

配置对本地局域网的 AnyConnect 客户端访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[网络图](#)

[背景信息](#)

[配置AnyConnect安全移动客户端的本地LAN访问](#)

[通过 ASDM 配置 ASA](#)

[通过 CLI 配置 ASA](#)

[配置 Cisco AnyConnect Secure Mobility Client](#)

[用户首选项](#)

[XML 配置文件示例](#)

[验证](#)

[Cisco AnyConnect 安全移动客户端](#)

[通过 Ping 测试本地 LAN 访问](#)

[故障排除](#)

[无法按名称打印或浏览](#)

[相关信息](#)

简介

本文档介绍如何允许连接到 Cisco ASA 的 Cisco AnyConnect Secure Mobility Client 访问本地局域网。

先决条件

要求

本文档假设思科自适应安全设备(ASA)上已存在可正常运行的远程访问VPN配置。

如果需要，请参阅[CLI手册3：思科ASA系列VPN CLI配置指南9.17](#) 以获取配置帮助。

使用的组件

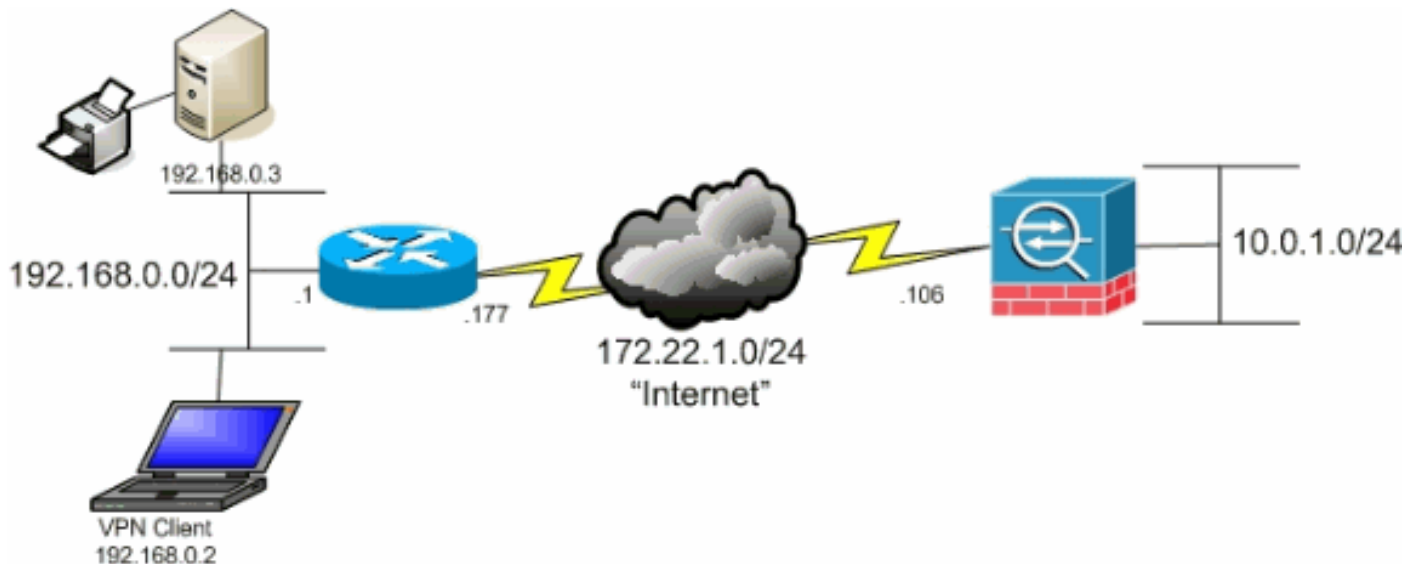
本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 5500 系列版本 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) 版本 7.1(6)
- Cisco AnyConnect Secure Mobility Client 版本 3.1.05152

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

网络图

客户端位于典型的小型办公室/家庭办公室 (SOHO) 网络中，并通过互联网连接到总部。



背景信息


此配置允许Cisco AnyConnect安全移动客户端通过IPsec、安全套接字层(SSL)或互联网密钥交换版本2 (IKEv2)安全访问企业资源，并且仍然允许客户端执行活动，例如打印客户端所在的位置。如果允许，要发送到 Internet 的流量仍通过隧道传输到 ASA。

与典型的拆分隧道场景（其中所有互联网流量均以未加密方式发送）不同，当您为 VPN 客户端启用本地局域网访问时，它允许这些客户端仅与其所在网络上的设备进行不加密通信。例如，允许本地LAN访问的客户端在从家连接到ASA时可以打印到其自己的打印机，但无法访问Internet，除非它首先通过隧道发送流量。

使用访问列表的目的是按分割隧道在 ASA 上的相似配置方式允许本地 LAN 访问。但是，与分割隧道方案不同，此访问列表不定义必须加密哪些网络。而是定义哪些网络不能加密。并且，与分割隧道方案不同的是，此列表中的实际网络不必是已知网络。相反，ASA 提供一个默认网络 0.0.0.0/255.255.255.255，它被视为客户端的本地局域网。



注意：这不是分割隧道的配置，其中客户端在连接到ASA时可以对Internet进行未加密访问。有关如何在ASA上配置分割隧道的信息，请参阅CLI手册3：思科ASA系列VPN CLI配置指南9.17 中的[设置分割隧道策略](#)。

 注意：当客户端已连接且已针对本地LAN访问配置时，您无法在本地LAN上按名称打印或浏览。但是，可以按 IP 地址浏览或打印。有关详细信息以及此情况的解决方法，请参阅本文档的[故障排除部分](#)。

