Exemplo de Configuração de Acesso de Cliente VPN e AnyConnect para LAN Local

Contents

Introduction

Este documento descreve como permitir que o Cisco VPN Client ou o Cisco AnyConnect Secure Mobility Client **acessem somente** sua LAN local enquanto são encapsulados em um Cisco Adaptive Security Appliance (ASA) 5500 Series ou no ASA 5500-X Series. Essa configuração permite que os Cisco VPN Clients ou o Cisco AnyConnect Secure Mobility Client acessem de forma segura os recursos corporativos através de IPsec, Secure Sockets Layer (SSL) ou Internet Key Exchange Version 2 (IKEv2) e ainda dá ao cliente a capacidade de realizar atividades como imprimir onde o cliente está localizado. Se for permitido, o tráfego destinado à Internet ainda será encapsulado para o ASA.

> Nota: Esta não é uma configuração para tunelamento dividido, em que o cliente tem acesso não criptografado à Internet enquanto está conectado ao ASA ou PIX. Refira ao PIX/ASA 7.x: Allow Split Tunneling for VPN Clients no ASA Configuration Example para obter informações sobre como configurar o tunelamento dividido no ASA.

Prerequisites

Requirements

Este documento pressupõe que já existe uma configuração de VPN de acesso remoto funcional no ASA.

Consulte o PIX/ASA 7.x como um Servidor VPN Remoto usando o Exemplo de Configuração de ASDM para o Cisco VPN Client se um ainda não estiver configurado.

Consulte Exemplo de Configuração do ASA 8.x VPN Access com o AnyConnect SSL VPN Client para o Cisco AnyConnect Secure Mobility Client se um ainda não estiver configurado.

Componentes Utilizados

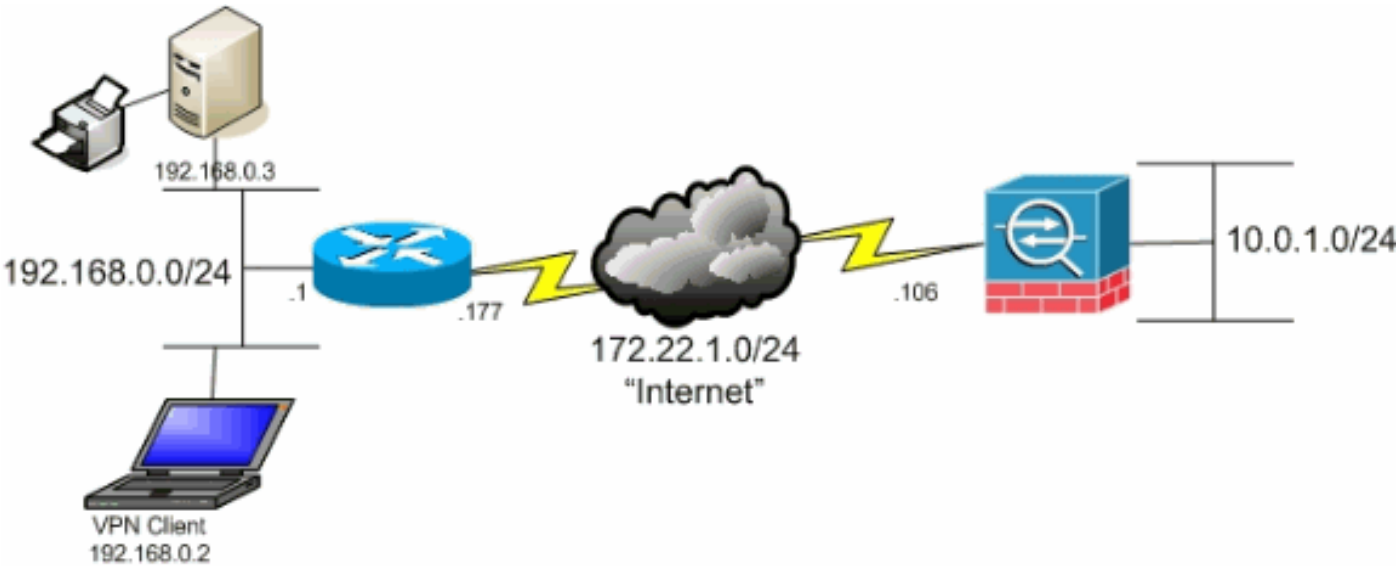
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASA 5500 Series versão 9(2)1
- Cisco Adaptive Security Device Manager (ASDM) versão 7.1(6)
- Cisco VPN Client Versão 5.0.07.0440
- Cisco AnyConnect Secure Mobility Client versão 3.1.05152

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. 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.

Diagrama de Rede

O cliente está localizado em uma rede típica de Escritório Pequeno / Escritório Doméstico (SOHO - Small Office / Home Office) e se conecta através da Internet ao escritório central.



Informações de Apoio

Ao contrário de um cenário de tunelamento dividido clássico no qual todo o tráfego da Internet é enviado sem criptografia, quando você habilita o acesso de LAN local para clientes VPN, ele permite que esses clientes se comuniquem sem criptografia somente com dispositivos na rede em que estão localizados. Por exemplo, um cliente que tem permissão de acesso à LAN local enquanto está conectado ao ASA de casa pode imprimir em sua própria impressora, mas não acessar a Internet sem primeiro enviar o tráfego pelo túnel.

Uma lista de acesso é usada para permitir o acesso à LAN local da mesma forma que o tunelamento dividido é configurado no ASA. No entanto, em vez de definir quais redes *devem ser* criptografadas, a lista de acesso nesse caso define quais redes *não devem ser* criptografadas. Além disso, ao contrário do cenário de tunelamento dividido, as redes reais na lista não precisam ser conhecidas. Em vez disso, o ASA fornece uma rede padrão de 0.0.0.0/255.255.255.255, que é entendida como a LAN local do cliente.

> Nota: Quando o cliente está conectado e configurado para acesso à LAN local, você *não pode imprimir ou procurar por nome* na LAN local. No entanto, você pode navegar ou imprimir por endereço IP. Consulte a seção Solução de problemas deste documento para obter mais informações, bem como soluções alternativas para esta situação.

Configurar o acesso de LAN local para clientes VPN ou o AnyConnect Secure Mobility Client

