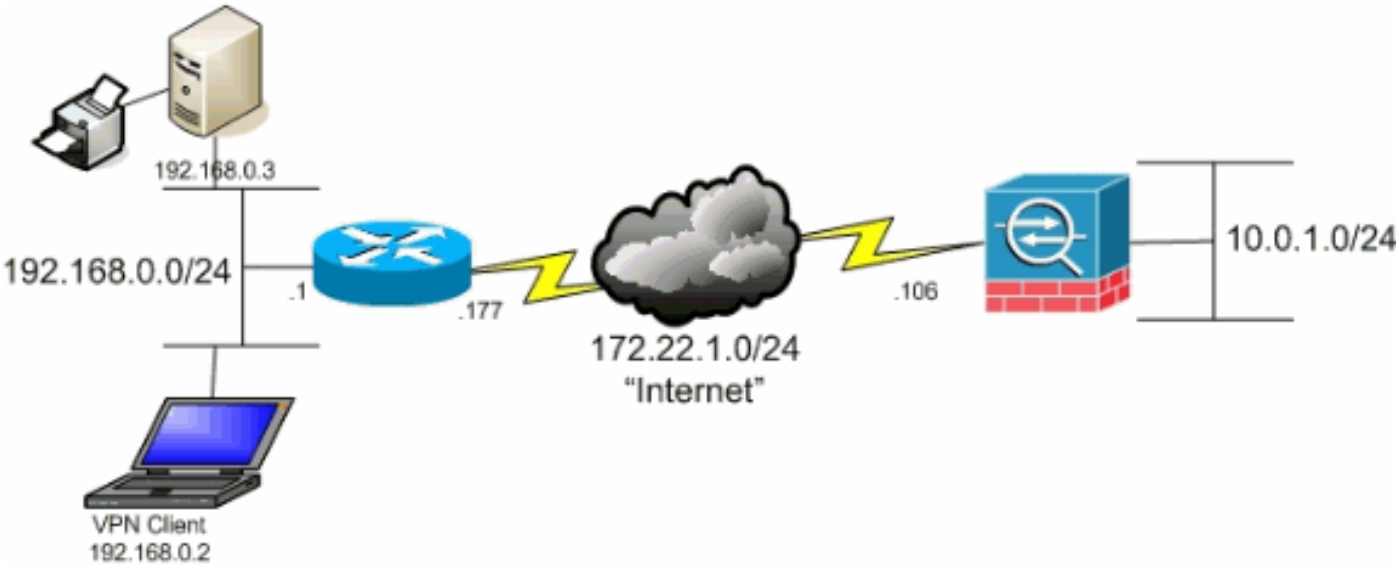
- Cisco ASA 5500 Series Version 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) Version 7.1(6)

- Cisco AnyConnect Secure Mobility Client Version 3.1.05152

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, ensure that you understand the potential impact of any command.

Network Diagram

The client is located on a typical Small Office / Home Office (SOHO) network and connects across the Internet to the main office.

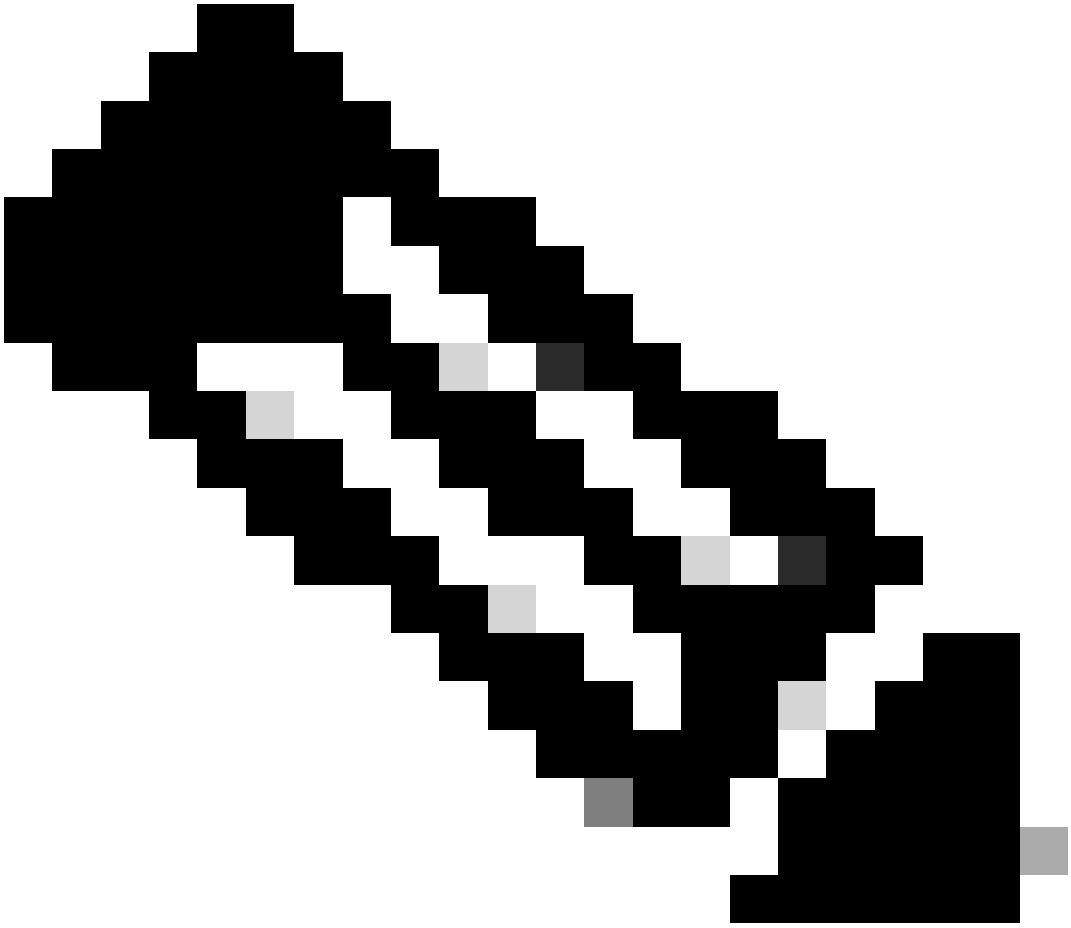


Background Information

This configuration allows the Cisco AnyConnect Secure Mobility Client secure access to corporate resources via IPsec, Secure Sockets Layer (SSL), or Internet Key Exchange Version 2 (IKEv2) and still gives the client the ability to carry out activities such as printing where the client is located. If it is permitted, traffic destined for the Internet is still tunneled to the ASA.

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 client that is allowed local LAN access while connected to the ASA from home can print to its own printer but cannot access the Internet unless it first sends 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, unlike the split tunneling scenario, this access list does not define which networks must *be* encrypted. Instead, it defines which networks must 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 client.



Note: This is not a configuration for split tunneling where the client has unencrypted access to the Internet while connected to the ASA. Refer to Set the Split-Tunneling Policy in *CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17* for information on how to configure split tunneling on the ASA.

Note: When the 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 Troubleshoot section of this document for more information as well as workarounds for this situation.

Configure Local LAN Access for the AnyConnect Secure Mobility Client

Complete these tasks in order to allow Cisco AnyConnect Secure Mobility Clients access to their local LAN while connected to the ASA:

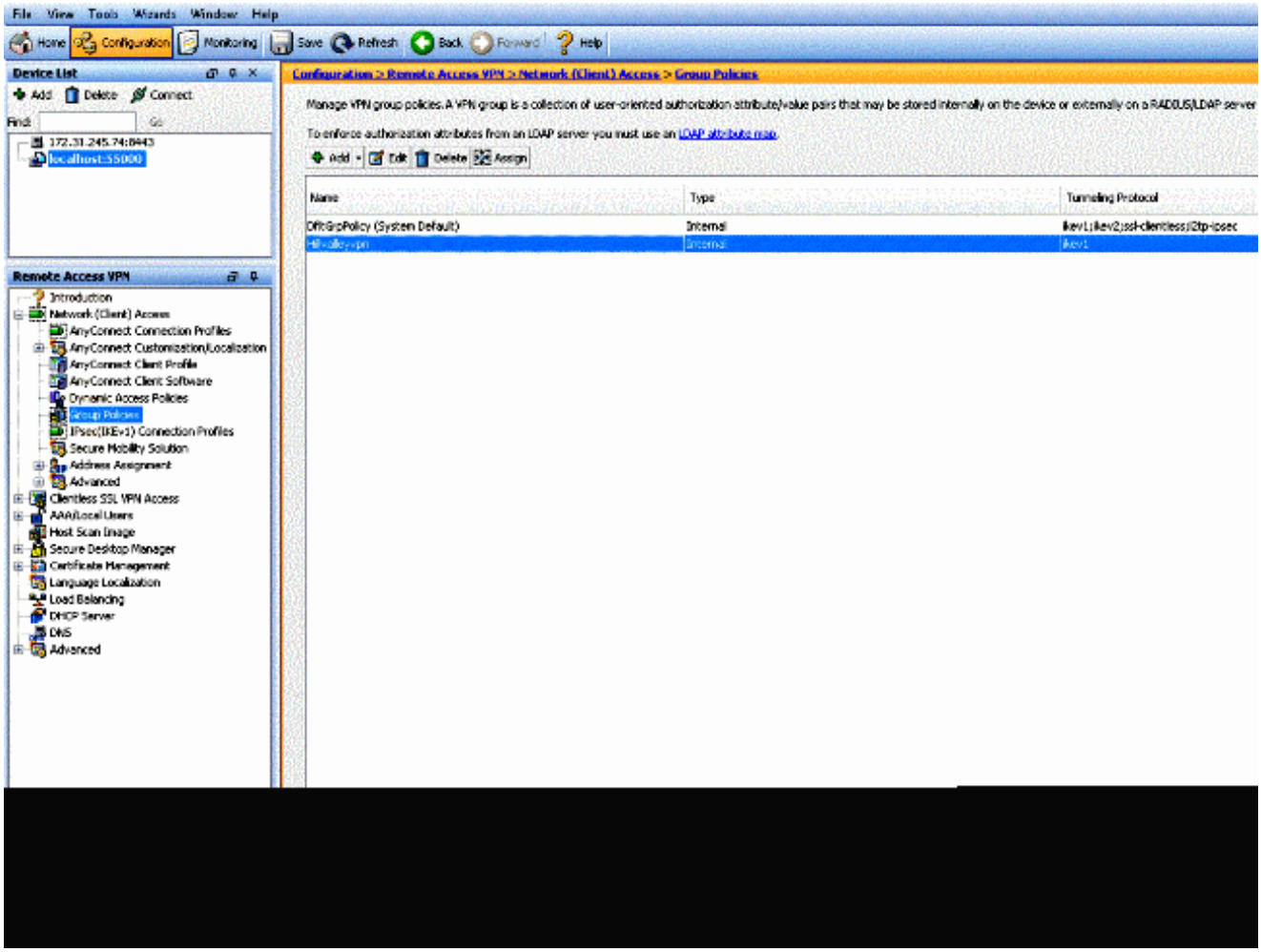
- Configure the ASA via the ASDM or Configure the ASA via the CLI