配置AnyConnect安全移动客户端的本地LAN访问

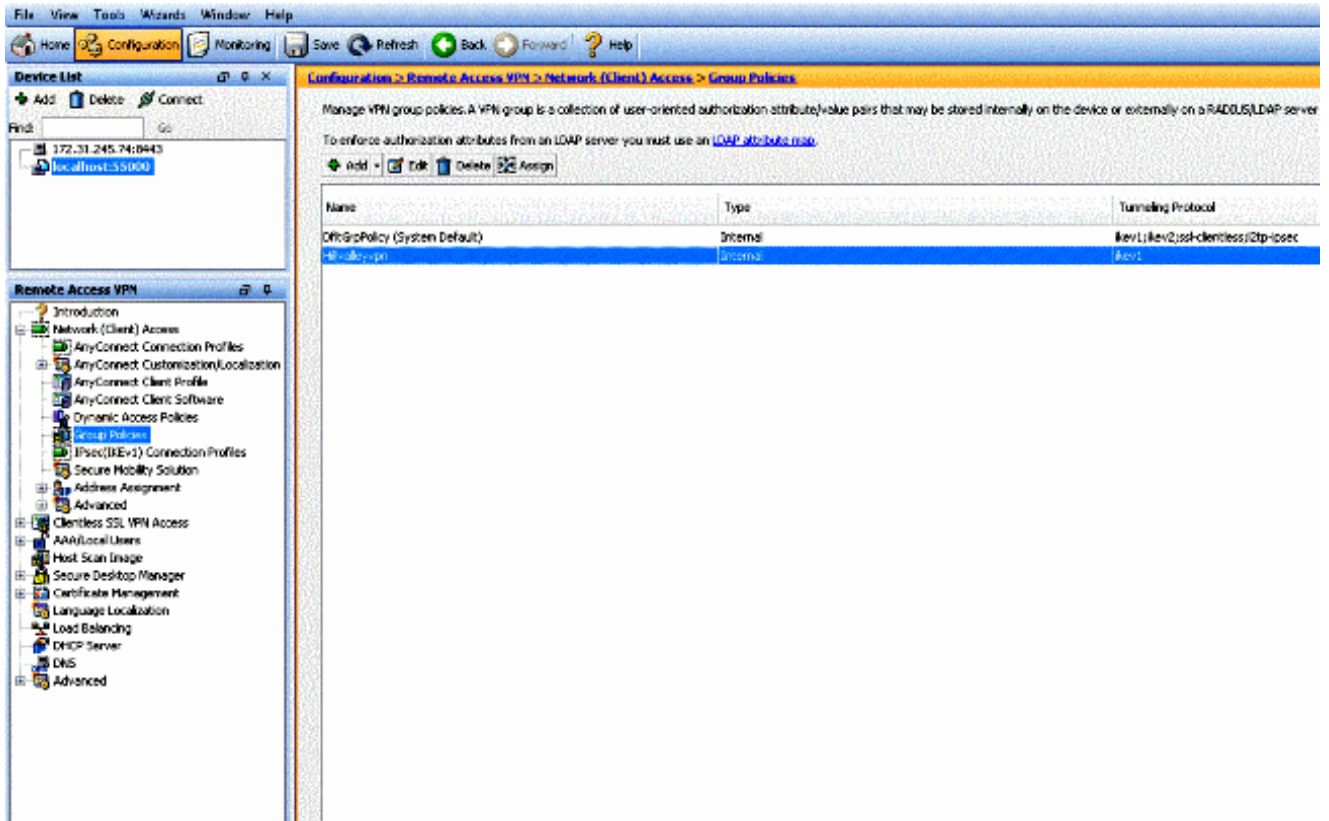
完成以下任务，以允许Cisco AnyConnect安全移动客户端在连接到ASA时访问其本地LAN：

- [通过 ASDM 配置 ASA 或通过 CLI 配置 ASA](#)
- [配置 Cisco AnyConnect Secure Mobility Client](#)

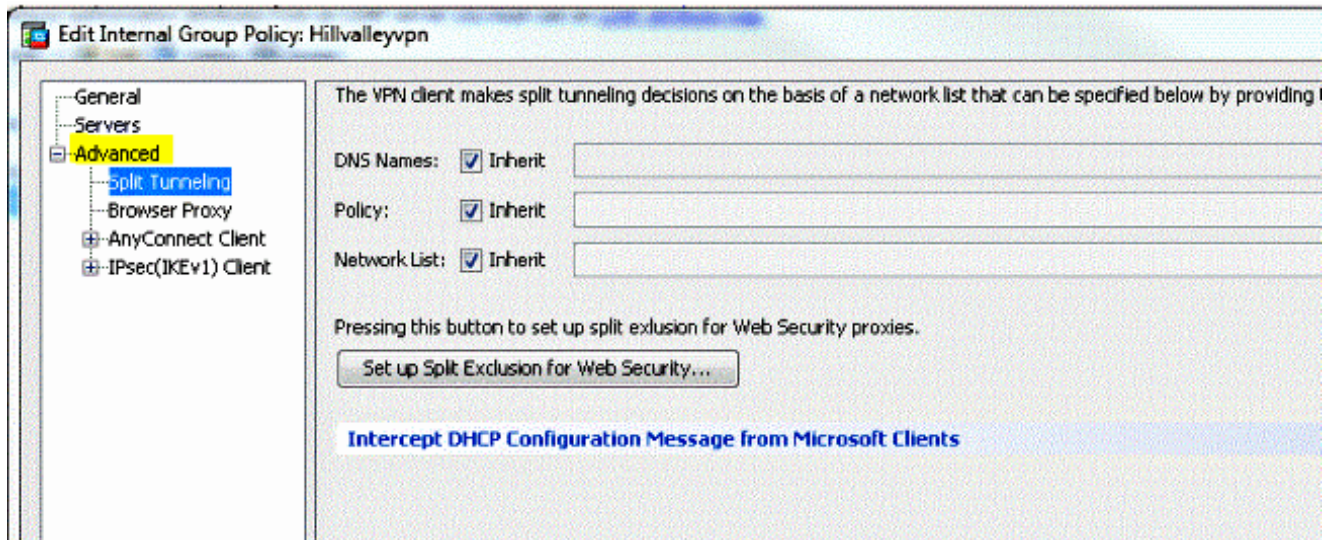
通过 ASDM 配置 ASA

在 ASDM 中完成以下步骤，以使 VPN 客户端能够在连接 ASA 的同时访问本地局域网：

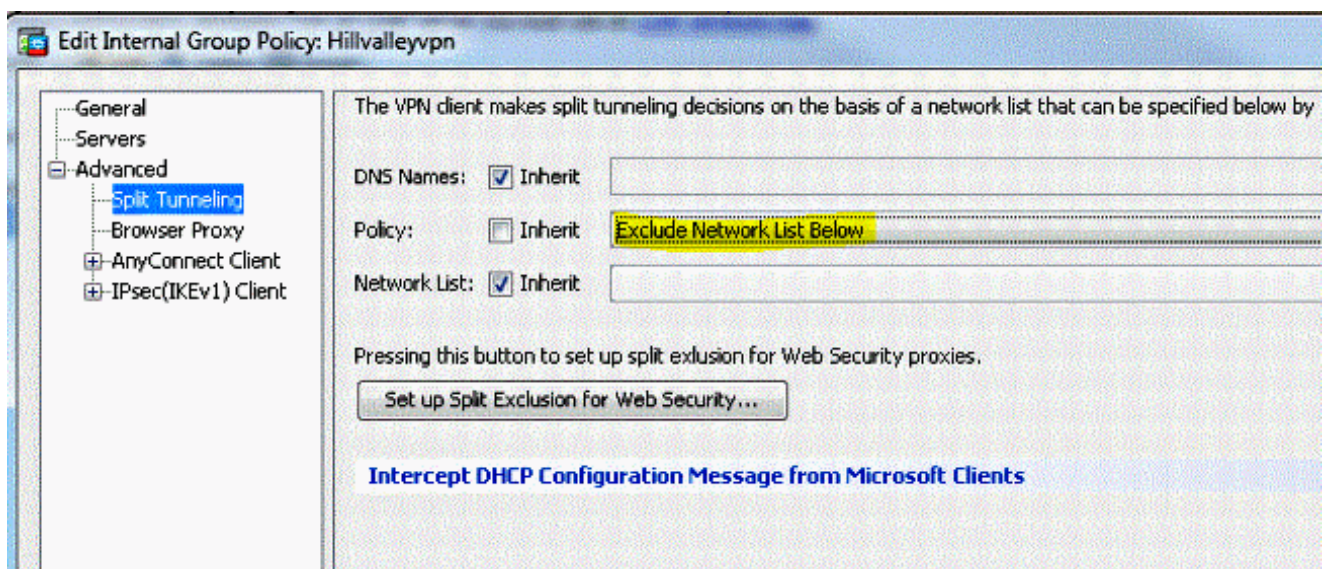
1. 选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** 并选择您希望在其中启用本地 LAN 访问的组策略。?? 然后单击 **Edit**



