ASA/PIX: Split Tunneling für VPN-Clients im ASA-Konfigurationsbeispiel zulassen

Inhalt

Einführung

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

Hinweis: Vollständiges Tunneling gilt als die sicherste Konfiguration, da es nicht den gleichzeitigen Gerätezugriff auf das Internet und das Firmen-LAN ermöglicht. Ein Kompromiss zwischen Voll-Tunneling und Split-Tunneling ermöglicht nur den lokalen LAN-Zugriff von VPN-Clients. Siehe PIX/ASA 7.x: Konfigurationsbeispiel für VPN-Clients den lokalen LAN-Zugriff für weitere Informationen zulassen.

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 unter Verwendung des ASDM-Konfigurationsbeispiels, falls dieser noch nicht konfiguriert ist.

Verwendete Komponenten

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

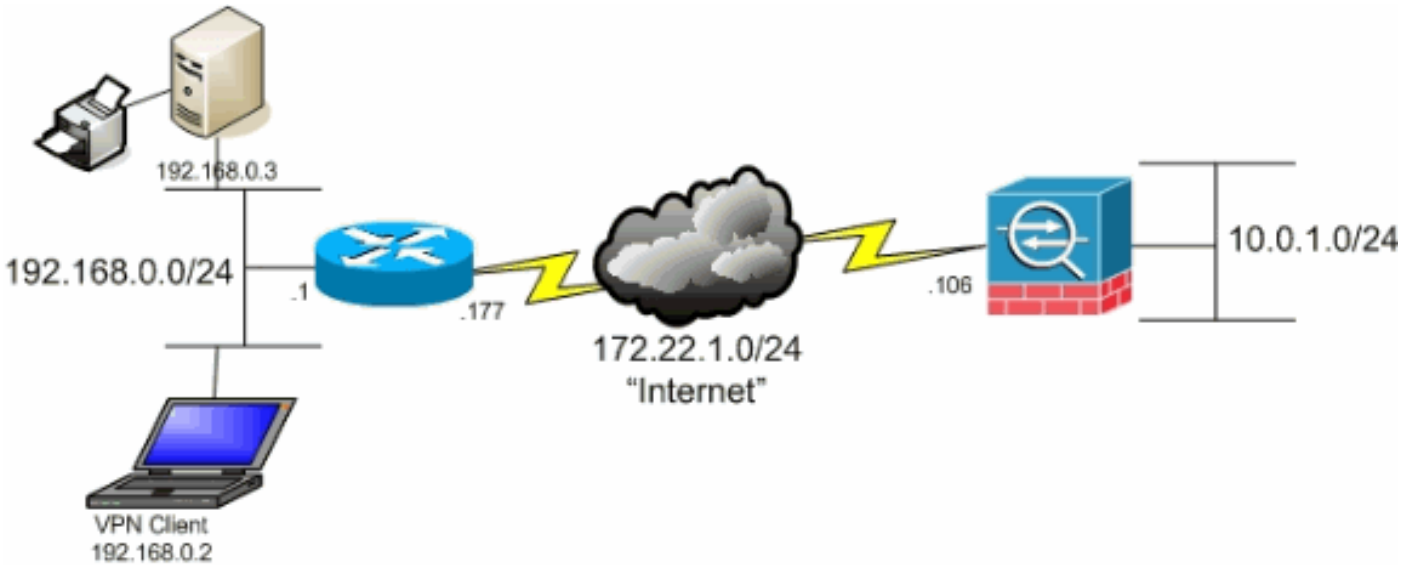
- Cisco Security Appliance der Serie ASA 5500 Softwareversion 7.x und höher
- Cisco Systems VPN Client Version 4.0.5

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

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



Zugehörige Produkte

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

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips

Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

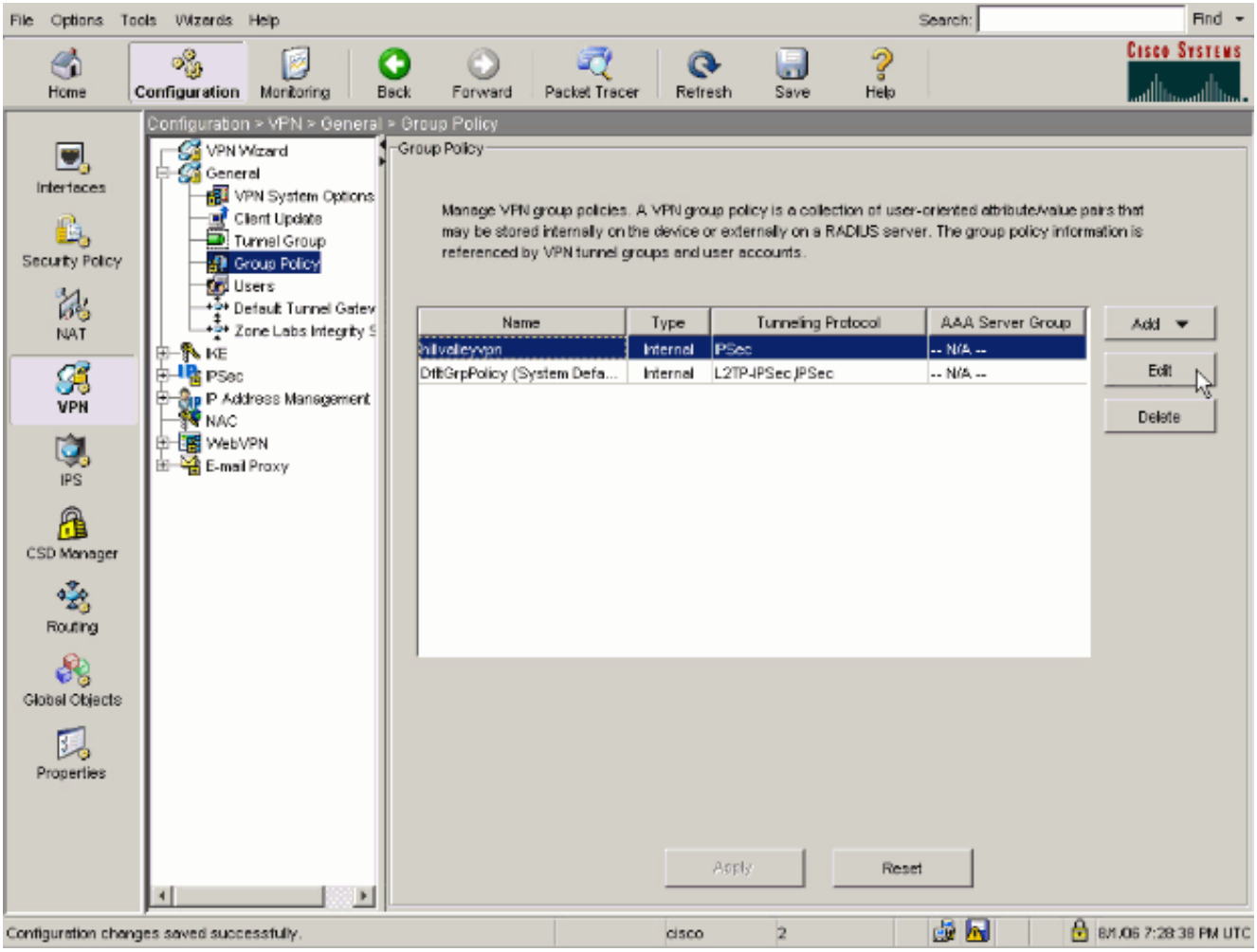
In einem grundlegenden VPN Client-zu-ASA-Szenario wird der gesamte Datenverkehr vom VPN-Client verschlüsselt und an die ASA gesendet, unabhängig von dessen Ziel. Basierend auf Ihrer Konfiguration und der Anzahl der unterstützten Benutzer kann eine solche Einrichtung bandbreitenintensiv sein. Durch Split-Tunneling kann dieses Problem behoben werden, da die Benutzer nur den Datenverkehr senden können, der für das Unternehmensnetzwerk bestimmt ist. Sämtlicher anderer Datenverkehr wie Instant Messaging, E-Mail oder gelegentliches Surfen wird über das lokale LAN des VPN-Clients ins Internet gesendet.

