Split-Tunneling für VPN-Clients auf der ASA konfigurieren

Inhalt

- Einleitung
- Voraussetzungen
  - Anforderungen
  - Verwendete Komponenten
  - Netzwerkdiagramm
  - Verwandte Produkte
  - Konventionen
- Hintergrundinformationen
- Split-Tunneling auf der ASA konfigurieren
  - ASA 7.x mit Adaptive Security Device Manager (ASDM) 5.x konfigurieren
  - Konfigurieren von ASA 8.x mit ASDM6.x
  - Konfigurieren von ASA 7.x oder höher über CLI
  - Konfigurieren von PIX 6.x über die CLI
- Überprüfung
  - Mit dem VPN-Client verbinden
  - VPN-Client-Protokoll anzeigen
  - Testen des lokalen LAN-Zugriffs mit Ping
- Fehlerbehebung
  - Beschränkung mit der Anzahl der Einträge in einer Split-Tunnel-ACL
- Zugehörige Informationen

Einleitung

In diesem Dokument wird der Prozess beschrieben, mit dem VPN-Clients auf das Internet zugreifen können, während sie sich über eine Cisco Sicherheitslösung der Serie ASA 5500 anmelden.

Voraussetzungen

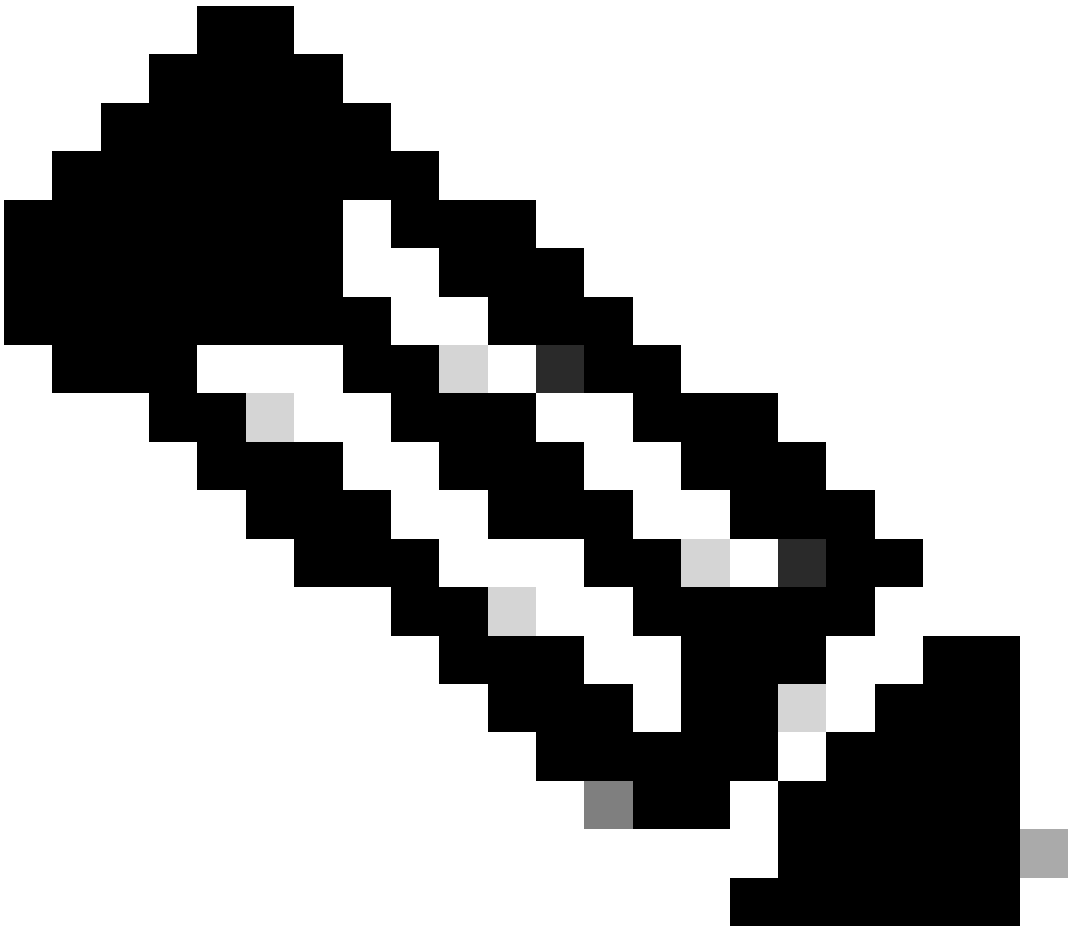
Anforderungen

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, falls noch kein Server konfiguriert ist.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Security Appliances der Serie ASA 5500, Software-Version 7.x und höher
- Cisco Systems VPN Client Version 4.0.5
- Adaptive Security Device Manager (ASDM)

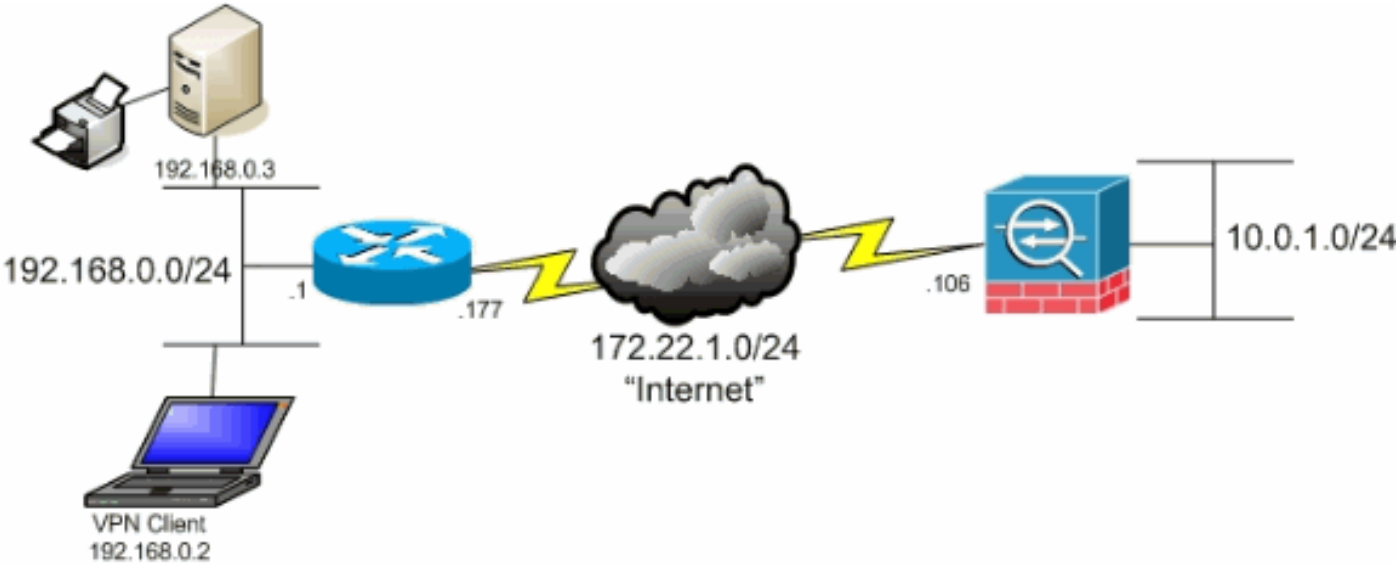


Hinweis: Dieses Dokument enthält auch die PIX 6.x CLI-Konfiguration, die mit dem Cisco VPN Client 3.x kompatibel ist.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Der VPN-Client befindet sich in einem typischen SOHO-Netzwerk und wird über das Internet mit der Hauptniederlassung verbunden.



Netzwerkdiagramm

Verwandte Produkte

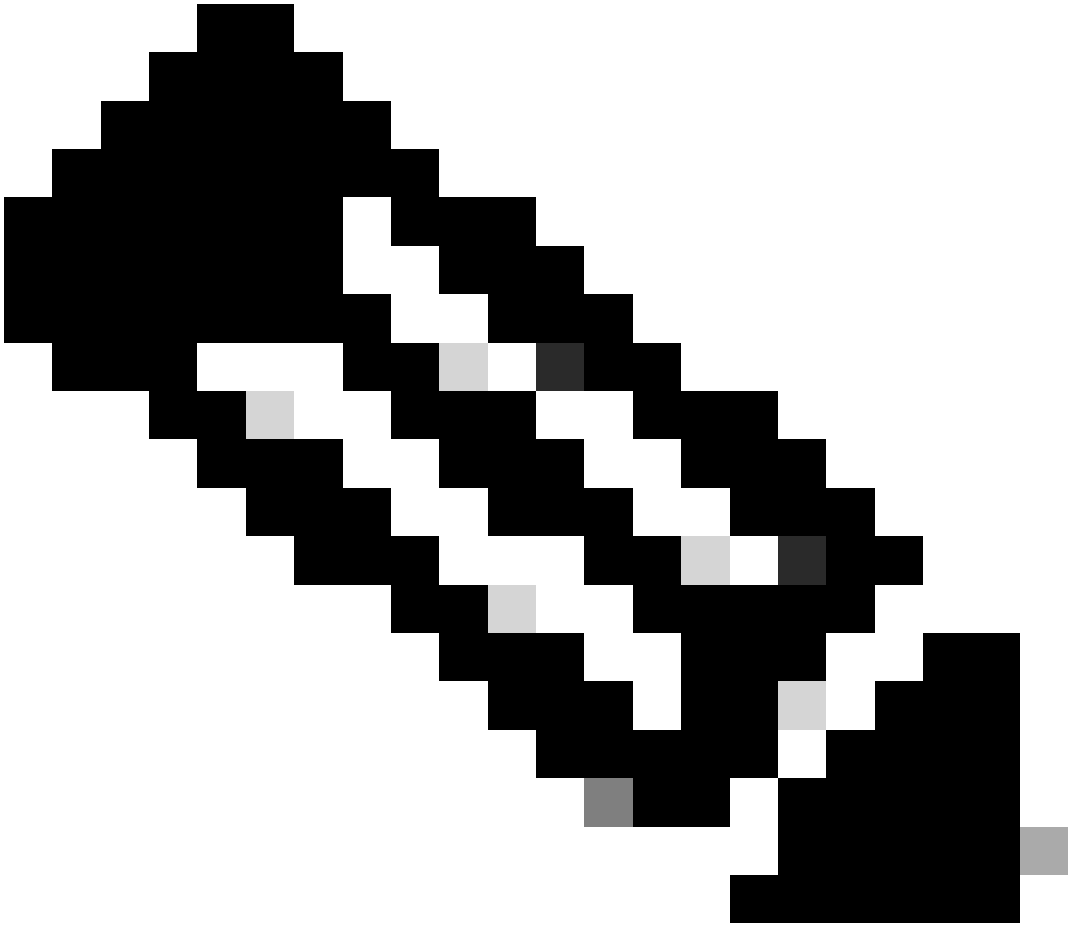
Diese Konfiguration kann auch mit der Software der Cisco Security Appliance der Serie PIX 500, Version 7.x, verwendet werden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Dieses Dokument enthält schrittweise Anleitungen, wie VPN-Clients der Zugriff auf das Internet gewährt wird, während sie über eine Cisco Adaptive Security Appliance (ASA) Security Appliance der Serie 5500 getunnelt werden. Diese Konfiguration ermöglicht VPN-Clients den sicheren Zugriff auf Unternehmensressourcen über IPsec und gewährt gleichzeitig ungesicherten Zugriff auf das Internet.



Hinweis: Vollständiges Tunneling gilt als sicherste Konfiguration, da es nicht den gleichzeitigen Gerätezugriff auf das Internet und das Firmen-LAN ermöglicht. Bei einem Kompromiss zwischen vollständigem Tunneling und Split-Tunneling ist nur der lokale LAN-Zugriff von VPN-Clients zulässig. Weitere Informationen finden Sie unter PIX/ASA 7.x: Allow Local LAN Access for VPN Clients Configuration Example (Konfigurationsbeispiel für lokalen LAN-Zugriff für VPN-Clients zulassen).

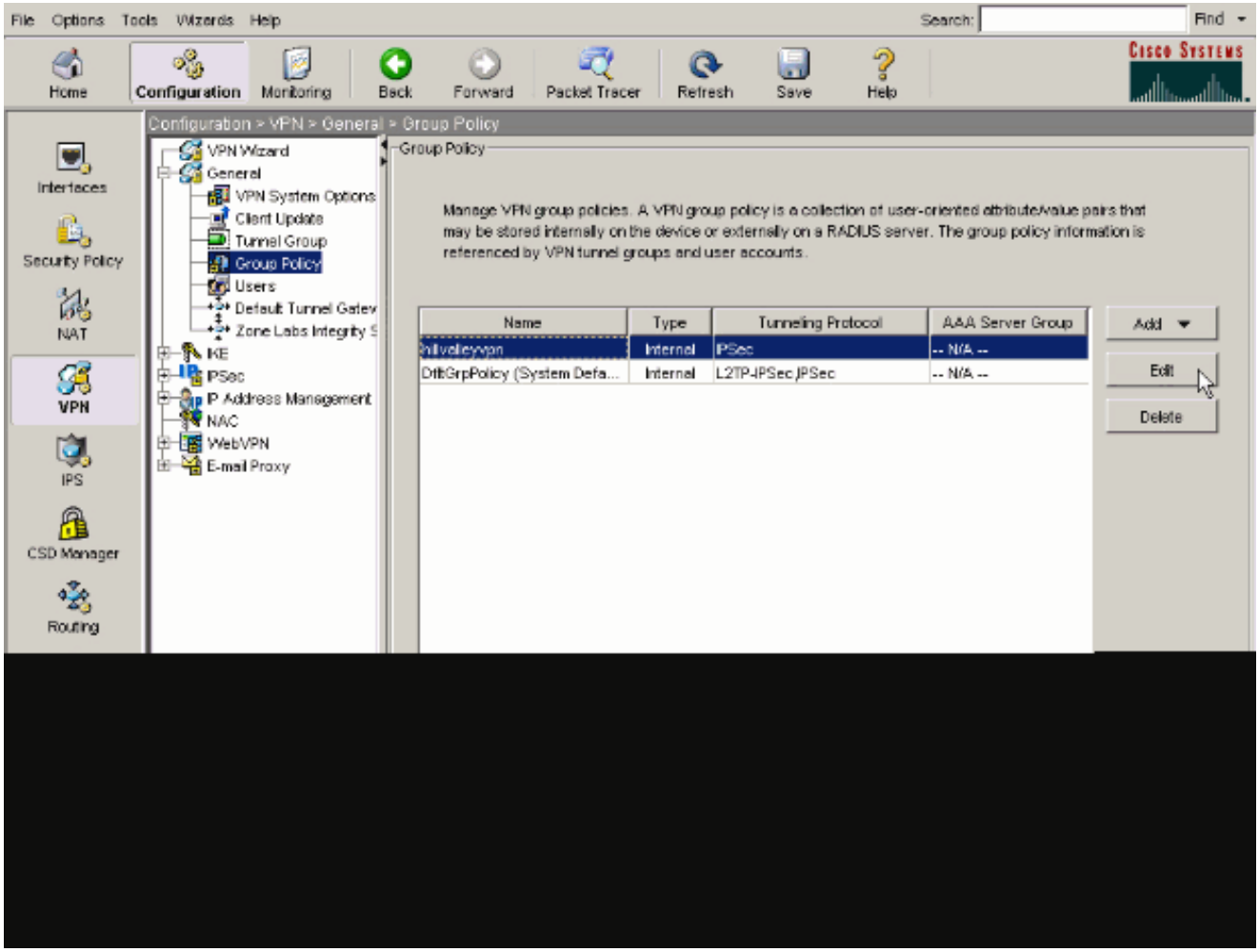
In einem grundlegenden Szenario von VPN-Client zu ASA wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an die ASA gesendet, unabhängig vom Ziel. Je nach Konfiguration und Anzahl der unterstützten Benutzer kann eine solche Einrichtung sehr bandbreitenintensiv sein. Split-Tunneling kann dieses Problem beheben, da Benutzer nur den Datenverkehr über den Tunnel senden können, der für das Unternehmensnetzwerk bestimmt ist. Der restliche Datenverkehr, wie Instant Messaging, E-Mail oder gelegentliches Surfen, wird über das lokale LAN des VPN Clients an das Internet gesendet.

