Konfigurationsbeispiel für VPN-Client und AnyConnect-Client-Zugriff auf lokales LAN

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der Cisco VPN Client oder der Cisco AnyConnect Secure Mobility Client **nur** auf ihr lokales LAN zugreifen darf, wenn sie in eine Cisco Adaptive Security Appliance (ASA) 5500 oder die Serie ASA 5500-X getunnelt werden. Diese Konfiguration ermöglicht Cisco VPN-Clients oder den Cisco AnyConnect Secure Mobility Client den sicheren Zugriff auf Unternehmensressourcen über IPsec, Secure Sockets Layer (SSL) oder Internet Key Exchange Version 2 (IKEv2) und gibt dem Client weiterhin die Möglichkeit, Aktivitäten wie das Drucken am Standort des Clients auszuführen. Wenn dies zulässig ist, wird Datenverkehr, der für das Internet bestimmt ist, weiterhin an die ASA getunnelt.

> **Hinweis**: Hierbei handelt es sich nicht um eine Konfiguration für Split-Tunneling, bei der der Client während der Verbindung mit ASA oder PIX unverschlüsselten Zugriff auf das Internet hat. Siehe PIX/ASA 7.x: Zulassen von Split Tunneling für VPN-Clients im ASA-Konfigurationsbeispiel für Informationen zum Konfigurieren von Split-Tunneling auf der ASA.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass auf der ASA bereits eine funktionierende VPN-Konfiguration für den Remote-Zugriff vorhanden ist.

Weitere Informationen finden Sie unter PIX/ASA 7.x als Remote-VPN-Server mit ASDM-Konfigurationsbeispiel für den Cisco VPN-Client, falls dieser noch nicht konfiguriert ist.

Weitere Informationen für den Cisco AnyConnect Secure Mobility Client finden Sie unter ASA 8.x VPN Access mit dem Konfigurationsbeispiel des AnyConnect SSL VPN Client, falls dieser noch nicht konfiguriert ist.

Verwendete Komponenten

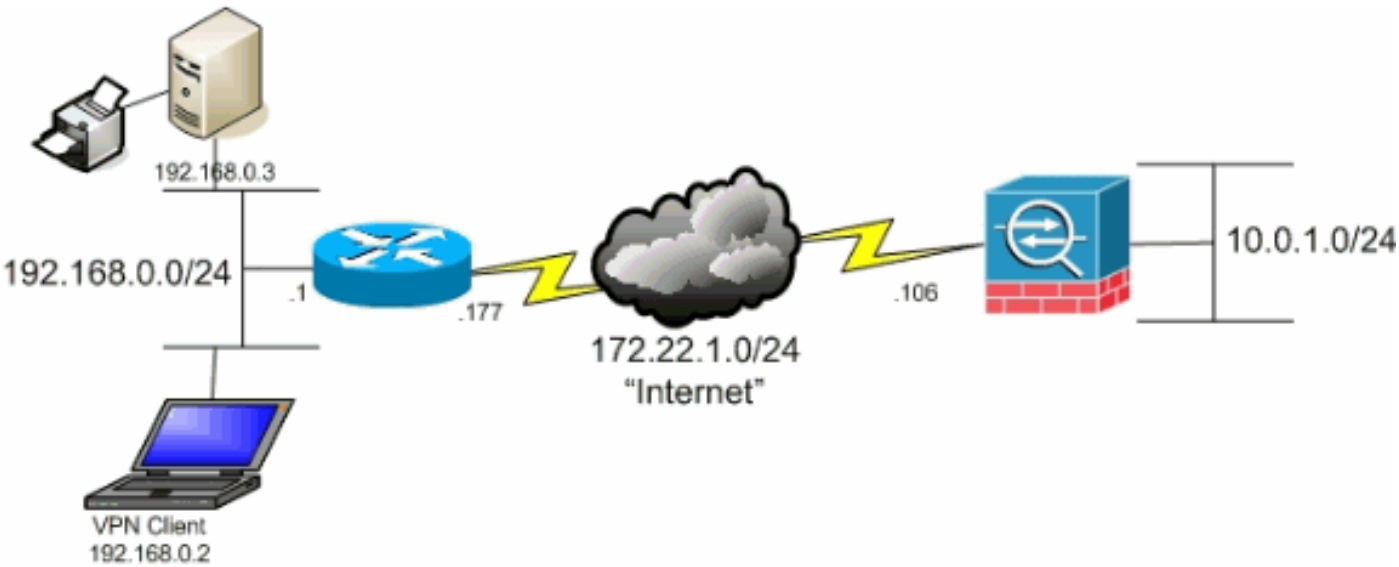
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Netzwerkdiagramm

Der Client befindet sich in einem typischen Netzwerk für kleine Büros/Heimbüros und stellt über das Internet eine Verbindung zur Hauptniederlassung her.



Hintergrundinformationen

Anders als bei einem klassischen Split-Tunneling-Szenario, bei dem der gesamte Internetdatenverkehr unverschlüsselt gesendet wird, ermöglicht es das Aktivieren des lokalen LAN-Zugriffs für VPN-Clients diesen Clients, unverschlüsselt mit nur Geräten im Netzwerk zu kommunizieren, in dem sie sich befinden. Beispielsweise kann ein Client, der lokalen LAN-Zugriff

erlaubt, während er von zu Hause aus mit der ASA verbunden ist, auf seinen eigenen Drucker drucken, aber nicht auf das Internet zugreifen, ohne zuerst den Datenverkehr über den Tunnel zu senden.

Eine Zugriffsliste wird verwendet, um lokalen LAN-Zugriff auf die gleiche Weise zuzulassen, wie Split-Tunneling auf der ASA konfiguriert wird. Anstatt jedoch zu definieren, welche Netzwerke verschlüsselt *werden sollen*, definiert die Zugriffsliste in diesem Fall, welche Netzwerke *nicht* verschlüsselt *werden sollten*. Anders als beim Split-Tunneling-Szenario müssen die tatsächlichen Netzwerke in der Liste ebenfalls nicht bekannt sein. Stattdessen stellt die ASA ein Standardnetzwerk von 0.0.0.0/255.255.255.255 bereit, das als lokales LAN des Clients verstanden wird.

> **Hinweis**: Wenn der Client angeschlossen und für den lokalen LAN-Zugriff konfiguriert ist, *können* Sie *nicht* im lokalen LAN *nach Namen drucken oder suchen*. Sie können jedoch nach IP-Adresse suchen oder drucken. Weitere Informationen sowie Problemumgehungen finden Sie im Abschnitt Problembehebung dieses Dokuments.

Konfigurieren des lokalen LAN-Zugriffs für VPN-Clients oder den AnyConnect Secure Mobility Client