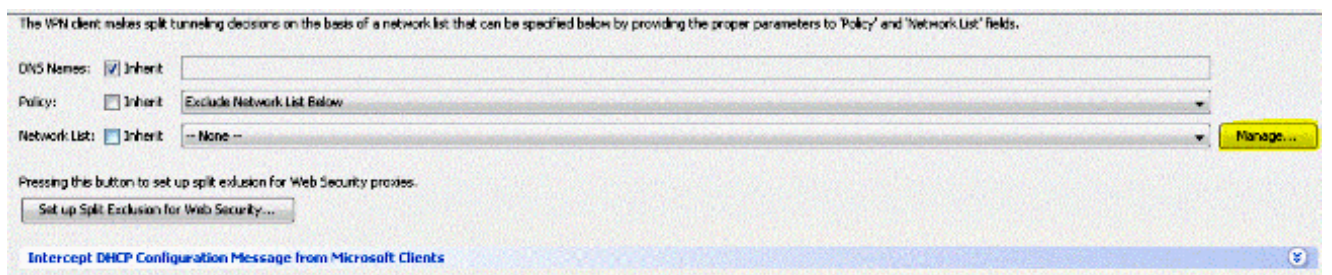
- 转到访问。 **Advanced > Split Tunneling**



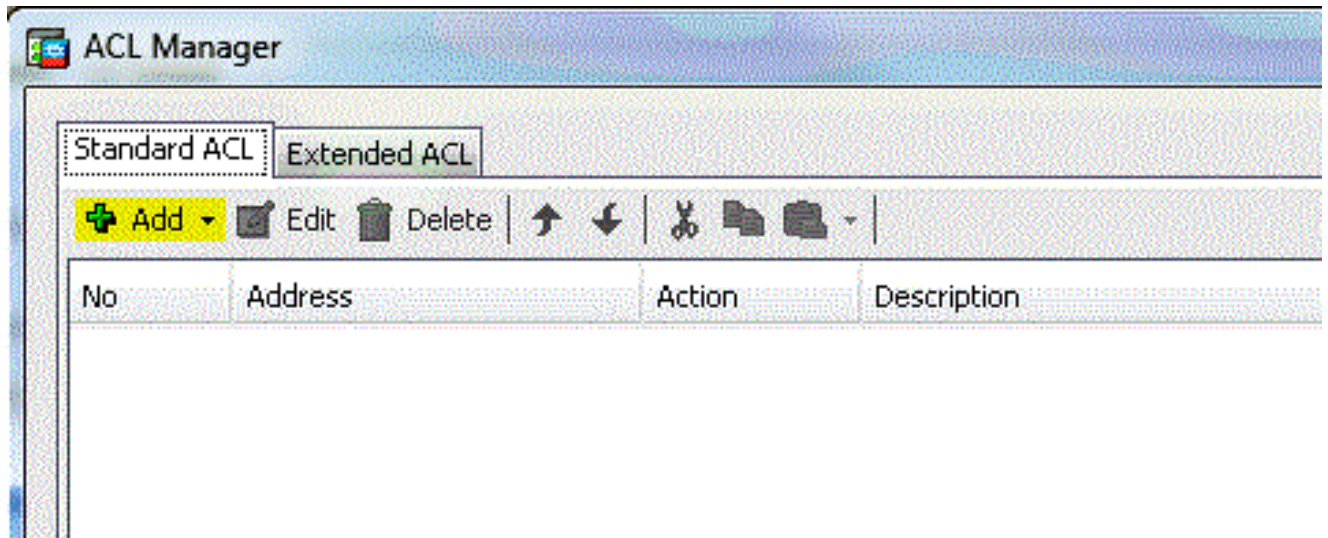
- 取消选中Policy所对应的 **Inherit** 框，然后选择 **Exclude Network List Below**。



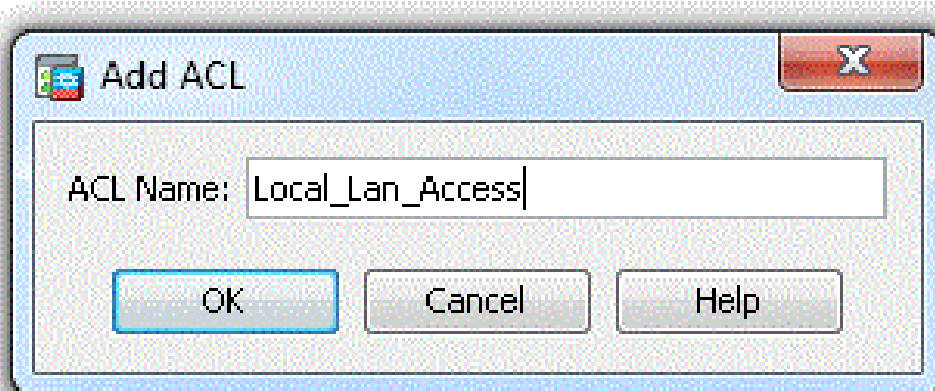
- 取消选中Network List的 **Inherit** 复选框，然后单击 **Manage** 以启动访问控制列表(ACL)管理器。