Split-Tunneling auf der ASA konfigurieren

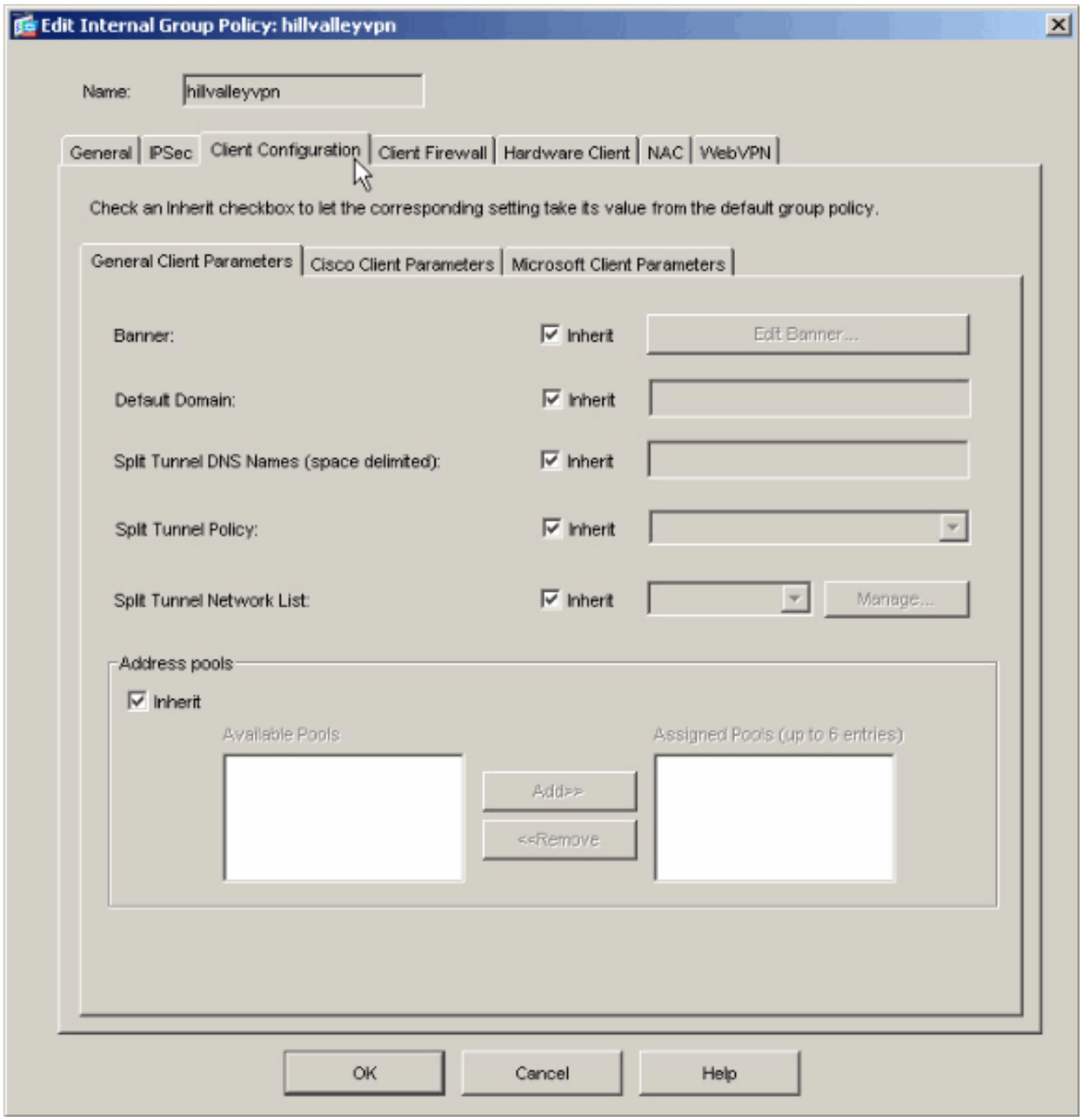
ASA 7.x mit Adaptive Security Device Manager (ASDM) 5.x konfigurieren

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für die Benutzer in der Gruppe zugelassen wird.

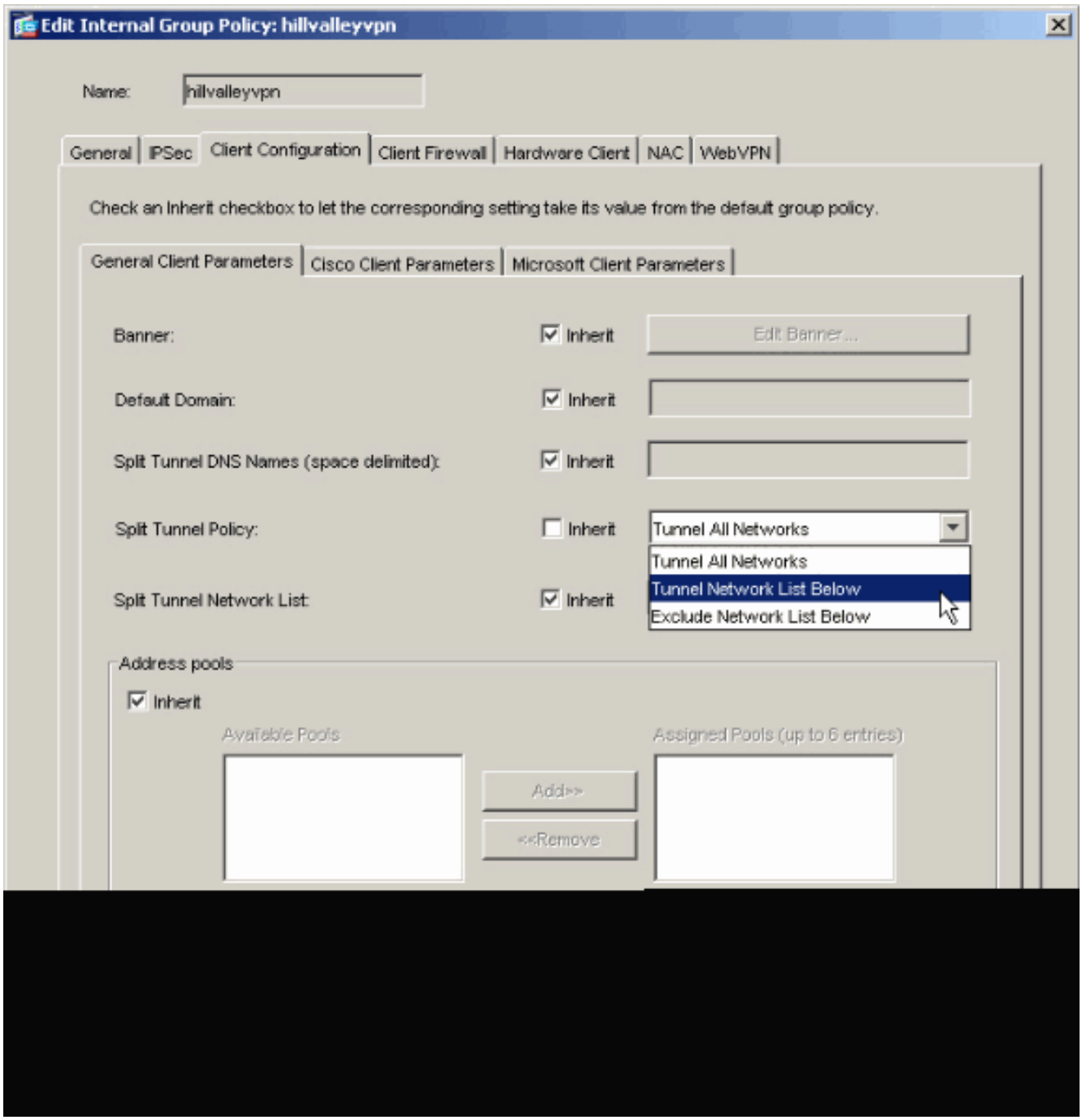
1. Wählen Sie Configuration > VPN > General > Group Policy aus, und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie dann auf Edit (Bearbeiten).



2. Wechseln Sie zur Registerkarte Client-Konfiguration.

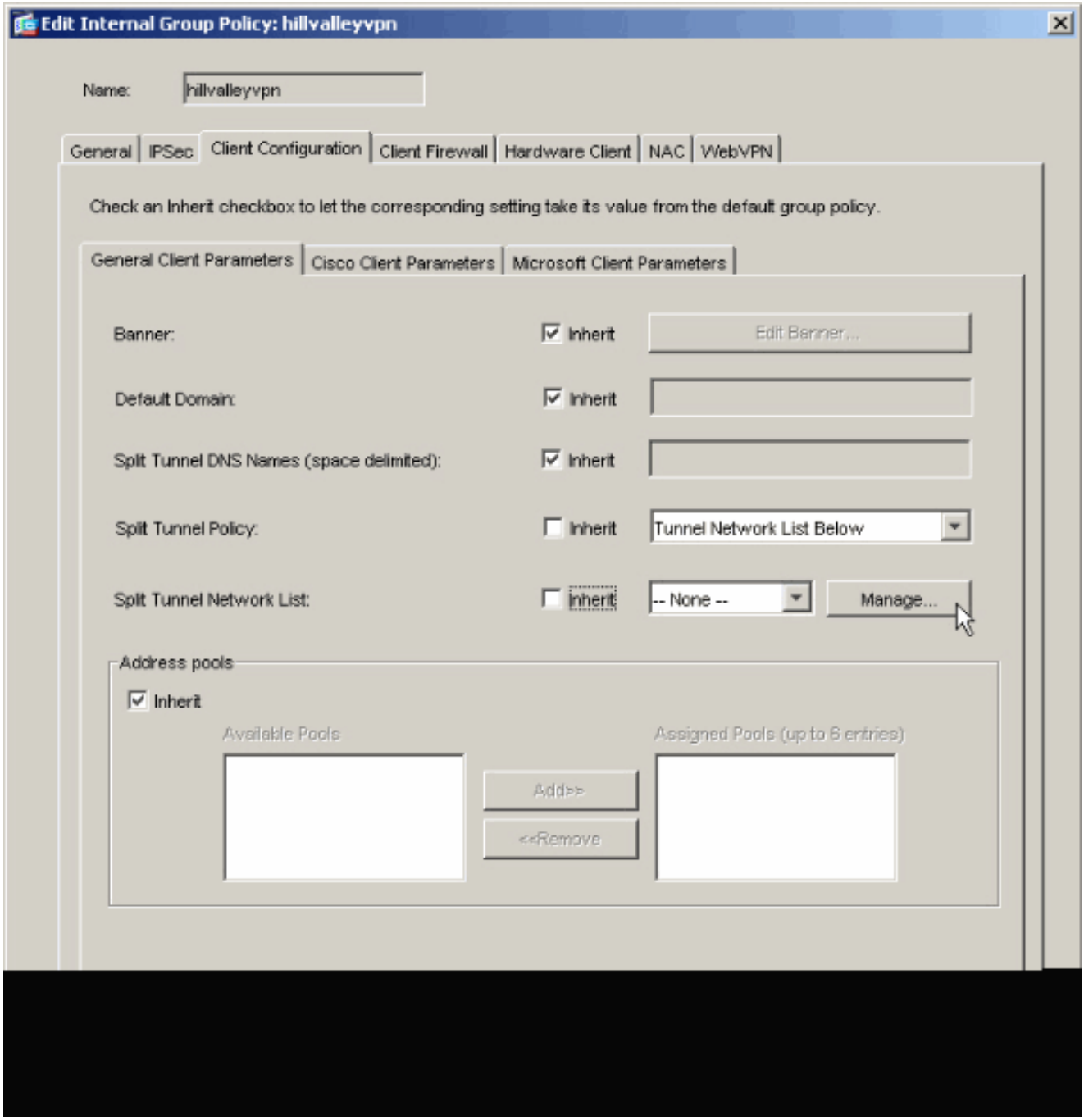


3. Deaktivieren Sie das Kontrollkästchen Vererben für die Split Tunnel Policy, und wählen Sie Tunnel Network List Below ..



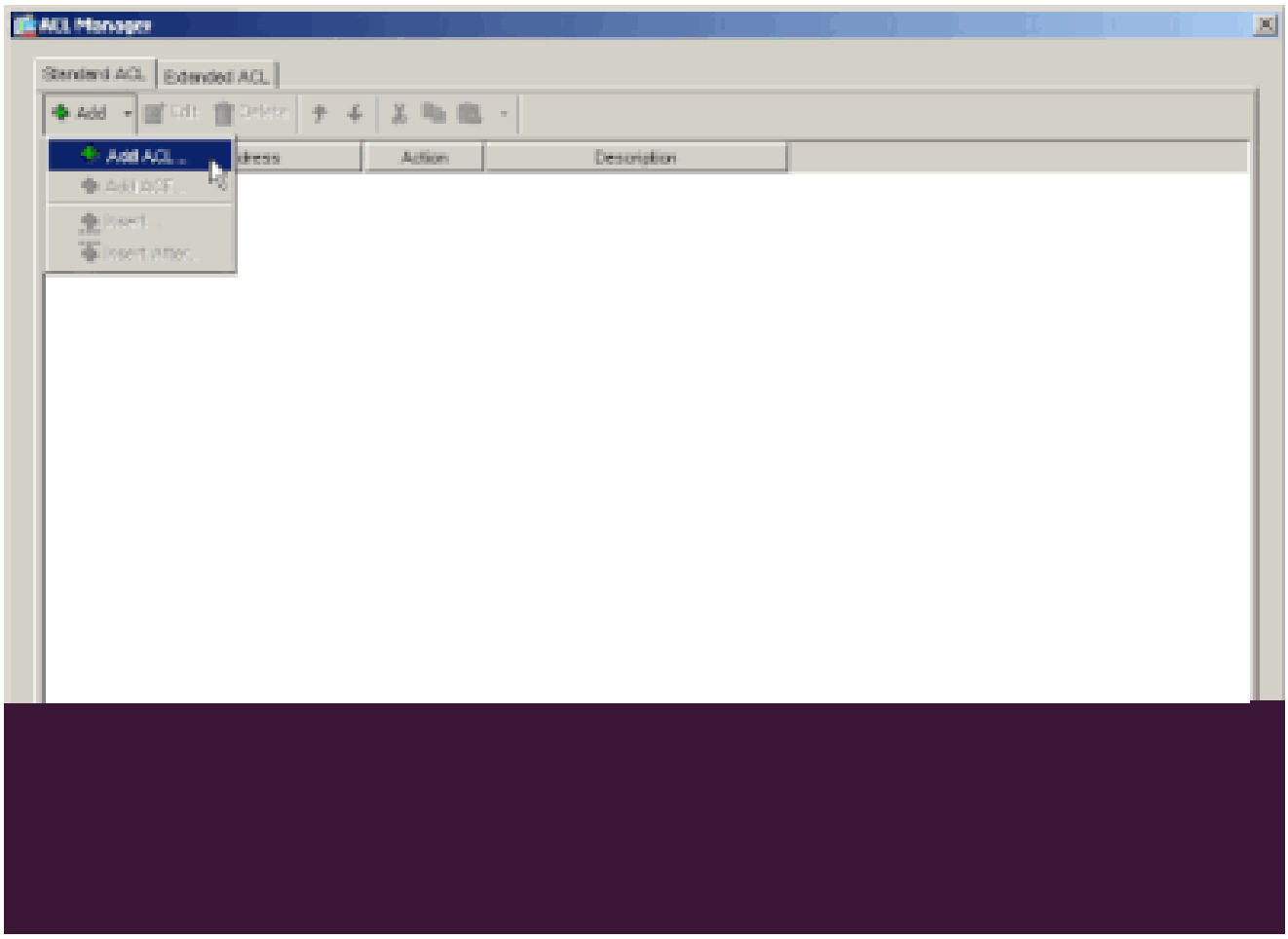
•

Deaktivieren Sie für Split Tunnel Network List das Kontrollkästchen **Inherit** (**Vererben**), und klicken Sie dann auf **Manage (Verwalten**), um den ACL Manager zu starten.