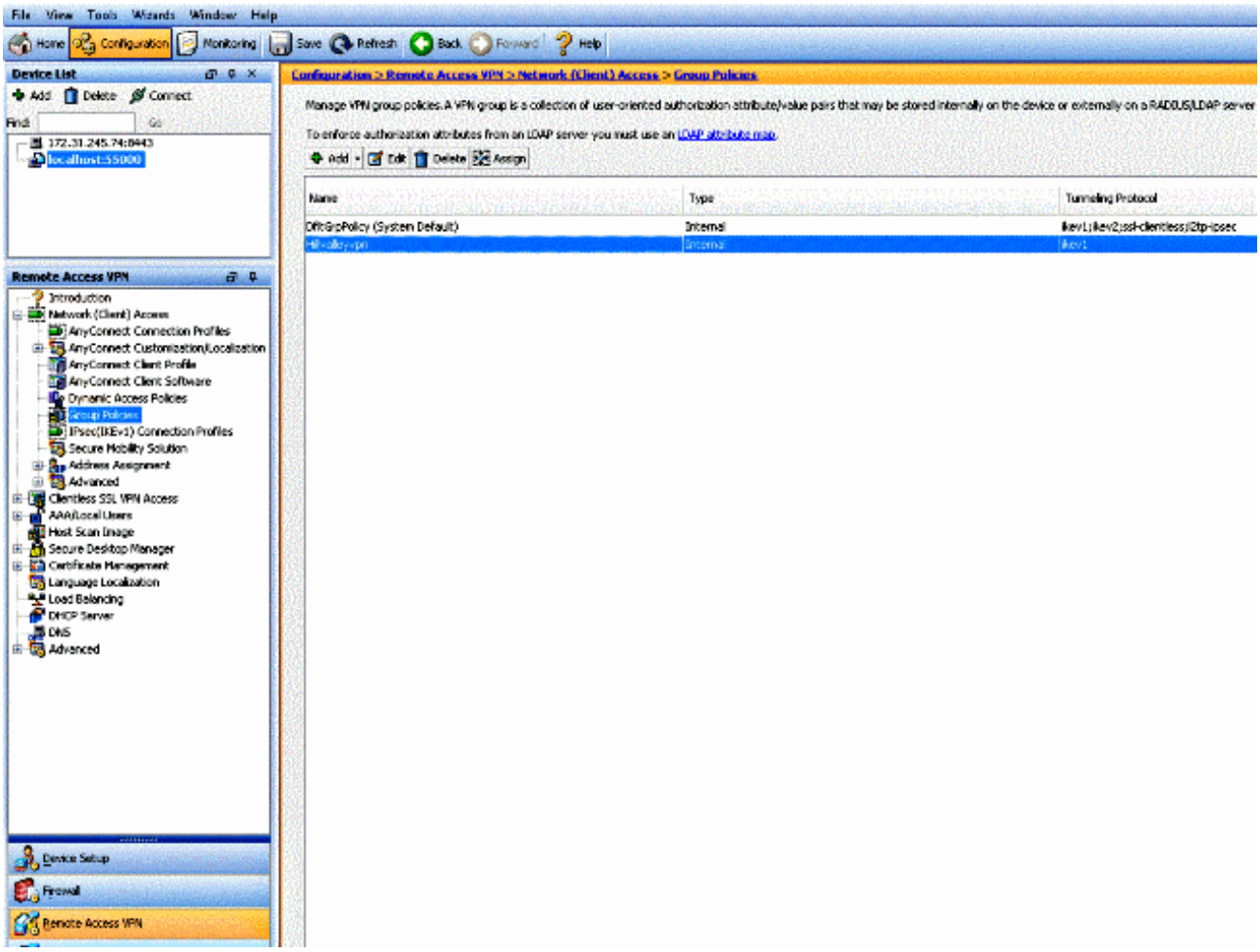
Führen Sie diese Aufgaben aus, um Cisco VPN-Clients oder Cisco AnyConnect Secure Mobility Clients den Zugriff auf ihr lokales LAN bei der Verbindung mit der ASA zu ermöglichen:

- Konfigurieren der ASA über den ASDM oder Konfigurieren der ASA über die CLI
- Konfigurieren des Cisco AnyConnect Secure Mobility Client

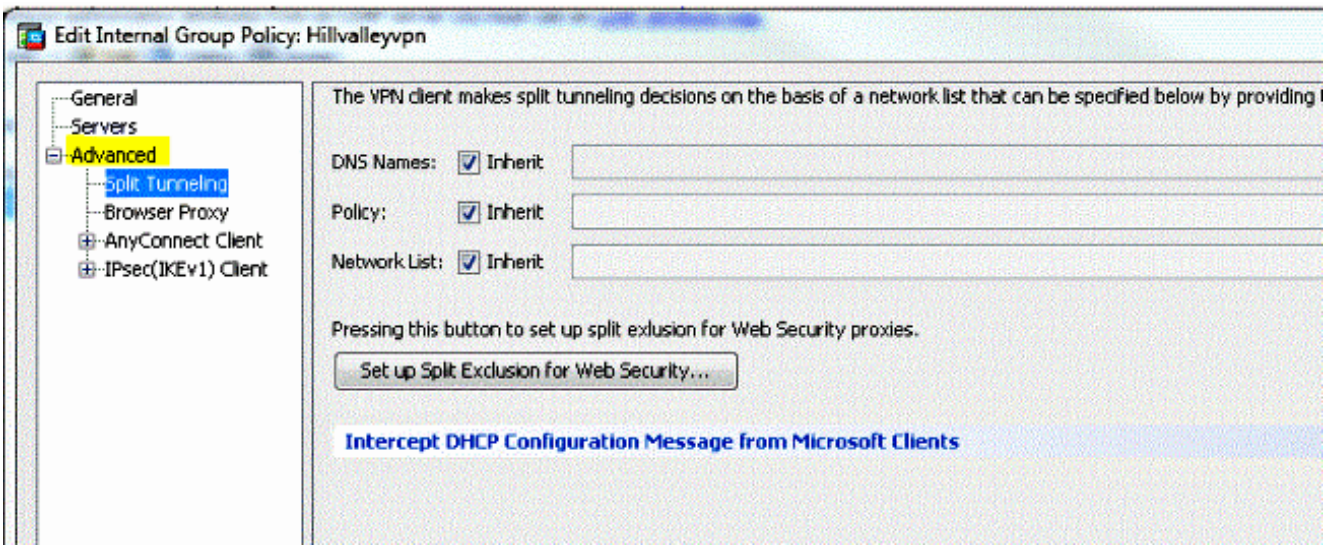
Konfigurieren der ASA über den ASDM

Gehen Sie wie folgt vor, um VPN-Clients bei der Verbindung mit der ASA lokalen LAN-Zugriff zu ermöglichen:

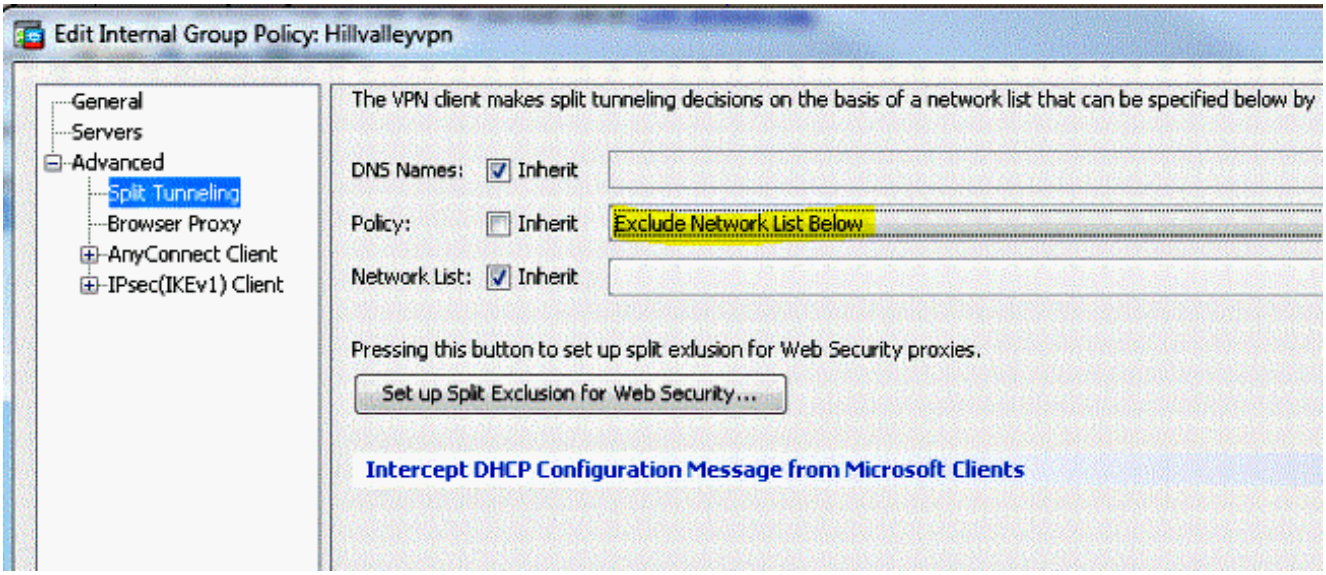
1. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policy (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policy (Konfiguration > Gruppenrichtlinie) aus,** und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie anschließend auf **Bearbeiten**.