Konfigurieren von Split Tunneling auf der ASA

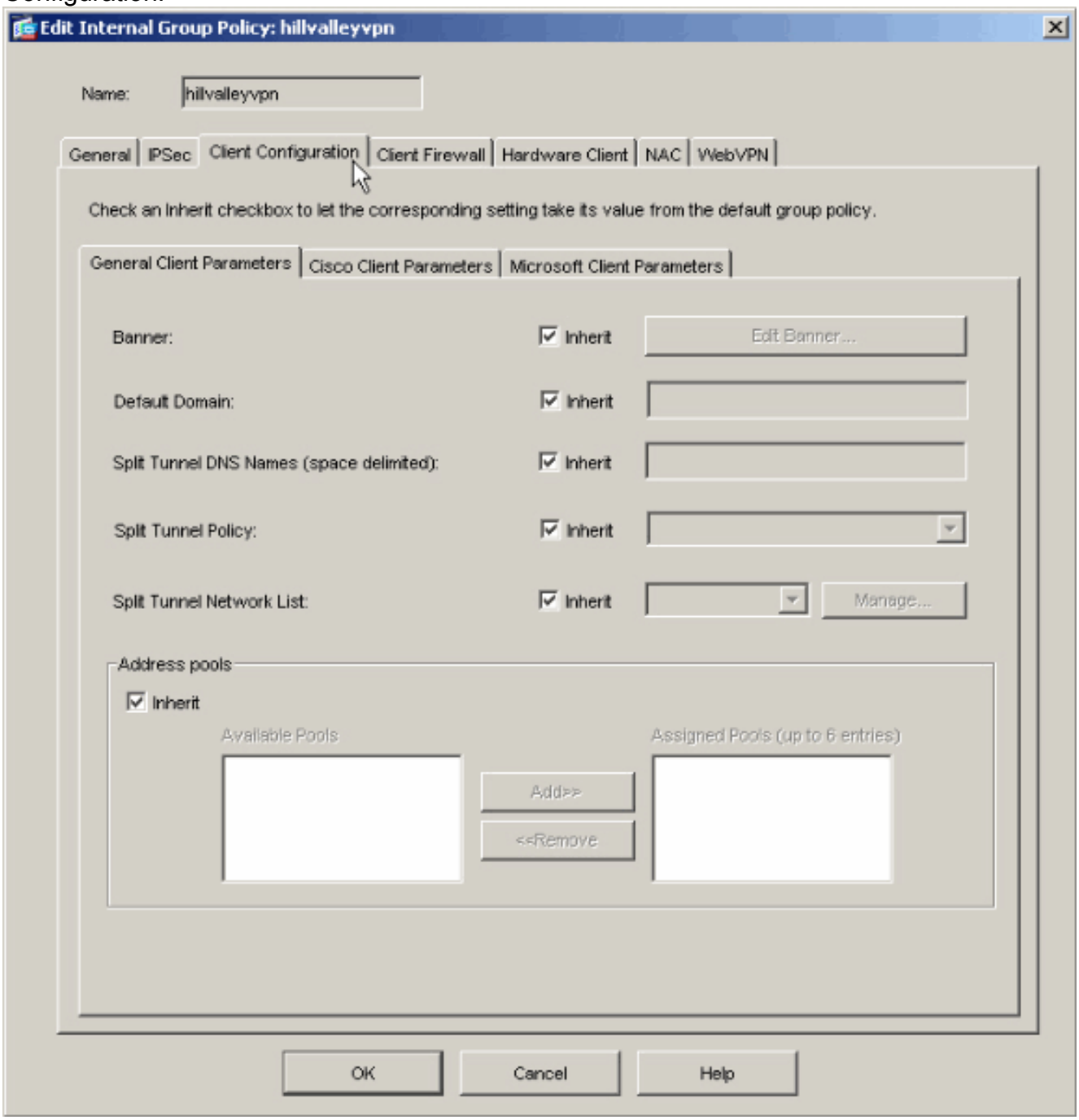
Konfigurieren Sie die ASA 7.x mit dem Adaptive Security Device Manager (ASDM) 5.x

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

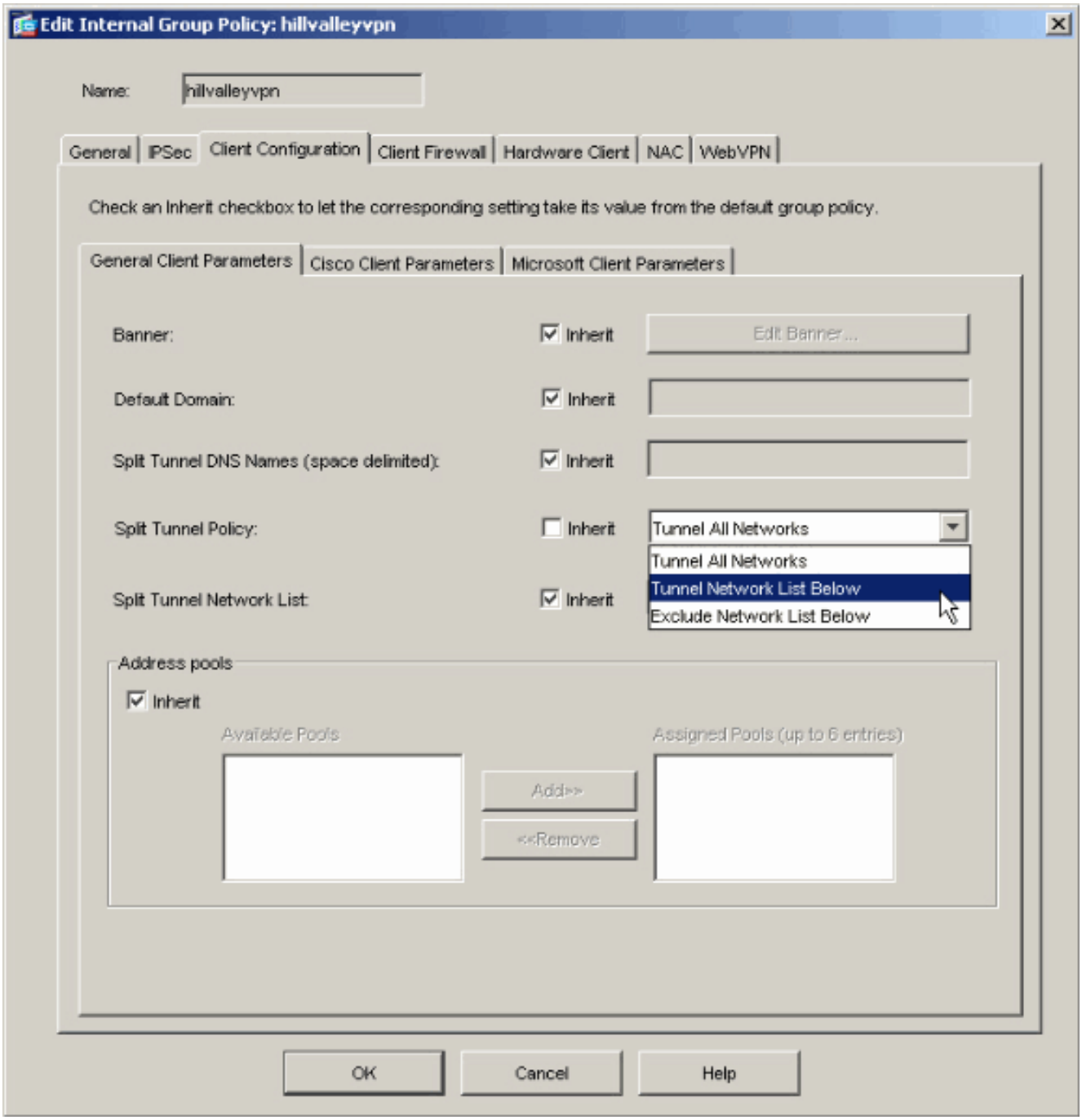
1. Wählen Sie **Configuration > VPN > General > Group Policy (Konfiguration > VPN > Allgemein > Gruppenrichtlinie)** und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken Sie anschließend auf **Bearbeiten**.



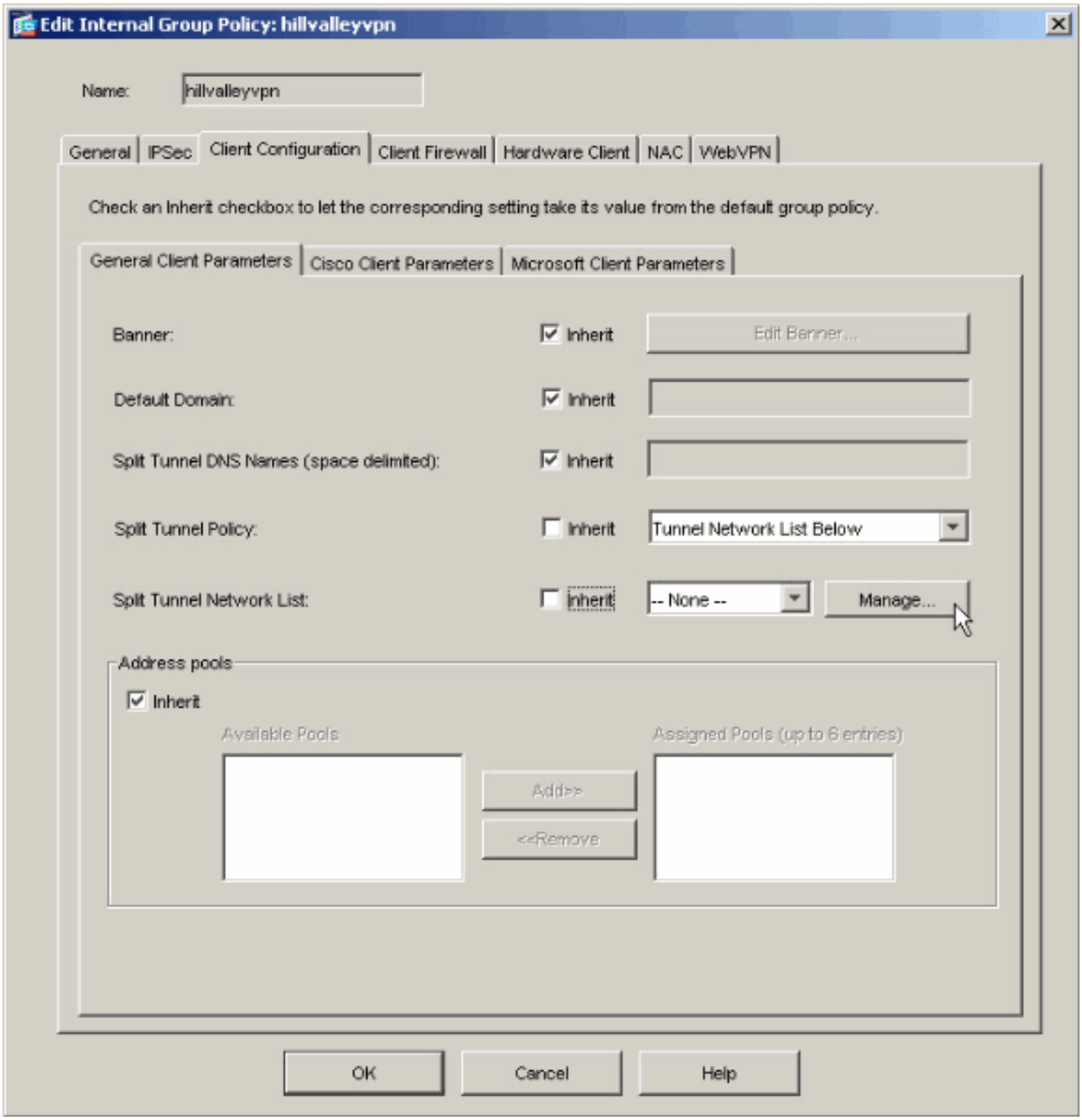
2. Öffnen Sie die Registerkarte Client Configuration.