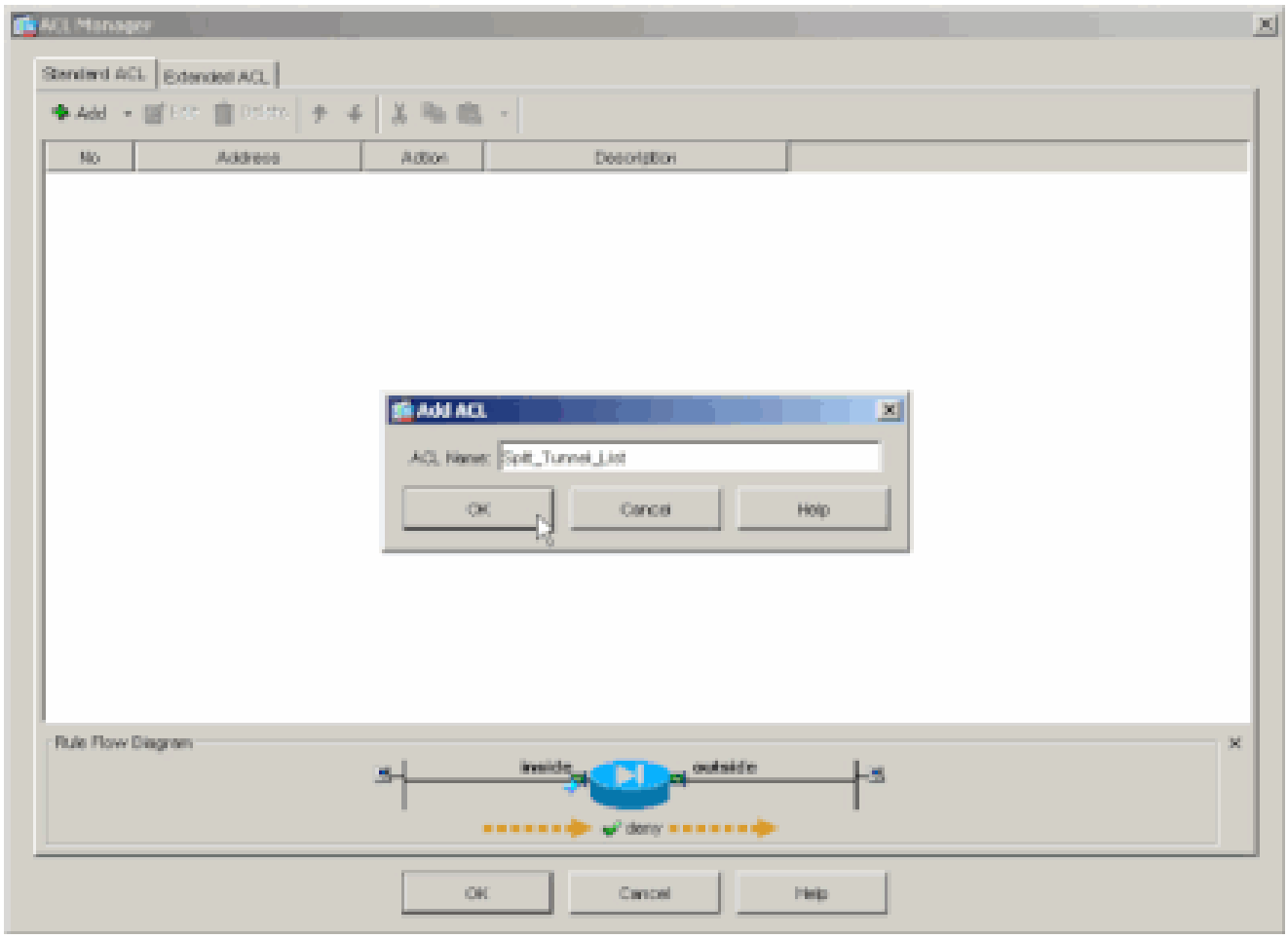
•

Wählen Sie in ACL Manager Add (Hinzufügen) > Add ACL ... (ACL hinzufügen ...) aus, um eine neue Zugriffsliste zu erstellen.



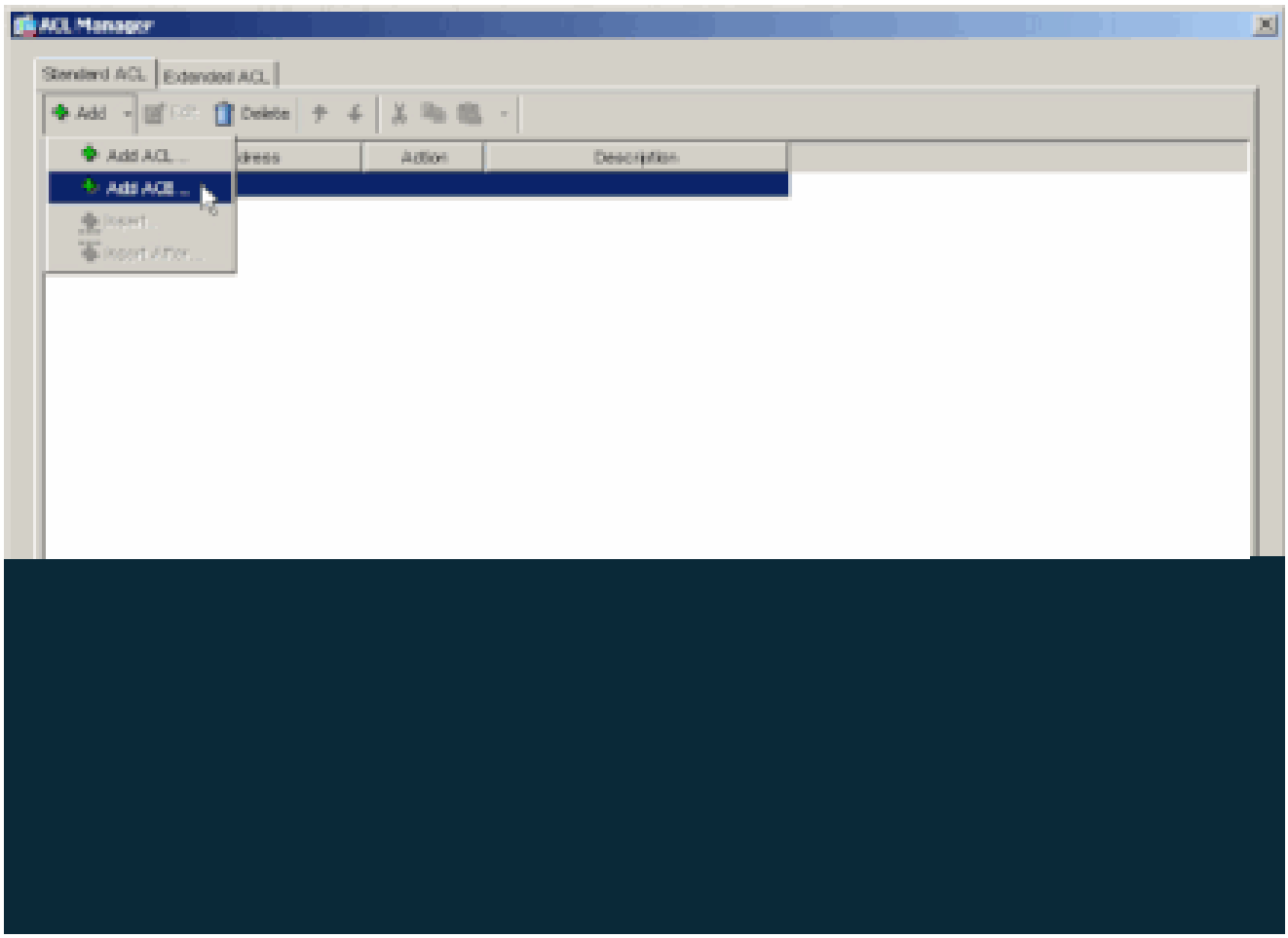
•

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



•

Nachdem die ACL erstellt wurde, wählen Sie **Hinzufügen > ACE hinzufügen. .**um einen Access Control Entry (ACE) hinzuzufügen.



•

Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.

a.

Wählen Sie Permit (Zulassen) aus.

b.

Wählen Sie als IP-Adresse 10.0.1.0 aus.

c.

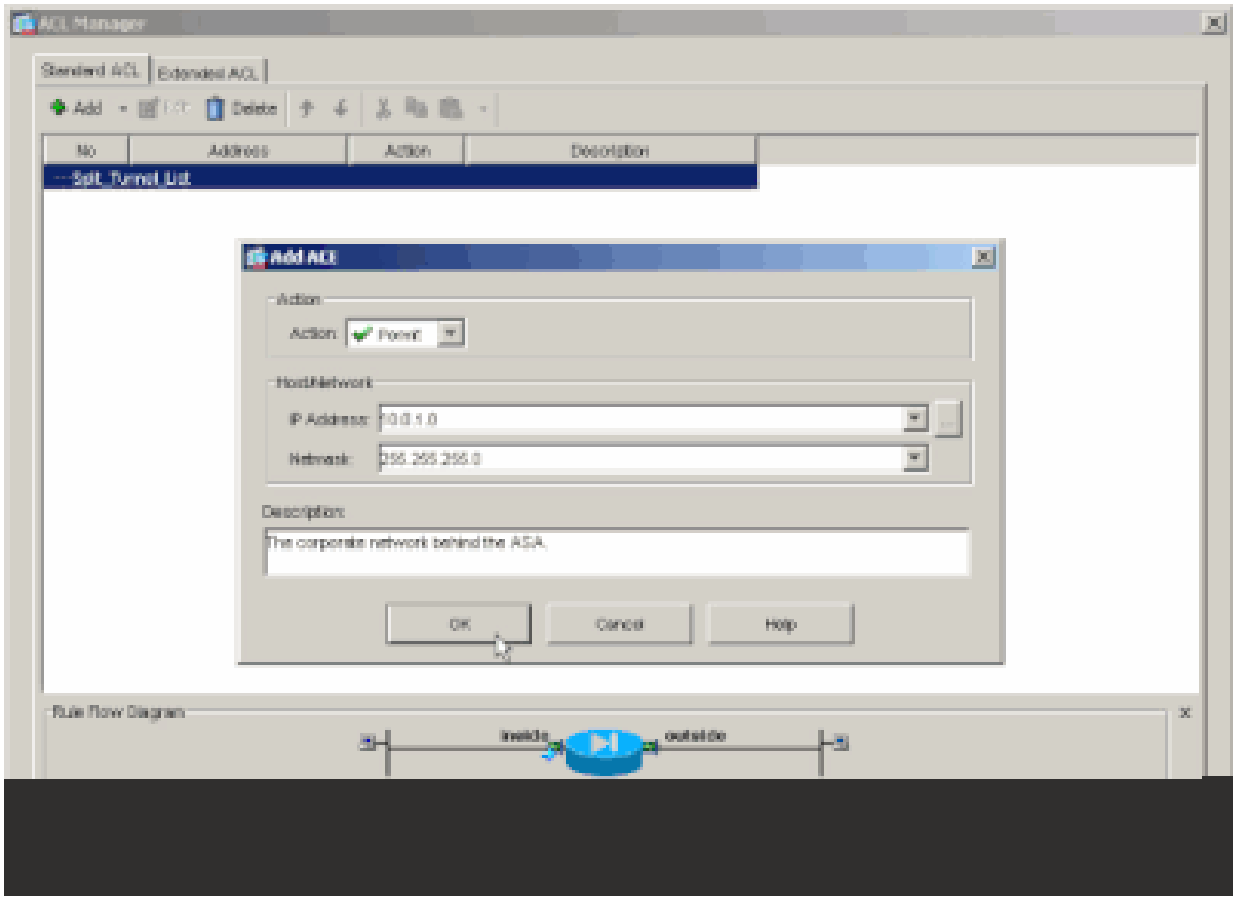
Wählen Sie die Netzmaske **255.255.255.0 aus**.

d.

*(Optional)*Geben Sie eine Beschreibung an.

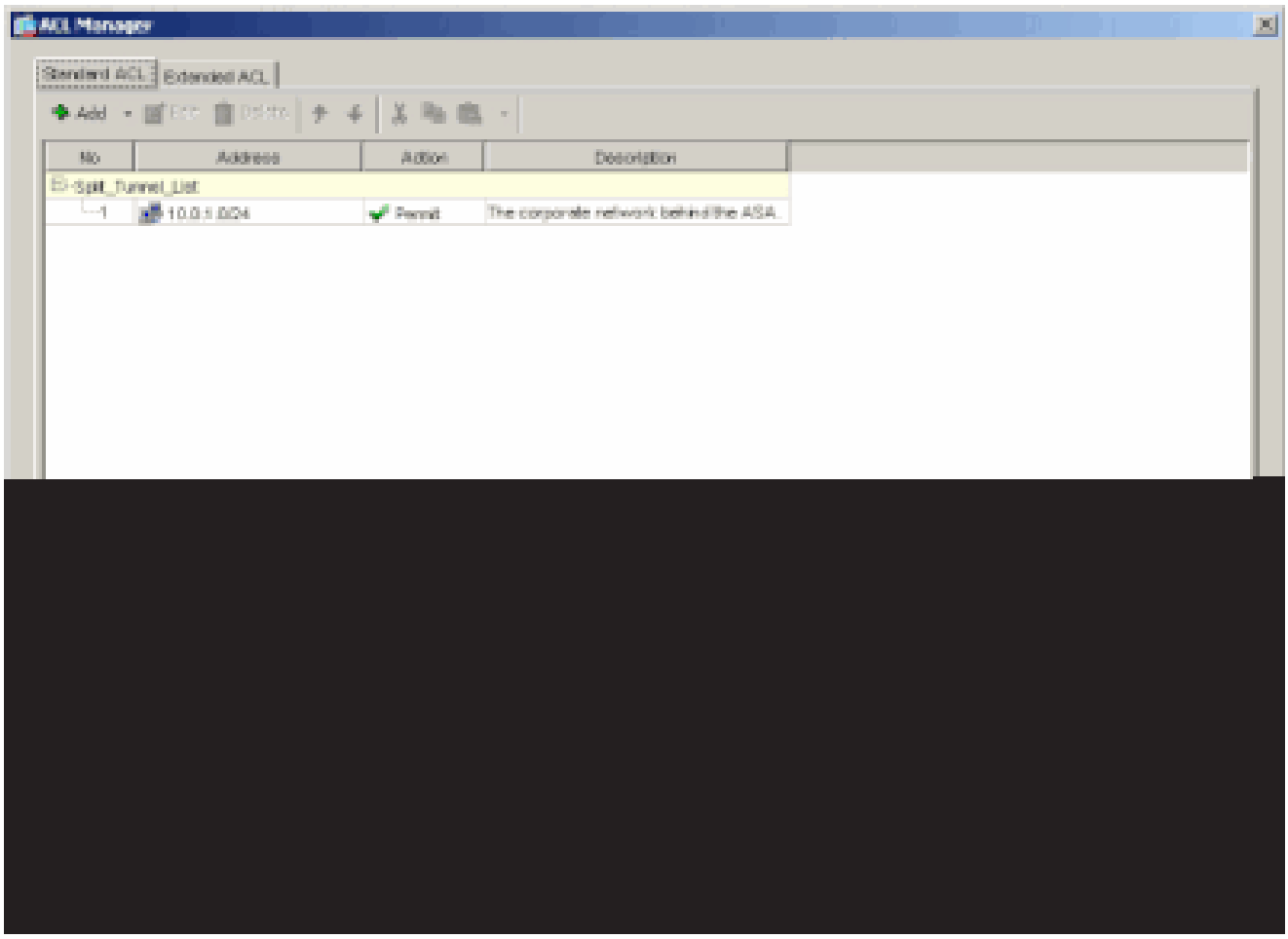
e.

Klicken Sie auf > **OK**.