- Configure the Cisco AnyConnect Secure Mobility Client

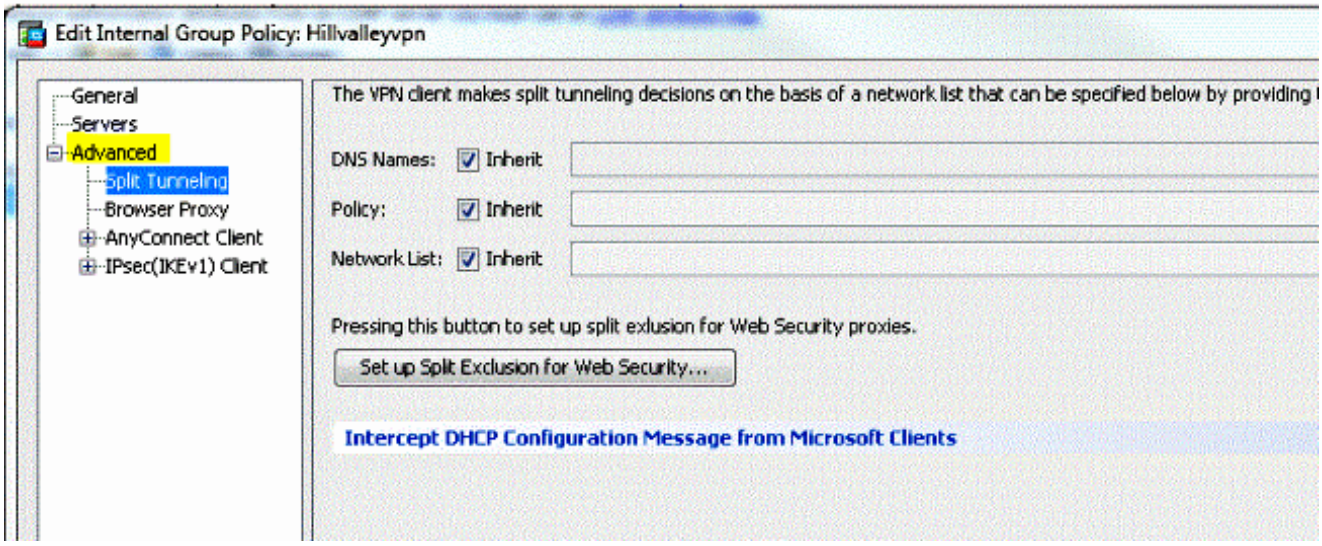
Configure the ASA via the ASDM

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

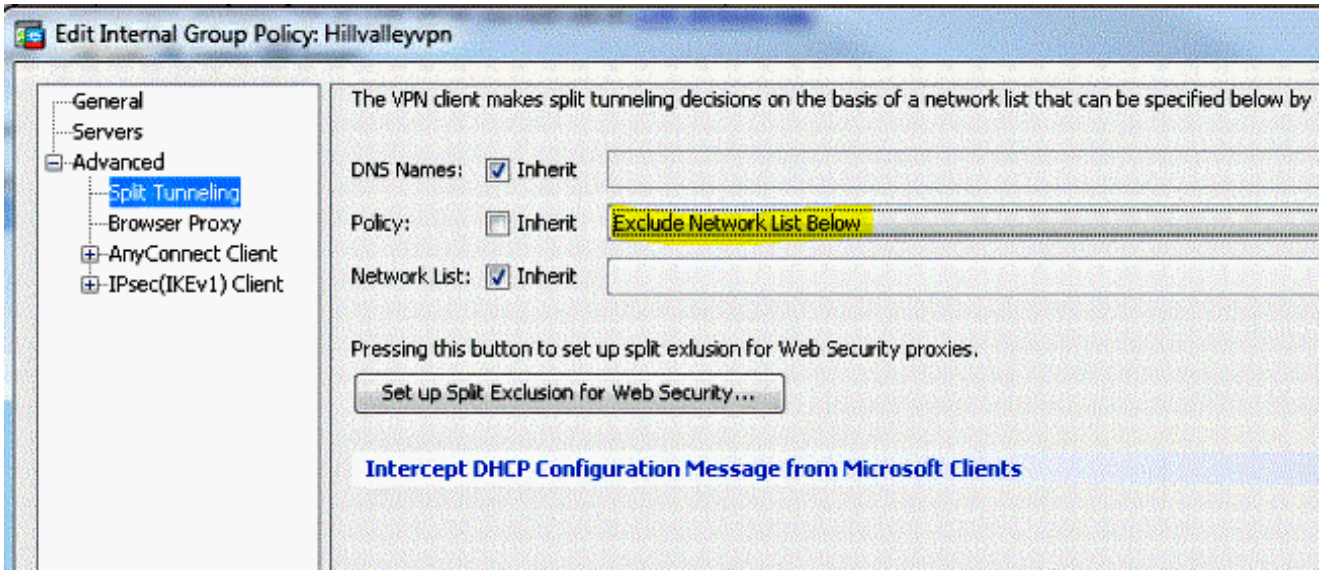
1. Choose **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** and select the Group Policy in which you wish to enable local LAN access. Then click **Edit.**



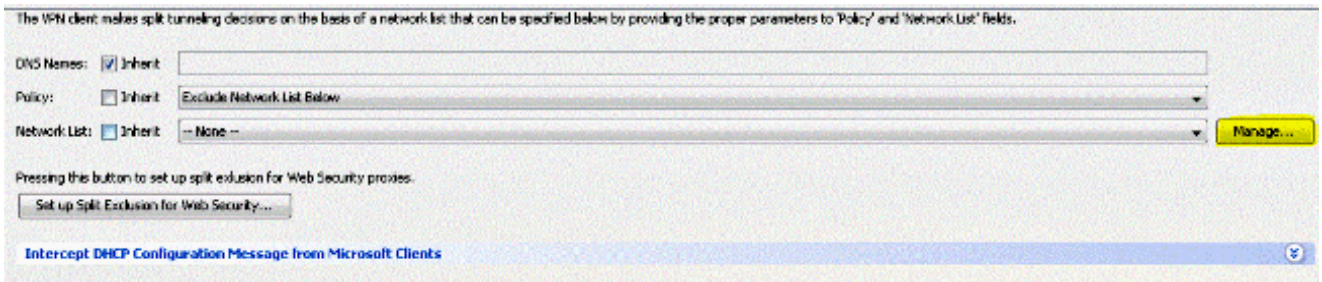
2. Go to **Advanced > Split Tunneling.**