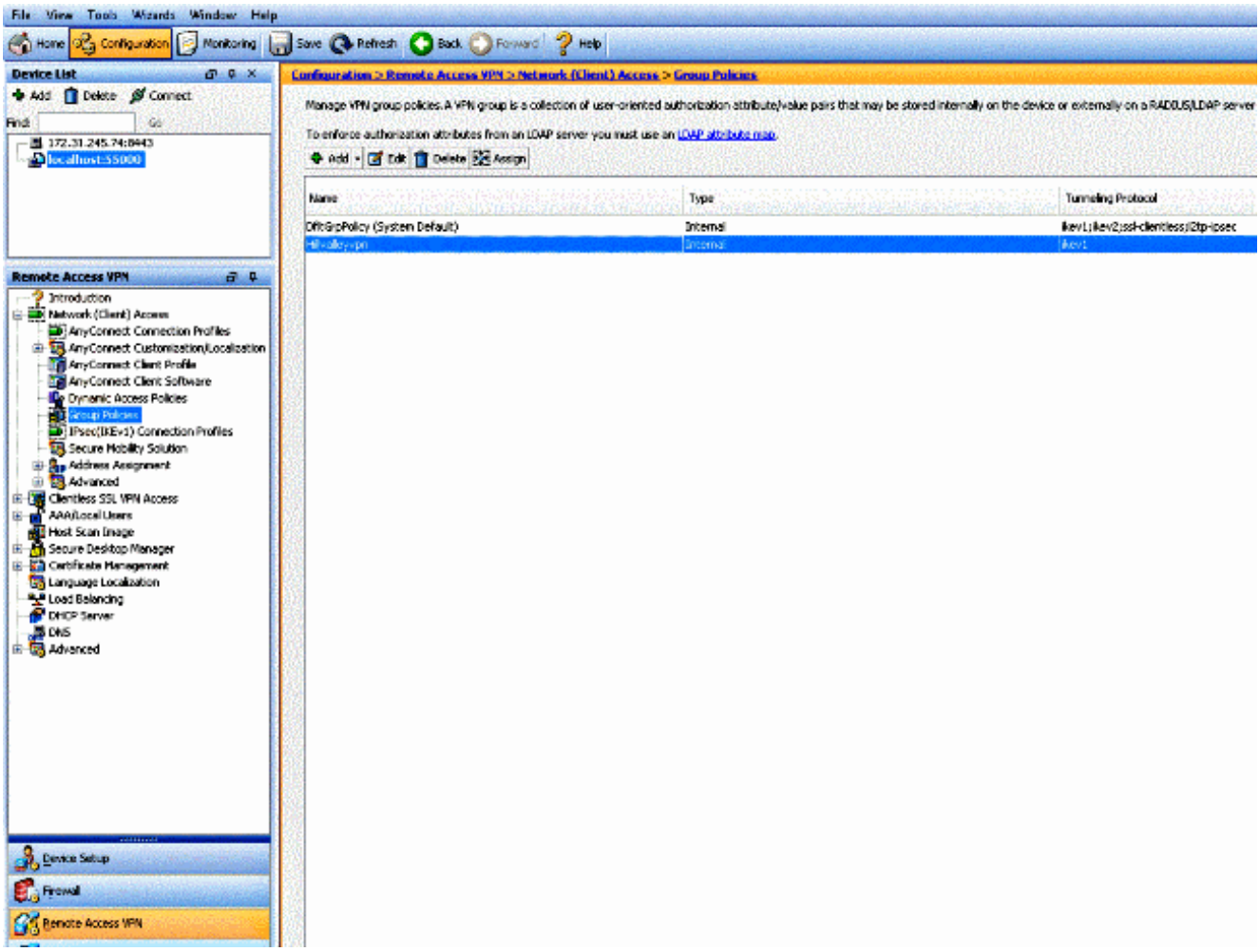
Conclua estas tarefas para permitir que os Cisco VPN Clients ou os Cisco AnyConnect Secure Mobility Clients acessem a LAN local enquanto estão conectados ao ASA:

- Configure o ASA via ASDM ou Configure o ASA via CLI
- Configurar o Cisco AnyConnect Secure Mobility Client

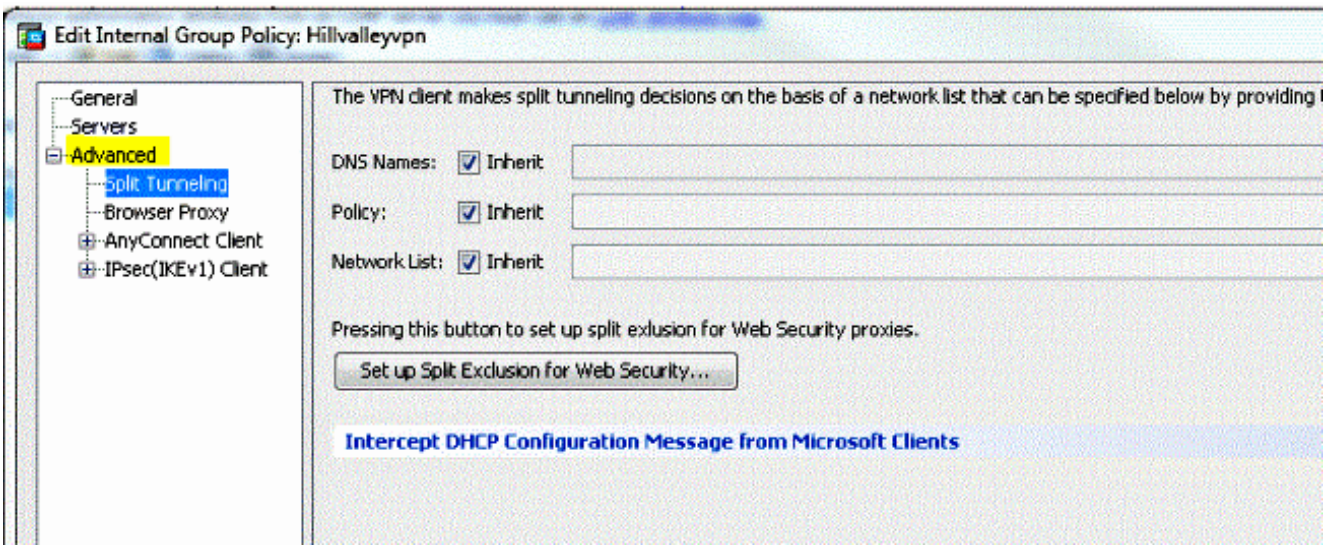
Configurar o ASA via ASDM

Conclua estes passos no ASDM para permitir que os VPN Clients tenham acesso à LAN local enquanto estão conectados ao ASA:

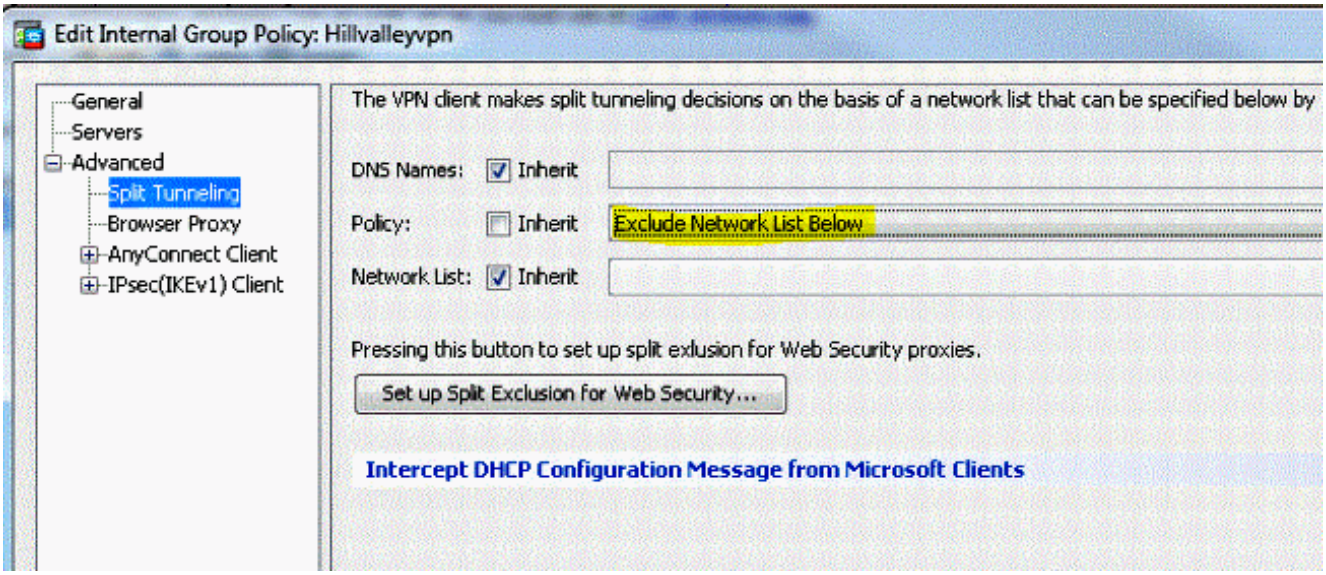
1. Escolha **Configuration > Remote Access VPN > Network (Client) Access > Group Policy** e selecione a Group Policy na qual deseja habilitar o acesso à LAN local. Em seguida, clique em **Editar**.