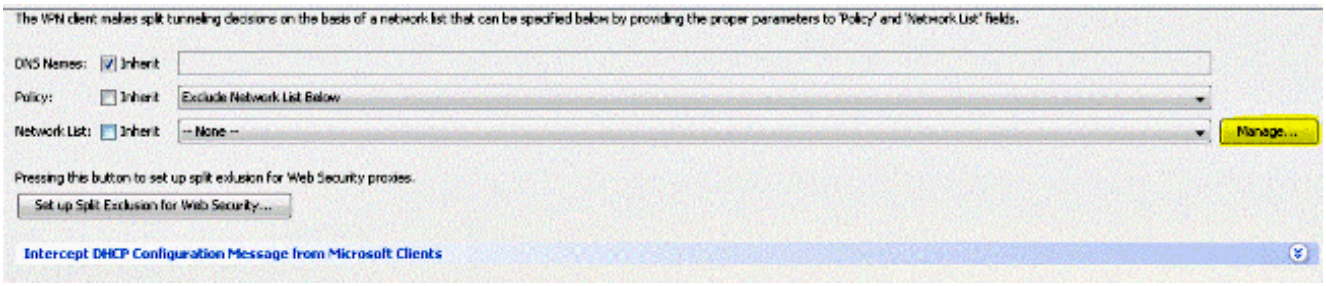
2. Gehen Sie zu **Erweitert > Getrenntes Tunneling**.



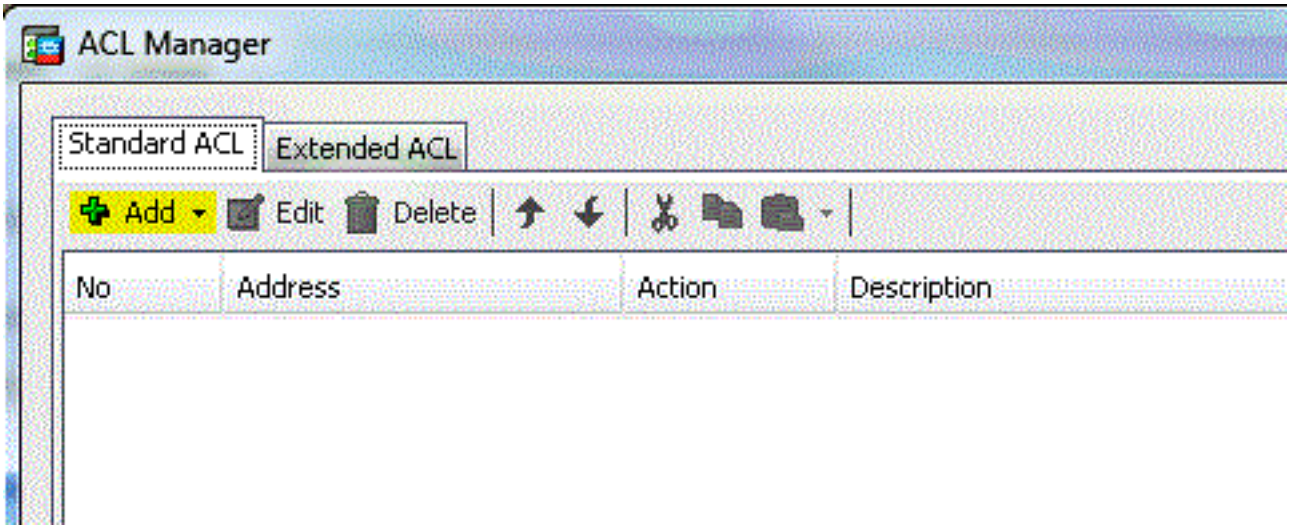
3. Deaktivieren Sie das Kontrollkästchen **Erben** für Richtlinie, und wählen Sie **unten Netzwerkliste ausschließen aus**.



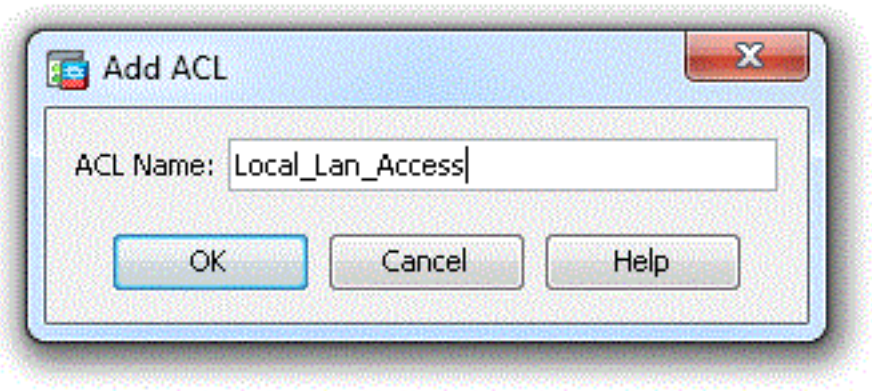
4. Deaktivieren Sie das Kontrollkästchen **Erben** für die Netzwerkliste, und klicken Sie dann auf **Verwalten**, um den ACL-Manager (Access Control List) zu starten.



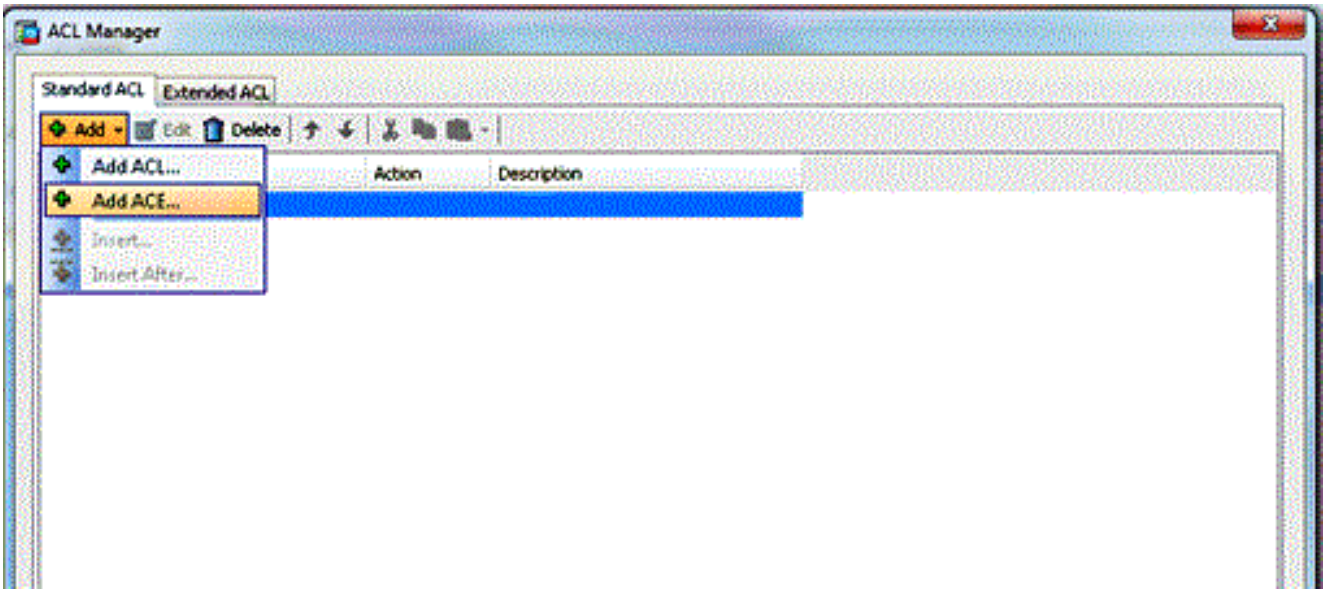
5. Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu erstellen.