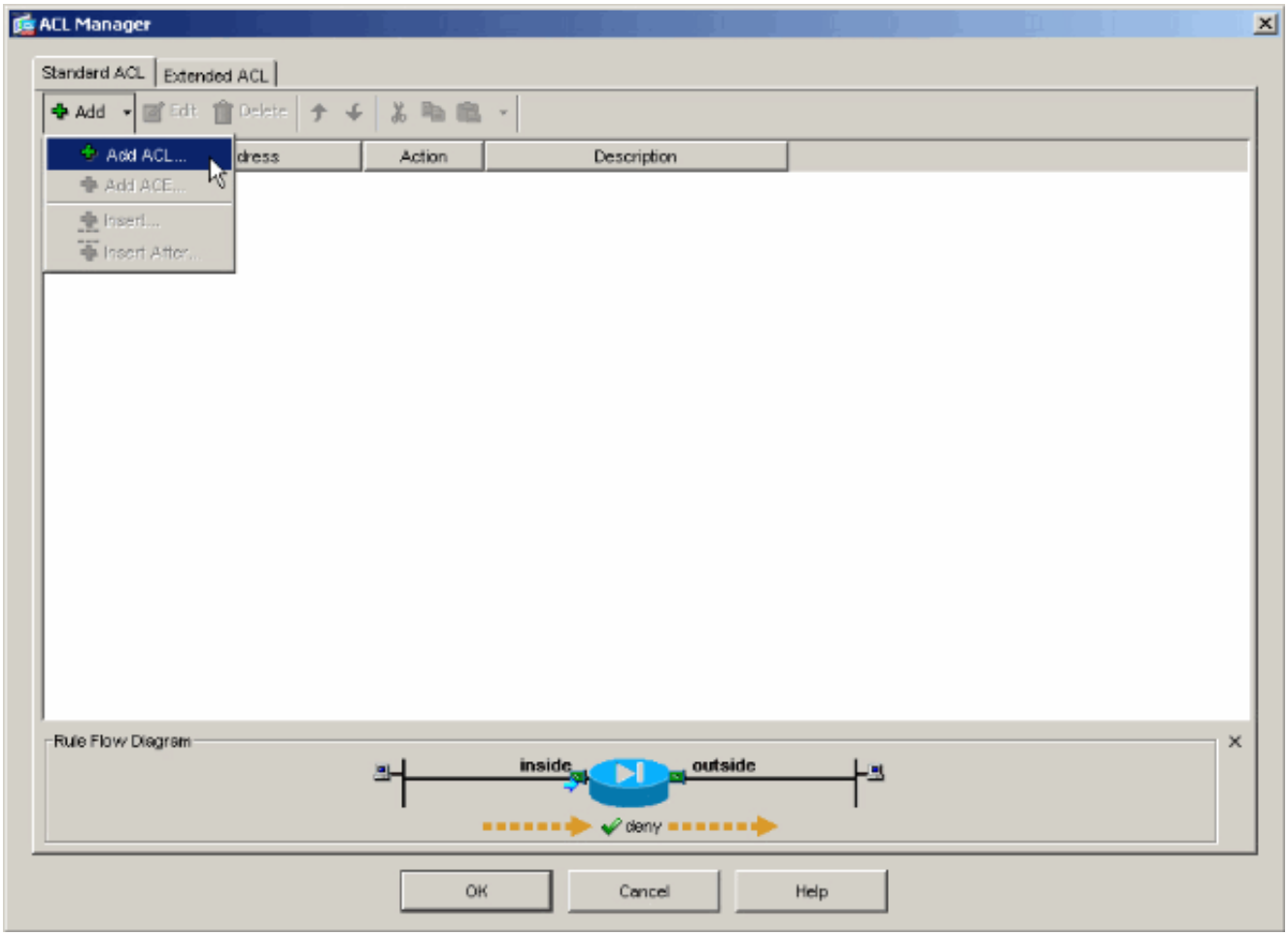
3. Deaktivieren Sie das Kontrollkästchen **Inherit** (**Erben**) für Split Tunnel Policy (Tunnelrichtlinie aufteilen), und wählen Sie **unten Tunnel Network List (Tunnelnetzwerkliste)**.



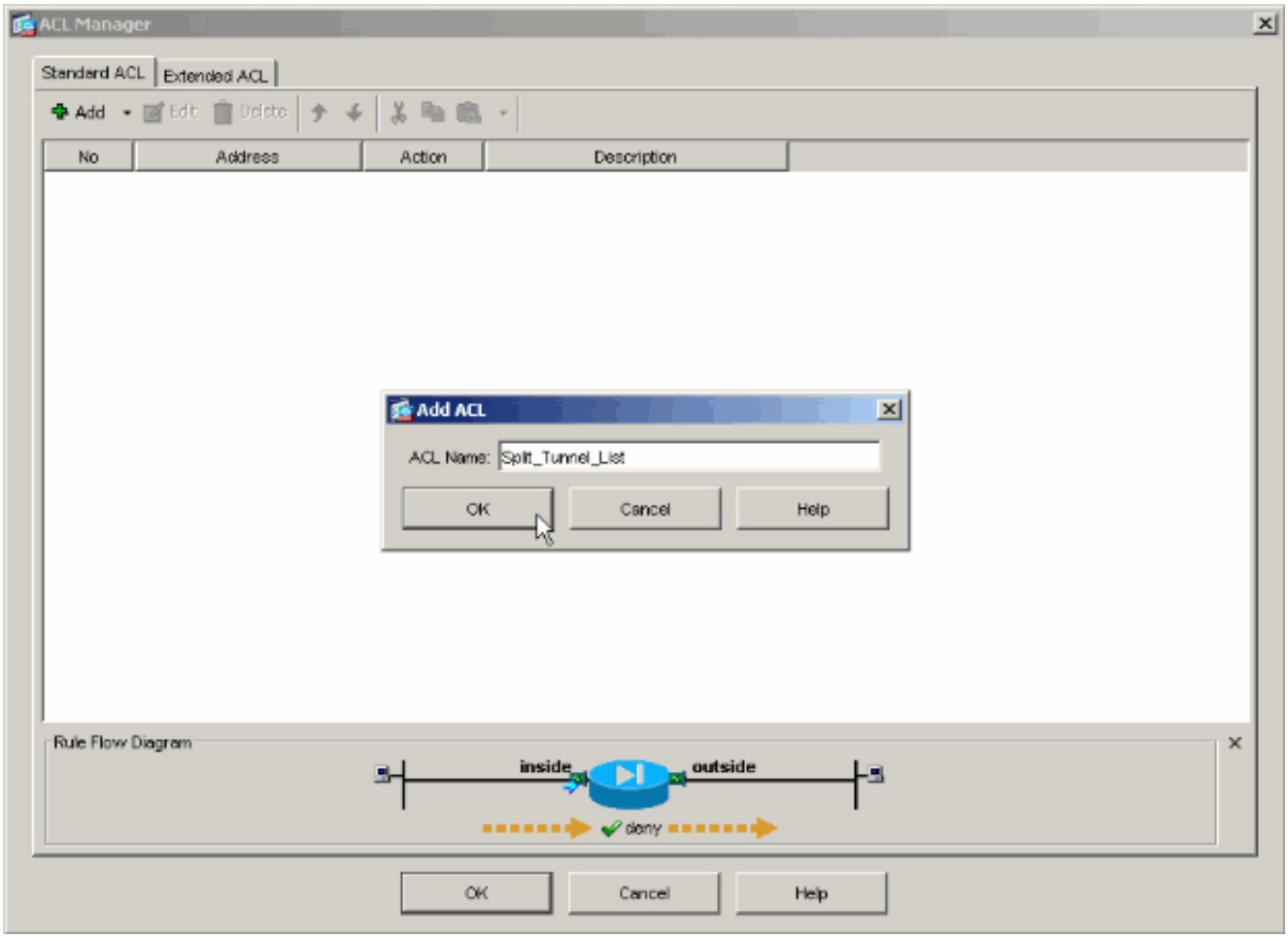
4. Deaktivieren Sie das Feld **Erben** für "Tunnel-Netzwerkliste teilen", und klicken Sie dann auf **Verwalten**, um den ACL Manager zu starten.