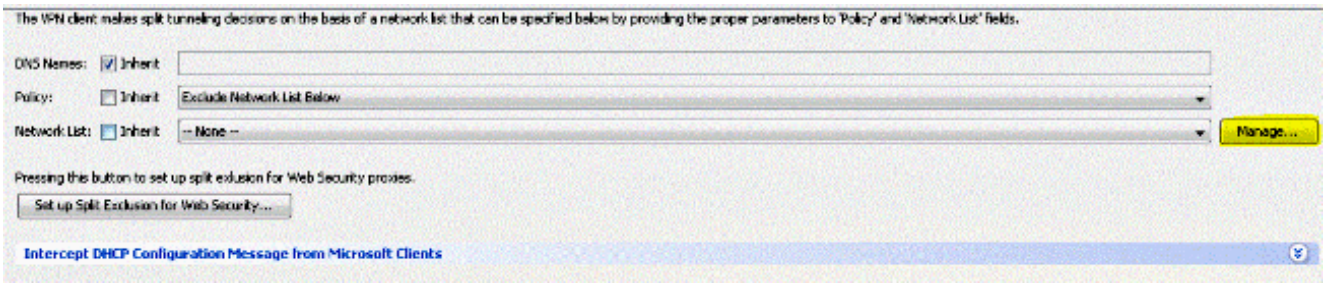
2. Vá para **Advanced > Split Tunneling**.



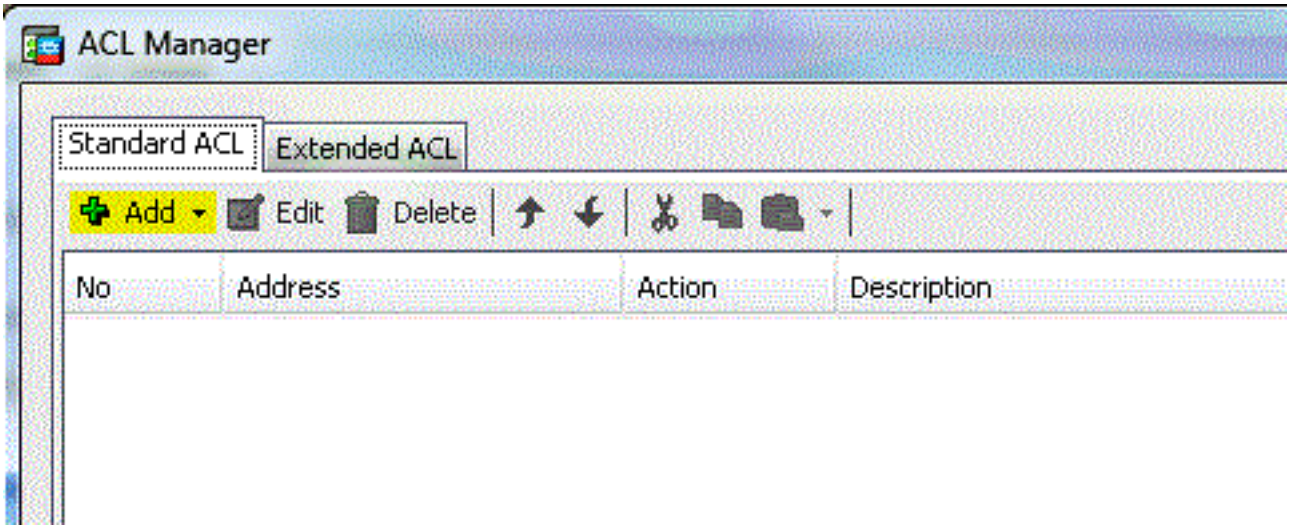
3. Desmarque a caixa **Herdar** para Política e escolha **Excluir lista de rede abaixo**.



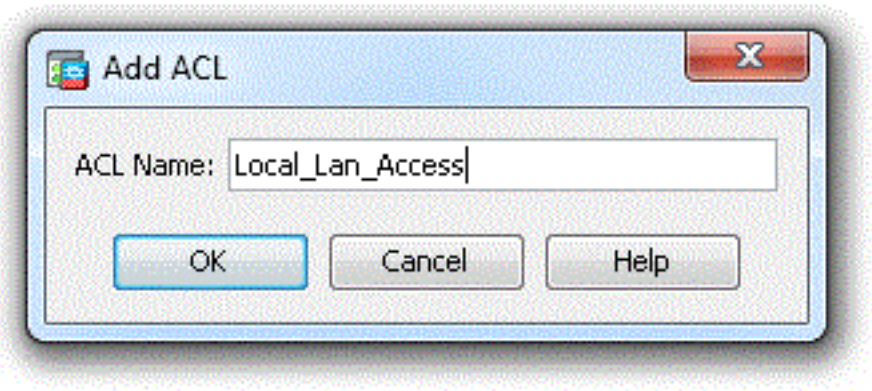
4. Desmarque a caixa **Inherit** para Network List (Lista de rede) e clique em **Manage (Gerenciar)** para iniciar o Access Control List (ACL) Manager.



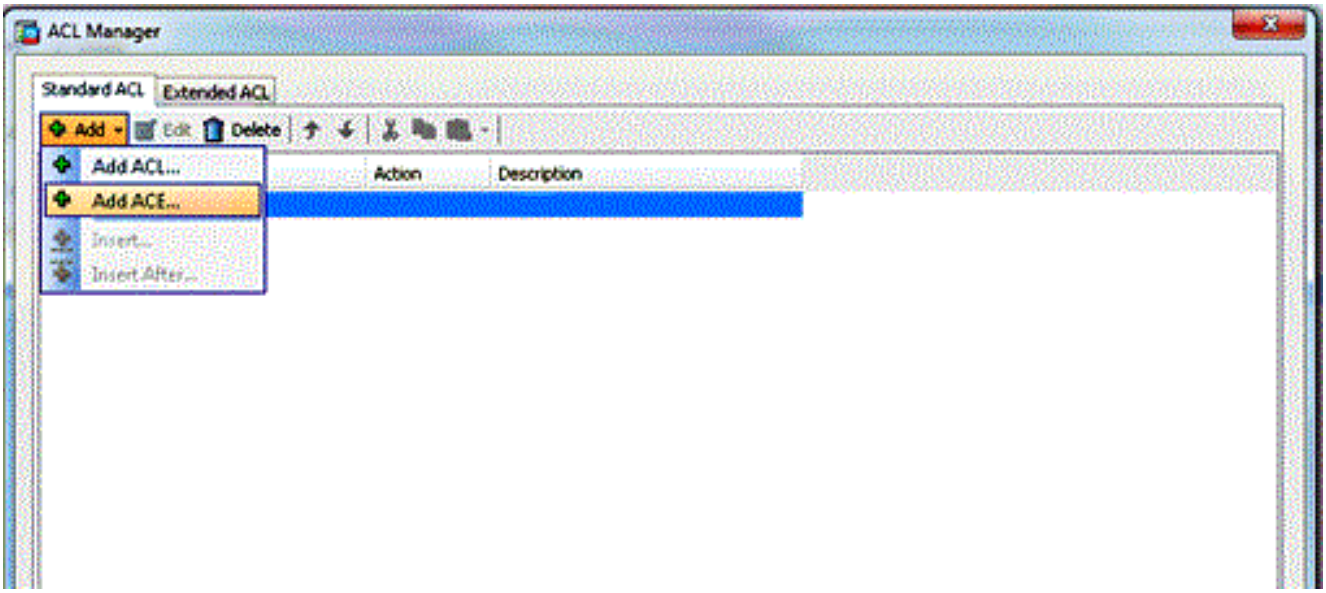
5. No ACL Manager, escolha **Add > Add ACL...** para criar uma nova lista de acesso.