6. Geben Sie einen Namen für die ACL an, und klicken Sie auf **OK**.

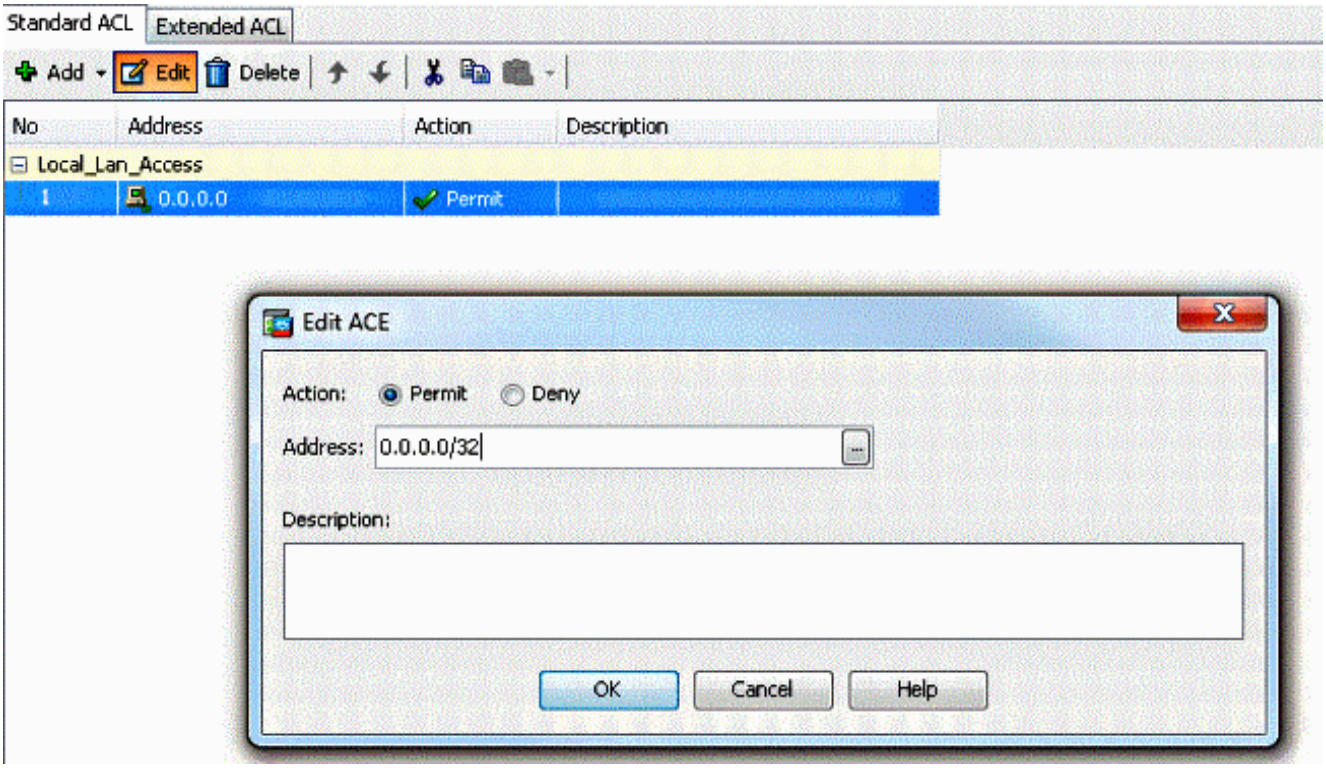


7. Wenn die ACL erstellt wurde, wählen Sie **Add > Add ACE.. (Hinzufügen > ACE hinzufügen) aus.** um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen.