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

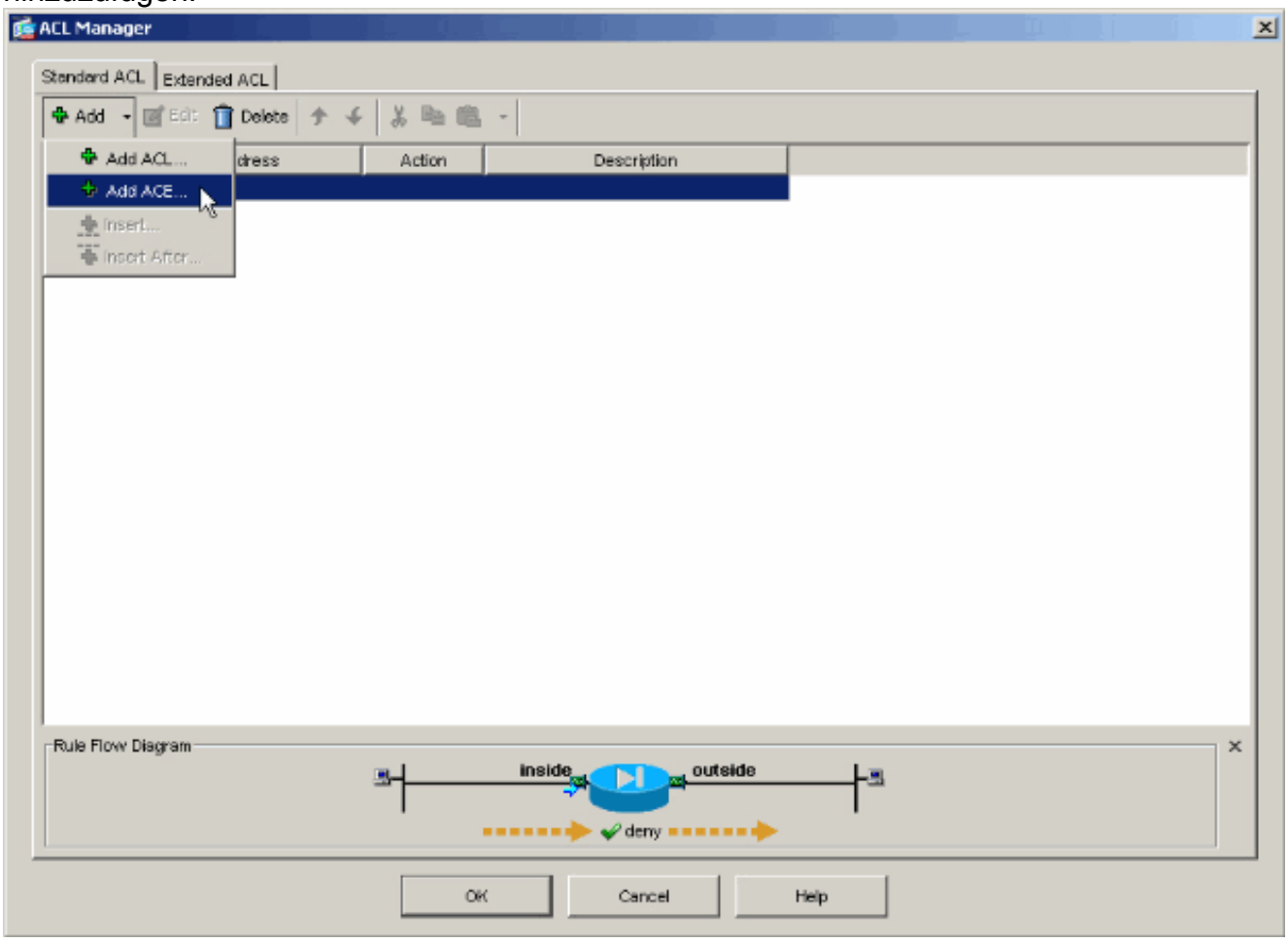


6. Geben Sie einen Namen für die ACL an, und klicken Sie auf **OK**.

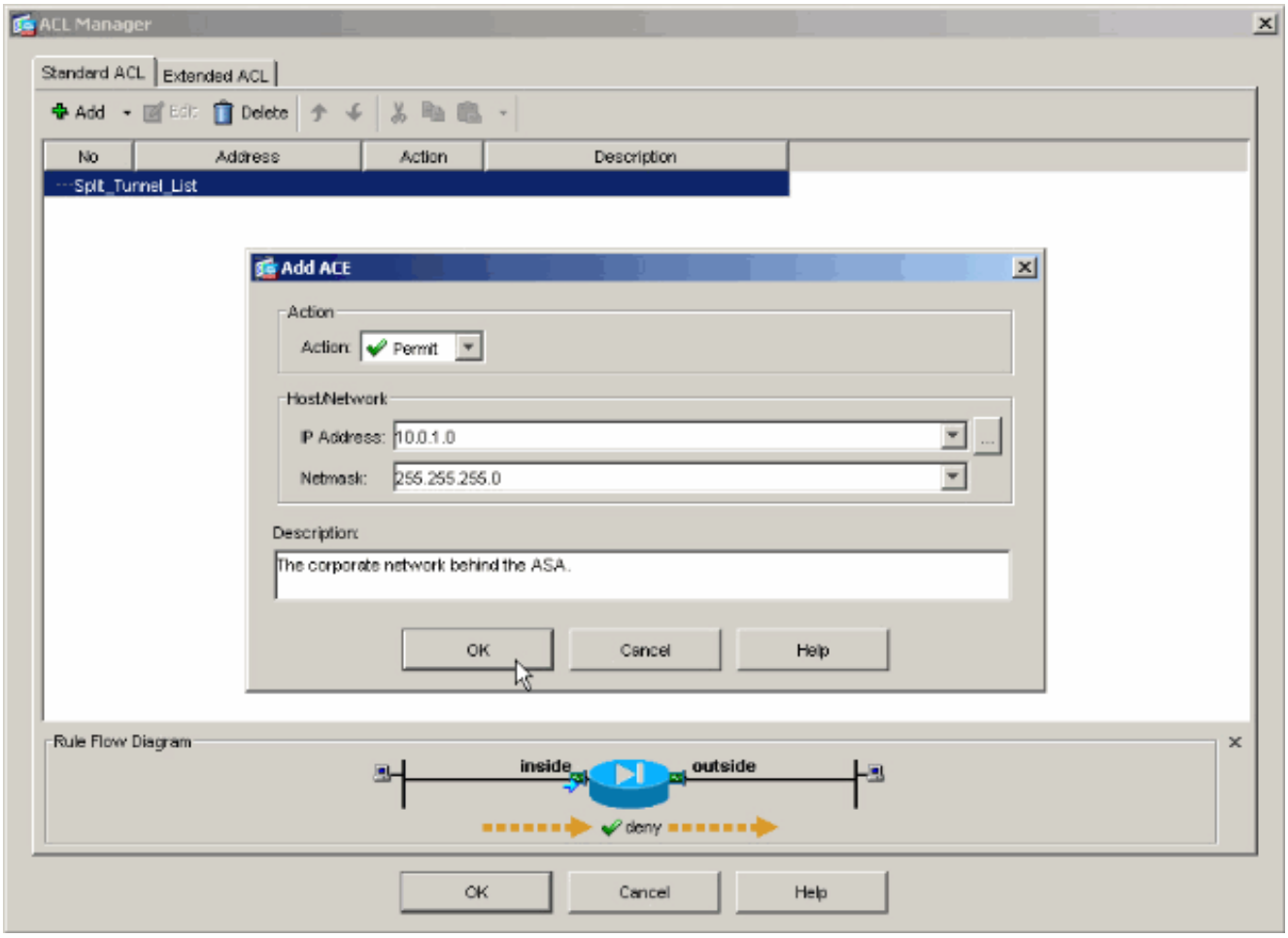


7. Wenn die ACL erstellt wurde, wählen Sie **Add > Add ACE.. (Hinzufügen > ACE hinzufügen)**

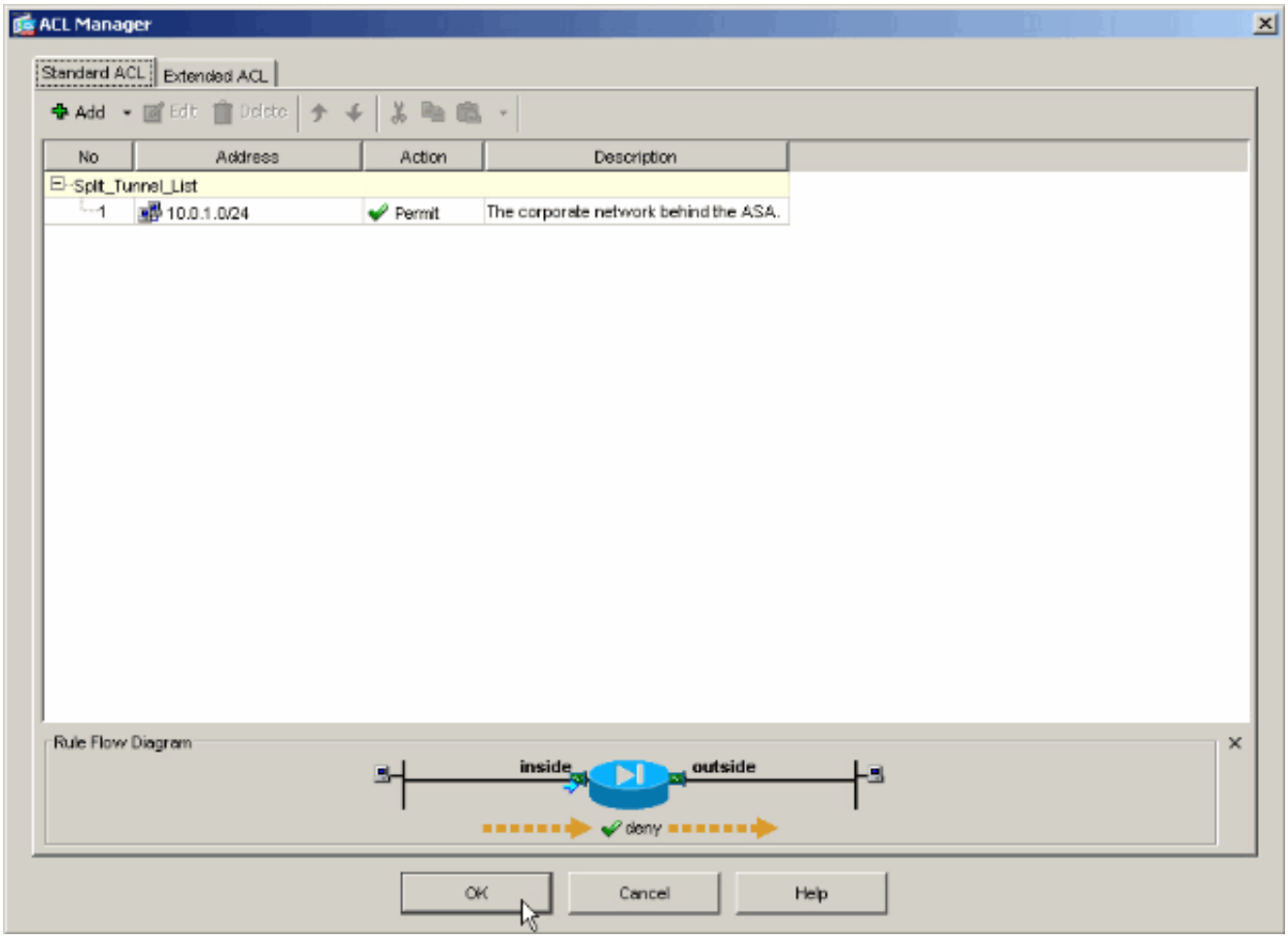
aus. um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen.



8. Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das Netzwerk 10.0.1.0/24.Wählen Sie **Zulassen aus**.Wählen Sie eine IP-Adresse von **10.0.1.0 aus.**Wählen Sie die Netzmaske **255.255.255.0 aus**.*(Optional)* Geben Sie eine Beschreibung an.Klicken Sie auf **OK**.

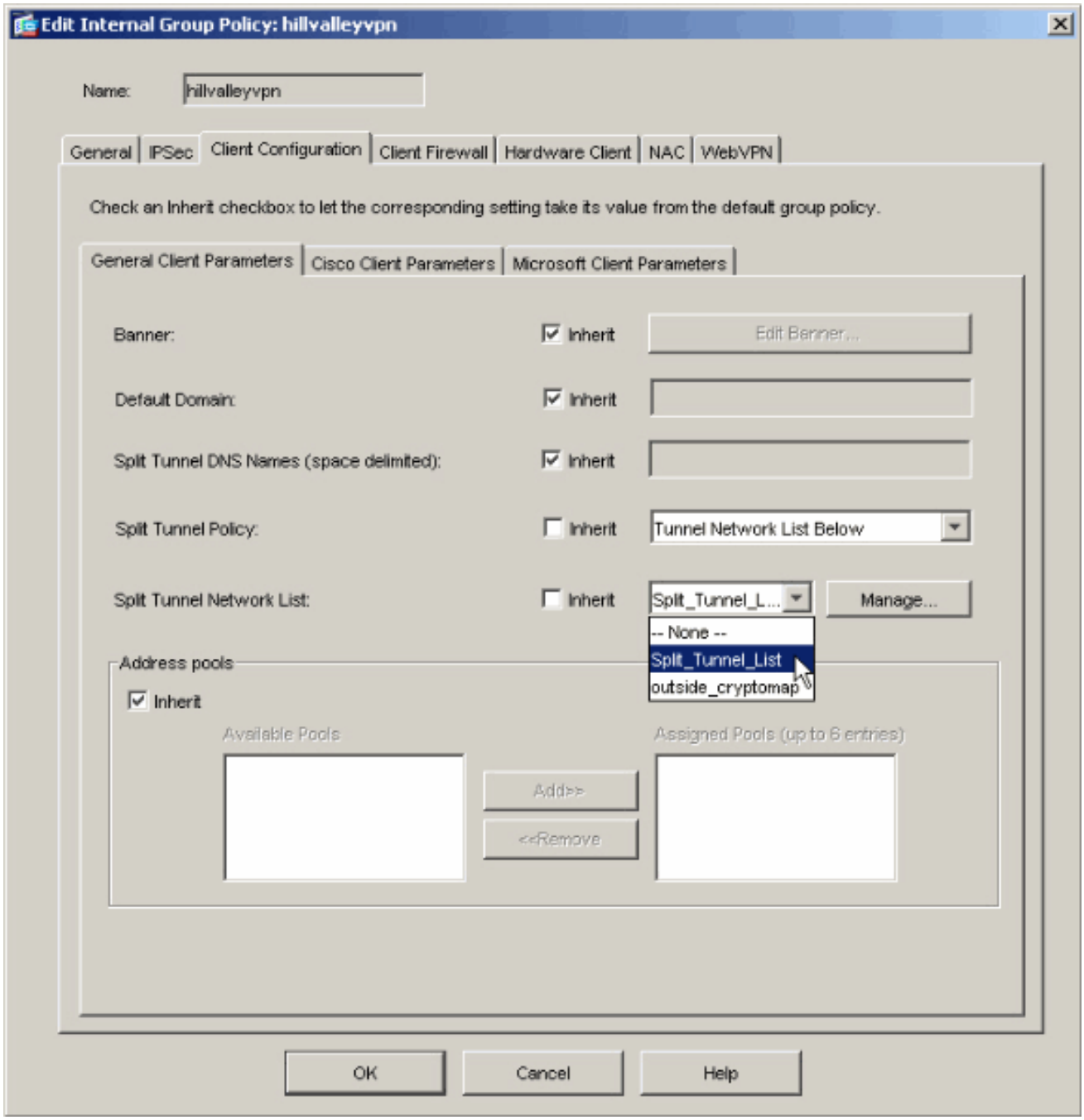


9. Klicken Sie auf **OK**, um den ACL Manager zu verlassen.

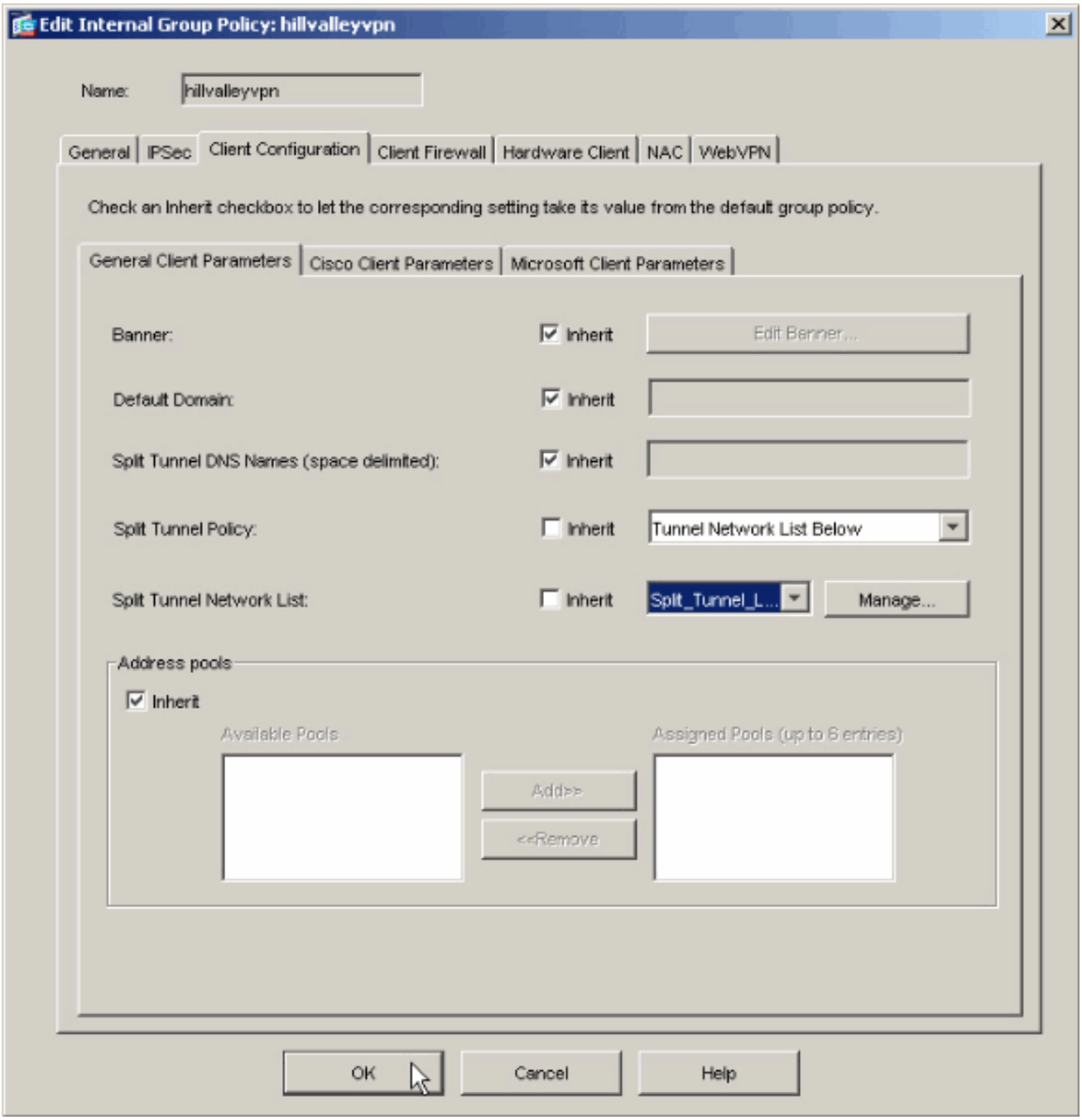


10. Stellen Sie sicher, dass die gerade erstellte ACL für die Split Tunnel Network List