6. Forneça um nome para a ACL e clique em OK.

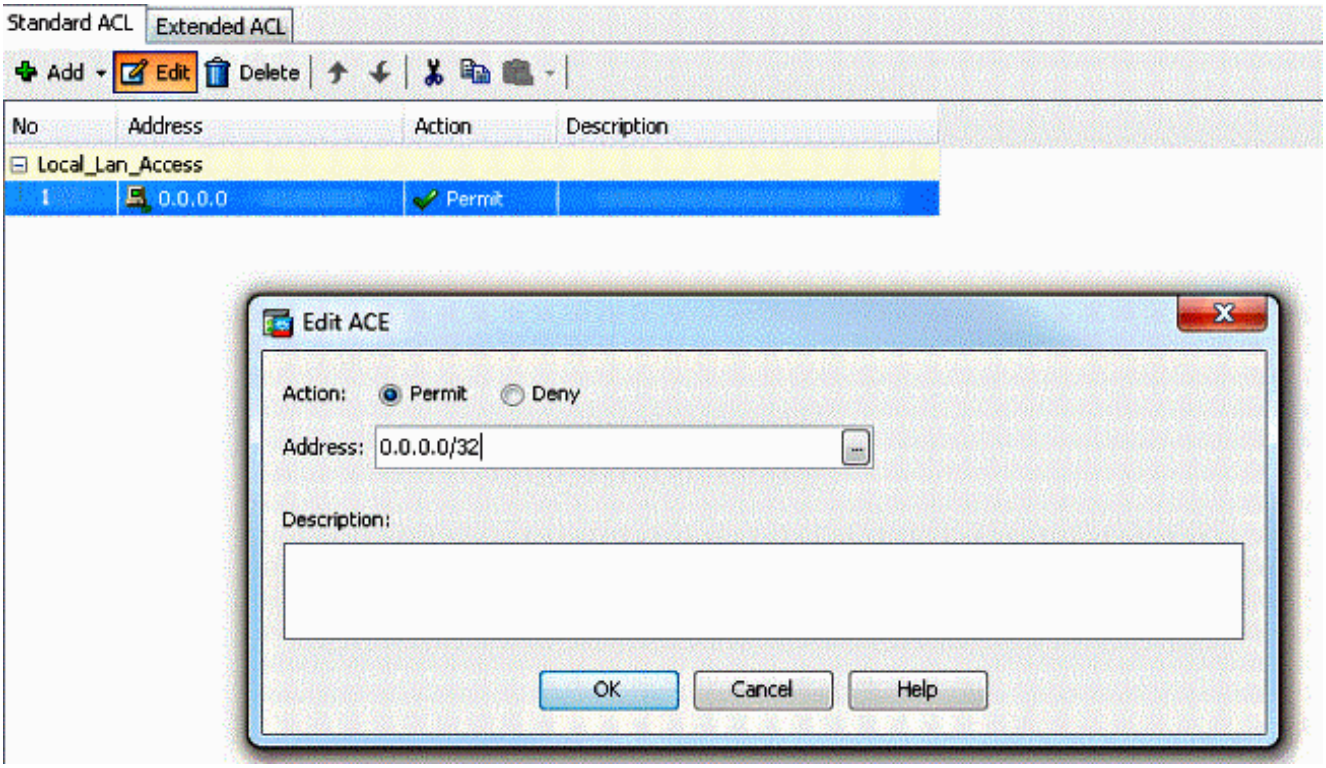


7. Depois que a ACL for criada, escolha **Add > Add ACE...** para adicionar uma entrada de controle de acesso (ACE).

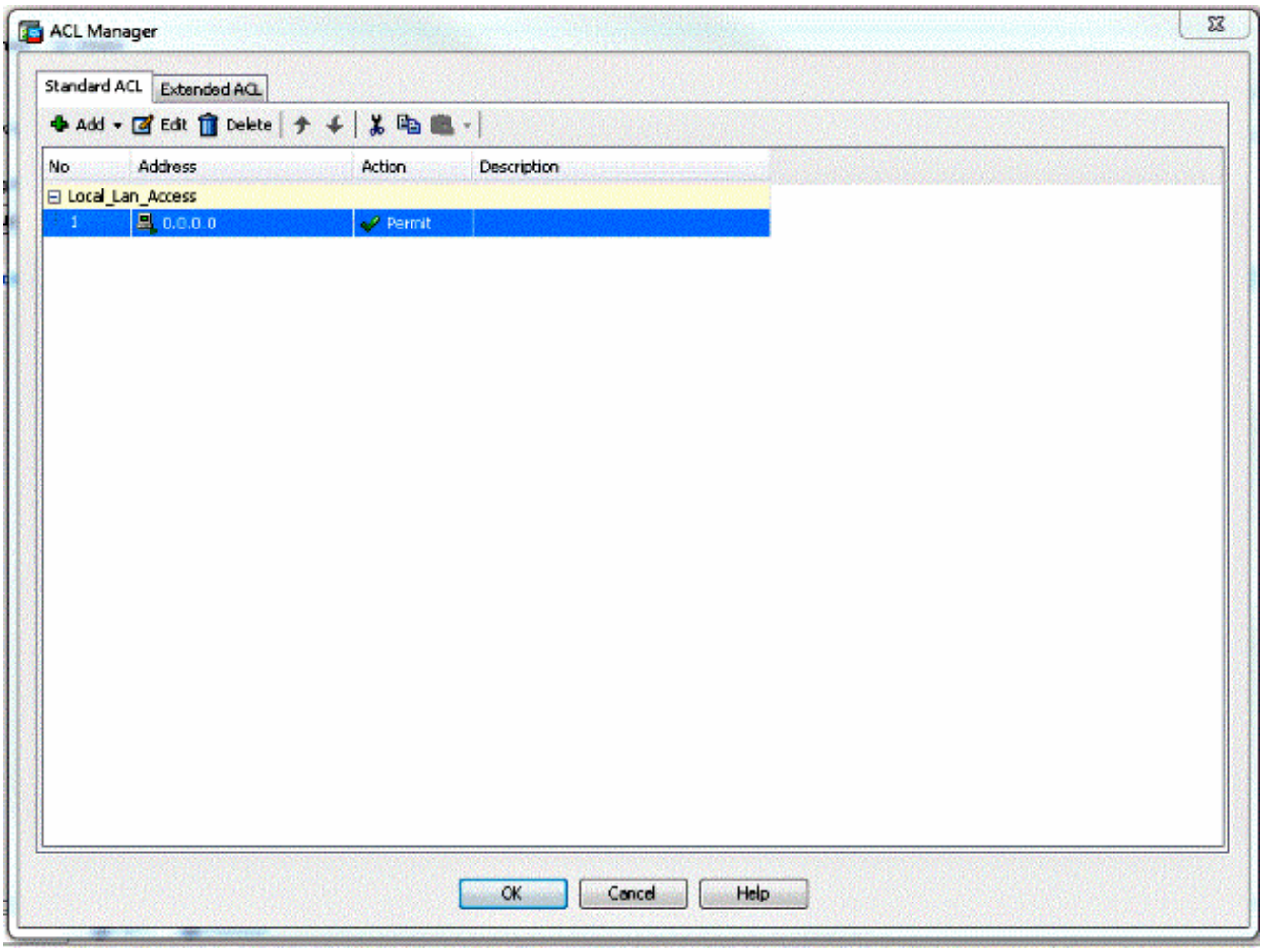


8. Defina a ACE que corresponde à LAN local do cliente.