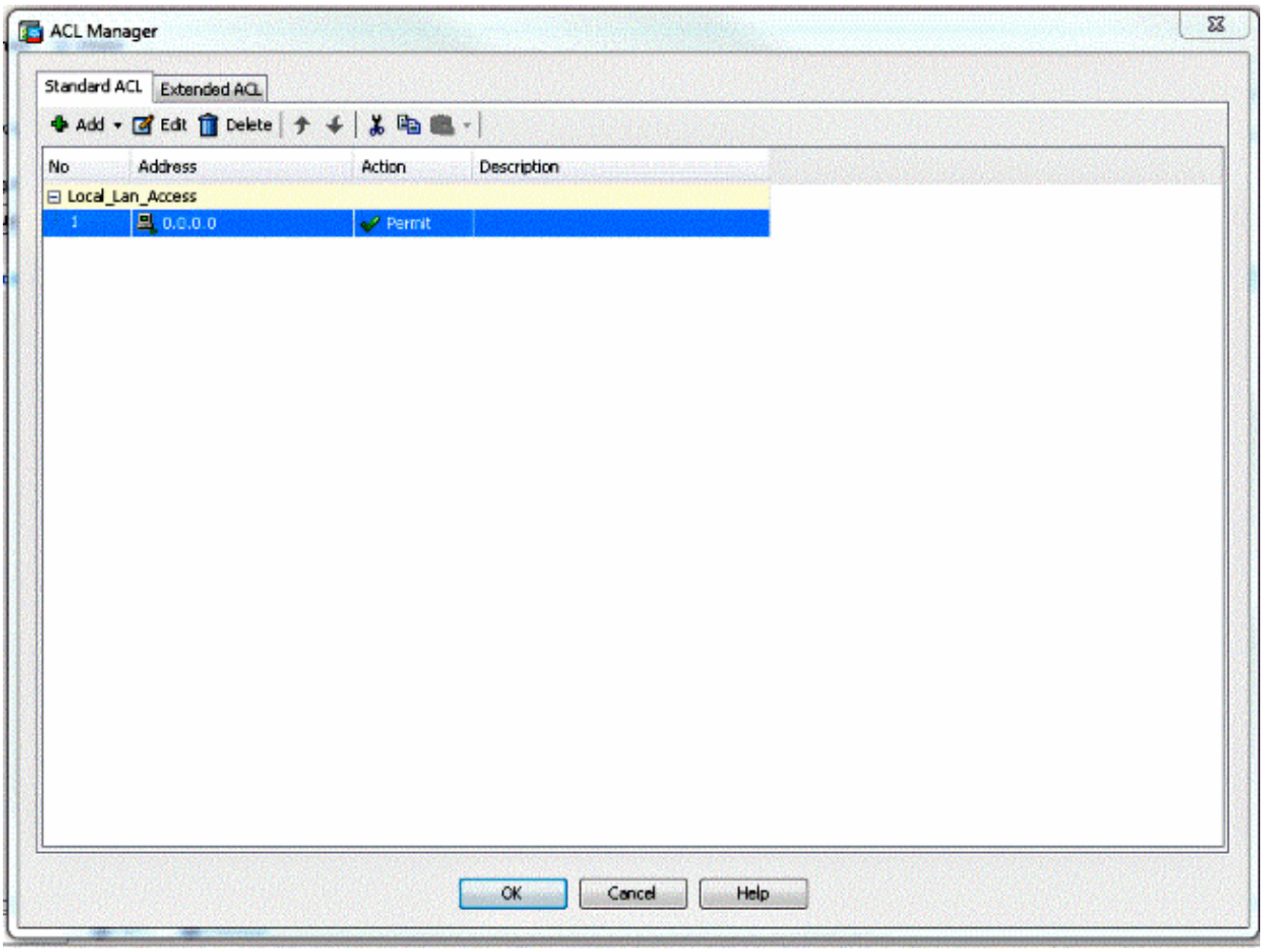


8. Definieren Sie den ACE, der dem lokalen LAN des Clients entspricht.

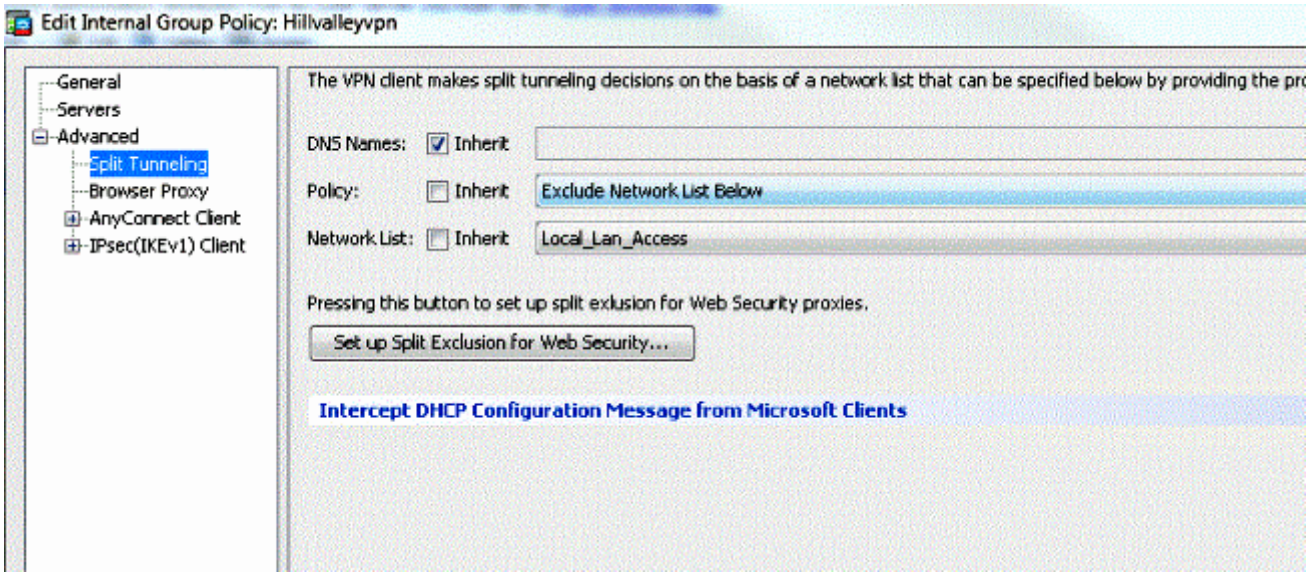
   Wählen Sie **Zulassen aus**.Wählen Sie eine IP-Adresse von **0.0.0.0 aus.**Wählen Sie eine Netzmaske von **/32 aus**.*(Optional)* Geben Sie eine Beschreibung an.Klicken Sie auf **OK**.



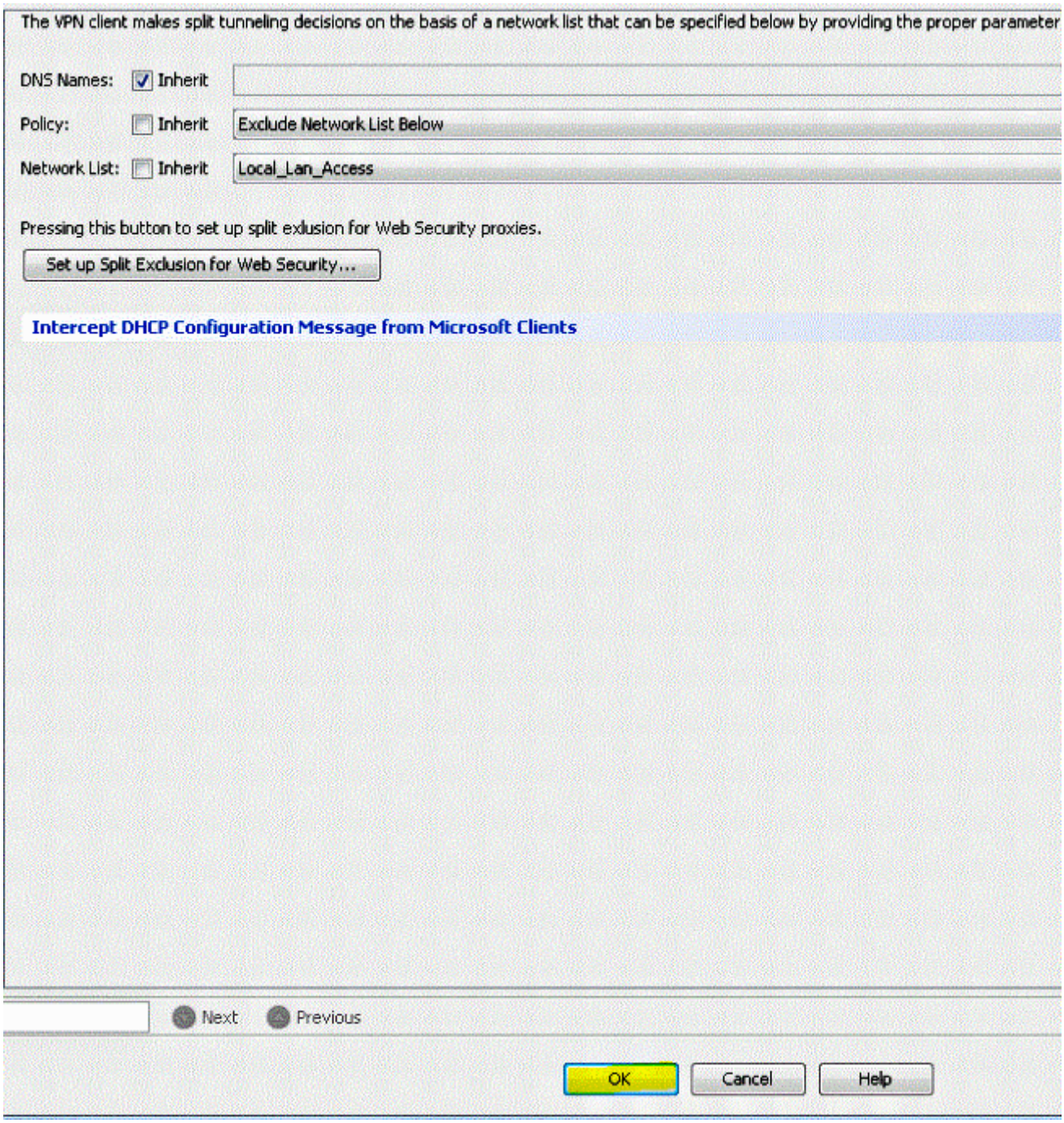
9. Klicken Sie auf **OK**, um den ACL Manager zu verlassen.