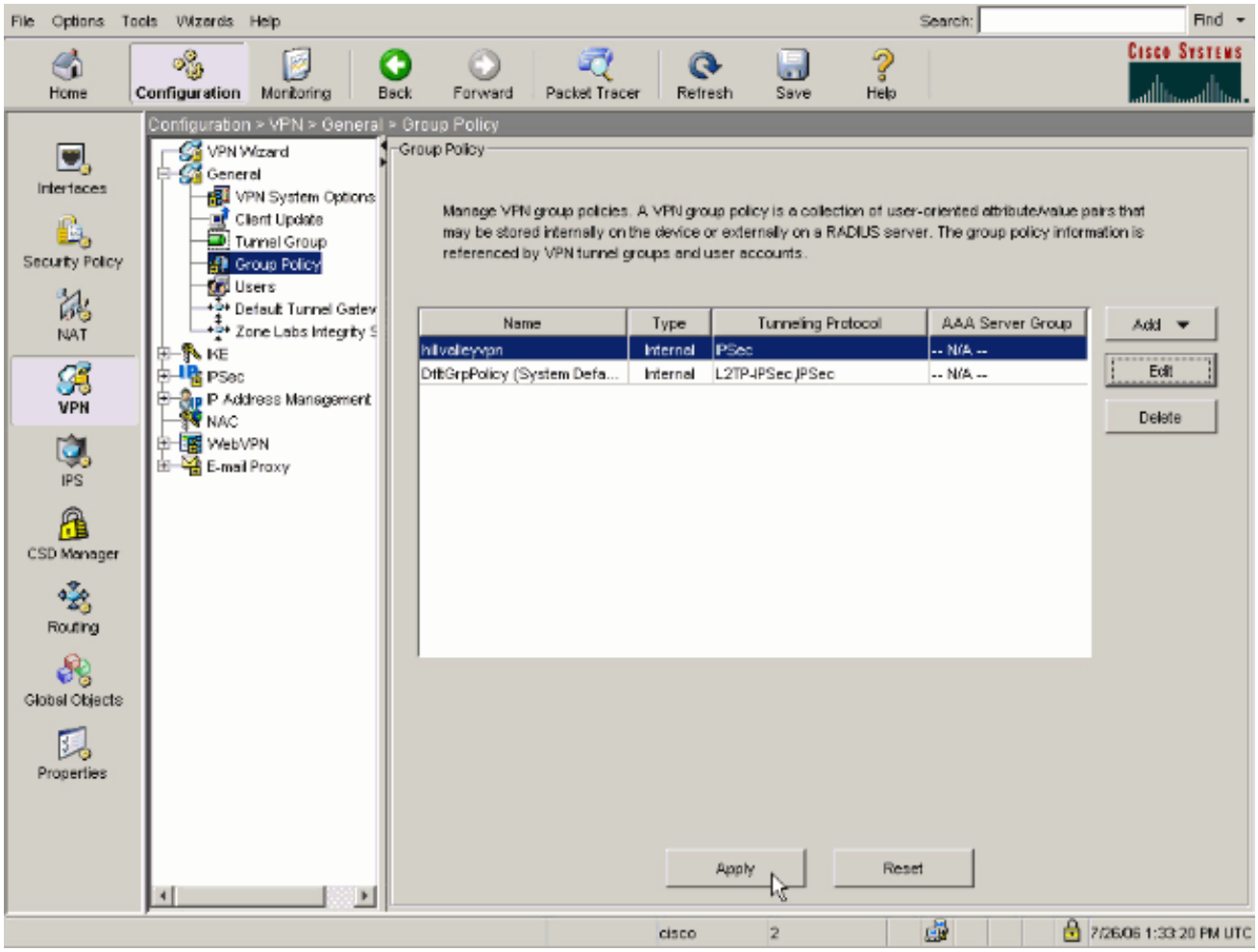
(Netzwerkliste des Split-Tunnels) ausgewählt ist.



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



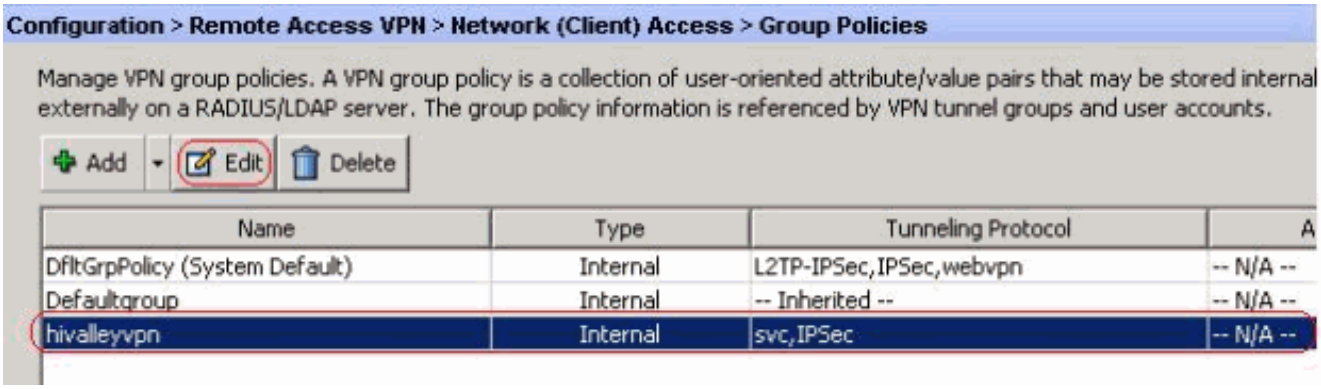
12. Klicken Sie auf **Apply** und dann **Send** (falls erforderlich), um die Befehle an die ASA zu senden.



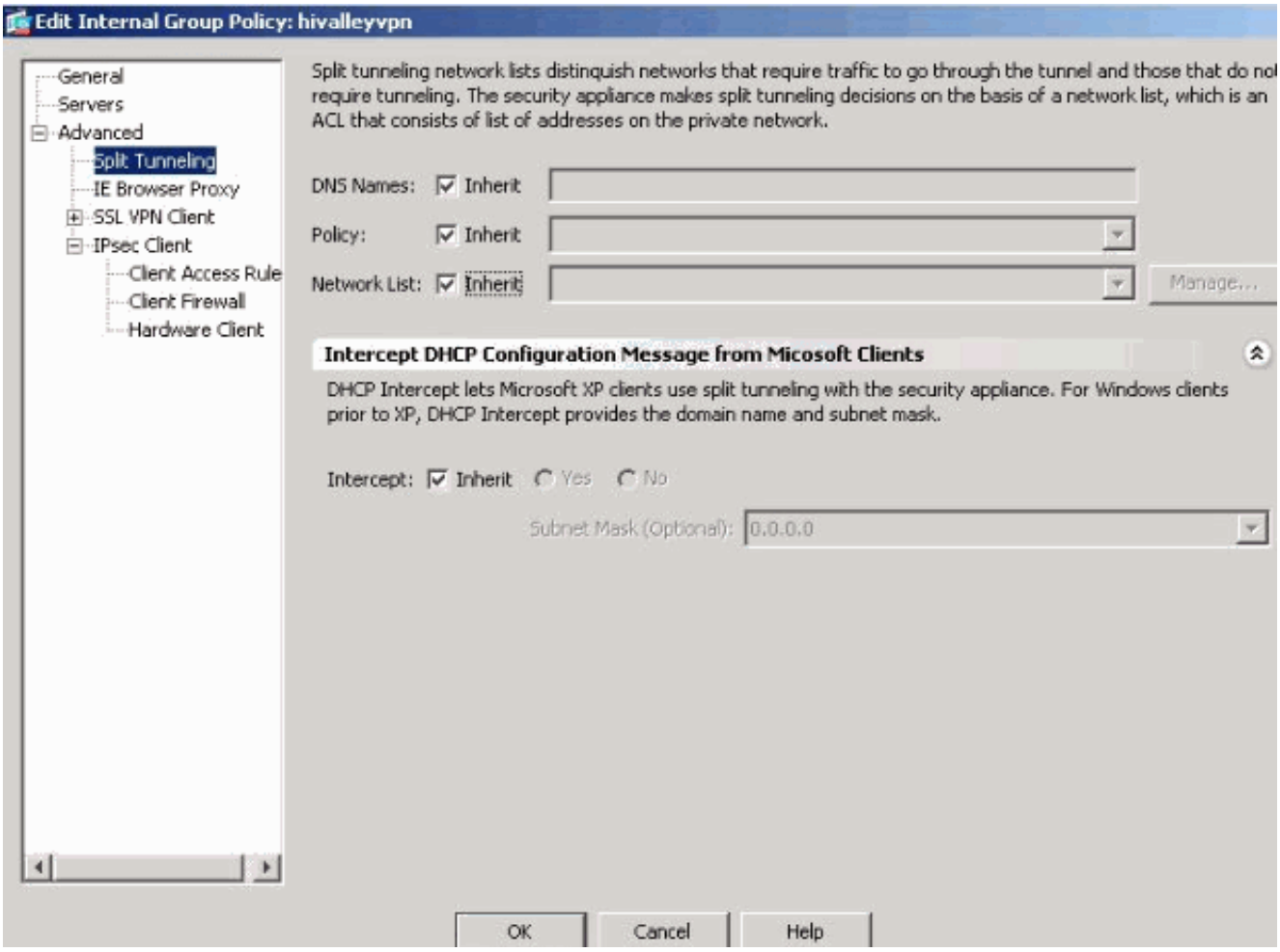
Konfigurieren der ASA 8.x mit dem Adaptive Security Device Manager (ASDM) 6.x