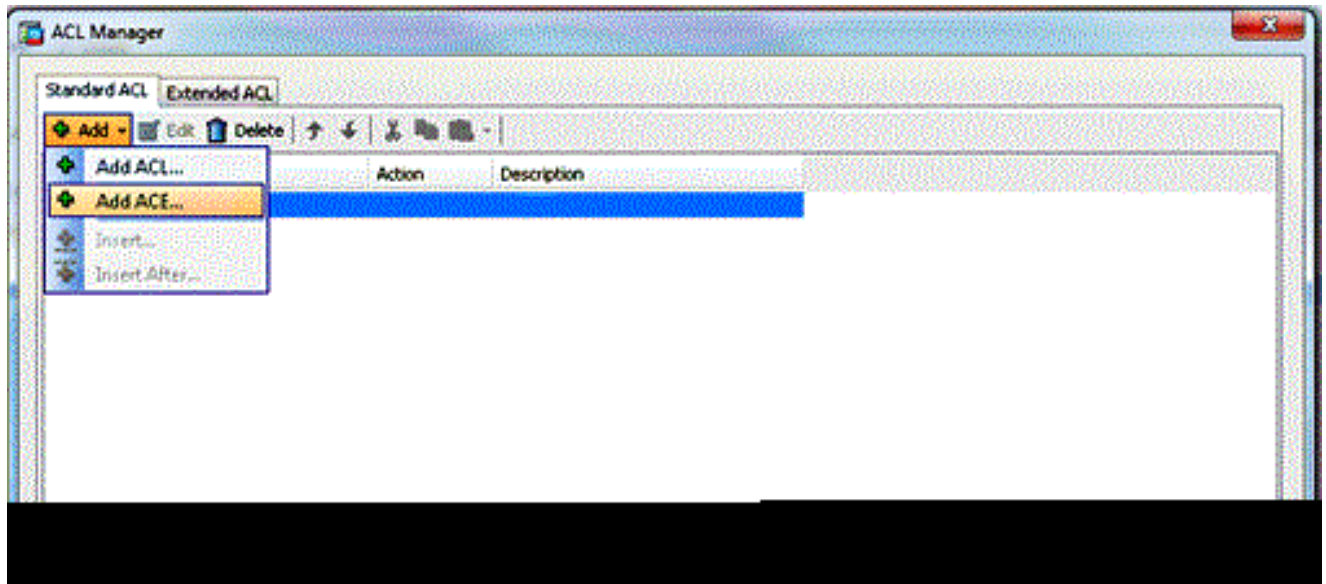
- 在ACL Manager中，选择 **Add > Add ACL...** 以创建新的访问列表。



- 为此ACL提供一个名称，然后单击 **OK**。



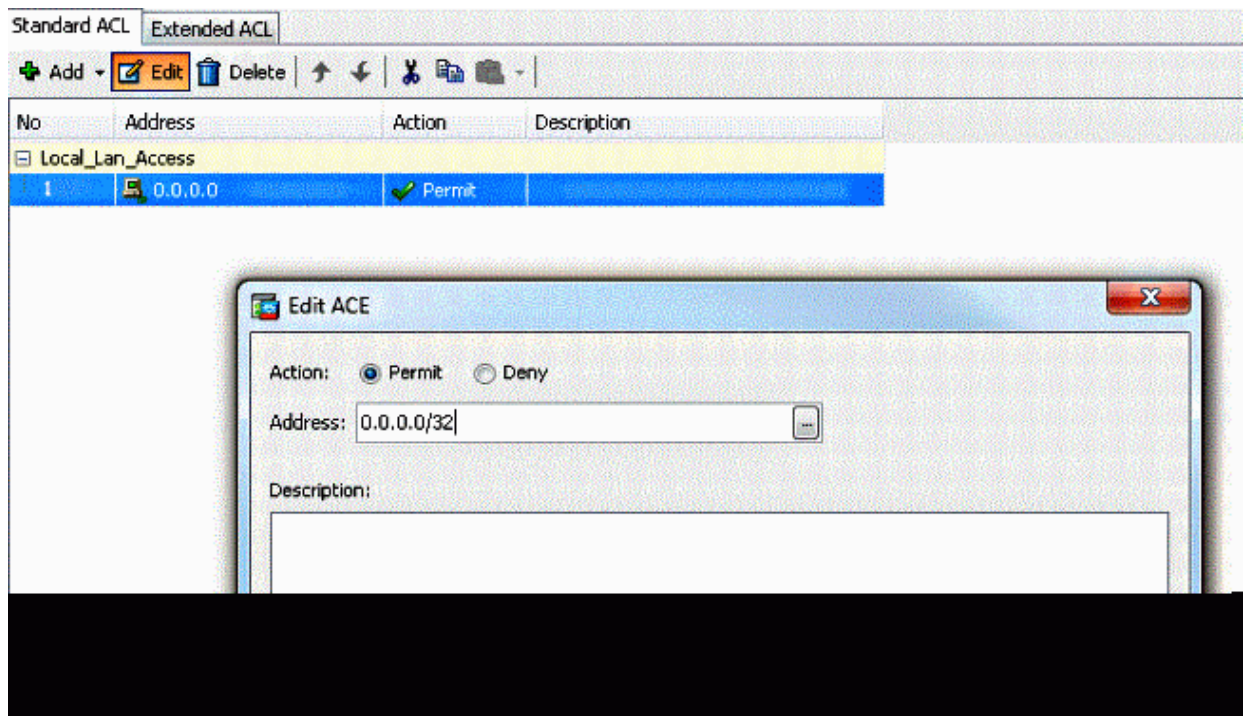
- 创建ACL后，选择 **Add > Add ACE...** 以添加访问控制条目(ACE)。