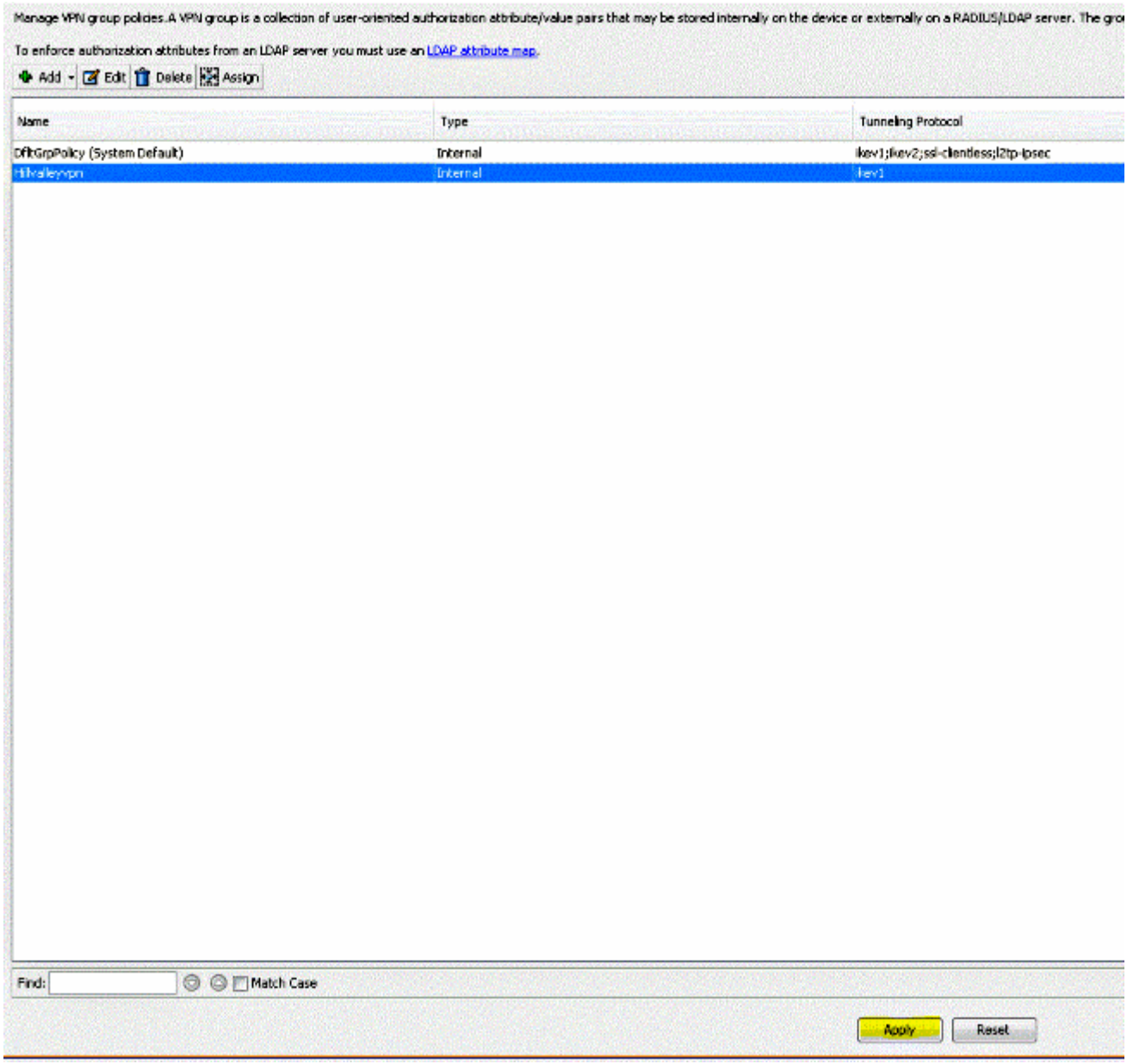
10. Stellen Sie sicher, dass die gerade erstellte ACL für die Split Tunnel Network List ausgewählt ist.



11. Klicken Sie auf **OK**, um zur Gruppenrichtlinienkonfiguration zurückzukehren.



12. Klicken Sie auf **Apply** und dann **Send** (falls erforderlich), um die Befehle an die ASA zu senden.



Konfigurieren der ASA über die CLI

Anstatt den ASDM zu verwenden, können Sie die folgenden Schritte in der ASA-CLI ausführen, um VPN-Clients bei der Verbindung mit der ASA lokalen LAN-Zugriff zu ermöglichen:

1. Wechseln in den Konfigurationsmodus

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

2. Erstellen Sie die Zugriffsliste, um den lokalen LAN-Zugriff zuzulassen.

```
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
```

Vorsicht: Aufgrund von Änderungen der ACL-Syntax zwischen ASA-Softwareversionen 8.x bis 9.x ist diese ACL nicht mehr zulässig, und Administratoren erhalten diese Fehlermeldung,

wenn sie versuchen, sie zu konfigurieren:

```
rtpvpnoutbound6(config)# access-list test standard permit host
0.0.0.0
FEHLER: ungültige IP-Adresse
```

Das Einzige, was erlaubt ist:

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

Dieses Problem ist bekannt und wurde mit der Cisco Bug-ID CSCut3131 behoben. Führen Sie ein Upgrade auf eine Version mit der Behebung dieses Fehlers durch, um den lokalen LAN-Zugriff konfigurieren zu können.

3. Geben Sie den Konfigurationsmodus für Gruppenrichtlinien für die Richtlinie ein, die Sie ändern möchten.

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

4. Geben Sie die Split-Tunnel-Richtlinie an. In diesem Fall ist die Richtlinie **nicht spezifiziert**.

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

5. Geben Sie die Liste für den geteilten Tunnel-Zugriff an. In diesem Fall lautet die Liste **Local_LAN_Access**.

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

6. Geben Sie den folgenden Befehl ein:

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

7. Ordnen Sie die Gruppenrichtlinie der Tunnelgruppe zu.

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

8. Schließen Sie die beiden Konfigurationsmodi.

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

9. Speichern Sie die Konfiguration im nichtflüchtigen RAM (NVRAM), und drücken Sie bei Aufforderung **die Eingabetaste**, um den Quelldateinamen anzugeben.

```
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#
```

Konfigurieren des Cisco AnyConnect Secure Mobility Client

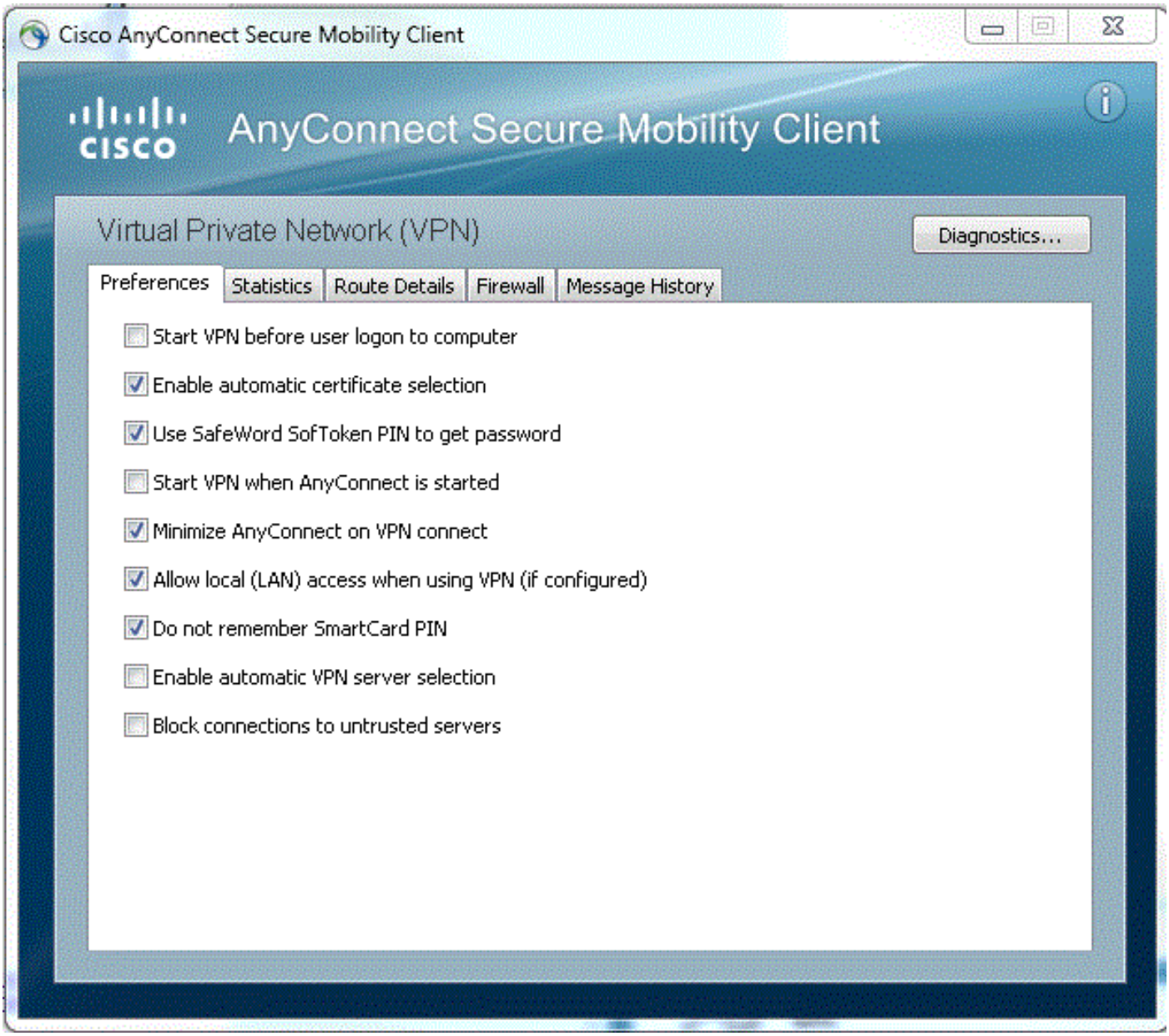
Informationen zur Konfiguration des Cisco AnyConnect Secure Mobility Client finden Sie im Abschnitt Einrichtung der SSL VPN-Verbindung mit SVC in **ASA 8.x: Zulassen von Split Tunneling für den AnyConnect VPN-Client im ASA-Konfigurationsbeispiel**.