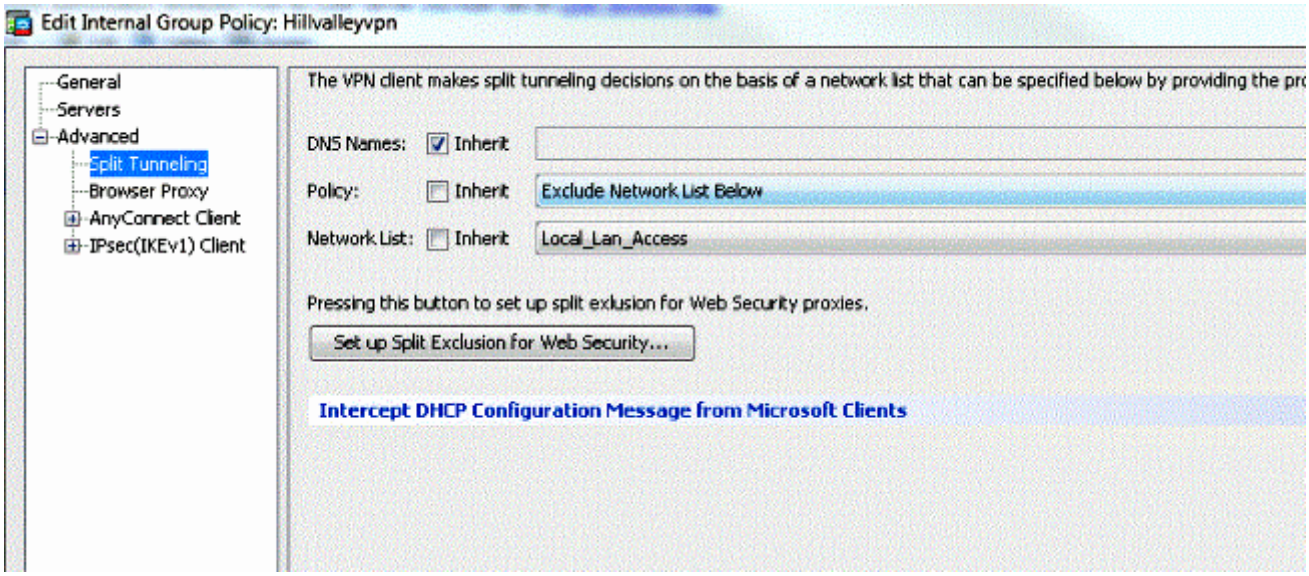
   Escolha **Permitir**.Escolha o endereço IP 0.0.0.0Escolha uma máscara de rede de **/32**.*(Opcional)* Forneça uma descrição.Click OK.



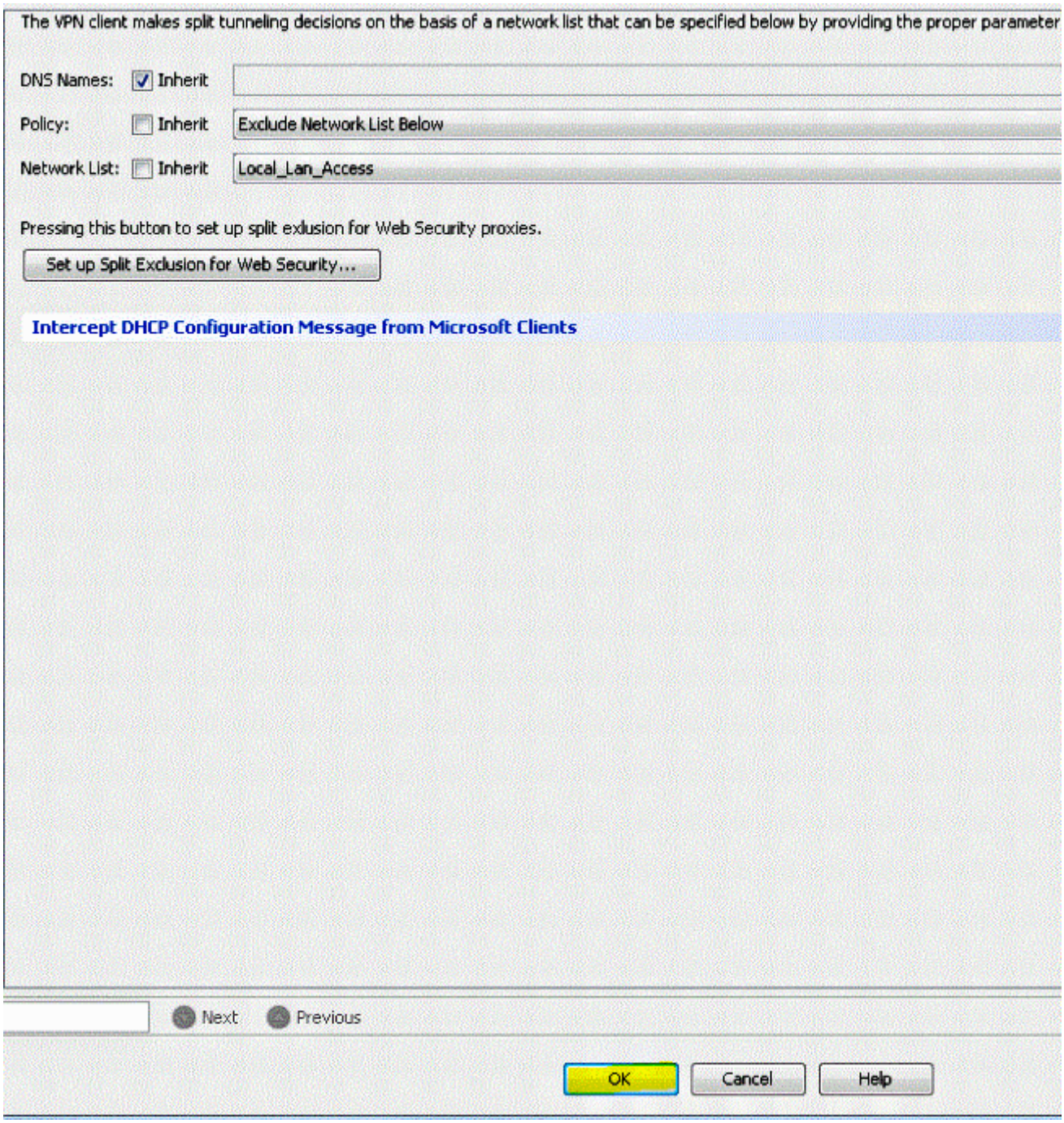
9. Clique em OK para sair do ACL Manager.