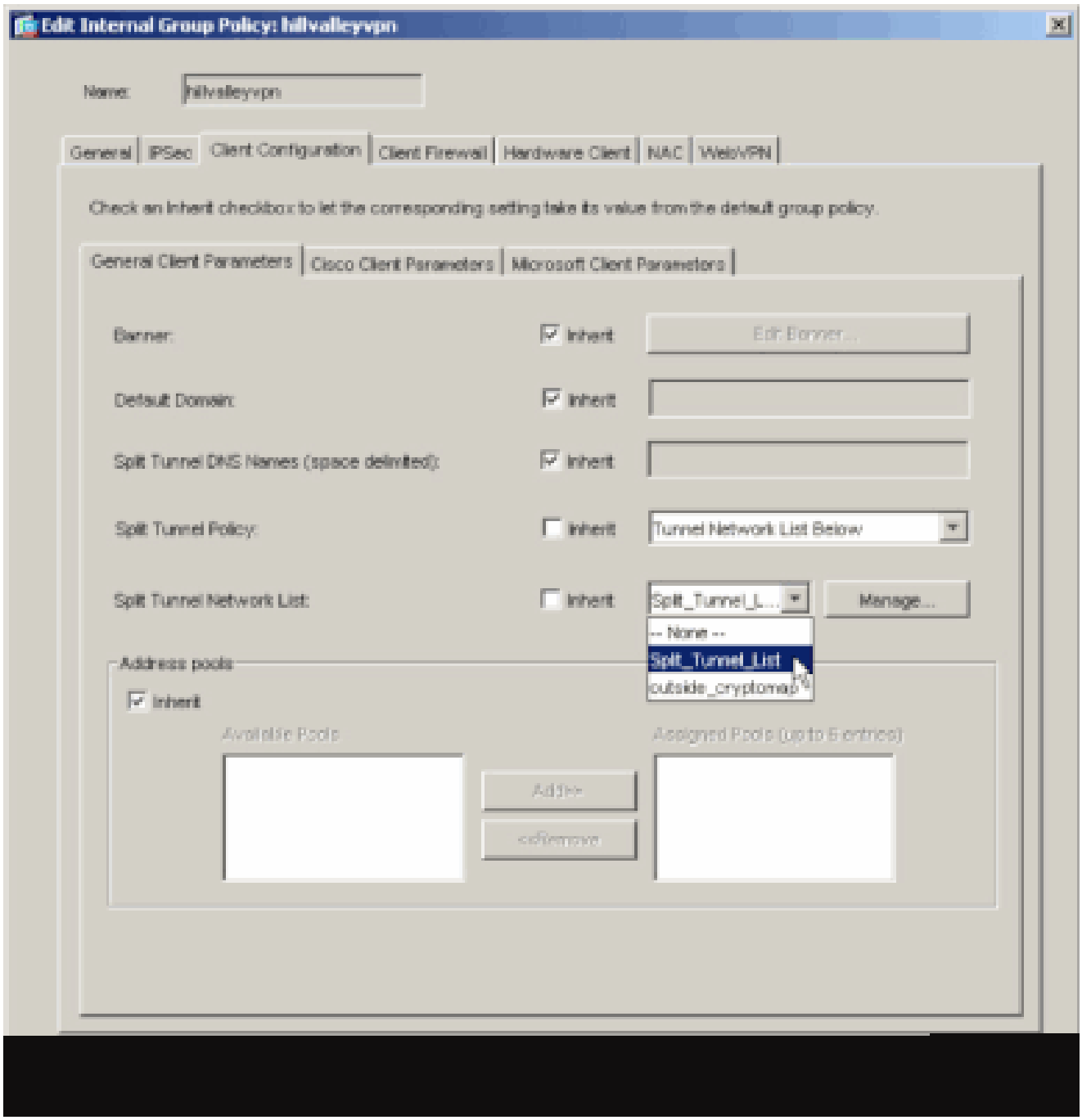
-

Klicken Sie auf **OK, um ACL Manager zu beenden.**



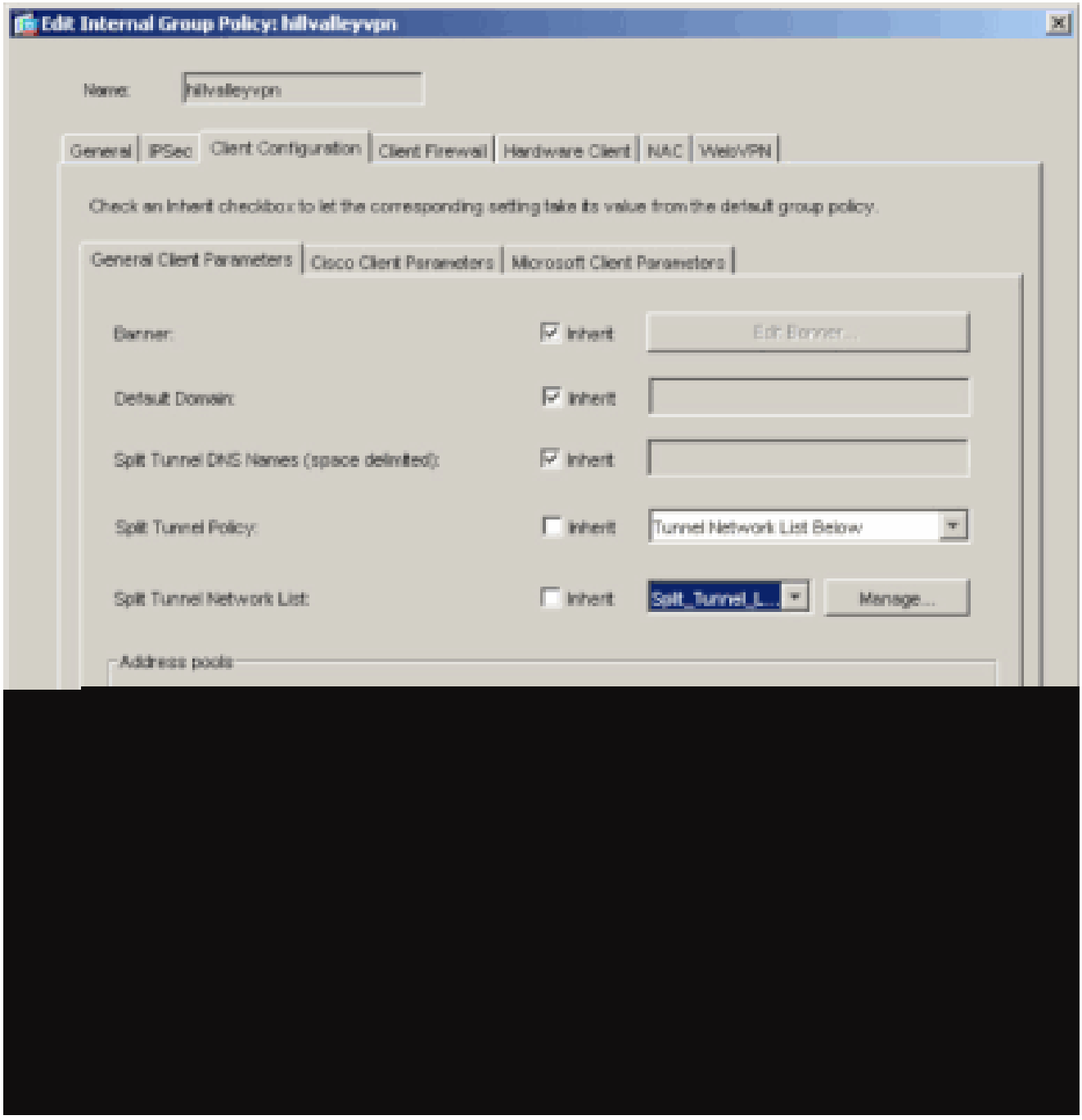
•

Vergewissern Sie sich, dass die soeben erstellte ACL für "Split Tunnel Network List" ausgewählt ist.



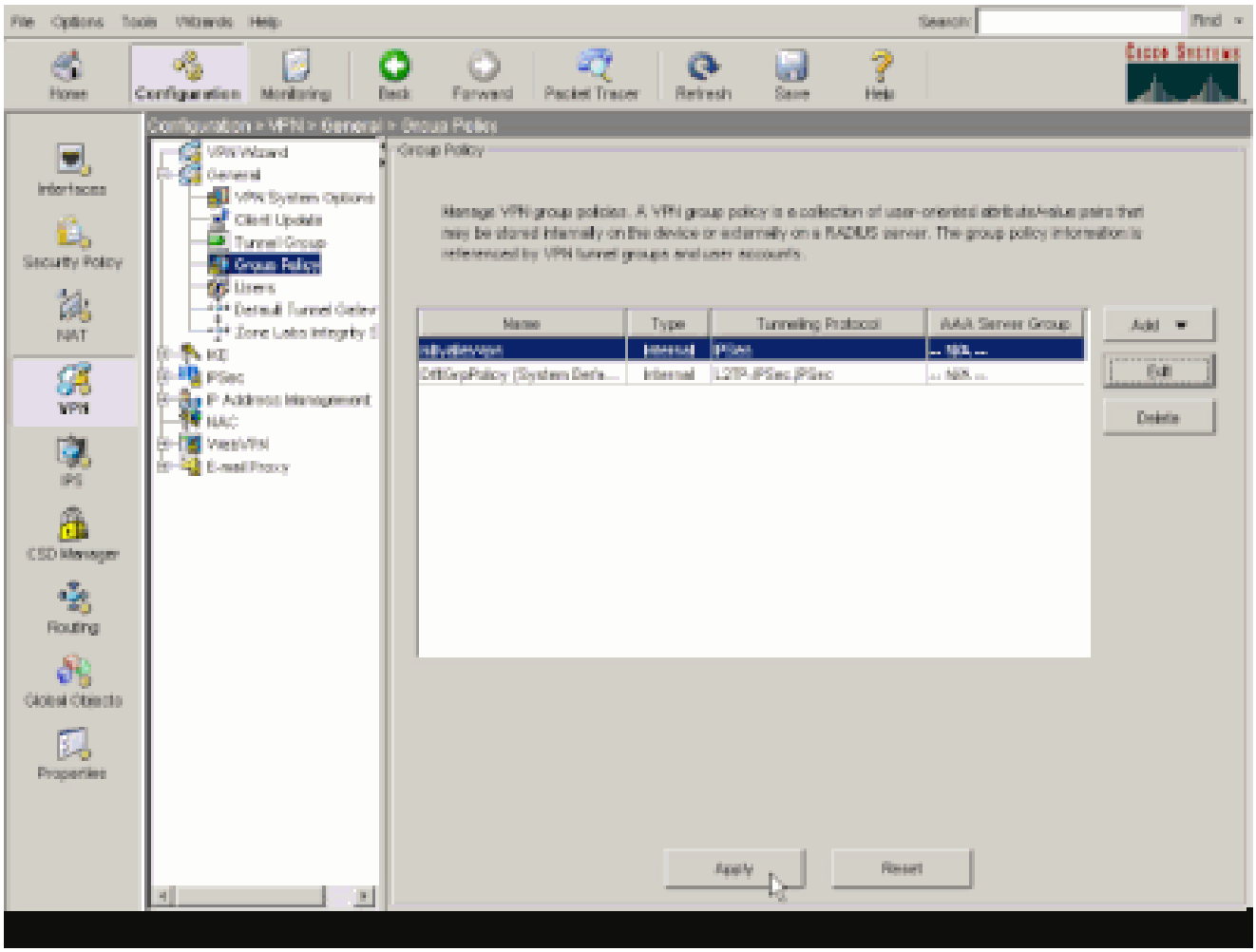
•

Klicken Sie auf **OK, um zur Konfiguration der Gruppenrichtlinie zurückzukehren.**



•

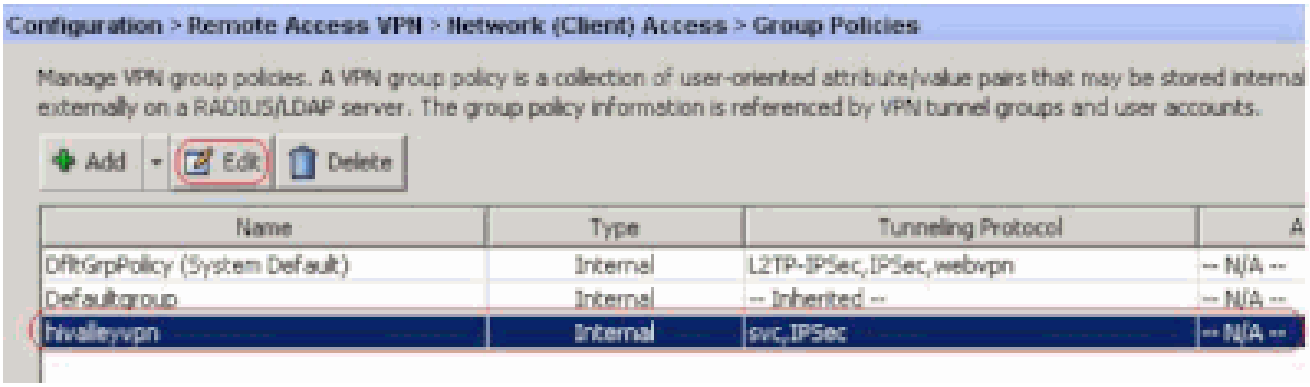
Klicken Sie auf Apply (Übernehmen) und dann ggf. auf Send (Senden), um die Befehle an die ASA zu senden.



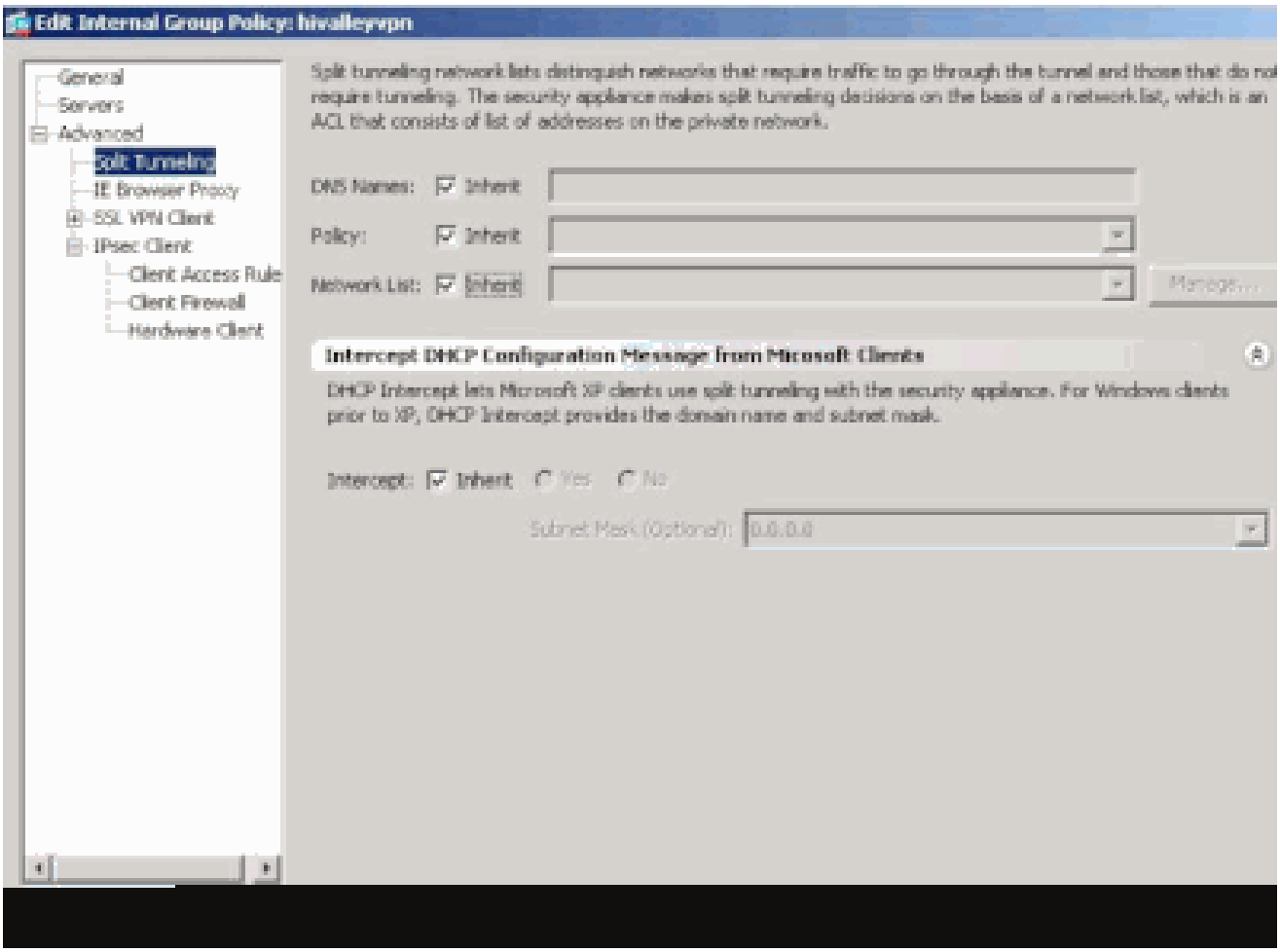
Konfigurieren von ASA 8.x mit ASDM 6.x

Führen Sie diese Schritte aus, um Ihre Tunnelgruppe so zu konfigurieren, dass Split-Tunneling für die Benutzer in der Gruppe zugelassen wird.

- Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remotezugriff-VPN > Netzwerkzugriff (Client) > Group Policies (Gruppenrichtlinien)** und dann die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie dann auf Edit (Bearbeiten).

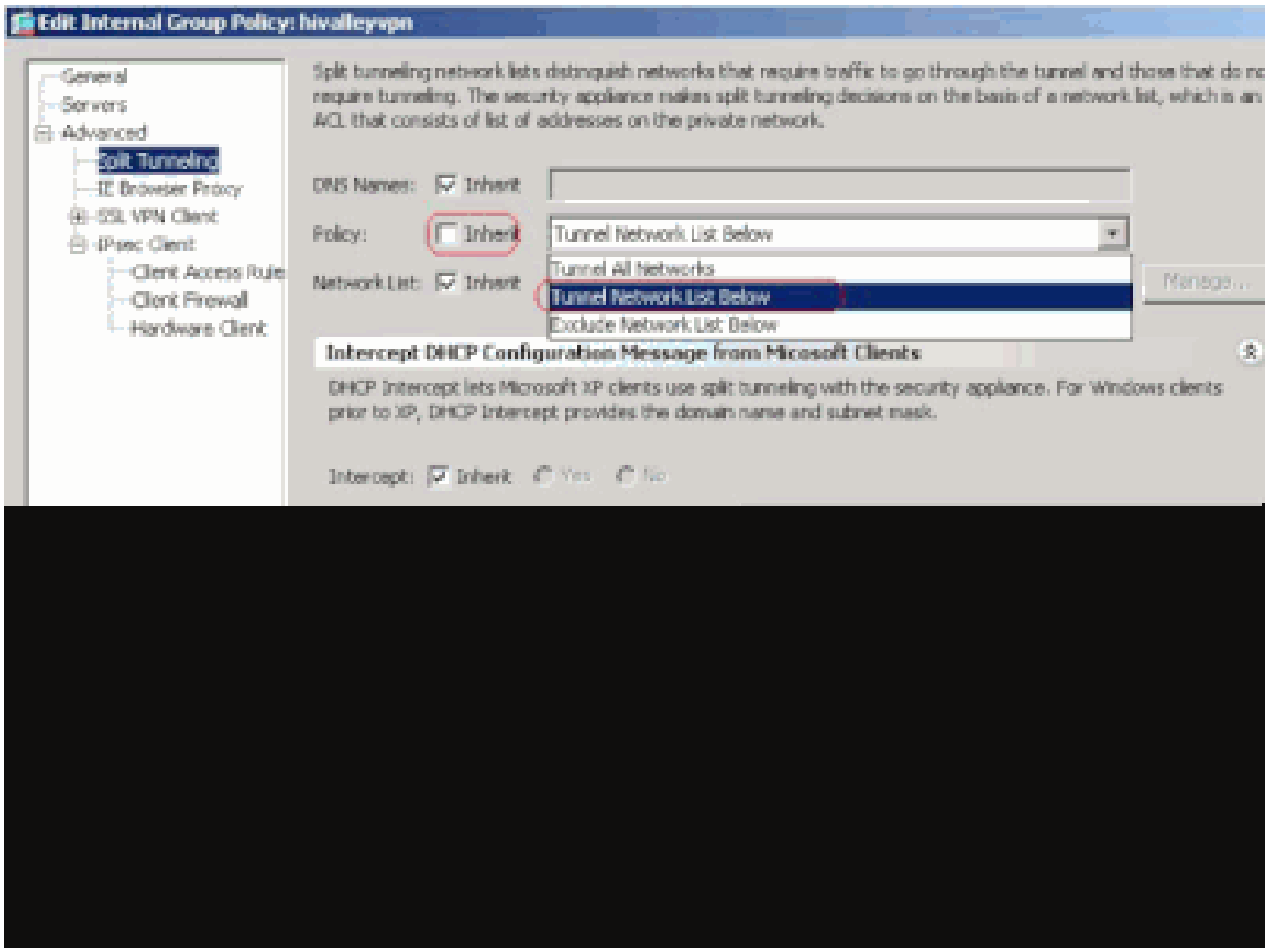


- Klicken Sie auf **Split Tunneling**.



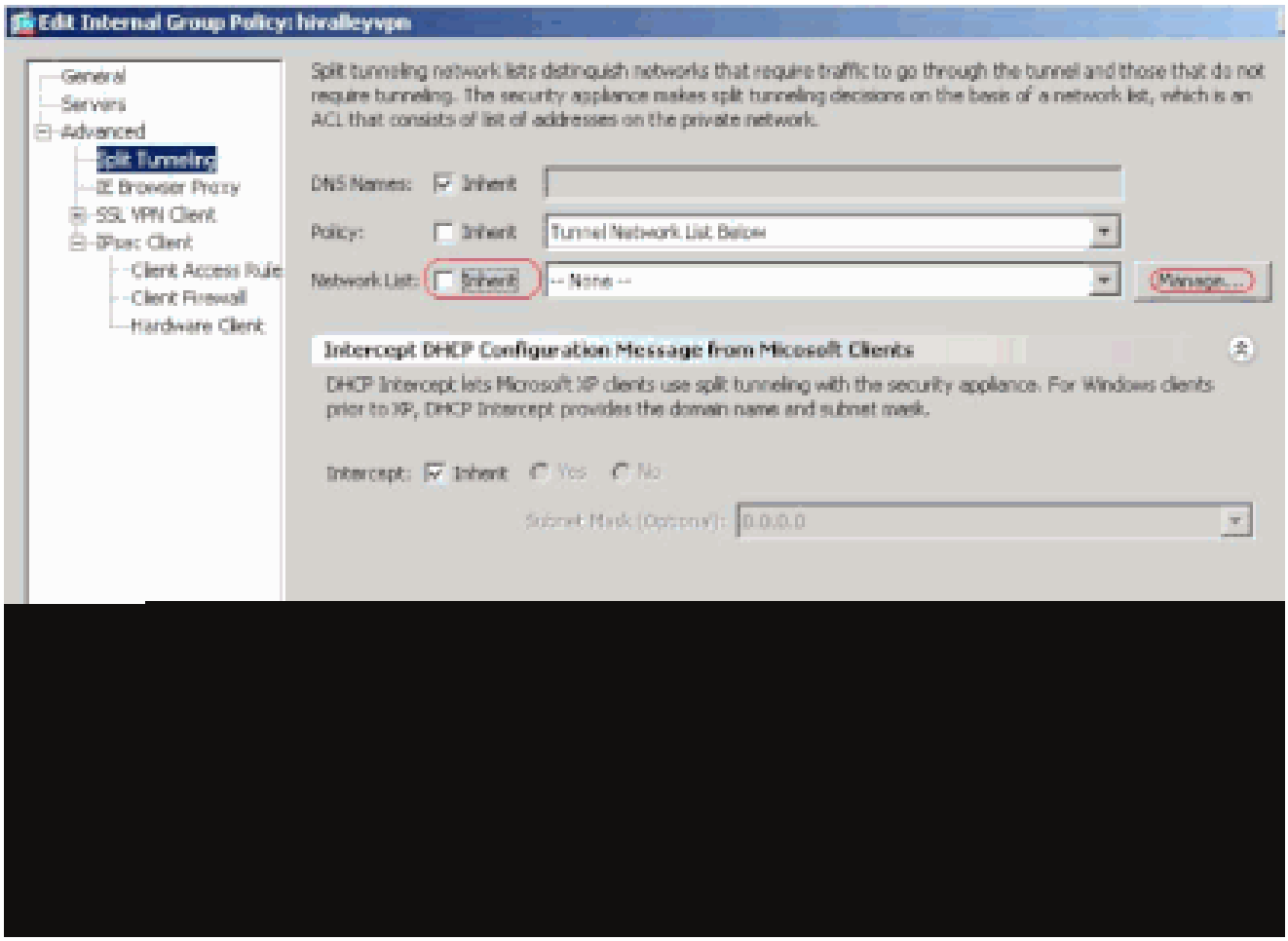
•

Deaktivieren Sie das Kontrollkästchen **Vererben** für Split Tunnel Policy, und wählen Sie **Tunnel Network List (Tunnelnetzliste unten) aus**.



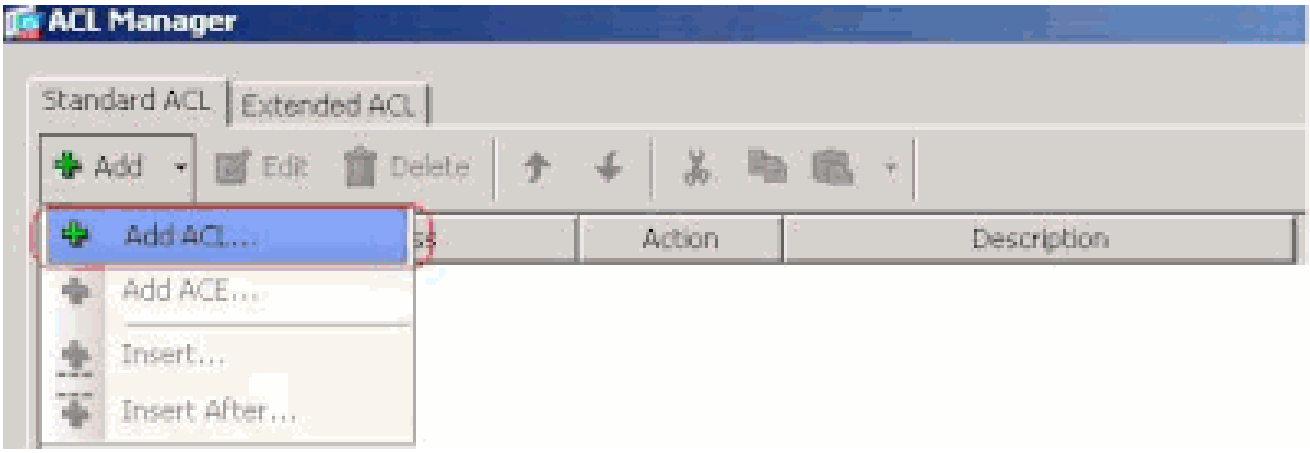
•

Deaktivieren Sie das Kontrollkästchen **Inherit** für Split Tunnel Network List, und klicken Sie dann auf **Manage (Verwalten)**, um den ACL Manager zu starten.



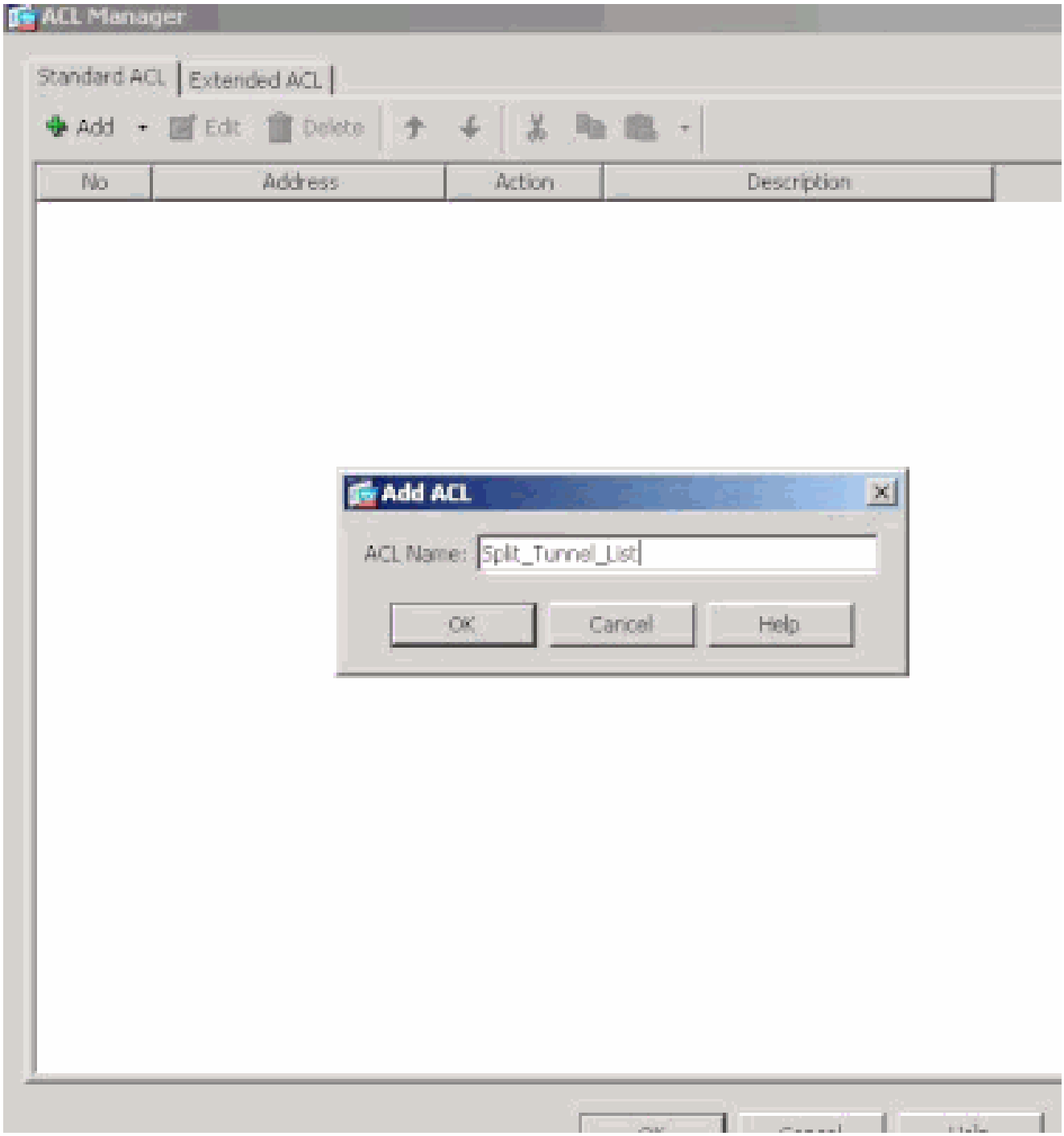
•

Wählen Sie in ACL Manager Add (Hinzufügen) > Add ACL ... (ACL hinzufügen ...) aus, um eine neue Zugriffsliste zu erstellen.