Beim Split-exclude-Tunneling müssen Sie **AllowLocalLanAccess** im AnyConnect-Client aktivieren. Sämtliches Split-Exclusion-Tunneling gilt als lokaler LAN-Zugang. Um die Funktion zum Ausschließen von Split-Tunneling zu verwenden, müssen Sie die **AllowLocalLanAccess**-Voreinstellung in den **AnyConnect VPN-Client-Voreinstellungen** aktivieren. Standardmäßig ist der lokale LAN-Zugriff deaktiviert.

Um den lokalen LAN-Zugriff und somit das Tunneling ohne Spaltung zu ermöglichen, kann ein Netzwerkadministrator das Gerät im Profil aktivieren, oder die Benutzer können es in ihren Einstellungen aktivieren (siehe Bild im nächsten Abschnitt). Um lokalen LAN-Zugriff zuzulassen, aktiviert ein Benutzer das Kontrollkästchen **Lokalen LAN-Zugriff zulassen**, wenn Split-Tunneling auf dem sicheren Gateway aktiviert ist und mit der **Split-Tunnel-Richtlinie "Ausschließen" (Split-Tunnel)** konfiguriert ist. Darüber hinaus können Sie das VPN-Clientprofil konfigurieren, wenn der lokale LAN-Zugriff mit **<LocalLanAccess UserControllable="true">true</LocalLanAccess>** zulässig ist.

Benutzervoreinstellungen

Im Folgenden sind die Optionen aufgeführt, die Sie auf der Registerkarte "Preferences" (Voreinstellungen) des Cisco AnyConnect Secure Mobility Client vornehmen sollten, um den lokalen LAN-Zugriff zuzulassen.