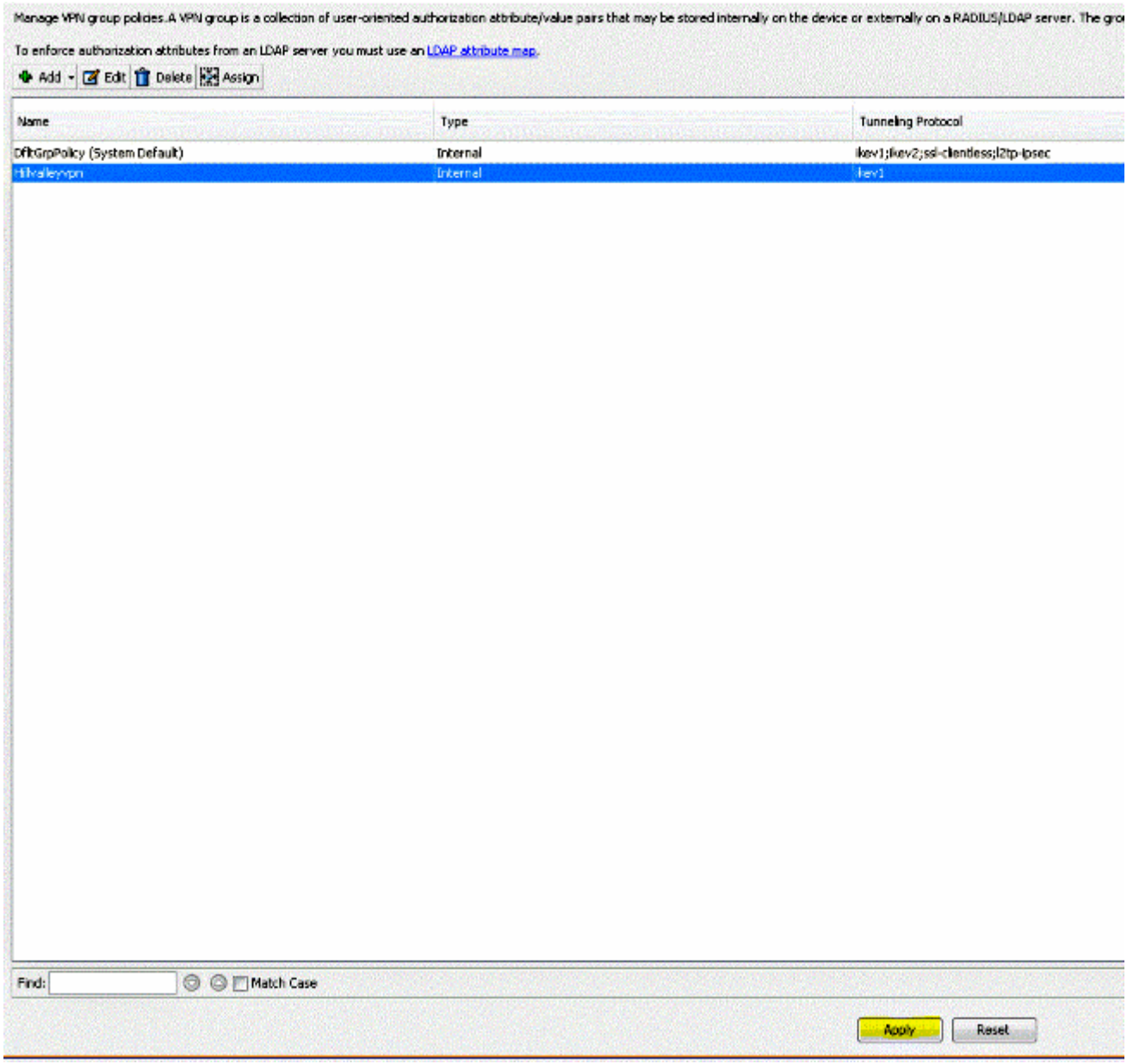
10. Certifique-se de que a ACL que você acabou de criar esteja selecionada para a Lista de rede de túnel dividido.



11. Clique em OK para retornar à configuração da Política de Grupo.



12. Clique em **Apply** e em **Send** (se necessário) para enviar os comandos ao ASA.



Configurar o ASA via CLI

Em vez de usar o ASDM, você pode concluir estas etapas na CLI do ASA para permitir que os VPN Clients tenham acesso à LAN local enquanto estão conectados ao ASA:

1. Entre no modo de configuração.

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

2. Crie a lista de acesso para permitir o acesso à LAN local.

```
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
```

Cuidado: Devido às alterações na sintaxe da ACL entre as versões 8.x a 9.x do software ASA, esta ACL não é mais permitida e os administradores verão esta mensagem de erro

quando tentarem configurá-la:

```
rtpvpnoutbound6(config)# access-list test standard permit host
0.0.0.0
ERRO: endereço IP inválido
```

A única coisa permitida é:

```
rtpvpnoutbound6(config)# access-list test standard permit any4
```

Este é um problema conhecido e foi tratado pela ID de bug da Cisco CSCut3131. Atualize para uma versão com a correção para este bug para poder configurar o acesso de LAN local.

3. Entre no modo de configuração de Diretiva de Grupo para a política que deseja modificar.

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

4. Especifique a política de túnel dividido. Nesse caso, a política é **excluída**.

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

5. Especifique a lista de acesso de túnel dividido. Nesse caso, a lista é **Local_LAN_Access**.

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

6. Emita este comando:

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

7. Associe a política do grupo ao grupo do túnel.

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

8. Saia dos dois modos de configuração.

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

9. Salve a configuração na RAM não volátil (NVRAM) e pressione Enter quando avisado para especificar o nome de arquivo de origem.

```
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#
```

Configurar o Cisco AnyConnect Secure Mobility Client

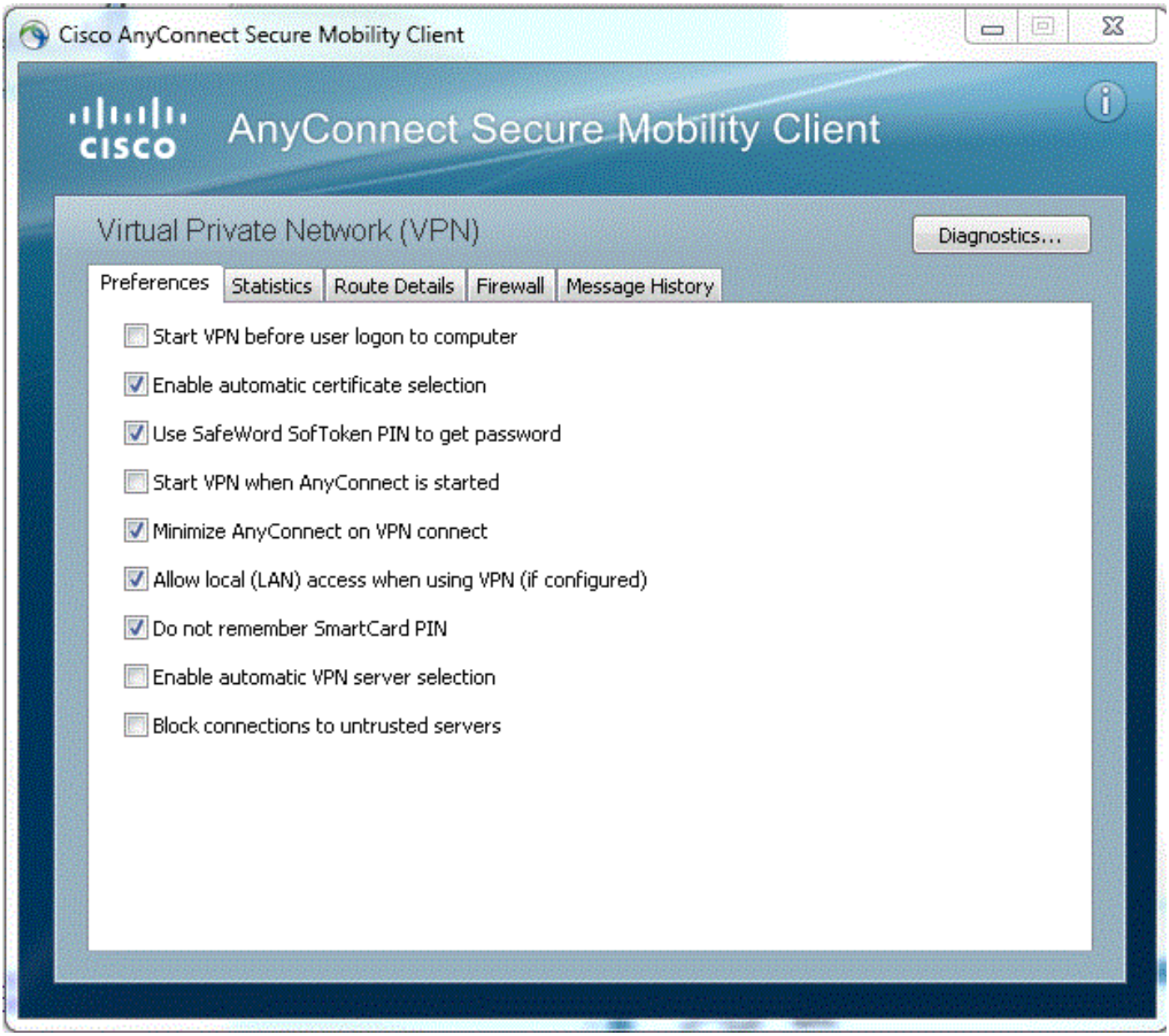
Para configurar o Cisco AnyConnect Secure Mobility Client, consulte a seção Estabelecer a conexão VPN SSL com SVC do **ASA 8.x : Permitir tunelamento dividido para AnyConnect VPN Client no exemplo de configuração do ASA**.