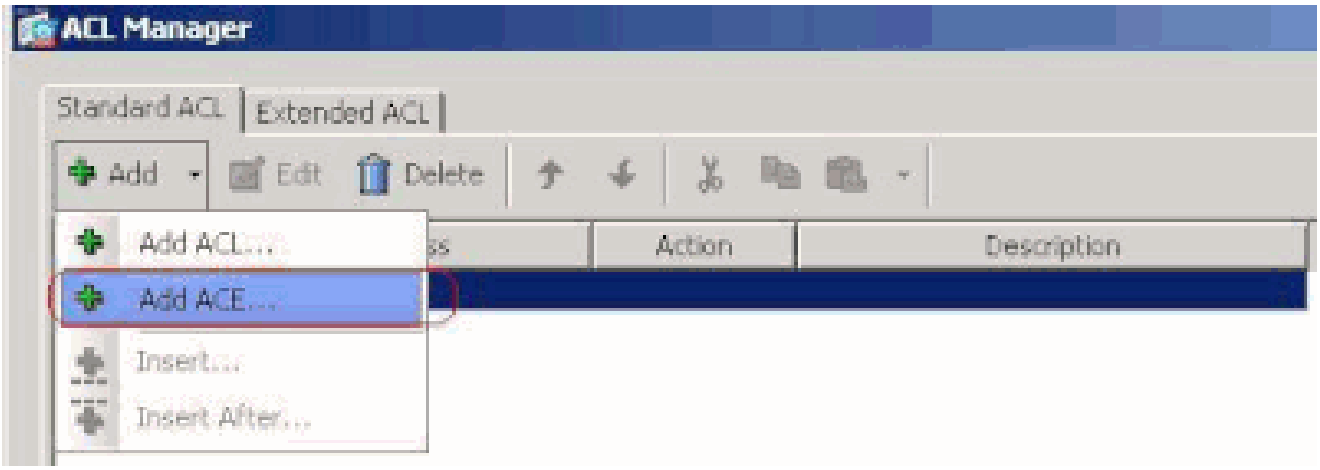
•

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



•

Wählen Sie nach Erstellung der ACL Add (Hinzufügen) > Add ACE ... (ACE hinzufügen ...) aus, um einen Zugriffskontrolleintrag (Access Control Entry, ACE) hinzuzufügen.



-

Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.

a.

Klicken Sie auf das Optionsfeld **Zulassen**.

b.

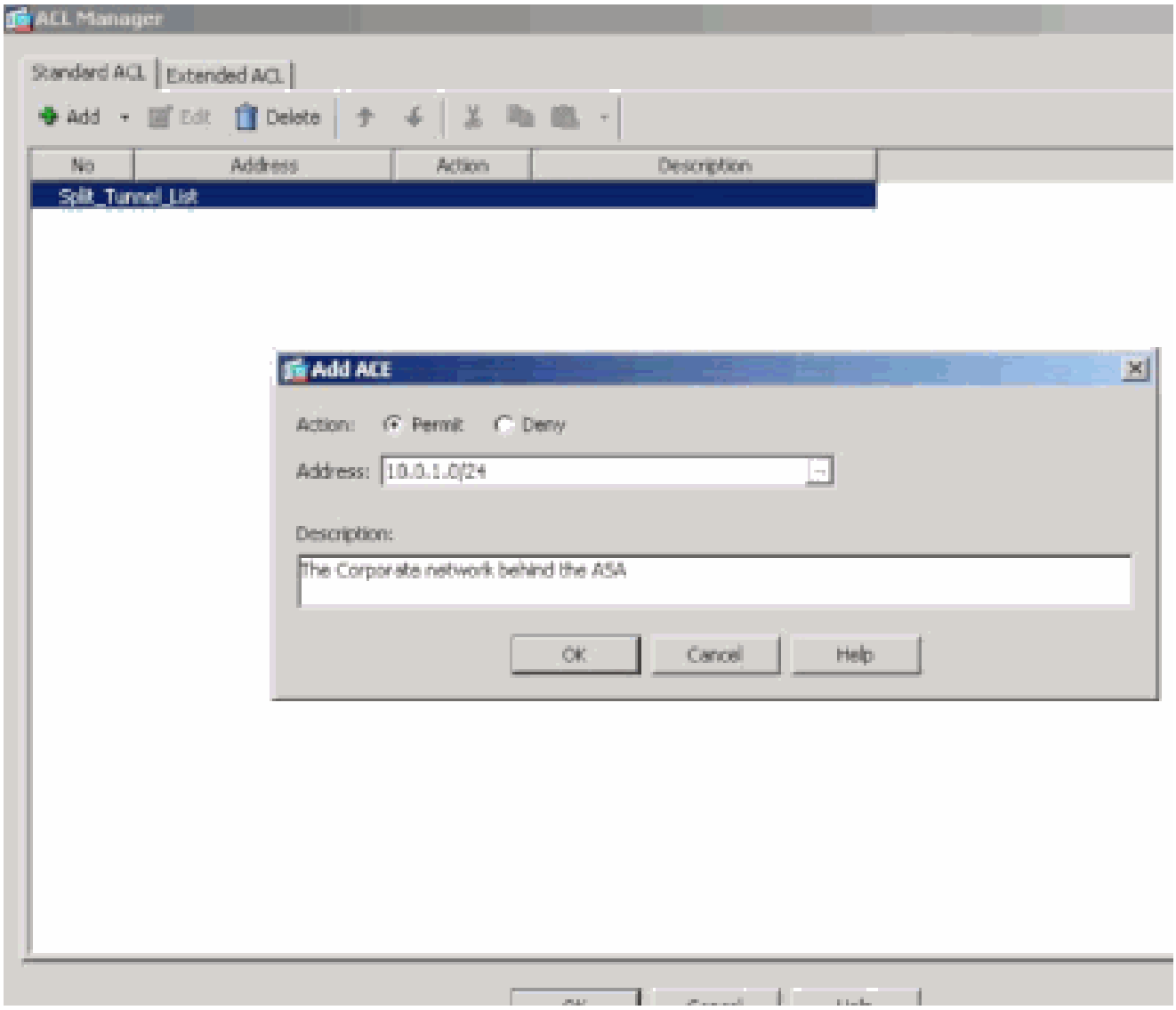
Wählen Sie die Netzwerkadresse mit der Maske **10.0.1.0/24 aus**.

c.

(Optional) Geben Sie eine Beschreibung ein.

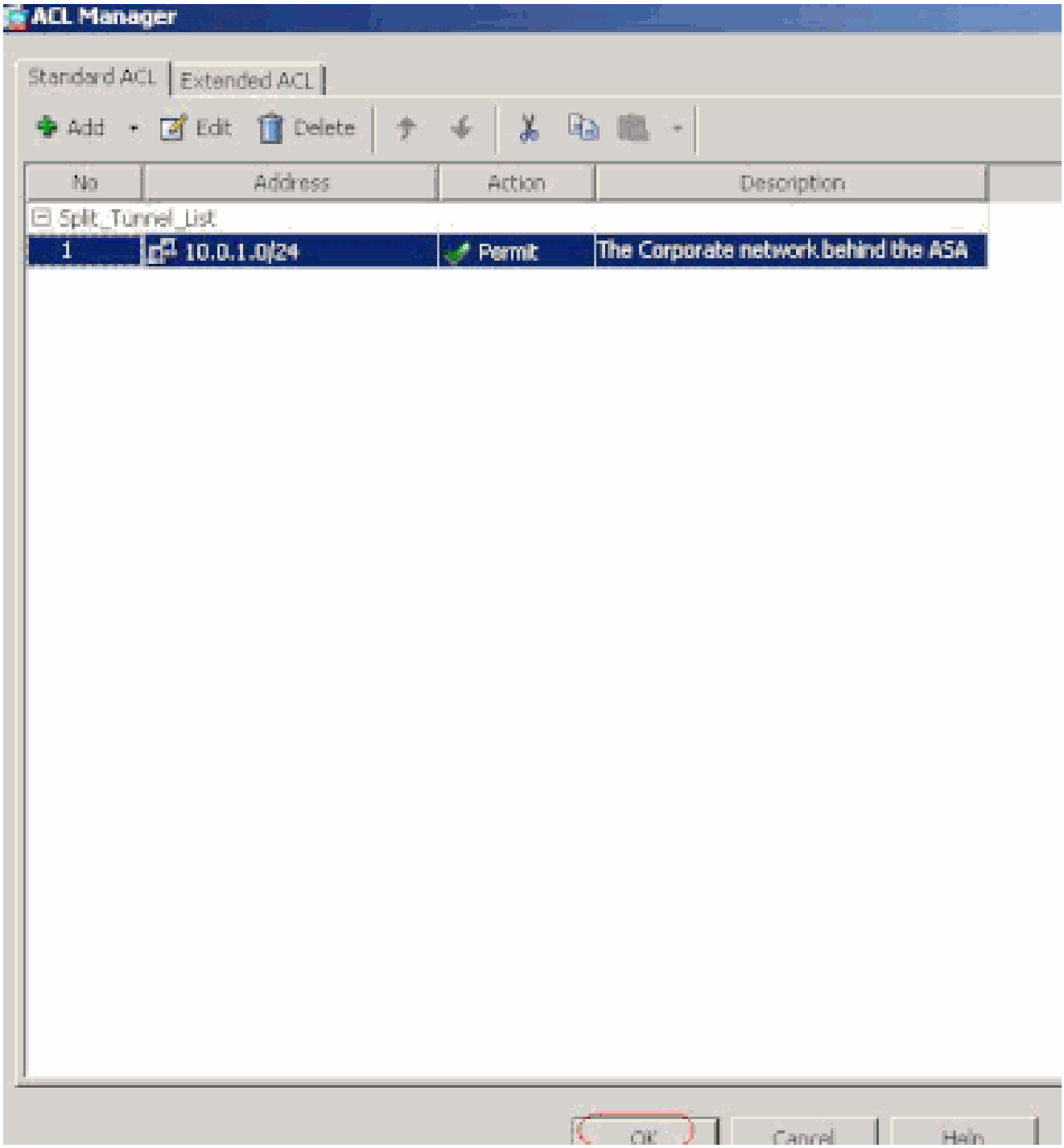
d.

Klicken Sie auf OK.



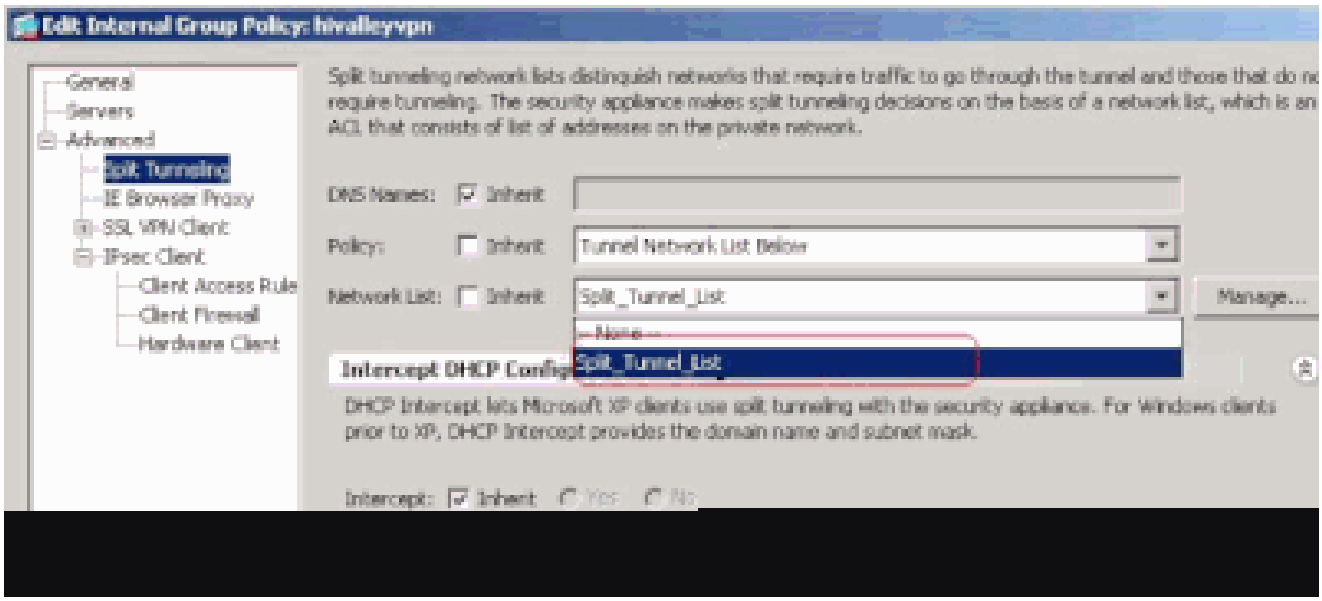
•

Klicken Sie auf OK, um ACL Manager zu beenden.



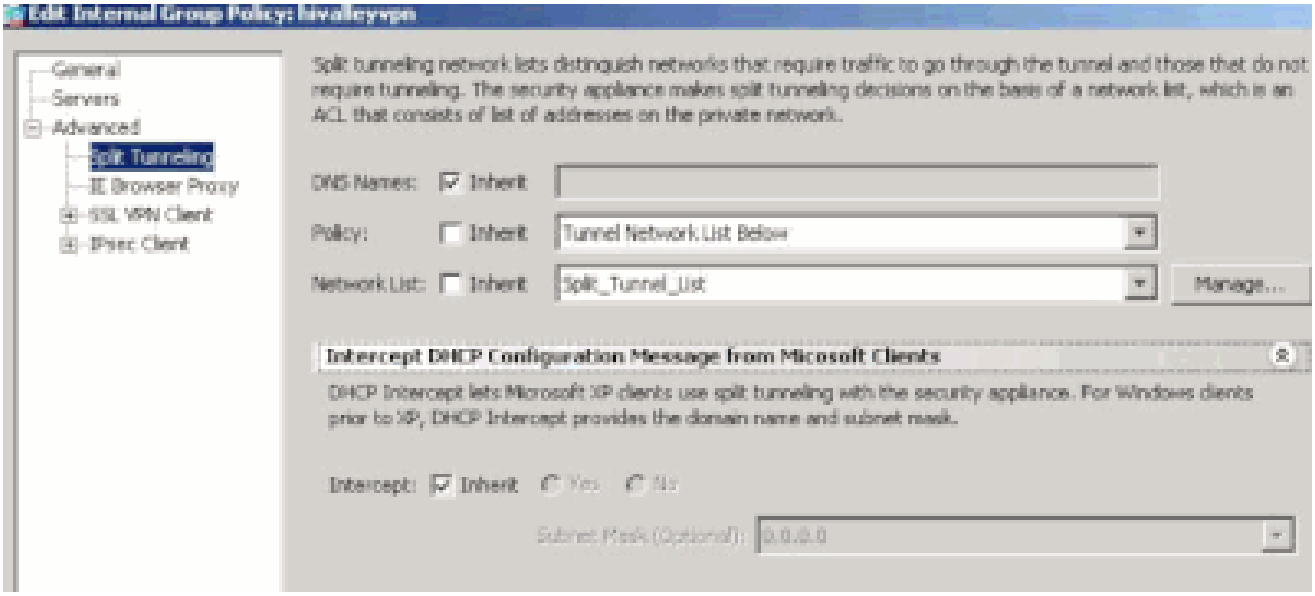
•

Vergewissern Sie sich, dass die soeben erstellte ACL für "Split Tunnel Network List" ausgewählt ist.