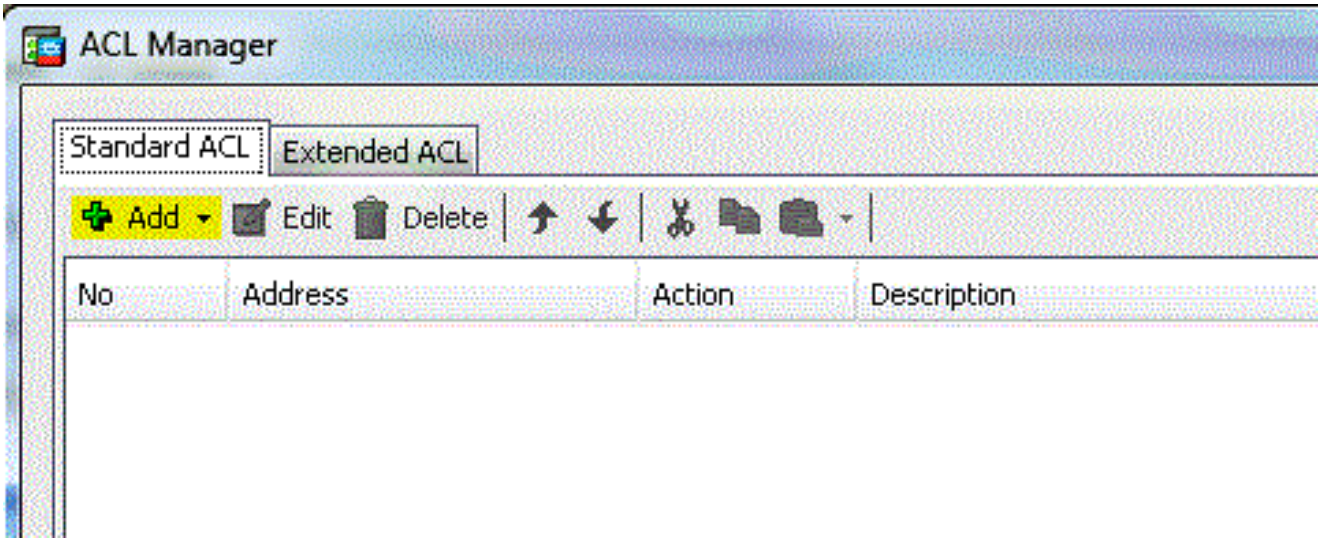
3. Uncheck the **Inherit** box for Policy and choose **Exclude Network List Below.**



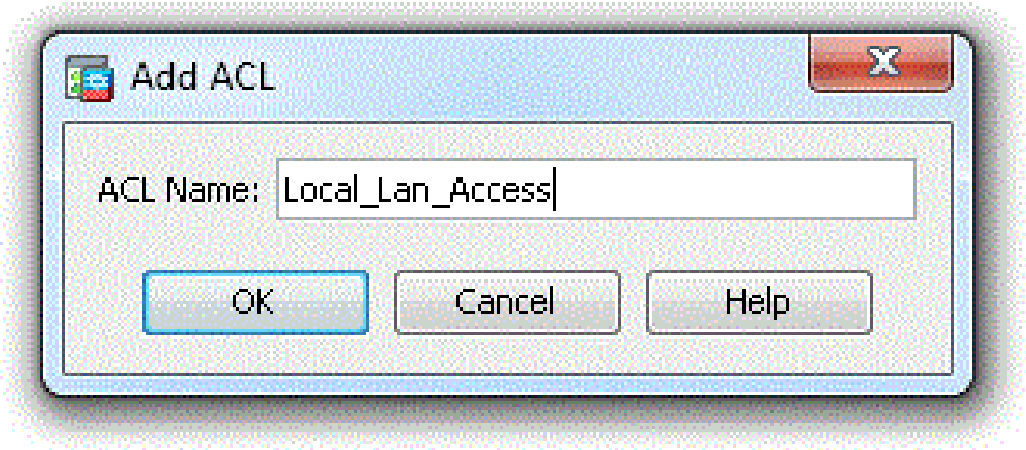
4. Uncheck the **Inherit** box for Network List and then click **Manage** in order to launch the Access Control List (ACL) Manager.



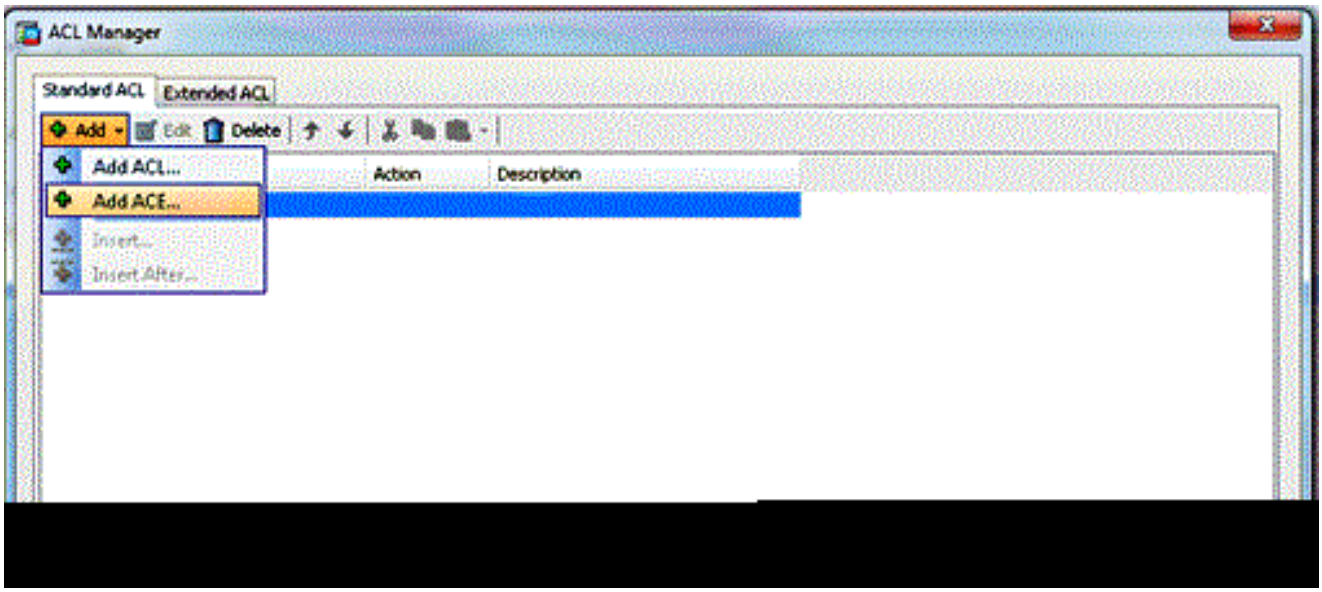
5. Within the ACL Manager, choose **Add** > **Add ACL...** in order to create a new access list.