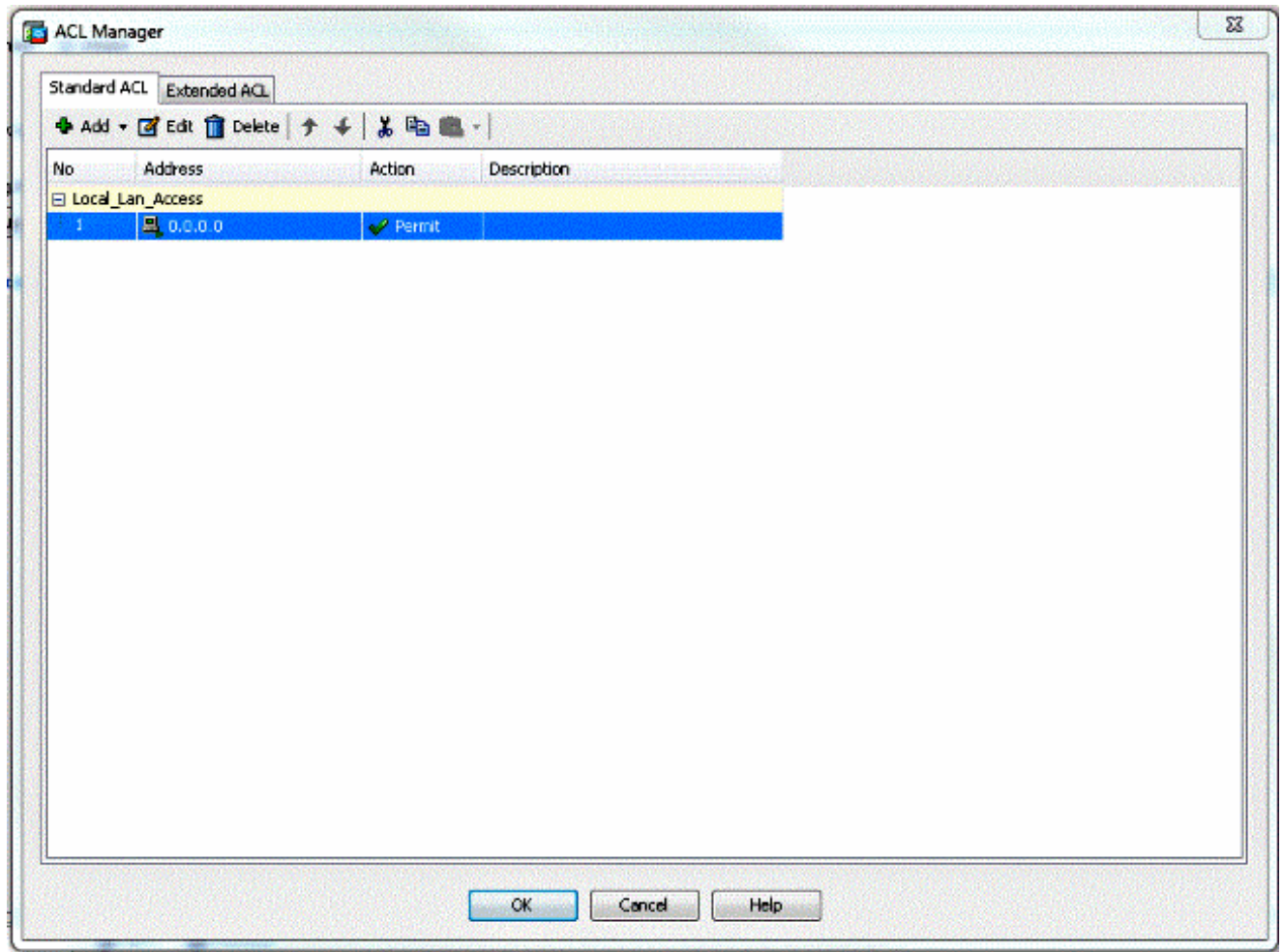
- 定义与客户端的本地 LAN 相对应的 ACE。

a. 选择。Permit

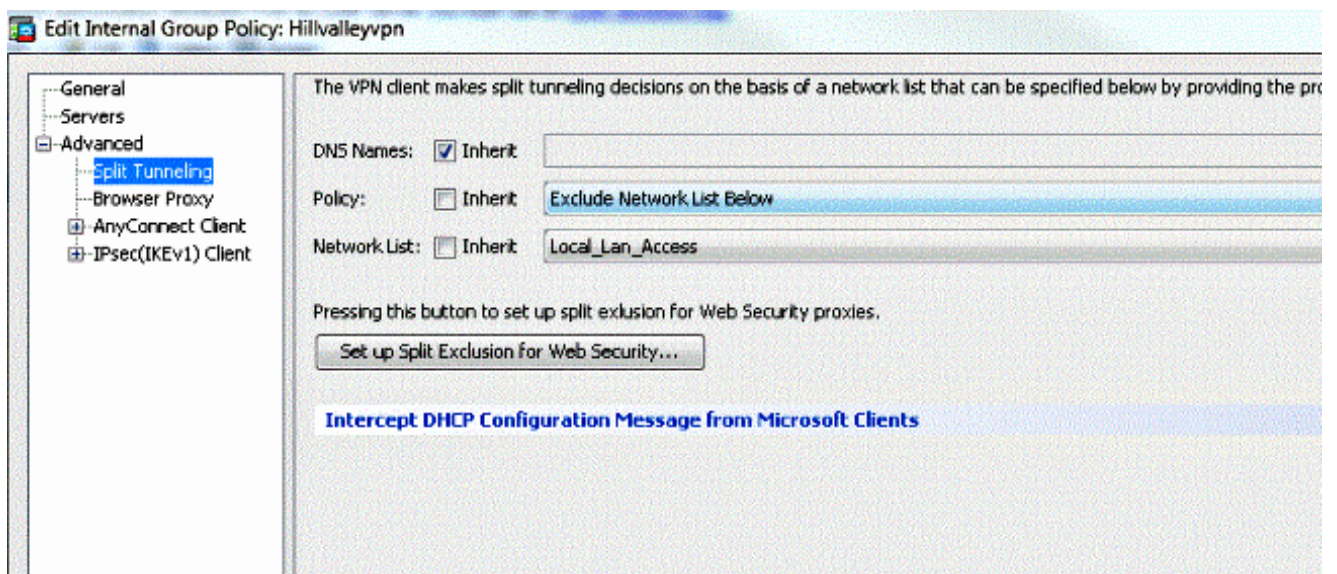
- 选择 IP 地址 **0.0.0.0**
- 选择网络掩码 /32。
- (可选) 提供相应说明。
- 单击。OK



- 单击 **OK** 以退出ACL Manager。



- 请确保已为拆分隧道网络列表选择您刚刚创建的 ACL。



- 单击 **OK** 以返回组策略配置。

The VPN client makes split tunneling decisions on the basis of a network list that can be specified below by providing the proper parameter

DNS Names: Inherit

Policy: Inherit Exclude Network List Below

Network List: Inherit Local_Lan_Access

Pressing this button to set up split exclusion for Web Security proxies.