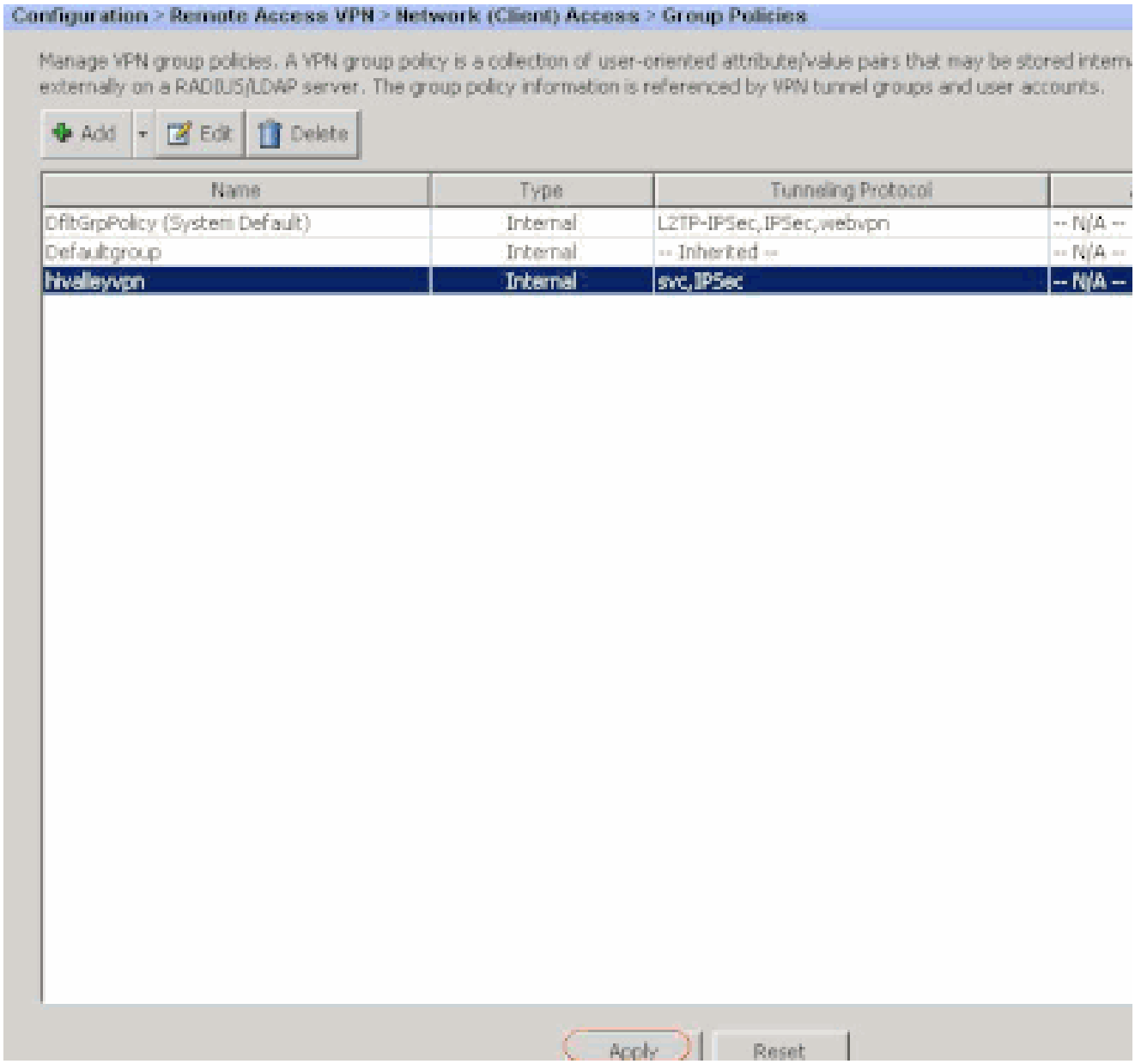
•

Klicken Sie auf OK, um zur Konfiguration der Gruppenrichtlinie zurückzukehren.



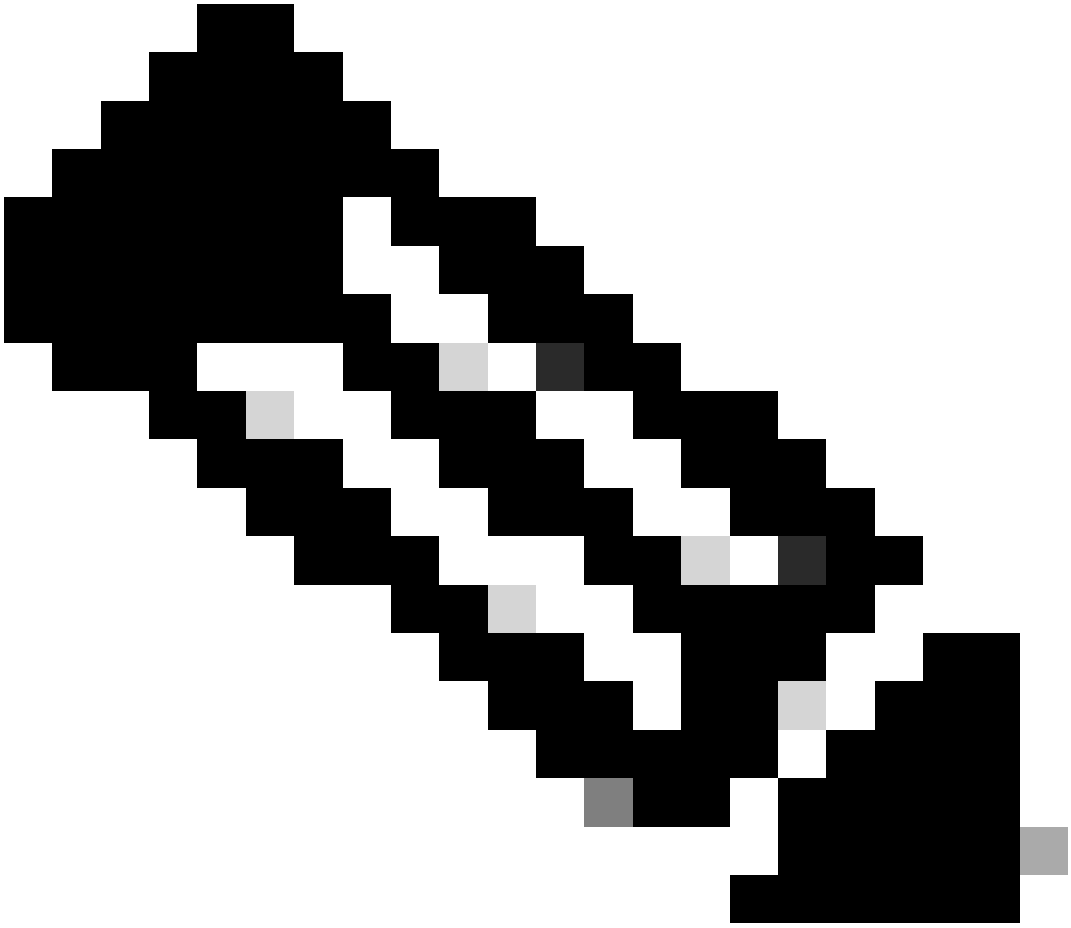
•

Klicken Sie auf Apply (Übernehmen) und dann ggf. auf Send (Senden), um die Befehle an die ASA zu senden.



Konfigurieren von ASA 7.x oder höher über CLI

Anstatt den ASDM zu verwenden, können Sie die folgenden Schritte in der ASA-CLI ausführen, um Split-Tunneling auf der ASA zu ermöglichen:



Hinweis: Die CLI Split Tunneling-Konfiguration ist für ASA 7.x und 8.x identisch.

- Wechseln Sie in den Konfigurationsmodus.

```
<#root>

ciscoasa>
```

```
enable
```

```
Password: ********
ciscoasa#
```

```
configure terminal
```

```
ciscoasa(config)#
```

-

Erstellen Sie die Zugriffsliste, die das Netzwerk hinter der ASA definiert.

```
<#root>
```

```
ciscoasa(config)#
```

```
 access-list Split_Tunnel_List remark The corporate network behind the ASA.
```

```
ciscoasa(config)#
```

```
 access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

-

Wechseln Sie in den Gruppenrichtlinienkonfigurationsmodus für die Richtlinie, die Sie ändern möchten.

```
<#root>
```

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

-

Geben Sie die Split-Tunnel-Richtlinie an. In diesem Fall ist die Richtlinie **tunnelspecified**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

-

Geben Sie die Split-Tunnel-Zugriffsliste an. In diesem Fall lautet die Liste **Split_Tunnel_List**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-network-list value Split_Tunnel_List
```

-

Führen Sie folgenden Befehl aus,

```
    <#root>

ciscoasa(config)#

 tunnel-group hillvalleyvpn general-attributes
```

-

Ordnen Sie die Gruppenrichtlinie der Tunnelgruppe zu

```
    <#root>

ciscoasa(config-tunnel-ipsec)#

 default-group-policy hillvalleyvpn
```

-

Beenden Sie die beiden Konfigurationsmodi.

```
    <#root>

ciscoasa(config-group-policy)#

 exit

ciscoasa(config)#

 exit
```

```
ciscoasa#
```

- Speichern Sie die Konfiguration im nichtflüchtigen RAM (NVRAM), und drücken Sie die Eingabetaste, wenn Sie aufgefordert werden, den Quelldateinamen anzugeben.

```
<#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#
```

Konfigurieren von PIX 6.x über die CLI

Führen Sie diese Schritte aus:

- Erstellen Sie die Zugriffsliste, die das Netzwerk hinter dem PIX definiert.