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

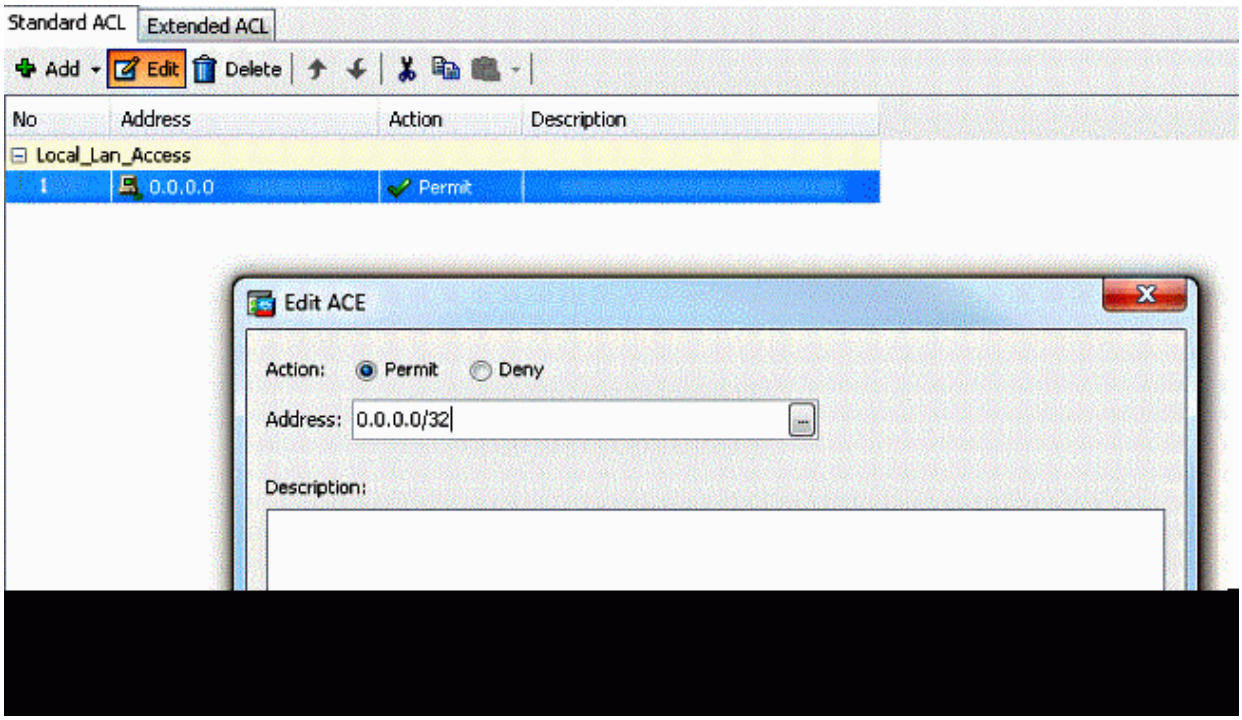


7. Once the ACL is created, choose **Add** > **Add ACE...** in order to add an Access Control Entry (ACE).

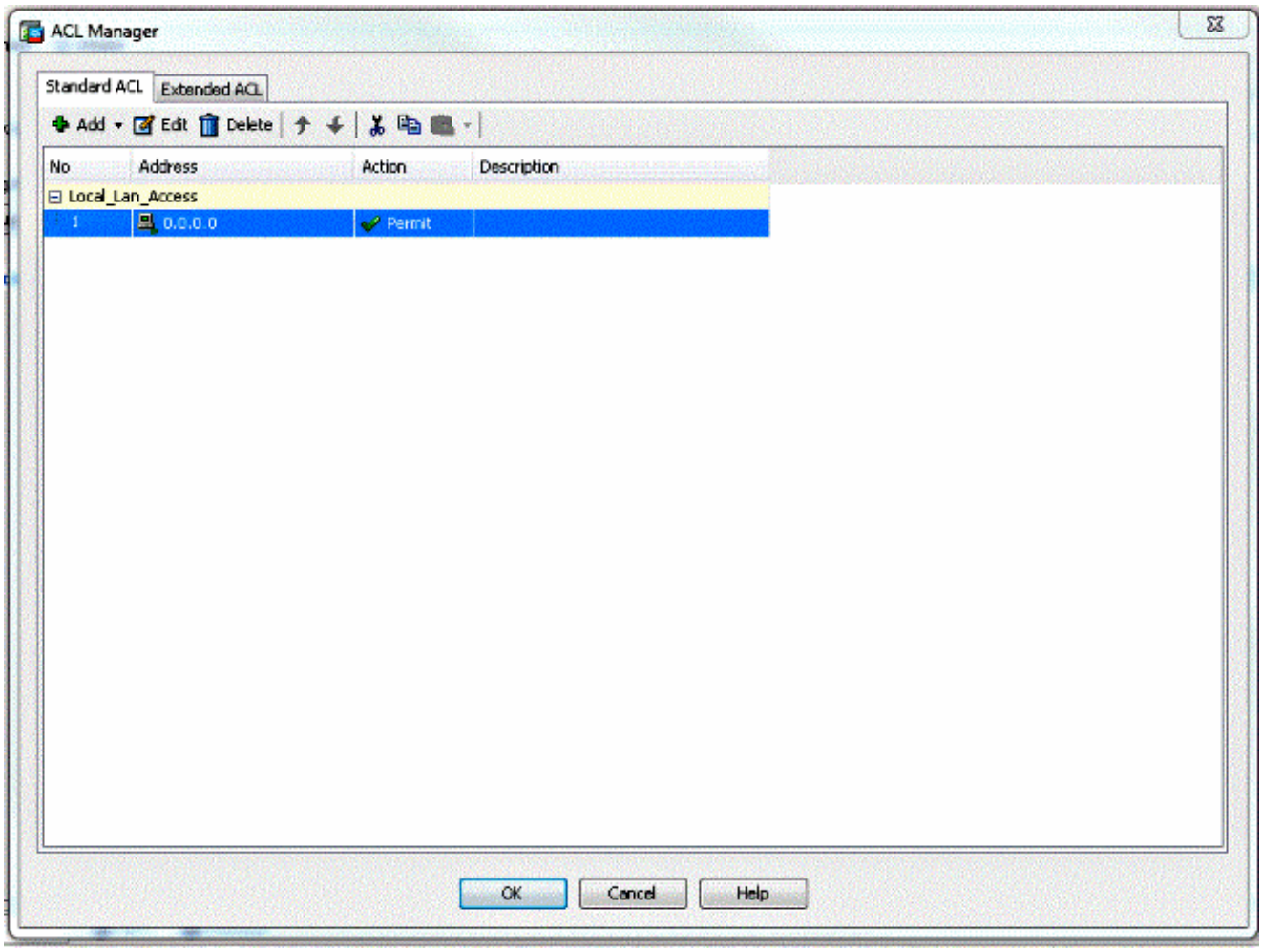


8. Define the ACE that corresponds to the local LAN of the client.

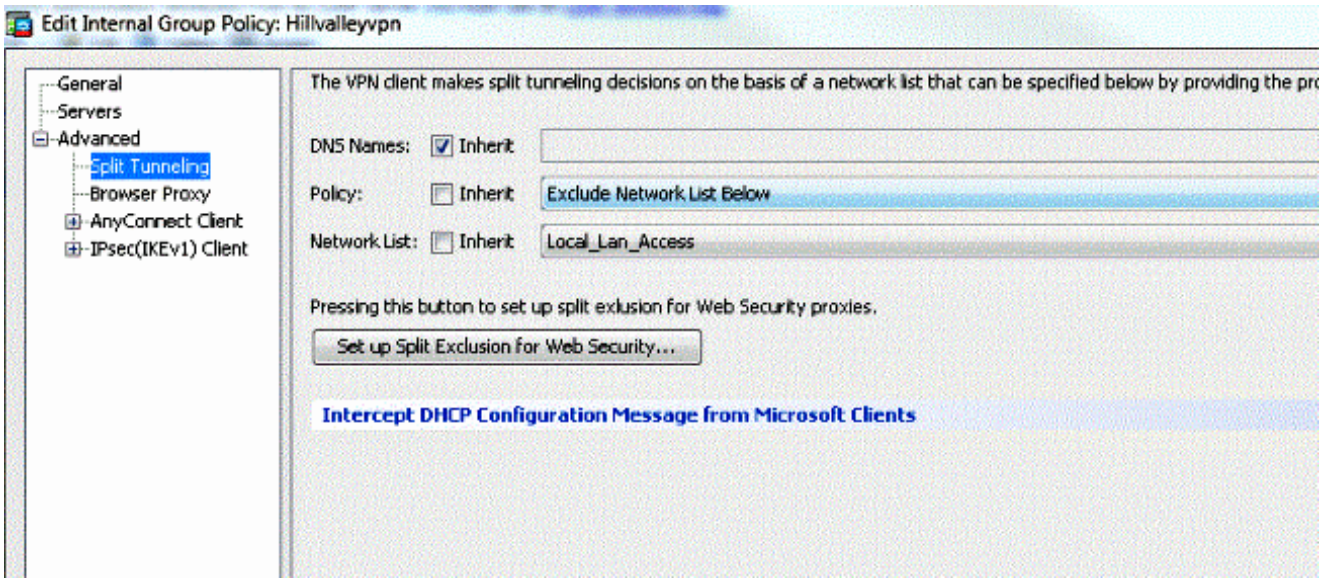
   a. Choose **Permit.**
   b. Choose an IP Address of **0.0.0.0**
   c. Choose a Netmask of **/32**.
   d. *(Optional)* Provide a description.
   e. Click **OK**.



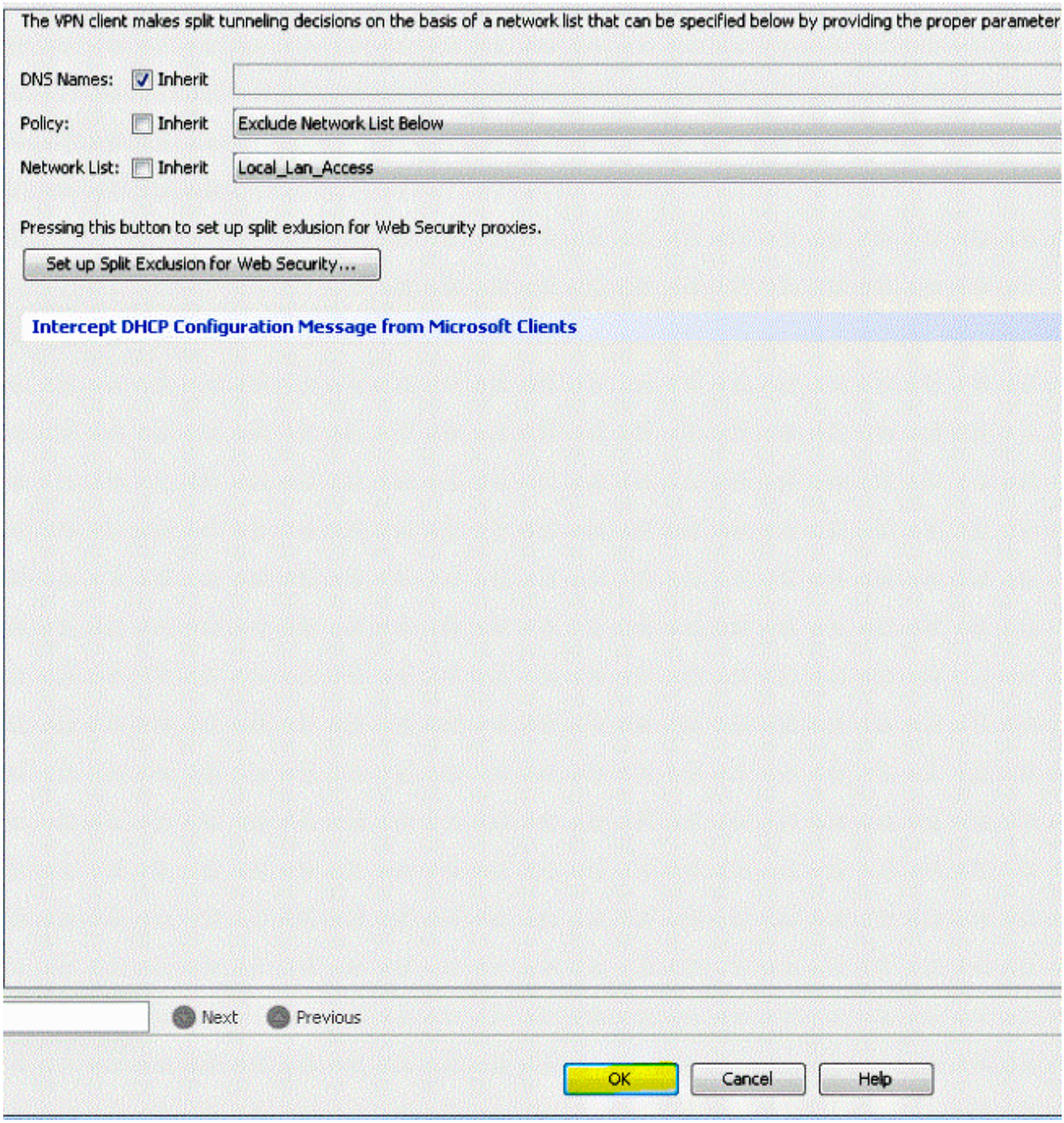
9. Click **OK** in order to exit the ACL Manager.