O tunelamento dividido-excluídos requer que você habilite **AllowLocalLanAccess** no AnyConnect Client. Todo o tunelamento split-exclude é considerado como acesso de LAN local. Para usar o recurso de exclusão de tunelamento dividido, você deve habilitar a preferência **AllowLocalLanAccess** nas **preferências do AnyConnect VPN Client**. Por padrão, o acesso à LAN local está desabilitado.

Para permitir o acesso à LAN local e, portanto, o tunelamento dividido-excluídos, um administrador de rede pode ativá-lo no perfil ou os usuários podem ativá-lo nas configurações de preferências (consulte a imagem na próxima seção). Para permitir o acesso à LAN local, um usuário seleciona a caixa de seleção **Permitir acesso à LAN Local** se o tunelamento dividido estiver ativado no gateway seguro e configurado com a política **especificada de exclusão de política de túnel dividido**. Além disso, você pode configurar o perfil do cliente VPN se o acesso à LAN local for permitido com **<LocalLanAccess UserControllable="true">true</LocalLanAccess>**.

Preferências do usuário

Aqui estão as seleções que você deve fazer na guia Preferências no Cisco AnyConnect Secure Mobility Client para permitir o acesso à LAN local.



Exemplo de perfil XML

Aqui está um exemplo de como configurar o perfil do cliente VPN com 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>
```

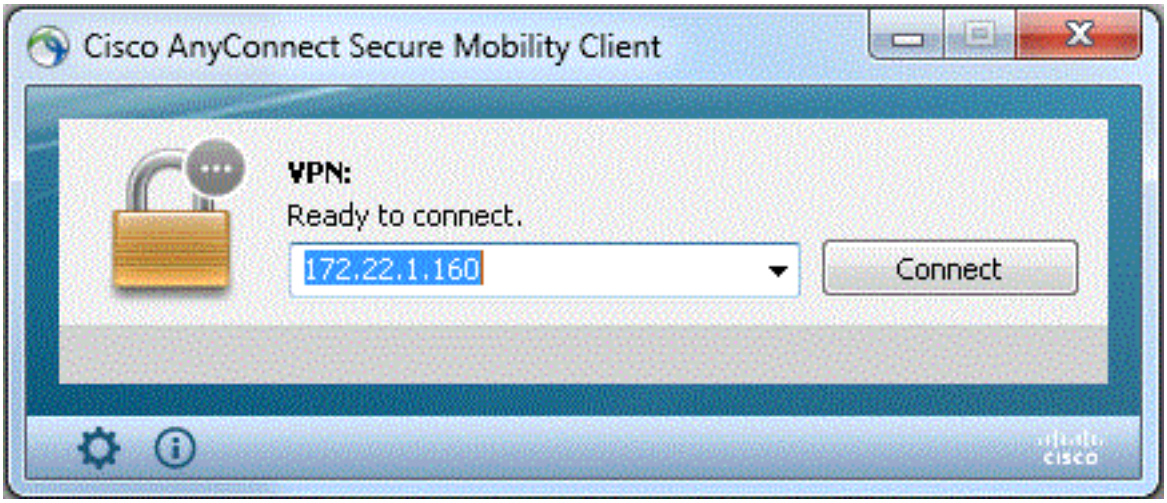
Verificar

Conclua as etapas nessas seções para verificar sua configuração.

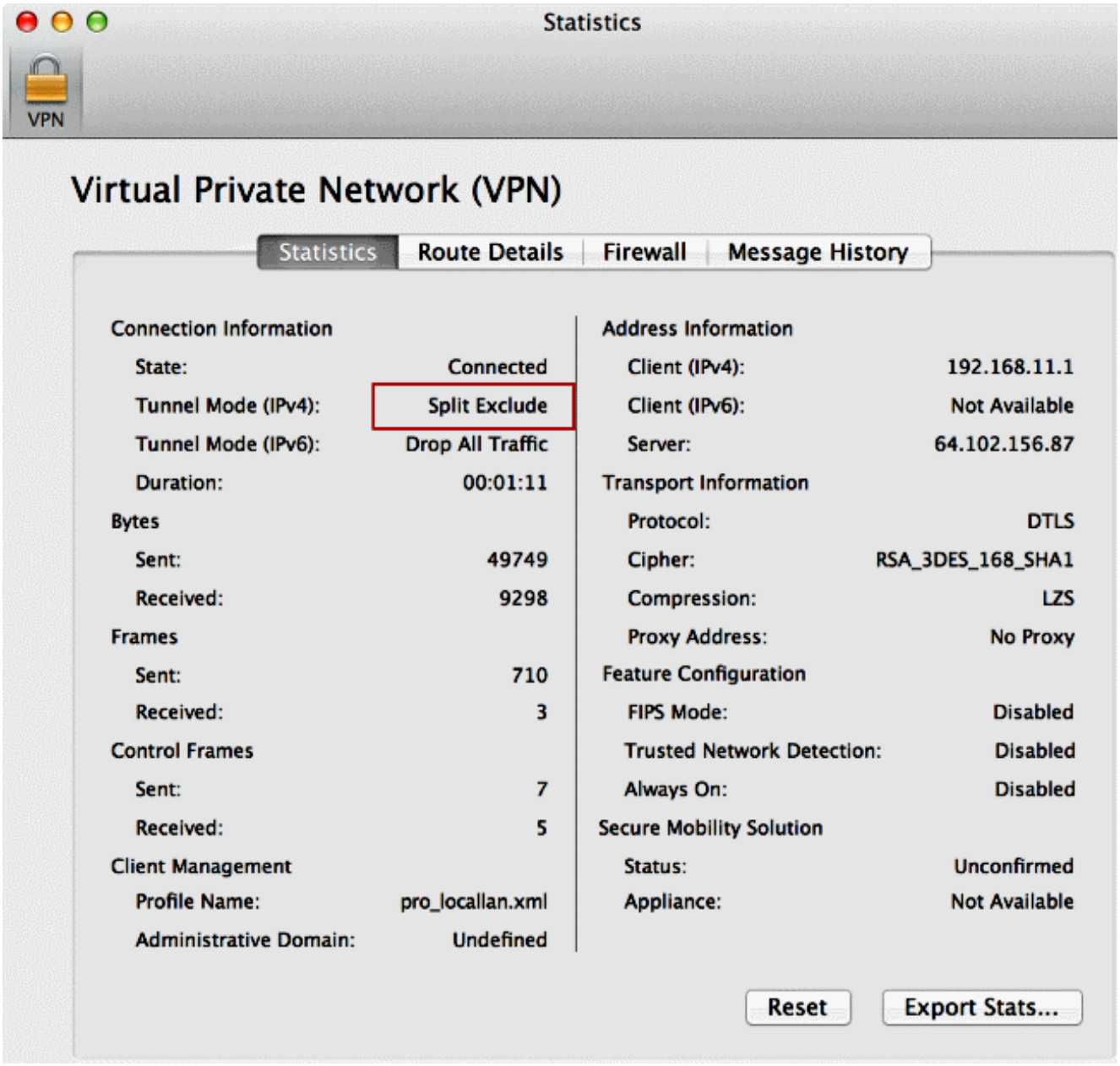
- Exibir o DART
- Testar o acesso à LAN local com ping

Conecte seu Cisco AnyConnect Secure Mobility Client ao ASA para verificar sua configuração.

1. Escolha sua entrada de conexão na lista de servidores e clique em **Conectar**.

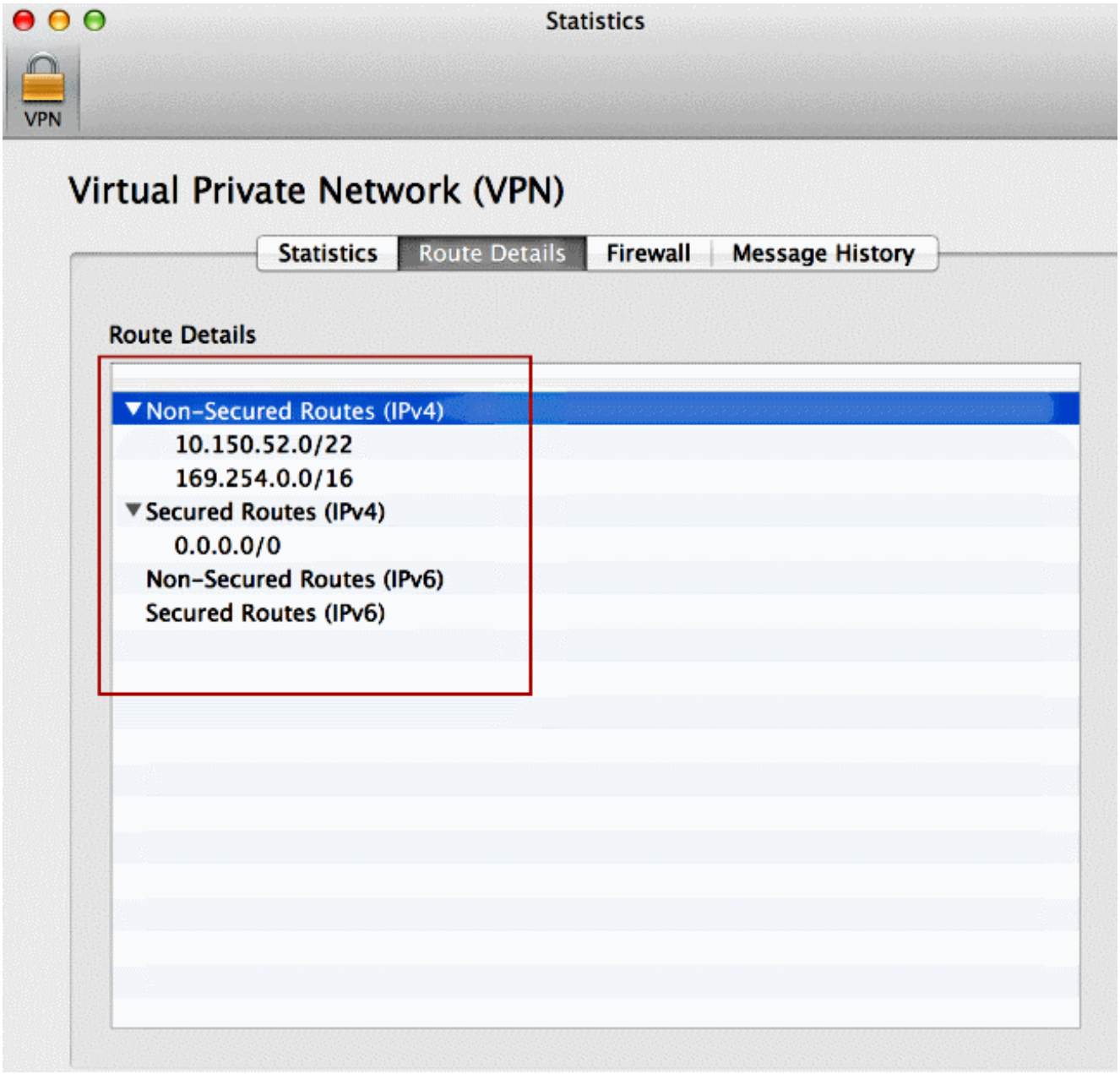


2. Escolha **Janela Avançada para Todos os Componentes > Estatísticas...** para exibir o modo de túnel.



3. Clique na guia **Route Details** para ver as rotas para as quais o Cisco AnyConnect Secure Mobility Client ainda tem acesso local.

   Neste exemplo, o cliente tem permissão de acesso à LAN local para 10.150.52.0/22 e 169.254.0.0/16 enquanto todo o tráfego restante é criptografado e enviado através do túnel.



Cisco AnyConnect Secure Mobility Client