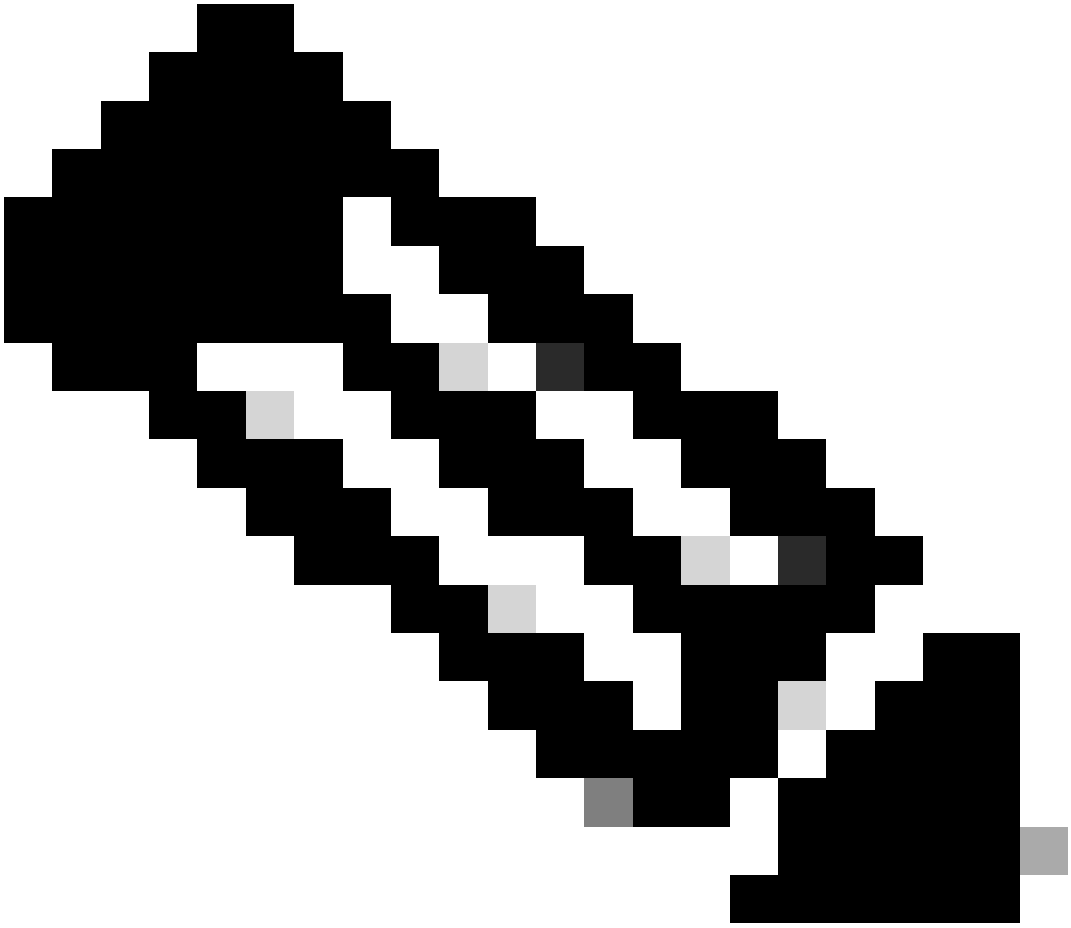
```
<#root>

 PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- Erstellen Sie eine VPN-Gruppe "**vpn3000**", und geben Sie die ACL des Split-Tunnels wie folgt an:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



Hinweis: Weitere Informationen zur Remotezugriff-VPN-Konfiguration für PIX 6.x finden Sie unter Cisco Secure PIX Firewall 6.x und Cisco VPN Client 3.5 für Windows mit Microsoft Windows 2000 und 2003 IAS RADIUS Authentication.

Überprüfung

Gehen Sie wie in diesem Abschnitt beschrieben vor, um Ihre Konfiguration zu überprüfen.

- Mit dem VPN-Client verbinden

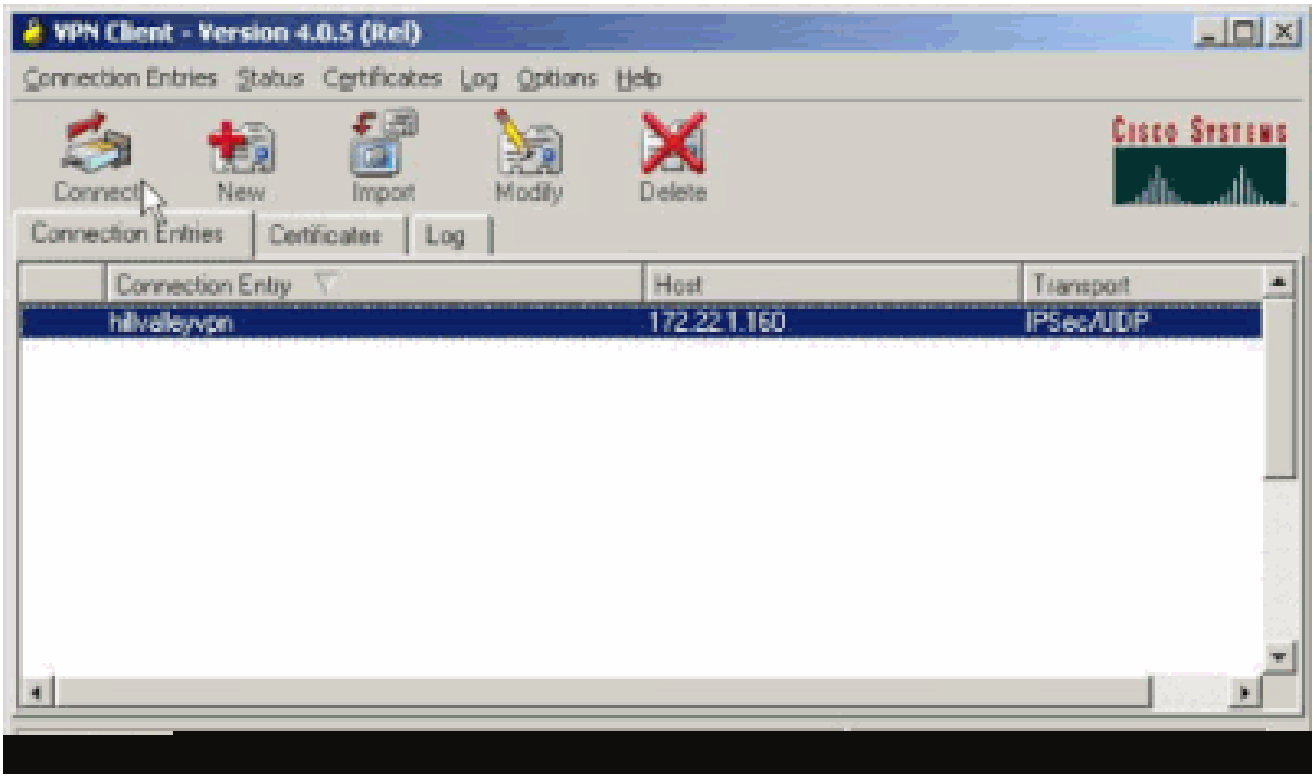
- VPN-Client-Protokoll anzeigen

- Testen des lokalen LAN-Zugriffs mit Ping

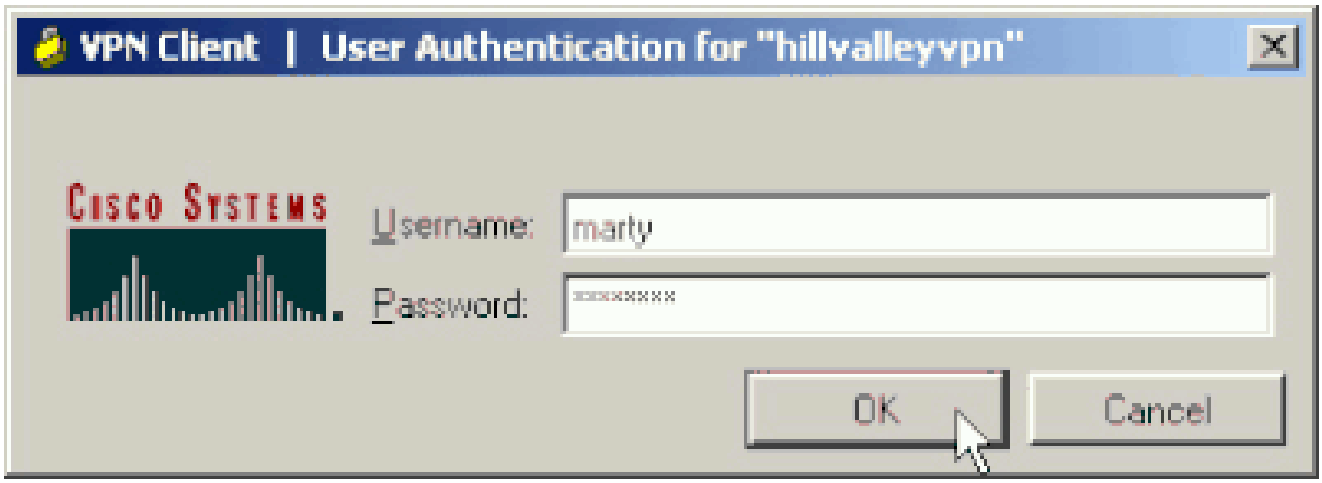
Mit dem VPN-Client verbinden

Verbinden Sie den VPN-Client mit dem VPN Concentrator, um die Konfiguration zu überprüfen.

- Wählen Sie Ihren Verbindungseintrag aus der Liste aus, und klicken Sie auf **Verbinden**.

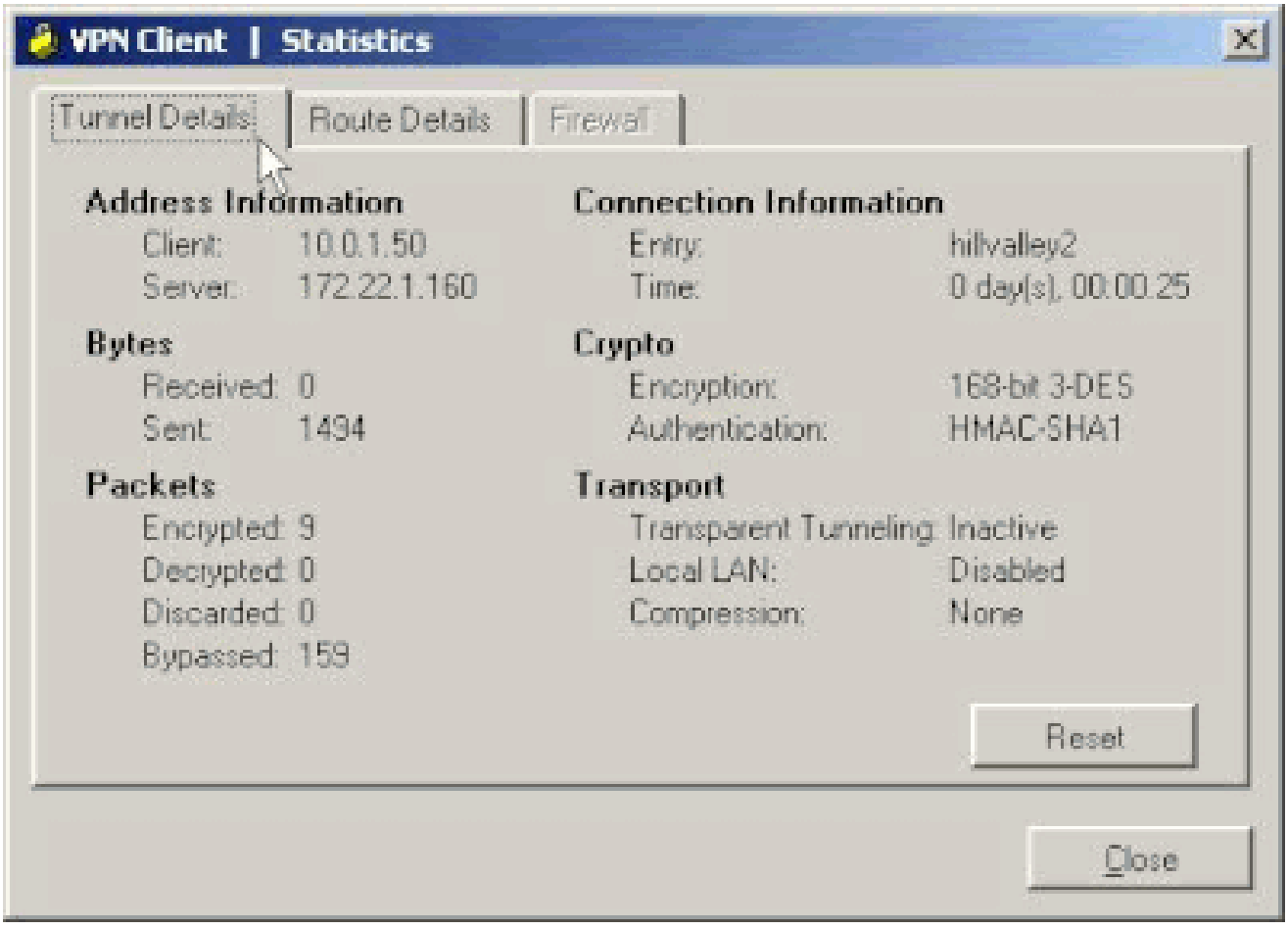


- Geben Sie Ihre Anmeldeinformationen ein.



-

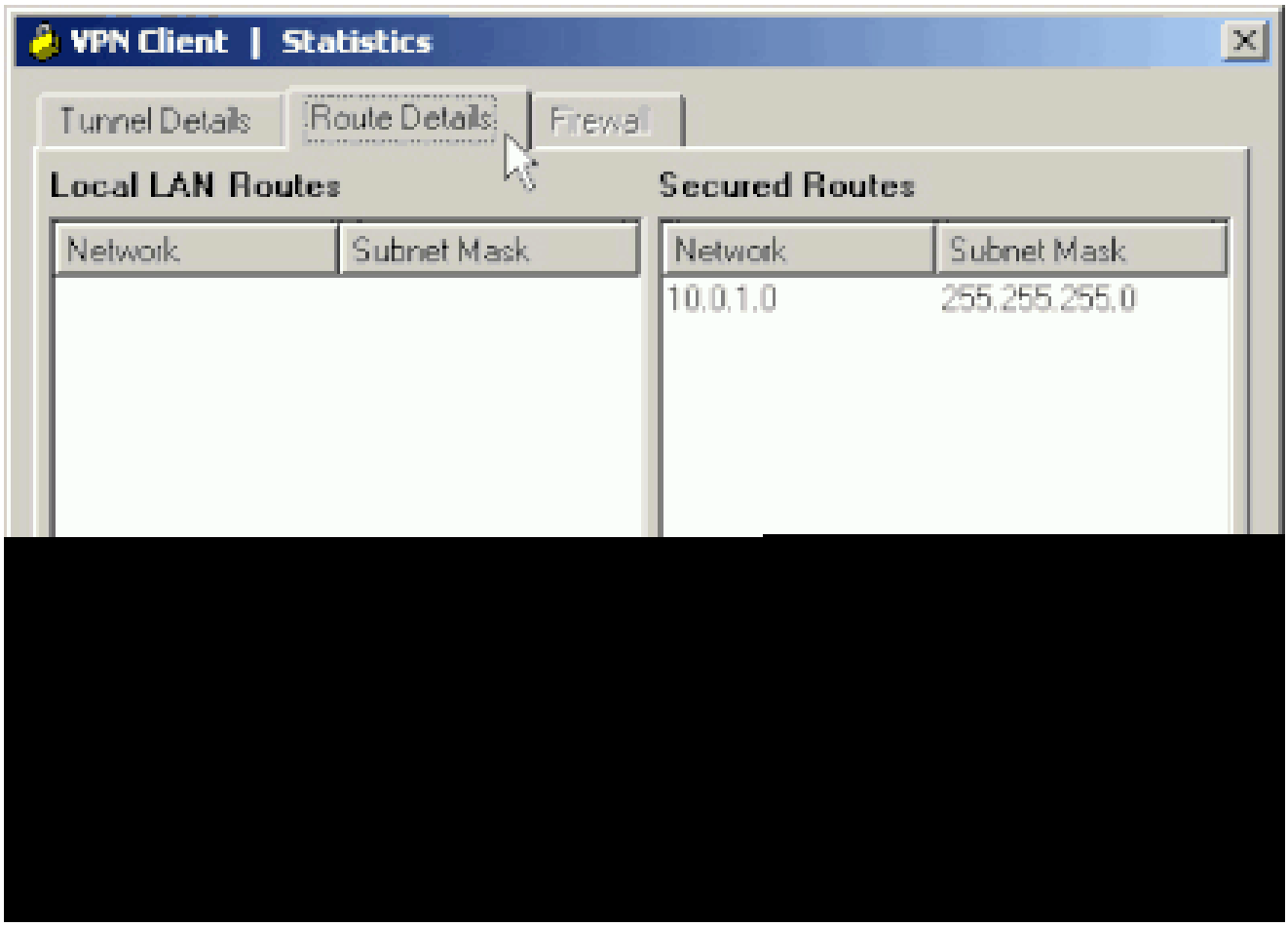
Wählen Sie **Status > Statistics... (Status > Statistik)**, um das Fenster "Tunnel Details" anzuzeigen, in dem Sie die Details des Tunnels überprüfen und den Verkehrsfluss sehen können.



-

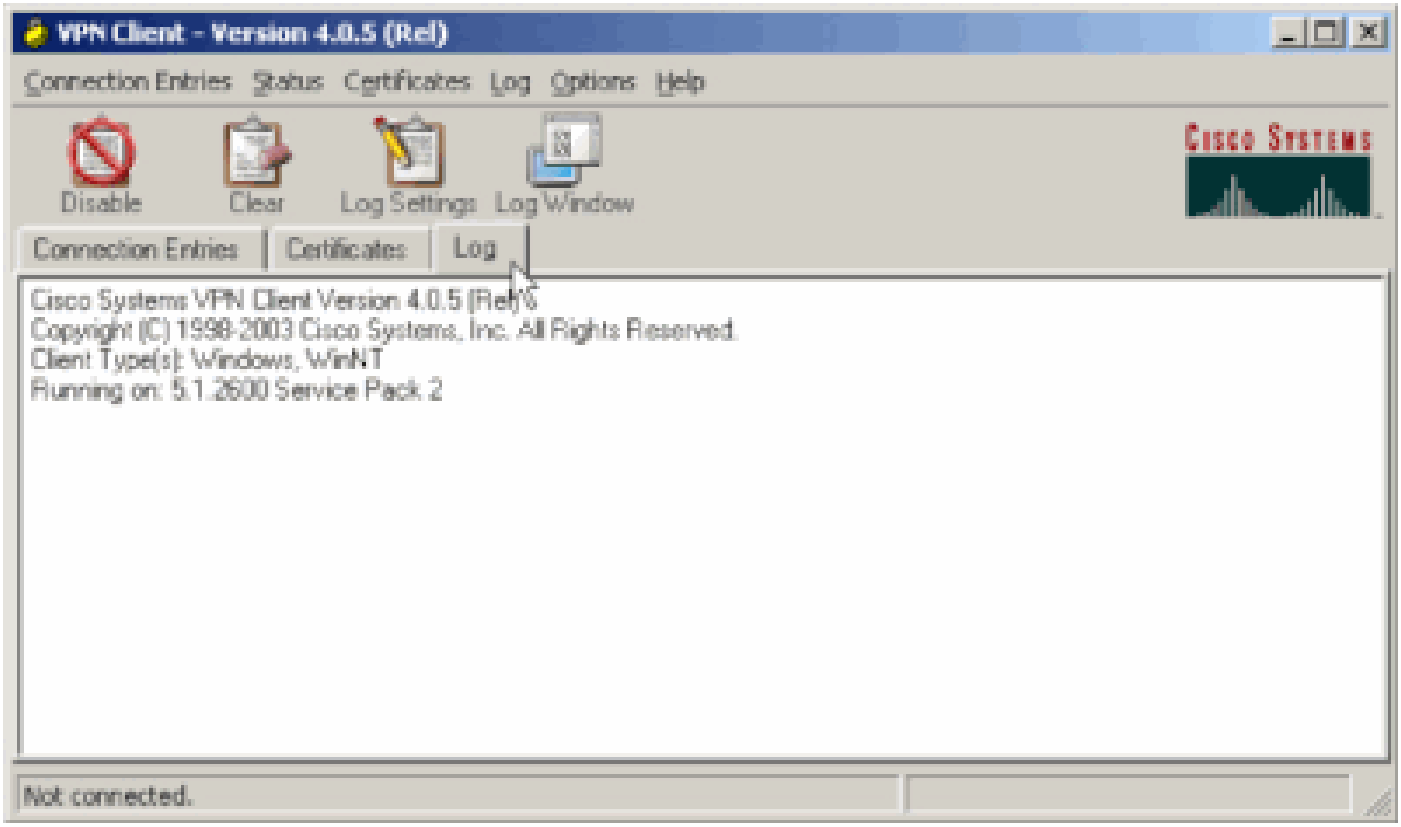
Rufen Sie die Registerkarte Route Details (Routendetails) auf, um die Routen anzuzeigen, die der VPN-Client mit der ASA sichert.

In diesem Beispiel sichert der VPN-Client den Zugriff auf 10.0.1.0/24, während der gesamte andere Datenverkehr nicht verschlüsselt wird und nicht über den Tunnel gesendet wird.



VPN-Client-Protokoll anzeigen

Wenn Sie das Protokoll des VPN-Clients überprüfen, können Sie bestimmen, ob der Parameter, der Split-Tunneling angibt, festgelegt ist. Um das Protokoll anzuzeigen, gehen Sie zur Registerkarte Log (Protokoll) im VPN Client. Klicken Sie dann auf **Log Settings**, um anzupassen, was protokolliert wird. In diesem Beispiel ist IKE auf **3 - Hoch** festgelegt, während alle anderen Protokollelemente auf **1 - Niedrig** festgelegt sind.




```
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 supressed


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

!--- Split tunneling is permitted and the remote LAN is defined.

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

30     14:20:14.238  07/27/06  Sev=Info/5    IKE/0x6300000F
SPLIT_NET #1
    subnet = 10.0.1.0
    mask = 255.255.255.0
    protocol = 0
    src port = 0
    dest port=0

!--- Output is supressed.
```

Testen des lokalen LAN-Zugriffs mit Ping

Eine weitere Möglichkeit, zu testen, ob der VPN-Client für Split-Tunneling konfiguriert ist, während er an die ASA getunnelt wird, besteht darin, den Befehl **ping** in der Windows-Befehlszeile zu verwenden. Das lokale LAN des VPN-Clients ist 192.168.0.0/24, und ein anderer Host ist im Netzwerk mit der IP-Adresse 192.168.0.3 vorhanden.

```
   <#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
```

Fehlerbehebung

Beschränkung mit der Anzahl der Einträge in einer Split-Tunnel-ACL

Die Anzahl der Einträge in einer ACL für Split-Tunnel ist begrenzt. Es wird empfohlen, nicht mehr als 50-60 ACE-Einträge zu verwenden, um eine zufriedenstellende Funktionalität sicherzustellen. Es wird empfohlen, die Subnetzfunktion zu implementieren, um einen Bereich von IP-Adressen abzudecken.

Zugehörige Informationen

- **PIX/ASA 7.x als Remote-VPN-Server mit ASDM-Konfigurationsbeispiel**
- **Cisco Adaptive Security Appliances der Serie ASA 5500**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.