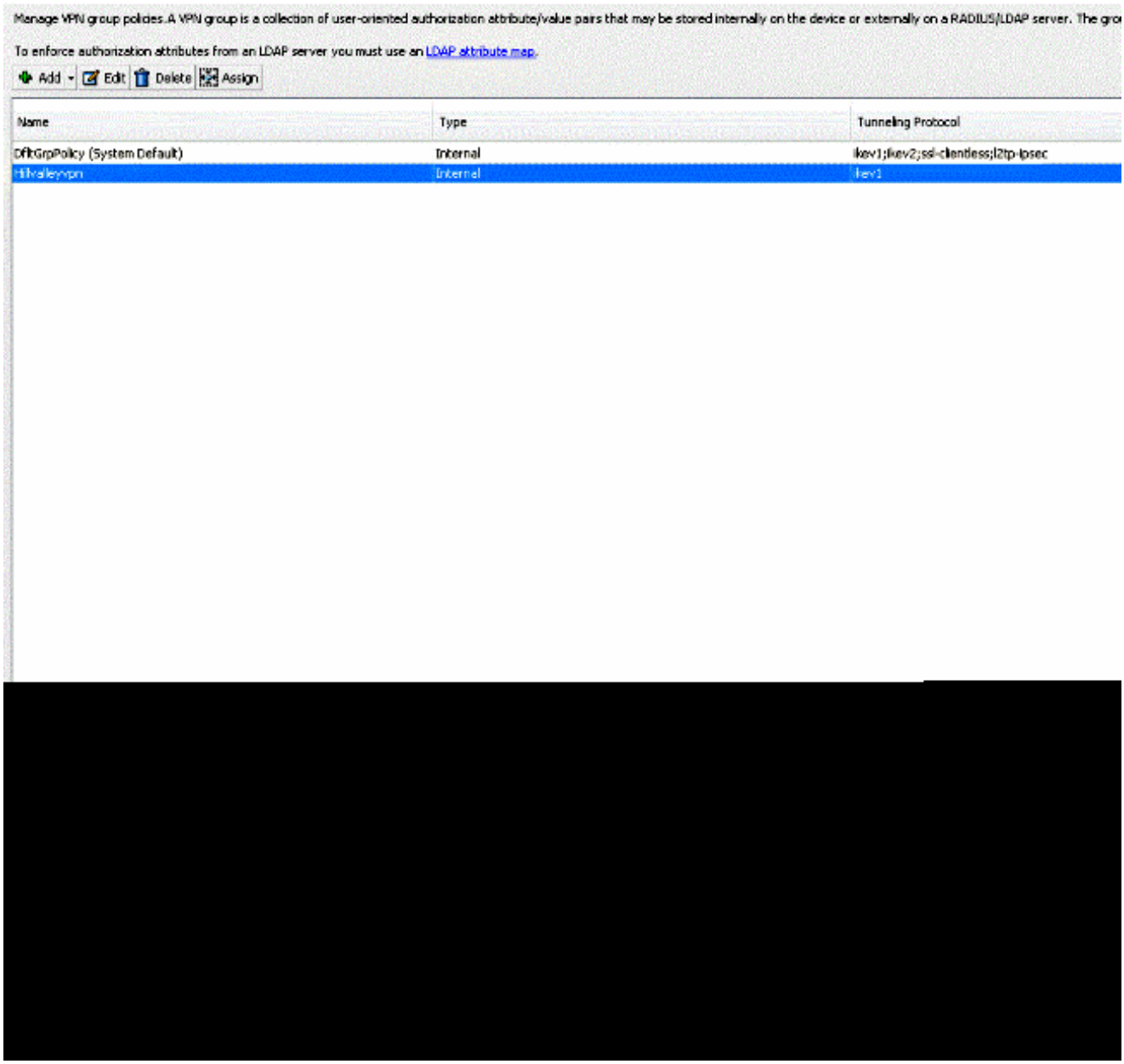
10. Be sure that the ACL you just created is selected for the Split Tunnel Network List.



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 the 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.

```
<#root>

ciscoasa>

enable


Password:
ciscoasa#

configure terminal
```

```
ciscoasa(config)#
```

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

```
<#root>
ciscoasa(config)#
access-list Local_LAN_Access remark Client Local LAN Access

ciscoasa(config)#
access-list Local_LAN_Access standard permit host 0.0.0.0
```

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

```
<#root>
ciscoasa(config)#
group-policy hillvalleyvpn attributes

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

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

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

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

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

6. Issue this command:

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

7. Associate the group policy with the tunnel group.

```
<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn
```

8. Exit the two configuration modes.

```
<#root>

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.

```
<#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#
```

Configure the Cisco AnyConnect Secure Mobility Client

In order to configure the Cisco AnyConnect Secure Mobility Client, refer to the Configure AnyConnect Connections section of *CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17*.

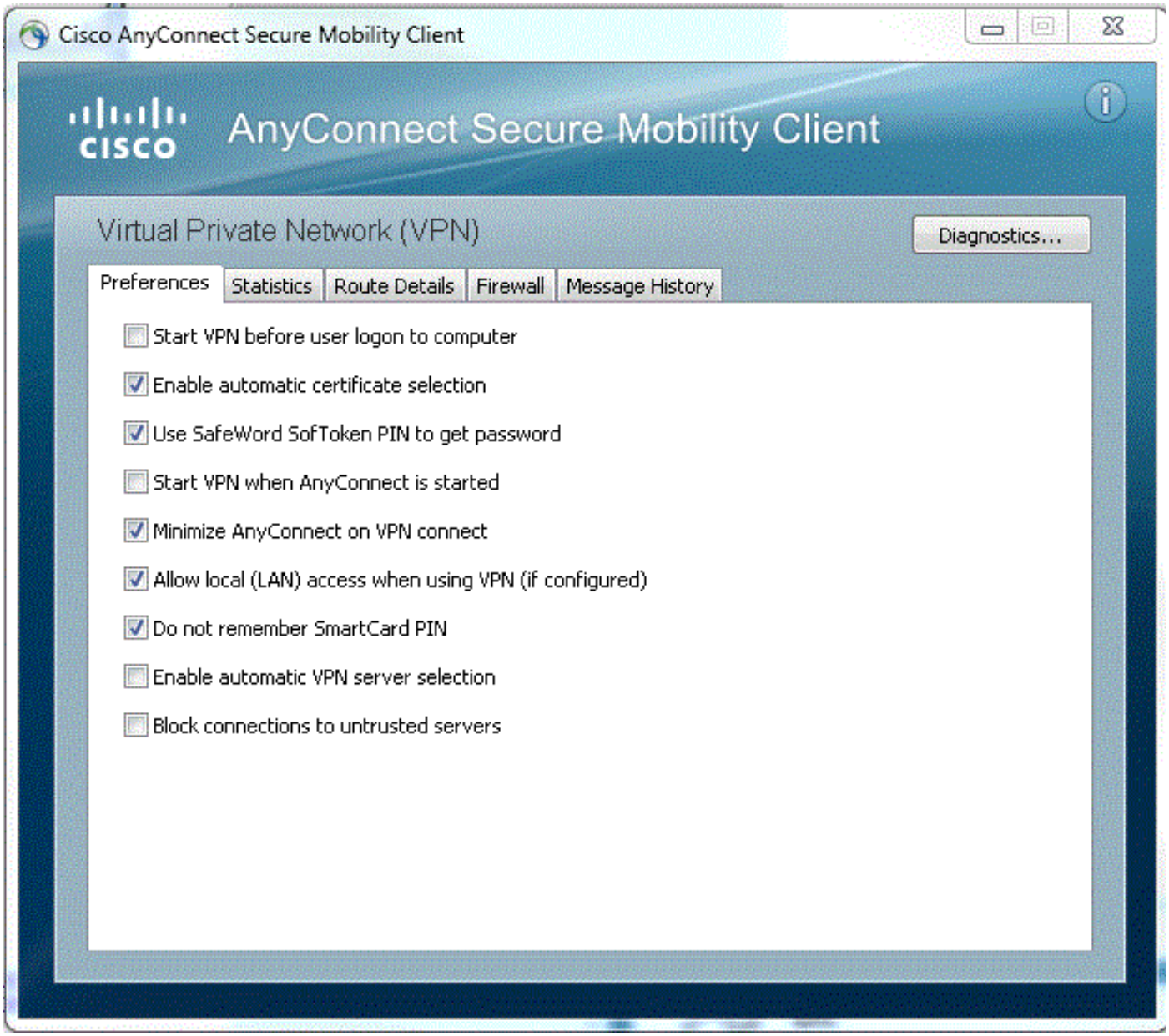
Split-exclude tunneling requires that you enable **AllowLocalLanAccess** in the AnyConnect Client. All split-exclude tunneling is regarded as local LAN access. In order to use the exclude feature of split-tunneling, you must enable the **AllowLocalLanAccess** preference in the AnyConnect VPN Client preferences. By default, local LAN access is disabled.