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

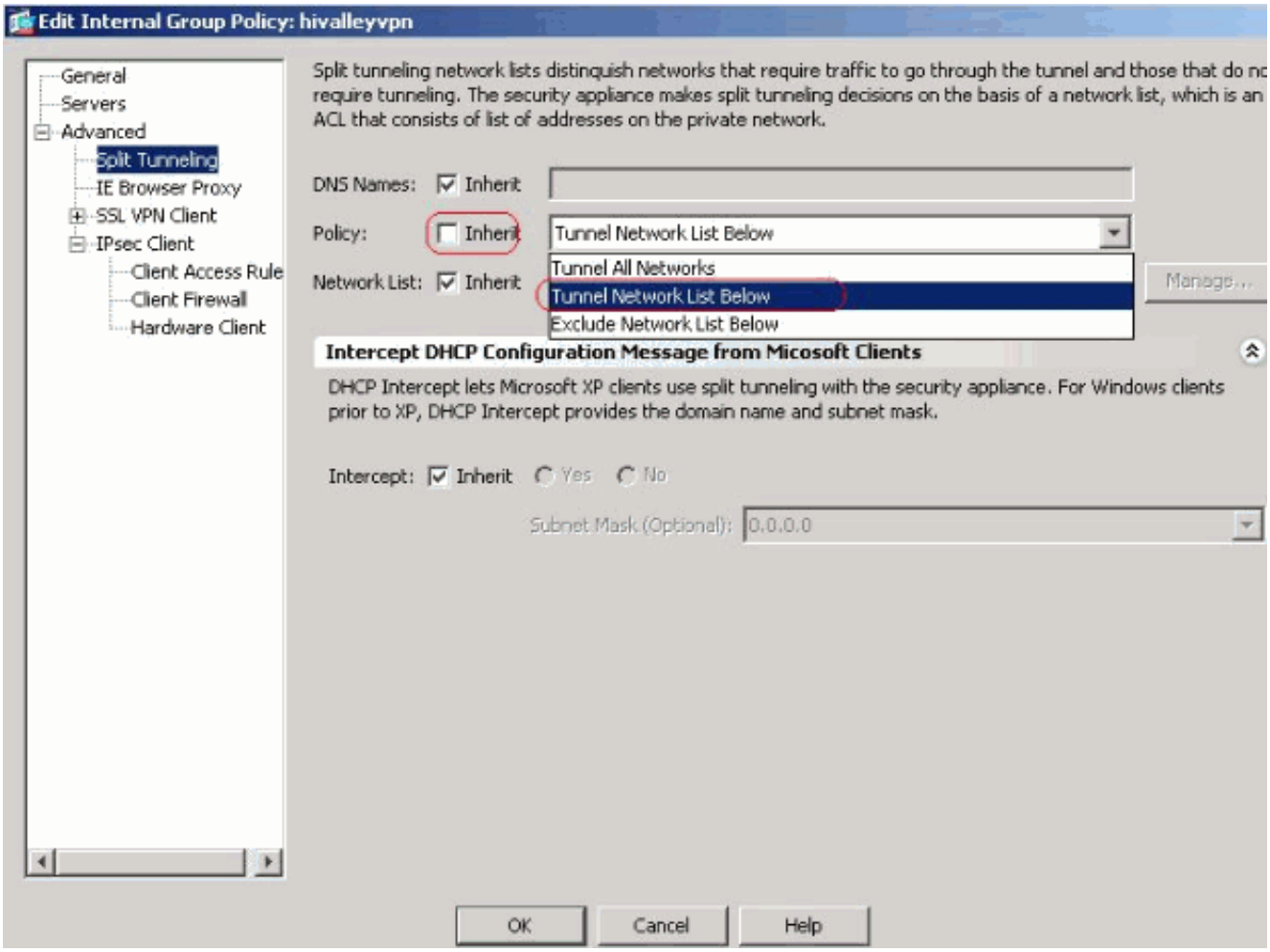
1. Wählen Sie **Configuration > Remote Access VPN > Network (Client) Access > Group Policies (Konfiguration > Remote Access VPN > Netzwerk (Client) Access > Group Policies (Gruppenrichtlinien) aus**, und wählen Sie die Gruppenrichtlinie aus, in der Sie den lokalen LAN-Zugriff aktivieren möchten. Klicken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



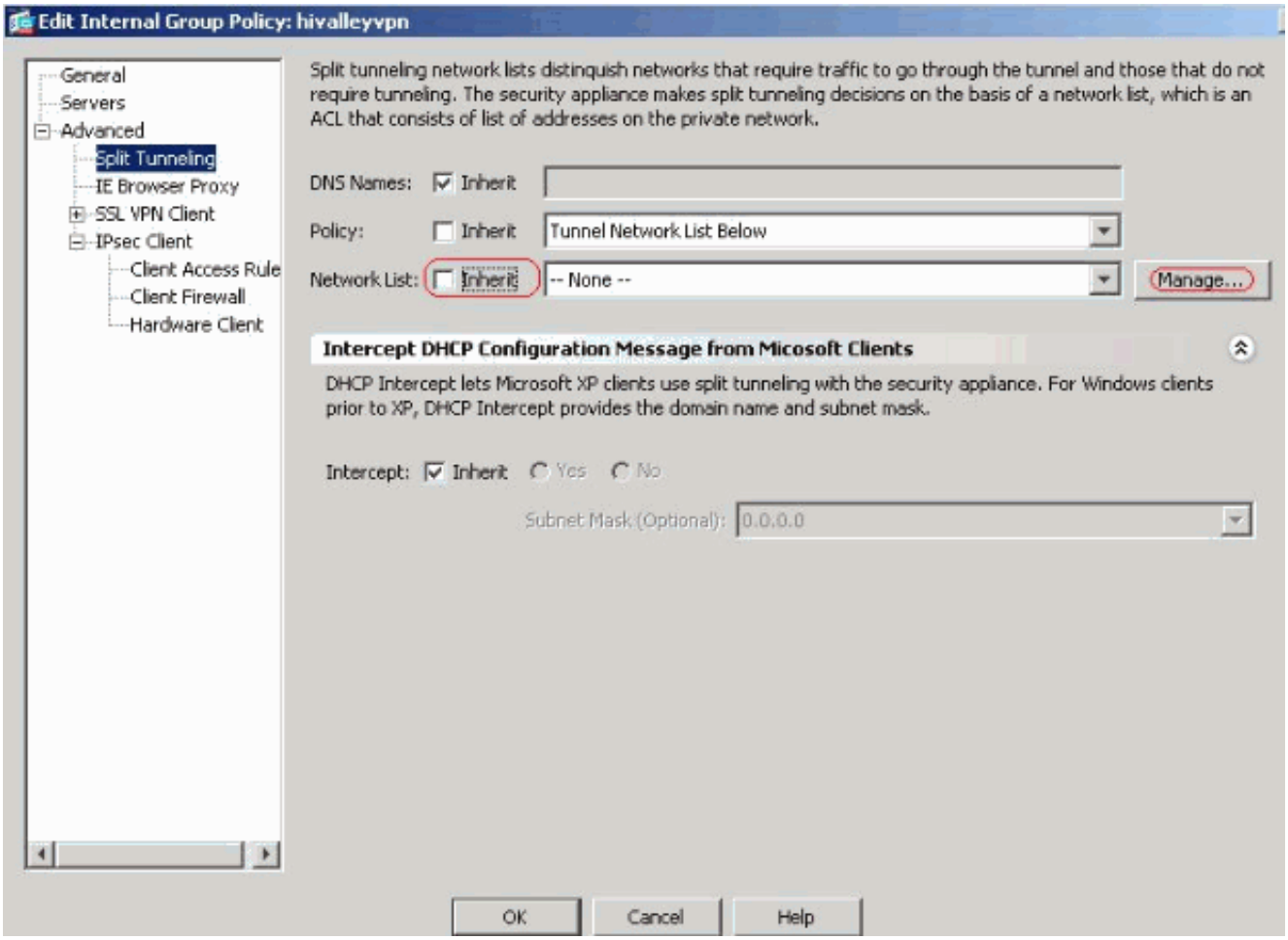
2. Klicken Sie auf **Getrenntes Tunneling aufteilen**.



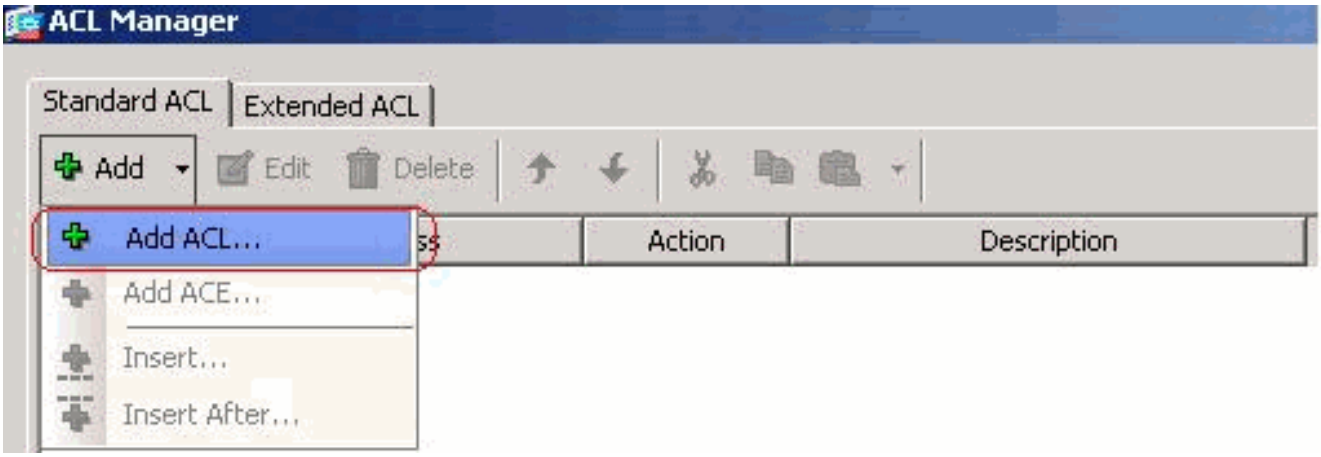
3. Deaktivieren Sie das Kontrollkästchen **Inherit** (**Erben**) für Split Tunnel Policy (Tunnelrichtlinie aufteilen), und wählen Sie **unten Tunnel Network List (Tunnelnetzwerkliste)**.