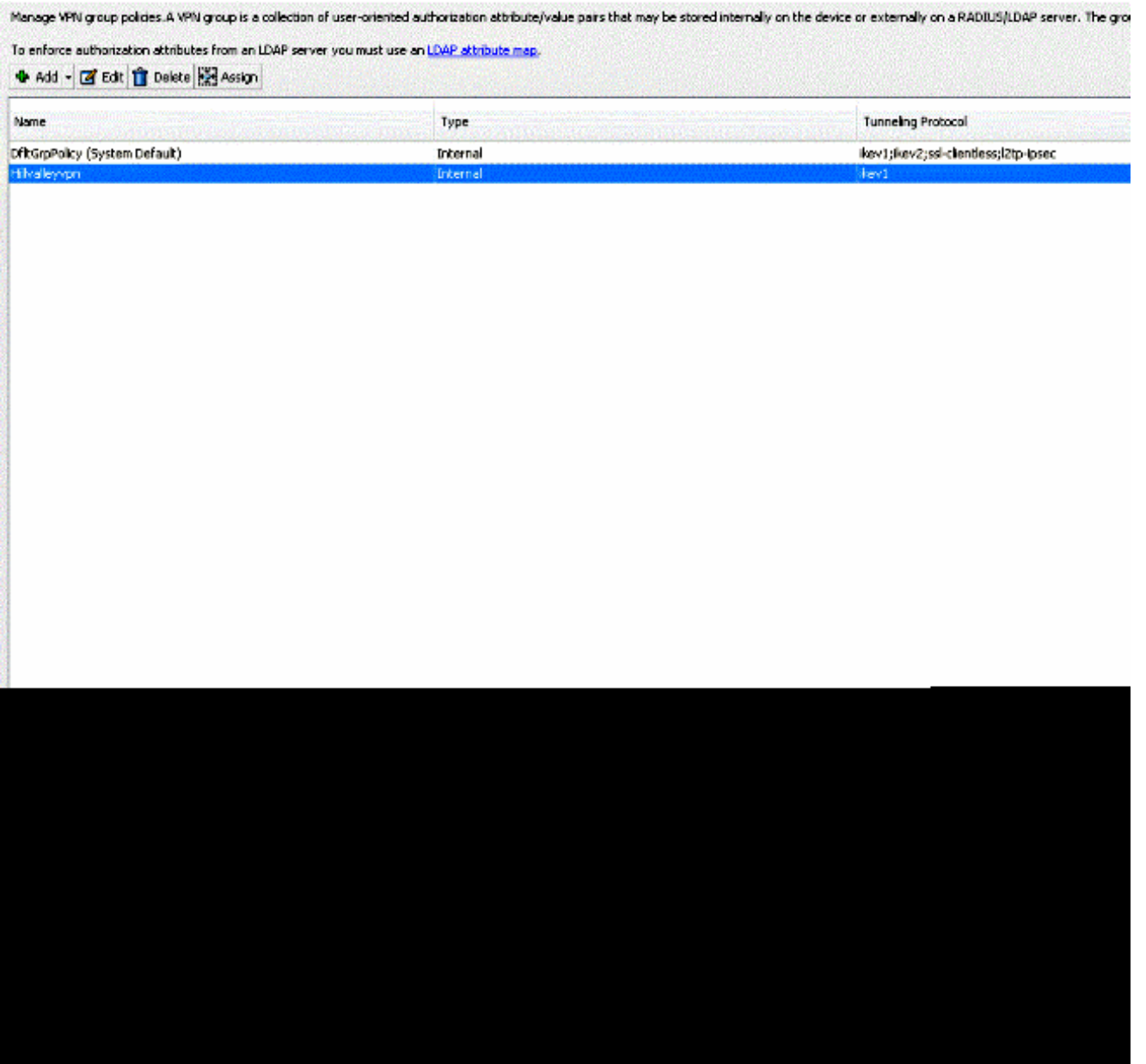
Set up Split Exclusion for Web Security...

Intercept DHCP Configuration Message from Microsoft Clients

Next Previous

OK Cancel Help

- 单击 **Apply** 然后单击 **Send**（如果需要），以将命令发送到ASA。



通过 CLI 配置 ASA

您可以在 ASA CLI 中完成以下步骤（而不是使用 ASDM），以便允许 VPN 客户端在连接到 ASA 时访问本地 LAN：

- 进入配置模式。

```
<#root>
```

```
ciscoasa>
```

```
enable
```

Password:
ciscoasa#

```
configure terminal
```

```
ciscoasa(config)#
```

- 创建访问列表以允许本地局域网访问。

```
<#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
```

- 输入要修改的策略的组策略配置模式。

```
<#root>
```

```
ciscoasa(config)#
```

```
group-policy hillvalleyvpn attributes
```

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

- 指定分割隧道策略。在本示例中，此策略为 `excludespecified`。

```
<#root>
```

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

```
split-tunnel-policy excludespecified
```

- 指定分割隧道访问列表。在本示例中，此列表为 `Local_LAN_Access`。

```
<#root>
```

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

```
split-tunnel-network-list value Local_LAN_Access
```

- 发出以下命令：

```
<#root>
```

```
ciscoasa(config)#
```

```
tunnel-group hillvalleyvpn general-attributes
```

- 将组策略与隧道组关联。

```
<#root>
```

```
ciscoasa(config-tunnel-ipsec)#
```

```
default-group-policy hillvalleyvpn
```

- 退出上述两种配置模式。

```
<#root>
```

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

```
exit
```

```
ciscoasa(config)#
```

```
exit
```

```
ciscoasa#
```

- 将配置保存到非易失性RAM (NVRAM)，并在系统提示时按 **Enter** 以指定源文件名。

```
<#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#
```

配置 Cisco AnyConnect Secure Mobility Client

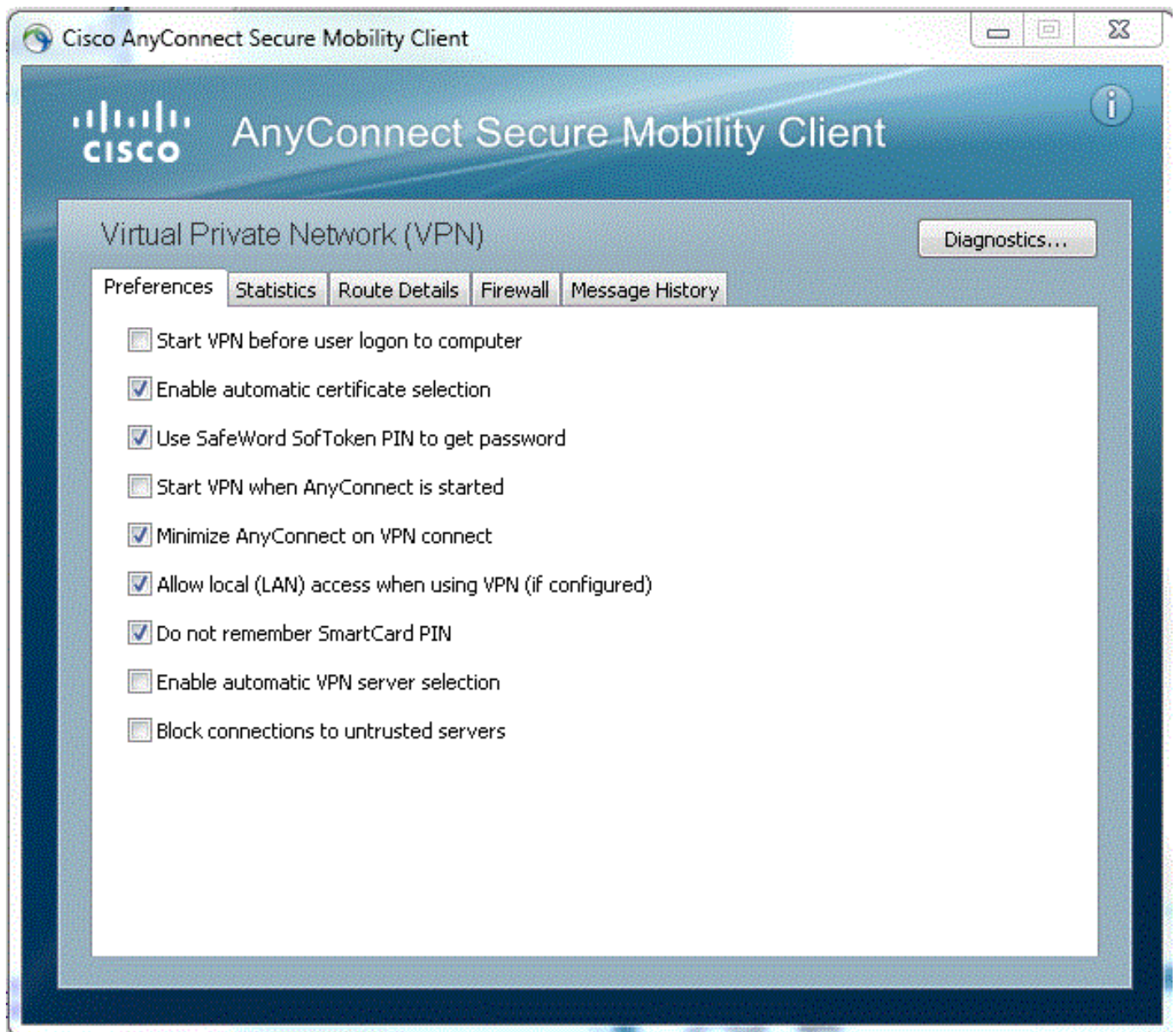
要配置Cisco AnyConnect安全移动客户端，请参阅CLI手册3：Cisco ASA系列VPN CLI配置指南9.17 的[配置AnyConnect连接](#)部分。