Ao examinar os logs do AnyConnect a partir do pacote da ferramenta de diagnóstico e relatório (DART), você pode determinar se o parâmetro que permite o acesso local à LAN está definido ou não.

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

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



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

Testar o acesso à LAN local com ping

Uma maneira adicional de testar se o VPN Client ainda tem acesso de LAN local enquanto está em túnel para o headend de VPN é usar o comando **ping** na linha de comando do Microsoft Windows. Aqui está um exemplo em que a LAN local do cliente é 192.168.0.0/24 e outro host está presente na rede com um endereço IP 192.168.0.3.

```
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
```

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Não é possível imprimir ou procurar por nome

Quando o VPN Client está conectado e configurado para acesso à LAN local, você *não pode imprimir ou procurar por nome* na LAN local. Há duas opções disponíveis para contornar essa situação:

- Procure ou imprima por endereço IP.

  Para navegar, em vez da sintaxe **\\sharename**, use a sintaxe **\\x.x.x.x** onde *x.x.x.x* é o endereço IP do computador.

  Para imprimir, altere as propriedades da impressora de rede para usar um endereço IP em vez de um nome. Por exemplo, em vez da sintaxe **\\sharename\printername**, use **\\x.x.x\printername**, onde *x.x.x.x* é um endereço IP.
- Crie ou modifique o arquivo LMHOSTS do cliente VPN. Um arquivo LMHOSTS em um PC com Microsoft Windows permite criar mapeamentos estáticos entre nomes de host e endereços IP. Por exemplo, um arquivo LMHOSTS pode ter a seguinte aparência:

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

  No Microsoft Windows XP Professional Edition, o arquivo LMHOSTS está localizado em **%SystemRoot%\System32\Drivers\Etc**. Consulte a documentação da Microsoft ou o artigo 314108 da base de conhecimento da Microsoft para obter mais informações.

Informações Relacionadas

- PIX/ASA 7.x como um Servidor VPN Remoto usando Exemplo de Configuração de ASDM
- Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM
- Dispositivos de segurança adaptáveis Cisco ASA 5500 Series
- Suporte Técnico e Documentação - Cisco Systems