In order to allow local LAN access, and therefore split-exclude tunneling, a network administrator can enable it in the profile or users can enable it in their preferences settings (see the image in the next section). In order to allow local LAN access, a user selects the **Allow Local LAN access** check box if split-tunneling is

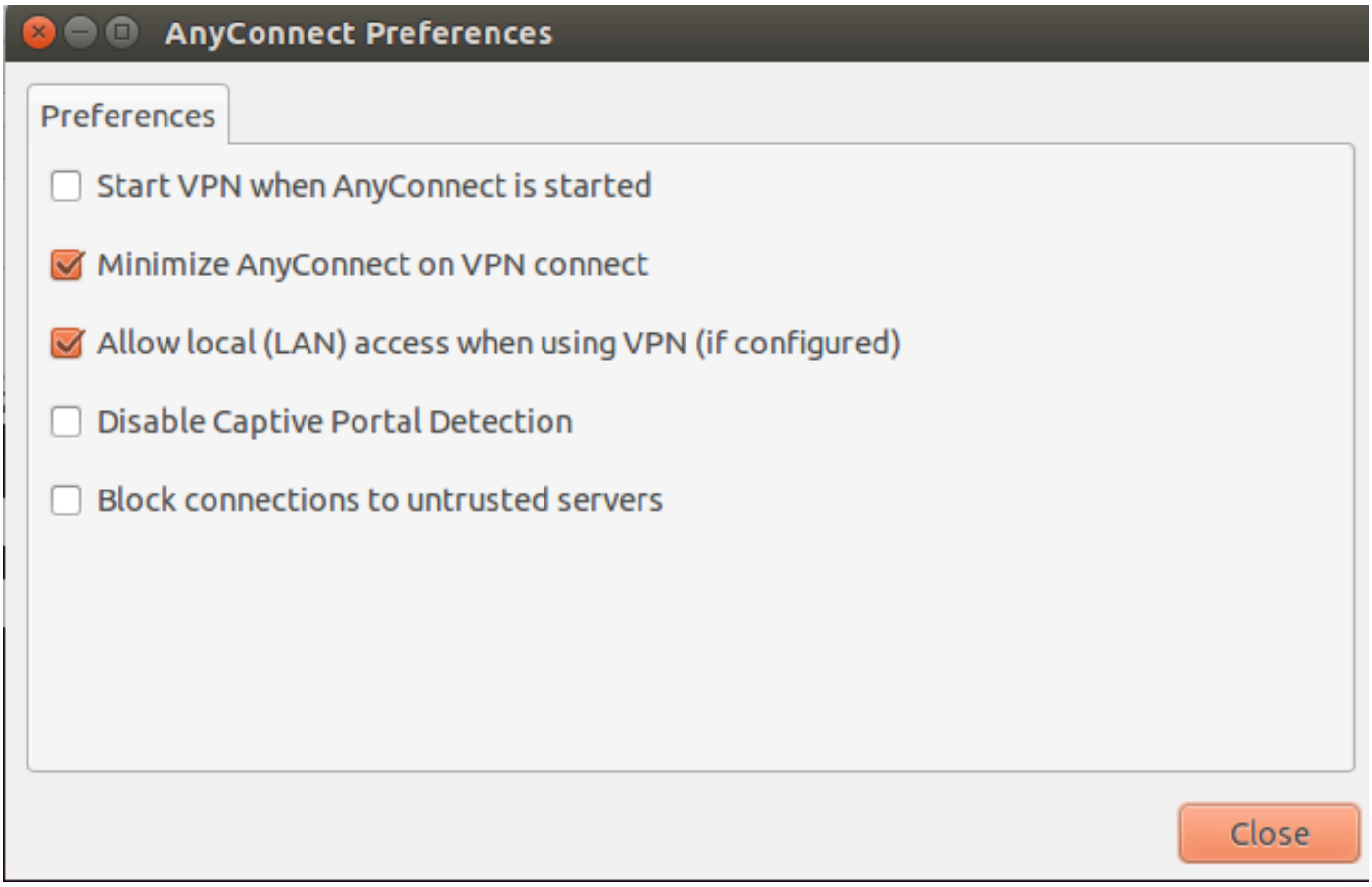
enabled on the secure gateway and is configured with the split-tunnel-policy exclude specified policy. In addition, you can configure the VPN Client Profile if local LAN access is allowed with **<LocalLanAccess UserControllable="true">true</LocalLanAccess>.**

User Preferences

Here are the selections that you must make in the Preferences tab on the Cisco AnyConnect Secure Mobility Client in order to allow local LAN access.



On Linux



XML Profile Example

Here is an example of how to configure the VPN Client Profile with XML.

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
    <ClientInitialization>
        <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
        <AutomaticCertSelection UserControllable="true">false</AutomaticCertSelection>
        <ShowPreConnectMessage>false</ShowPreConnectMessage>
        <CertificateStore>All</CertificateStore>
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>true</AllowLocalProxyConnections>
        <AuthenticationTimeout>12</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">true</LocalLanAccess>
        <ClearSmartcardPin UserControllable="true">true</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <AutoReconnect UserControllable="false">true
            <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend
            </AutoReconnectBehavior>
        </AutoReconnect>
        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic
        </RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
```