分离排除隧道需要您在AnyConnect客户端 **AllowLocalLanAccess** 中启用。所有拆分排除隧道都被视为本地局域网访问。要使用拆分隧道的排除功能，必须在AnyConnect VPN客户端首选项中启用 **AllowLocalLanAccess** 首选项。默认情况下，本地局域网访问处于禁用状态。

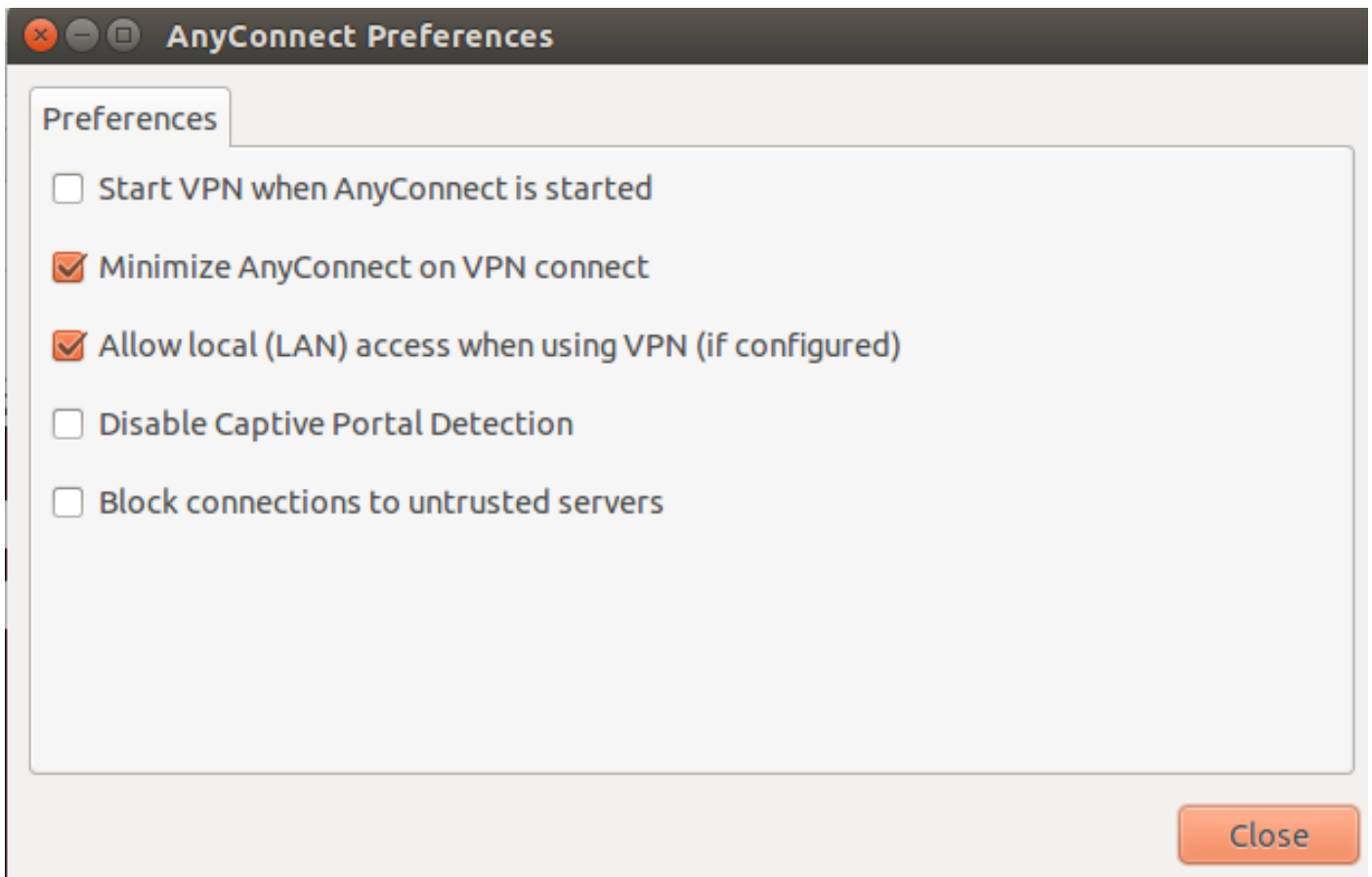
要允许本地局域网访问并因此使用拆分排除隧道，网络管理员可以在配置文件中将其启用，或者用户可以在首选项设置中将其启用（请参阅下一部分中的图像）。为了允许本地LAN访问，如果在安全网关上启用了分割隧道并配置了 `split-tunnel-policy exclude specified` 策略，用户将选择 **Allow Local LAN access** 复选框。此外，如果使用 `<LocalLanAccess UserControllable="true">true</LocalLanAccess>` 允许本地LAN访问，则可以配置VPN客户端配置文件。

用户首选项

以下是您必须在Cisco AnyConnect安全移动客户端的Preferences选项卡中进行选择才能允许本地LAN访问。



在Linux上



XML 配置文件示例

以下是如何配置 XML 格式 VPN 客户端配置文件的示例。

```
<?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>
<RSA SecurIDIntegration 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>
```