XML-Profilbeispiel

Im Folgenden finden Sie ein Beispiel für die Konfiguration des VPN-Clientprofils mit 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>
```

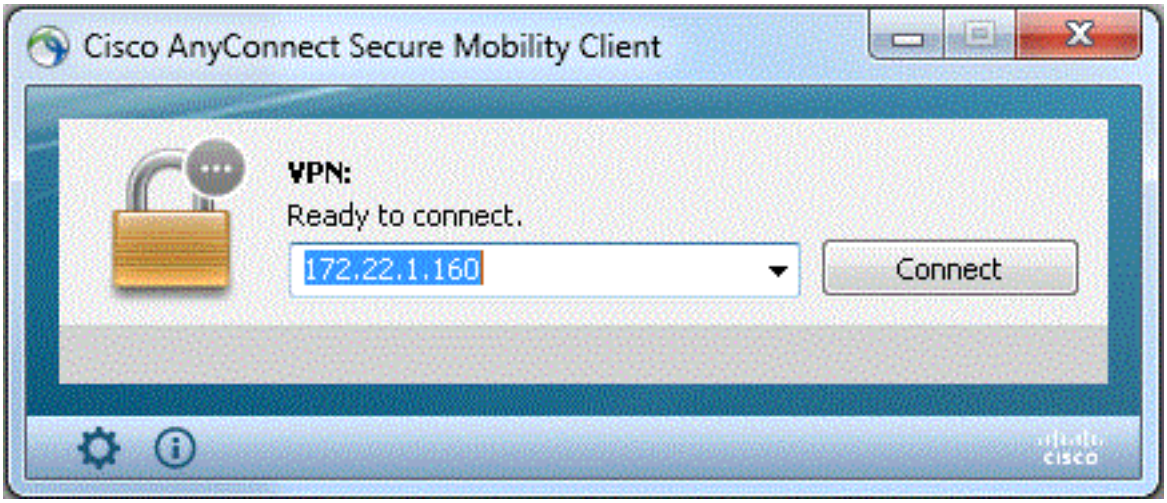
Überprüfen

Führen Sie die Schritte in diesen Abschnitten aus, um Ihre Konfiguration zu überprüfen.

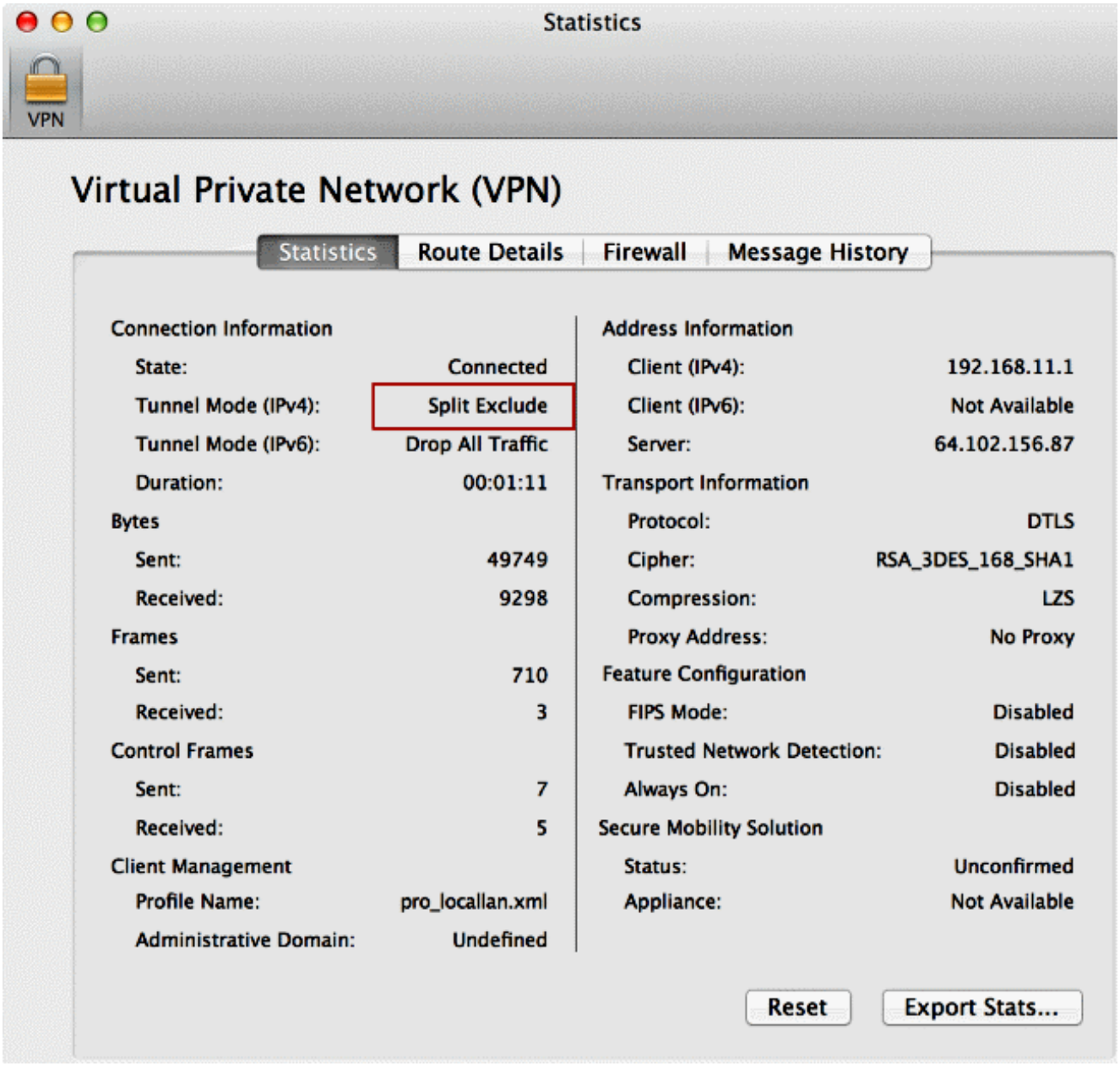
- DART anzeigen
- Testen des lokalen LAN-Zugriffs mit Ping

Verbinden Sie Ihren Cisco AnyConnect Secure Mobility Client mit der ASA, um Ihre Konfiguration zu überprüfen.

1. Wählen Sie den Eintrag für die Verbindung aus der Serverliste aus, und klicken Sie auf **Verbinden**.

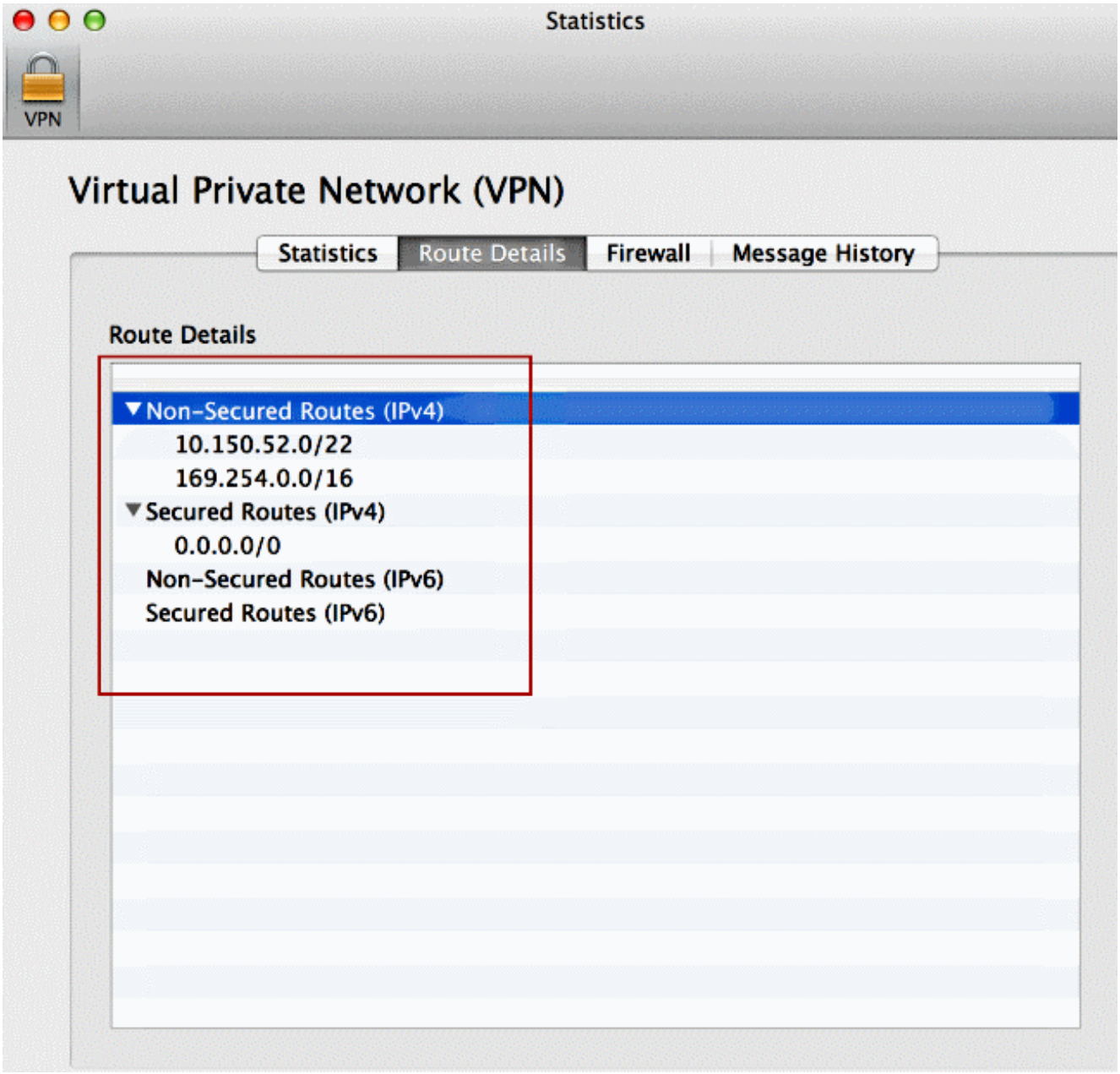


2. Wählen Sie **Erweitertes Fenster für alle Komponenten > Statistik..** um den Tunnelmodus anzuzeigen.



3. Klicken Sie auf die Registerkarte **Routendetails**, um die Routen anzuzeigen, auf die der Cisco AnyConnect Secure Mobility Client weiterhin lokalen Zugriff hat.

   In diesem Beispiel ist dem Client der lokale LAN-Zugriff auf 10.150.52.0/22 und 169.254.0.0/16 gestattet, während der gesamte andere Datenverkehr verschlüsselt und über den Tunnel gesendet wird.



Cisco AnyConnect Secure Mobility Client

Wenn Sie die AnyConnect-Protokolle aus dem DART-Paket (Diagnostics and Reporting Tool) überprüfen, können Sie bestimmen, ob der Parameter für den lokalen LAN-Zugriff festgelegt wurde.

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

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
```

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

Testen des lokalen LAN-Zugriffs mit Ping

Eine weitere Möglichkeit zum Testen, dass der VPN-Client noch über lokalen LAN-Zugriff verfügt, während er mit dem VPN-Headend getunnelt wird, besteht in der Verwendung des Befehls **ping** in der Microsoft Windows-Befehlszeile. Im folgenden Beispiel ist das lokale LAN des Clients 192.168.0.0/24 und ein anderer Host im Netzwerk mit der IP-Adresse 192.168.0.3 vorhanden.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Drucken oder Durchsuchen nicht nach Namen möglich

Wenn der VPN-Client verbunden und für den lokalen LAN-Zugriff konfiguriert ist, *können* Sie *nicht* im lokalen LAN *nach Namen drucken oder suchen*. Um dieses Problem zu umgehen, stehen zwei Optionen zur Verfügung:

- Durchsuchen oder nach IP-Adresse drucken.

  Verwenden Sie zum Durchsuchen statt der Syntax **\\Sharename** die Syntax **\\x.x.x.x.x,** wobei *x.x.x.x* die IP-Adresse des Hostcomputers ist.

  Ändern Sie zum Drucken die Eigenschaften des Netzwerkdruckers, um anstelle eines Namens eine IP-Adresse zu verwenden. Anstelle der Syntax **\\sharename\printername** verwenden Sie beispielsweise **\\x.x.x\printername**, wobei *x.x.x.x* eine IP-Adresse ist.
- Erstellen oder ändern Sie die Datei VPN Client LMHOSTS. Mit einer LMHOSTS-Datei auf einem Microsoft Windows-PC können Sie statische Zuordnungen zwischen Hostnamen und IP-Adressen erstellen. Eine LMHOSTS-Datei könnte beispielsweise wie folgt aussehen:

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

  In Microsoft Windows XP Professional Edition befindet sich die LMHOSTS-Datei in **%SystemRoot%\System32\Drivers\Etc**. Weitere Informationen finden Sie in der Microsoft-Dokumentation oder in der Microsoft Knowledge Base in Artikel 314108.

Zugehörige Informationen

- PIX/ASA 7.x als Remote-VPN-Server mit ASDM-Konfigurationsbeispiel
- SSL VPN Client (SVC) auf IOS mit SDM-Konfigurationsbeispiel
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Technischer Support und Dokumentation - Cisco Systems