```
        <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Disable
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="false">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
    </ClientInitialization>
</AnyConnectProfile>
```

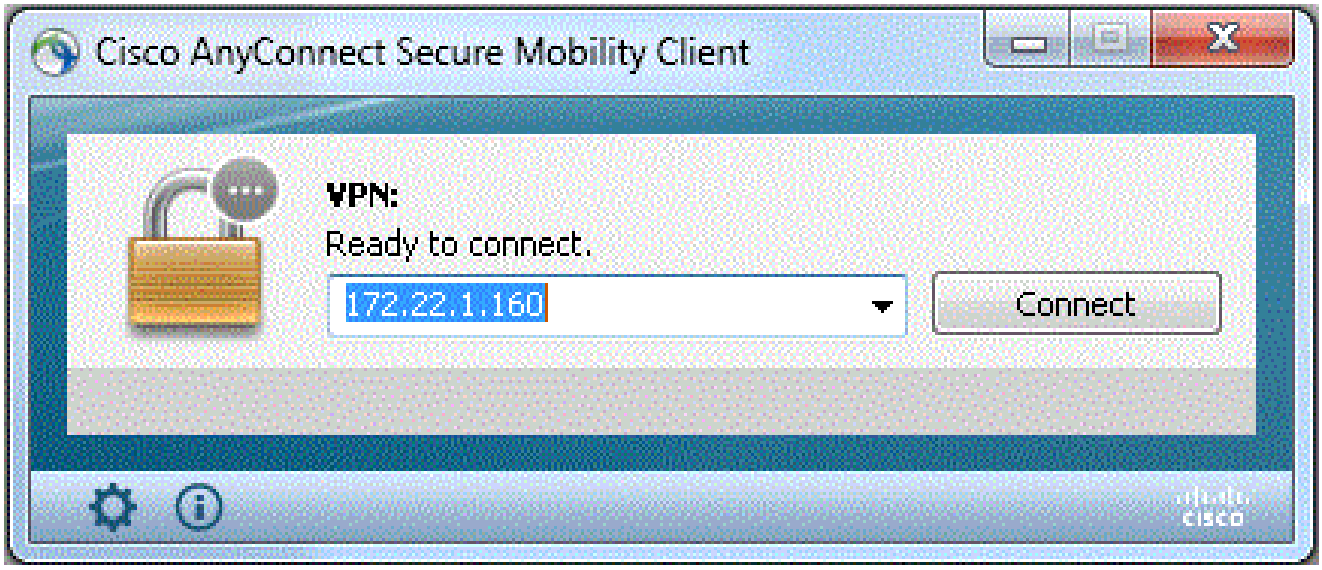
Verify

Complete the steps in these sections in order to verify your configuration:

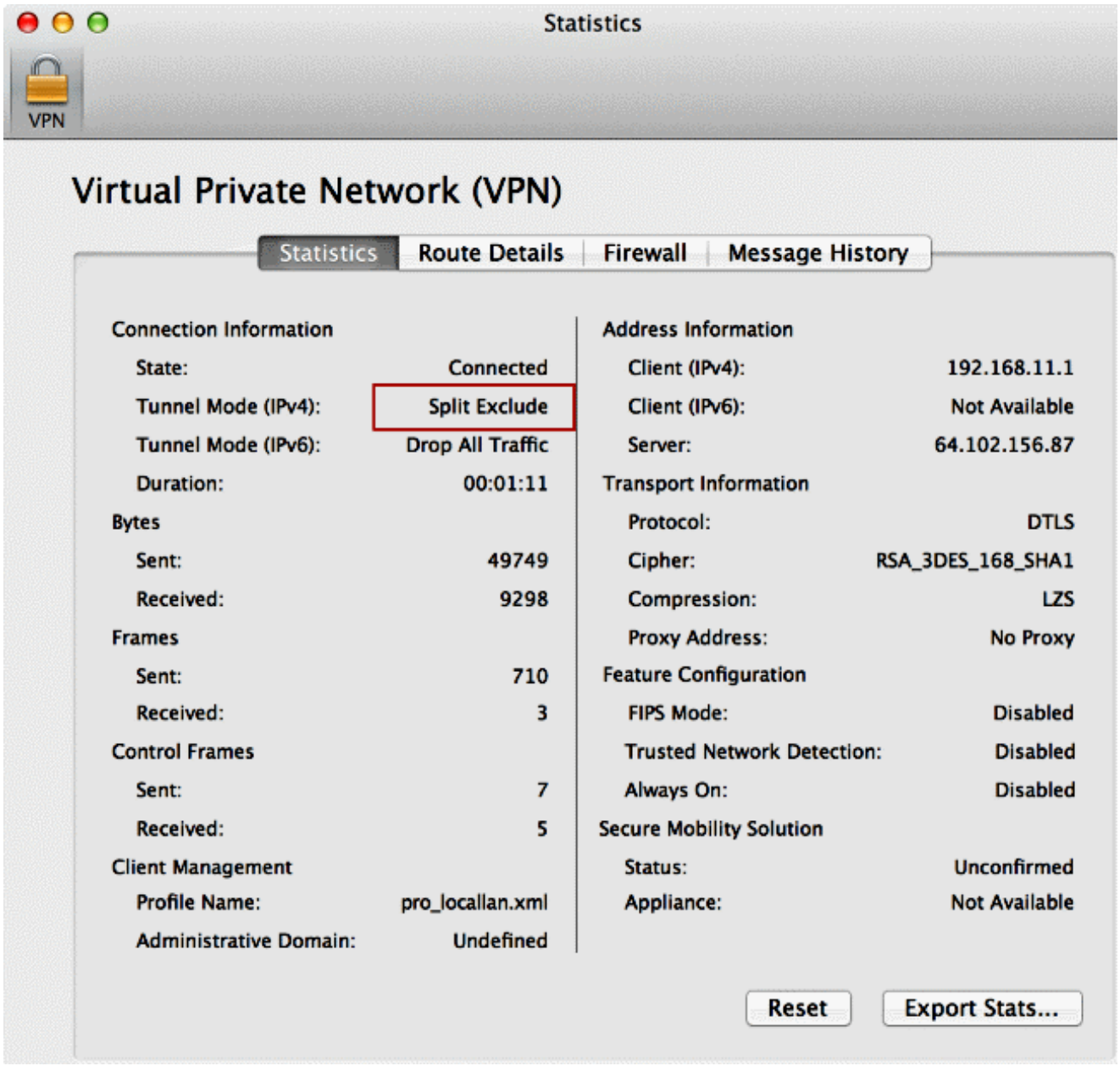
- View the DART
- Test Local LAN Access with Ping

Connect your Cisco AnyConnect Secure Mobility Client to the ASA in order to verify your configuration.

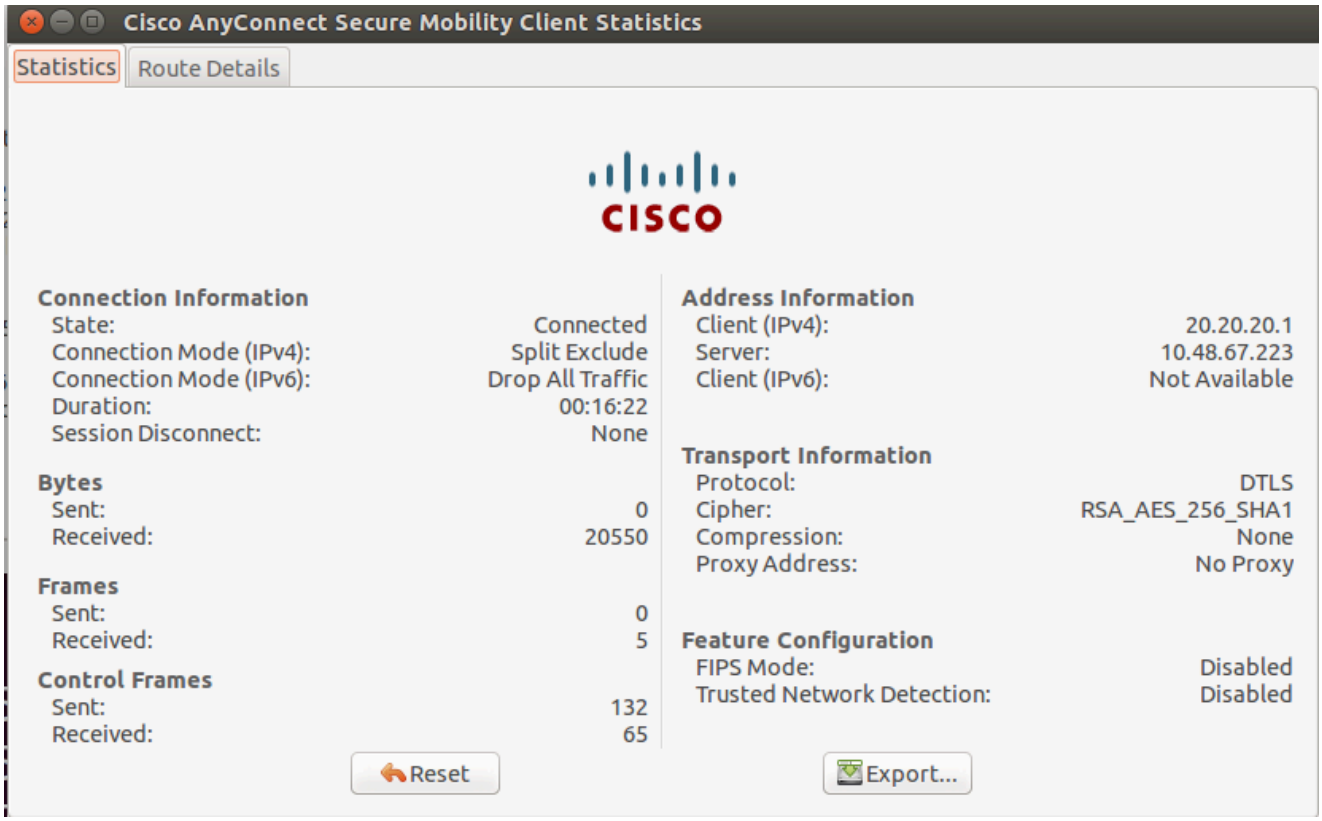
1. Choose your connection entry from the server list and click **Connect**.



2. Choose **Advanced Window for All Components** > **Statistics...** in order to display the Tunnel Mode.

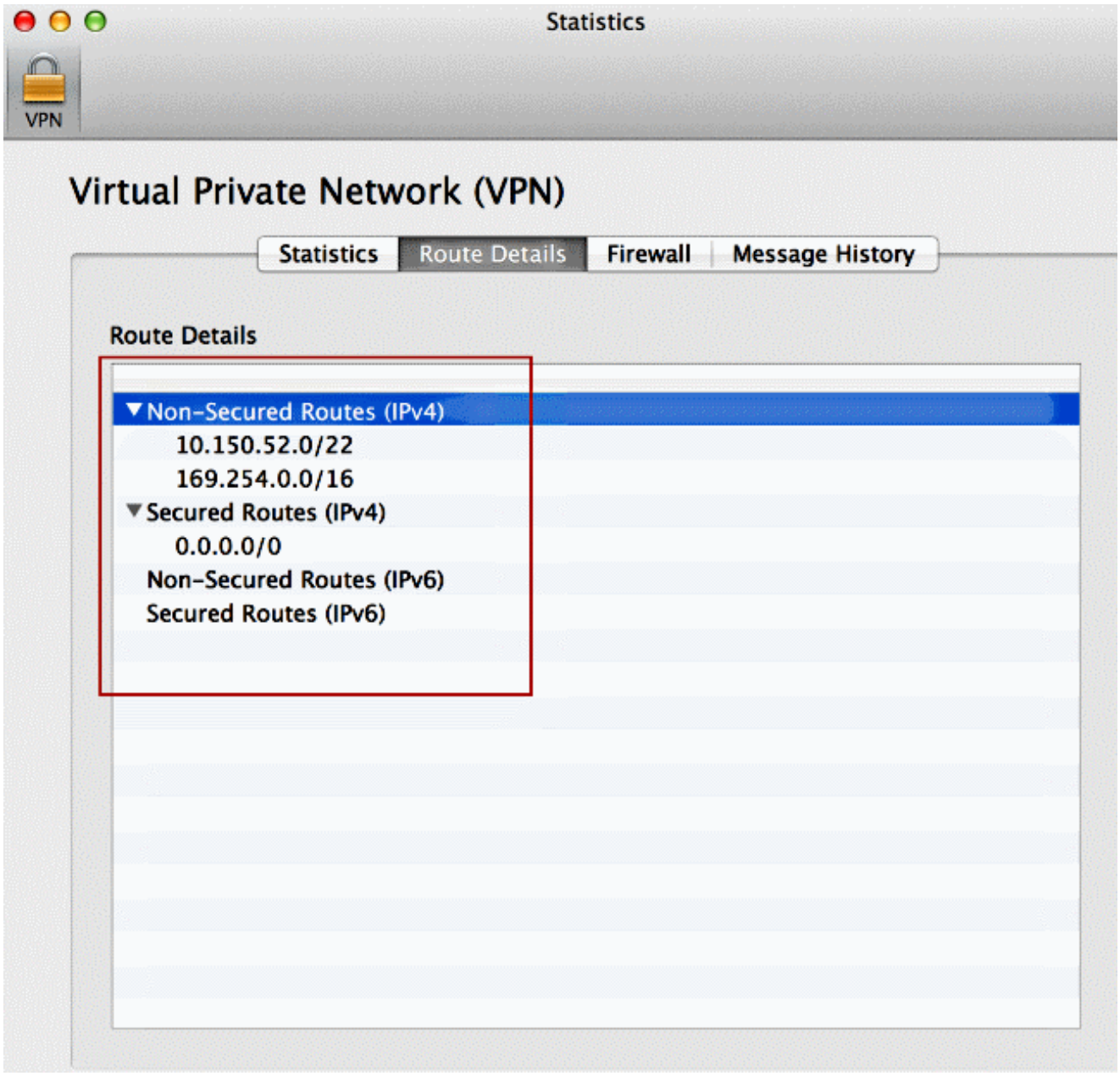

Statistics
VPN
Virtual Private Network (VPN)
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Exclude
Tunnel Mode (IPv6): Drop All Traffic
Duration: 00:01:11
Bytes
Sent: 49749
Received: 9298
Frames
Sent: 710
Received: 3
Control Frames
Sent: 7
Received: 5
Client Management
Profile Name: pro_locallan.xml
Administrative Domain: Undefined
Address Information
Client (IPv4): 192.168.11.1
Client (IPv6): Not Available
Server: 64.102.156.87
Transport Information
Protocol: DTLS
Cipher: RSA_3DES_168_SHA1
Compression: LZS
Proxy Address: No Proxy
Feature Configuration
FIPS Mode: Disabled
Trusted Network Detection: Disabled
Always On: Disabled
Secure Mobility Solution
Status: Unconfirmed
Appliance: Not Available
Reset
Export Stats...

On Linux

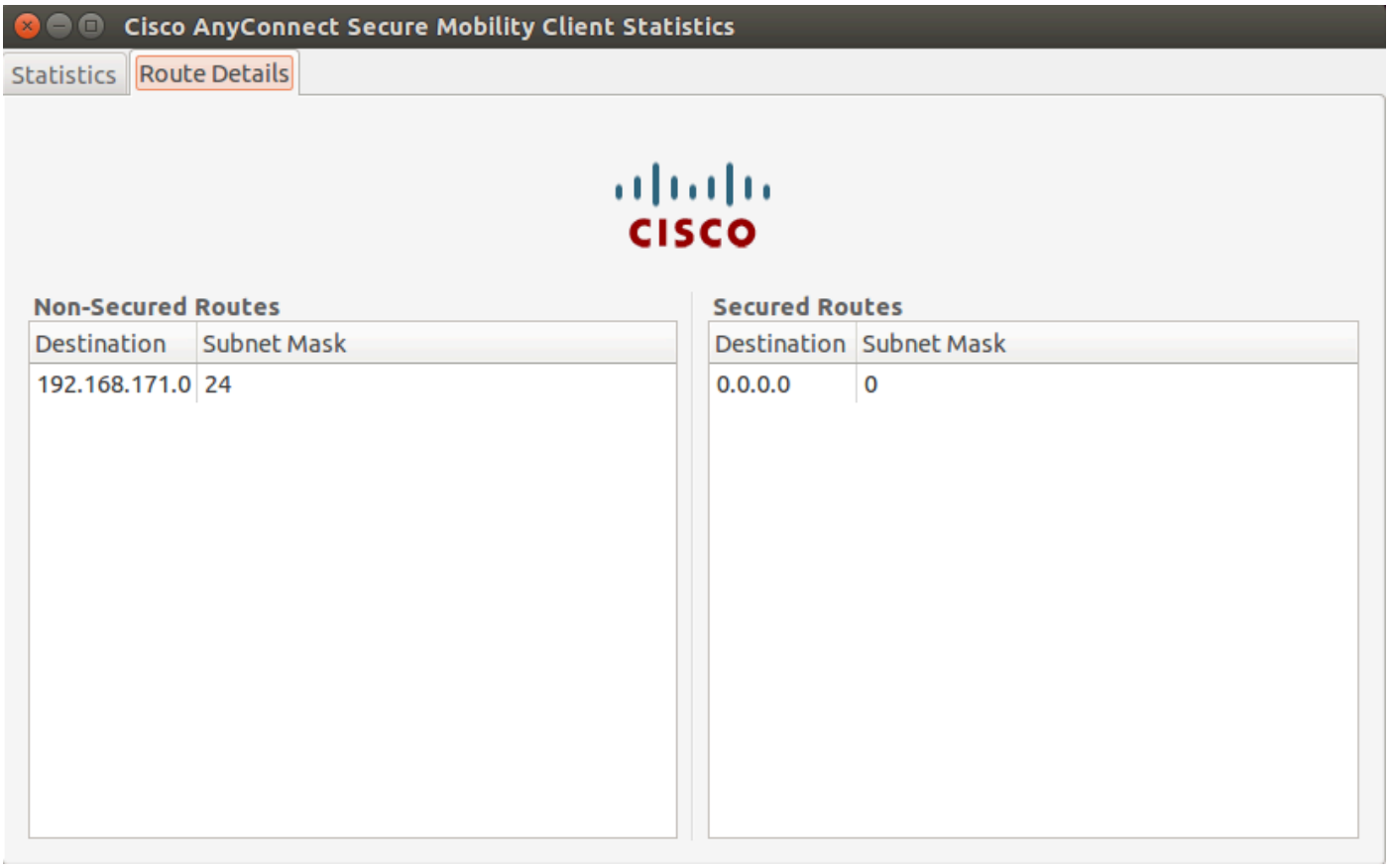


3. Click the **Route Details** tab in order to see the routes to which the Cisco AnyConnect Secure Mobility Client still has local access.

   In this example, the client is allowed local LAN access to 10.150.52.0/22 and 169.254.0.0/16 while all other traffic is encrypted and sent across the tunnel.


Statistics
VPN
Virtual Private Network (VPN)
Statistics
Route Details
Firewall
Message History
Route Details
Non-Secured Routes (IPv4)
10.150.52.0/22
169.254.0.0/16
Secured Routes (IPv4)
0.0.0.0/0
Non-Secured Routes (IPv6)
Secured Routes (IPv6)

On Linux



Cisco AnyConnect Secure Mobility Client

When you examine the AnyConnect logs from the Diagnostics and Reporting Tool (DART) bundle, you can determine whether or not the parameter that allows local LAN access is set.