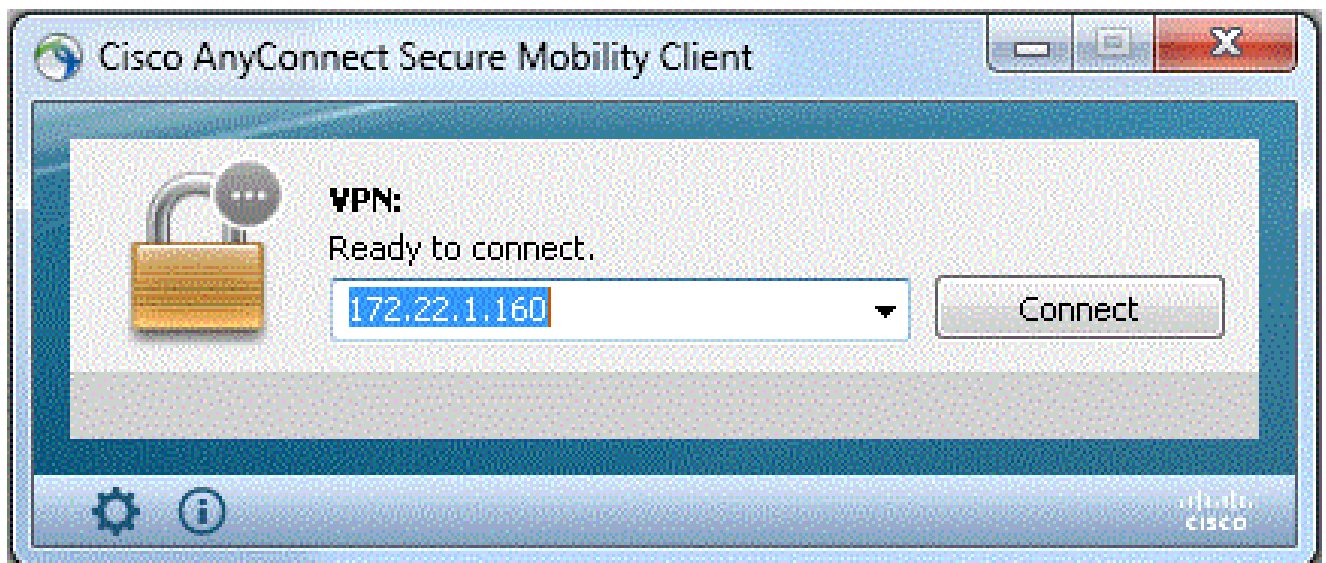
验证

要验证您的配置，请完成以下部分中的步骤：

- [查看 DART](#)
- [通过 Ping 测试本地 LAN 访问](#)

将您的 Cisco AnyConnect Secure Mobility Client 连接到 ASA，以验证您的配置。

- 从服务器列表中选择连接条目，并单击 **Connect**。



- 选择 Advanced Window for All Components > Statistics... 以显示隧道模式。

Statistics

VPN

Virtual Private Network (VPN)

Statistics | Route Details | Firewall | Message History


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

Reset Export Stats...

在Linux上

Cisco AnyConnect Secure Mobility Client Statistics

Statistics | Route Details



Connection Information		Address Information	
State:	Connected	Client (IPv4):	20.20.20.1
Connection Mode (IPv4):	Split Exclude	Server:	10.48.67.223
Connection Mode (IPv6):	Drop All Traffic	Client (IPv6):	Not Available
Duration:	00:16:22	Transport Information	
Session Disconnect:	None	Protocol:	DTLS
Bytes		Cipher:	RSA_AES_256_SHA1
Sent:	0	Compression:	None
Received:	20550	Proxy Address:	No Proxy
Frames		Feature Configuration	
Sent:	0	FIPS Mode:	Disabled
Received:	5	Trusted Network Detection:	Disabled
Control Frames			
Sent:	132		
Received:	65		

- 点击 **Route Details** 选项卡以查看Cisco AnyConnect安全移动客户端仍可对其进行本地访问的路由。


在本示例中，客户端被允许对 10.150.52.0/22 和 169.254.0.0/16 进行本地局域网访问，而所有其他流量都经过加密并通过隧道发送。



在Linux上

Cisco AnyConnect Secure Mobility Client Statistics

Statistics **Route Details**



Non-Secured Routes

Destination	Subnet Mask
192.168.171.0	24

Secured Routes

Destination	Subnet Mask
0.0.0.0	0

Cisco AnyConnect 安全移动客户端

当通过 Diagnostics and Reporting Tool (DART) 捆绑包查看 AnyConnect 日志时，您可以确定是否设置了允本地局域网访问的参数。

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
 RSA SecurID Integration: Automatic
 Windows Logon Enforcement: SingleLocalLogon
 Windows VPN Establishment: LocalUsersOnly
 Proxy Settings: Native
 AllowLocalProxyConnections: true
 PPP Exclusion: 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
SafeWordSoftTokenIntegration: false
AllowIPsecOverSSL: false
ClearSmartcardPin: true

通过 Ping 测试本地 LAN 访问

测试VPN客户端在通过隧道连接到VPN头端时是否仍可访问本地LAN的另一种方法是：在Microsoft Windows命令行中使用 **ping** 命令。下面是一个示例，其中客户端的本地局域网为192.168.0.0/24，网络中存在另一台 IP 地址为 192.168.0.3 的主机。

```
<#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
```

在Linux上

```
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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

无法按名称打印或浏览

当 VPN 客户端已连接且已针对本地 LAN 访问配置后，在本地 LAN 上无法按名称打印或浏览。可以使用以下两种选择方法来处理此情况：

- 按 IP 地址浏览或打印。
 - 要进行浏览，请使用语法 `\\x.x.x.x` (其中 `x.x.x.x` 是主机计算机的 IP 地址)，而不要使用语法 `\\sharename`。
 - 要进行打印，请更改网络打印机的属性，以使用 IP 地址而不是名称。例如，请不要使用语法 `\\sharename\printername`，而应使用 `\\x.x.x.x\printername`，其中 `x.x.x.x` 是 IP 地址。
- 创建或修改 VPN 客户端 LMHOSTS 文件。通过 Microsoft Windows PC 上的 LMHOSTS 文件，您可以在主机名和 IP 地址之间创建静态映射。例如，LMHOSTS 文件可能如下所示：

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

在 Microsoft Windows XP Professional Edition 中，LMHOSTS 文件位于 `%SystemRoot%\System32\Drivers\Etc` 中。有关详细信息，请参阅 Microsoft 文档。

相关信息

- [CLI手册3：思科ASA系列VPN CLI配置指南，9.17](#)
- [Cisco ASA 5500-X系列防火墙](#)
- [技术支持和文档 - Cisco Systems](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。