```
*******************************************

Date         : 11/25/2011
Time         : 13:01:48
Type         : Information
Source       : acvpndownloader

Description : Current Preference Settings:
ServiceDisable: false
CertificateStoreOverride: false
CertificateStore: All
ShowPreConnectMessage: false
AutoConnectOnStart: false
MinimizeOnConnect: true
LocalLanAccess: true
AutoReconnect: true
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: false
AutoUpdate: true
RSASecurIDIntegration: Automatic
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: Native
AllowLocalProxyConnections: true
PPPExclusion: Disable
PPPExclusionServerIP:
```

```
AutomaticVPNPolicy: false
TrustedNetworkPolicy: Disconnect
UntrustedNetworkPolicy: Connect
TrustedDNSDomains:
TrustedDNSServers:
AlwaysOn: false
ConnectFailurePolicy: Closed
AllowCaptivePortalRemediation: false
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: false
AllowVPNDisconnect: true
EnableScripting: false
TerminateScriptOnNextEvent: false
EnablePostSBLOnConnectScript: true
AutomaticCertSelection: true
RetainVpnOnLogoff: false
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: false
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
AuthenticationTimeout: 12
SafeWordSofTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true



****************************************
```

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 headend is to use the **ping** command at the Microsoft Windows command line. Here is an example where the local LAN of the client is 192.168.0.0/24 and another host is present on the network with an IP address of 192.168.0.3.

<#root>

```
C:\>
```

ping 192.168.0.3

```
Pinging 192.168.0.3 with 32 bytes of data&colon;

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
```

On Linux

```
malhyari@ubuntu:~$ ping 192.168.171.131
PING 192.168.171.131 (192.168.171.131) 56(84) bytes of data.
64 bytes from 192.168.171.131: icmp_seq=1 ttl=128 time=0.474 ms
64 bytes from 192.168.171.131: icmp_seq=2 ttl=128 time=0.315 ms
64 bytes from 192.168.171.131: icmp_seq=3 ttl=128 time=0.336 ms
64 bytes from 192.168.171.131: icmp_seq=4 ttl=128 time=0.475 ms
64 bytes from 192.168.171.131: icmp_seq=5 ttl=128 time=0.337 ms
64 bytes from 192.168.171.131: icmp_seq=6 ttl=128 time=0.286 ms
64 bytes from 192.168.171.131: icmp_seq=7 ttl=128 time=0.252 ms
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

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 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 in order 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 Microsoft Windows PC allows you to create static mappings between hostnames and IP addresses. For example, an LMHOSTS file can look like this:

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

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

Related Information

- CLI Book 3: Cisco ASA Series VPN CLI Configuration Guide, 9.17
- Cisco ASA 5500-X Series Firewalls
- Technical Support & Documentation - Cisco Systems