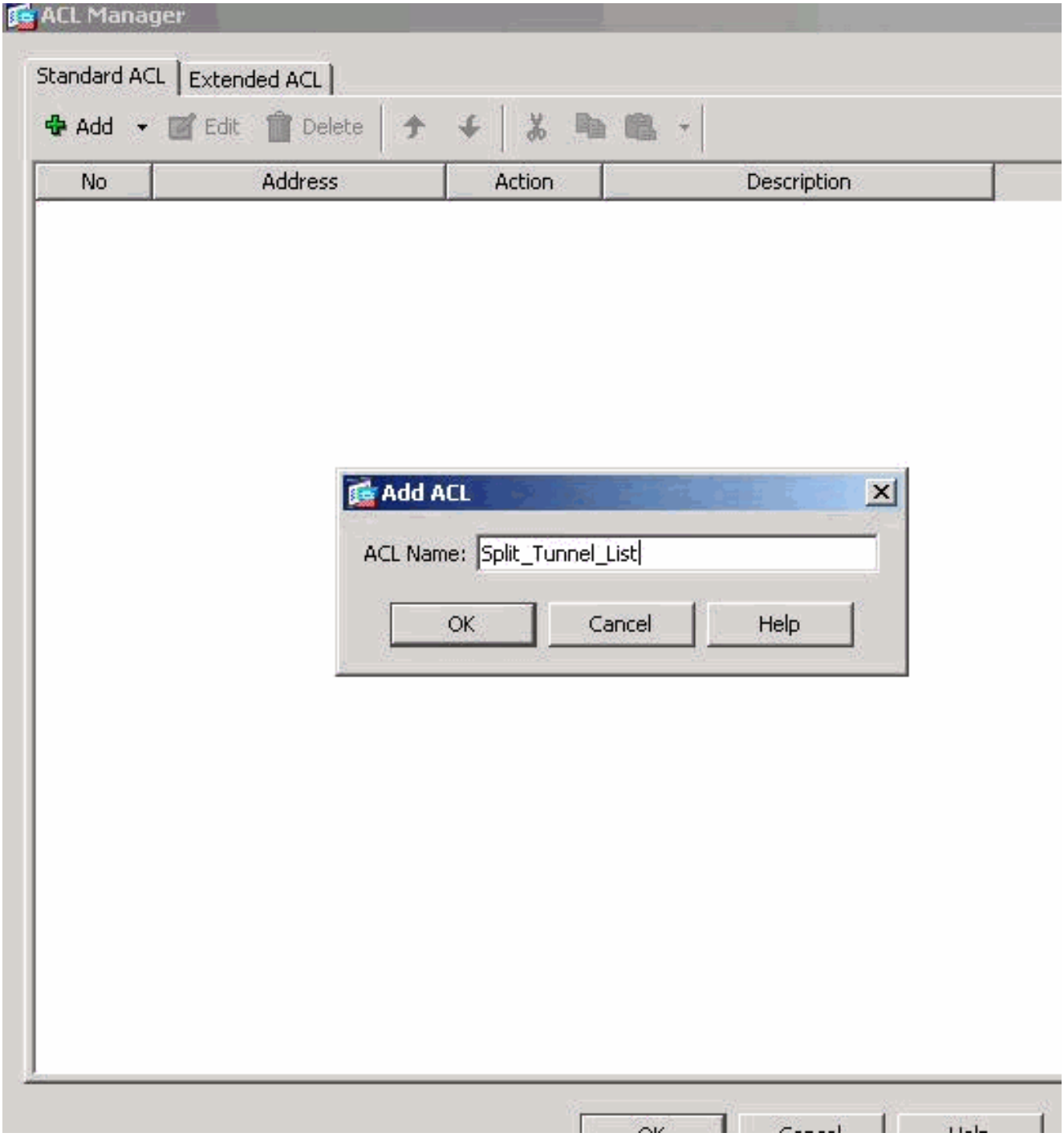
4. Deaktivieren Sie das Feld **Erben** für "Tunnel-Netzwerkliste teilen", und klicken Sie dann auf **Verwalten**, um den ACL Manager zu starten.



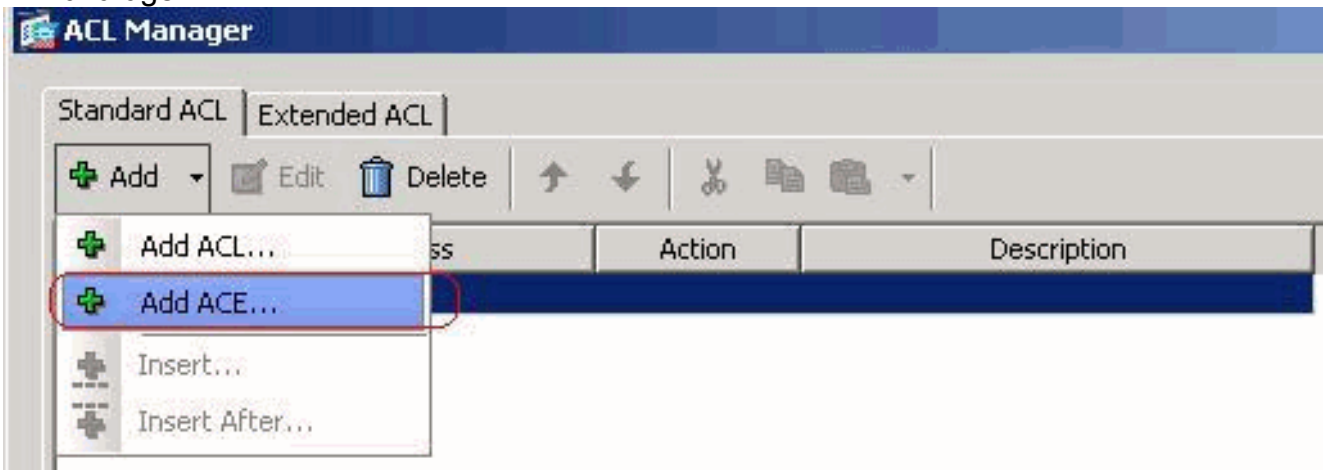
5. Wählen Sie im ACL Manager **Hinzufügen > ACL hinzufügen aus..** um eine neue Zugriffsliste zu
erstellen.



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

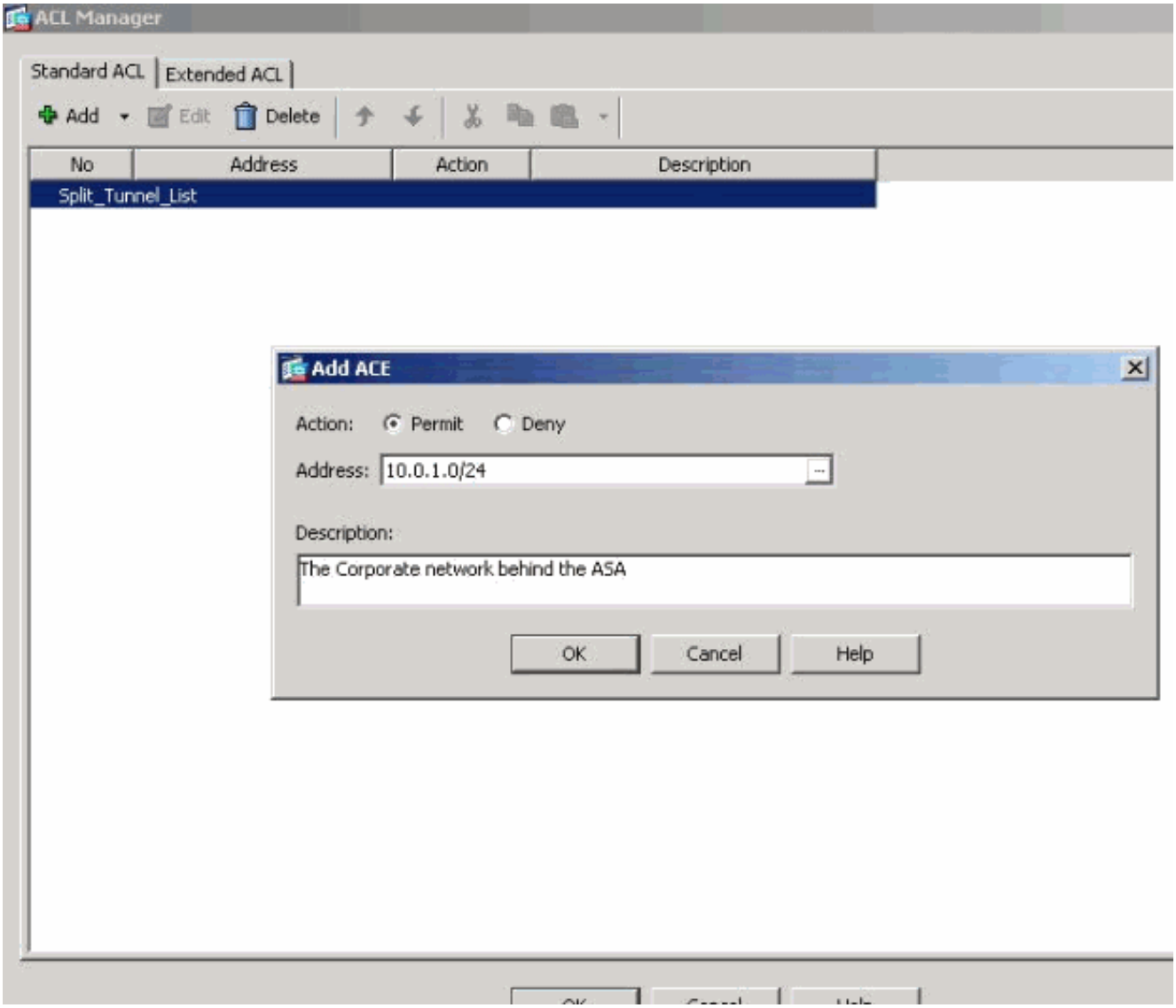


7. Wenn die ACL erstellt wurde, wählen Sie **Add > Add ACE.. (Hinzufügen > ACE hinzufügen) aus.** um einen Zugriffssteuerungseintrag (ACE) hinzuzufügen.

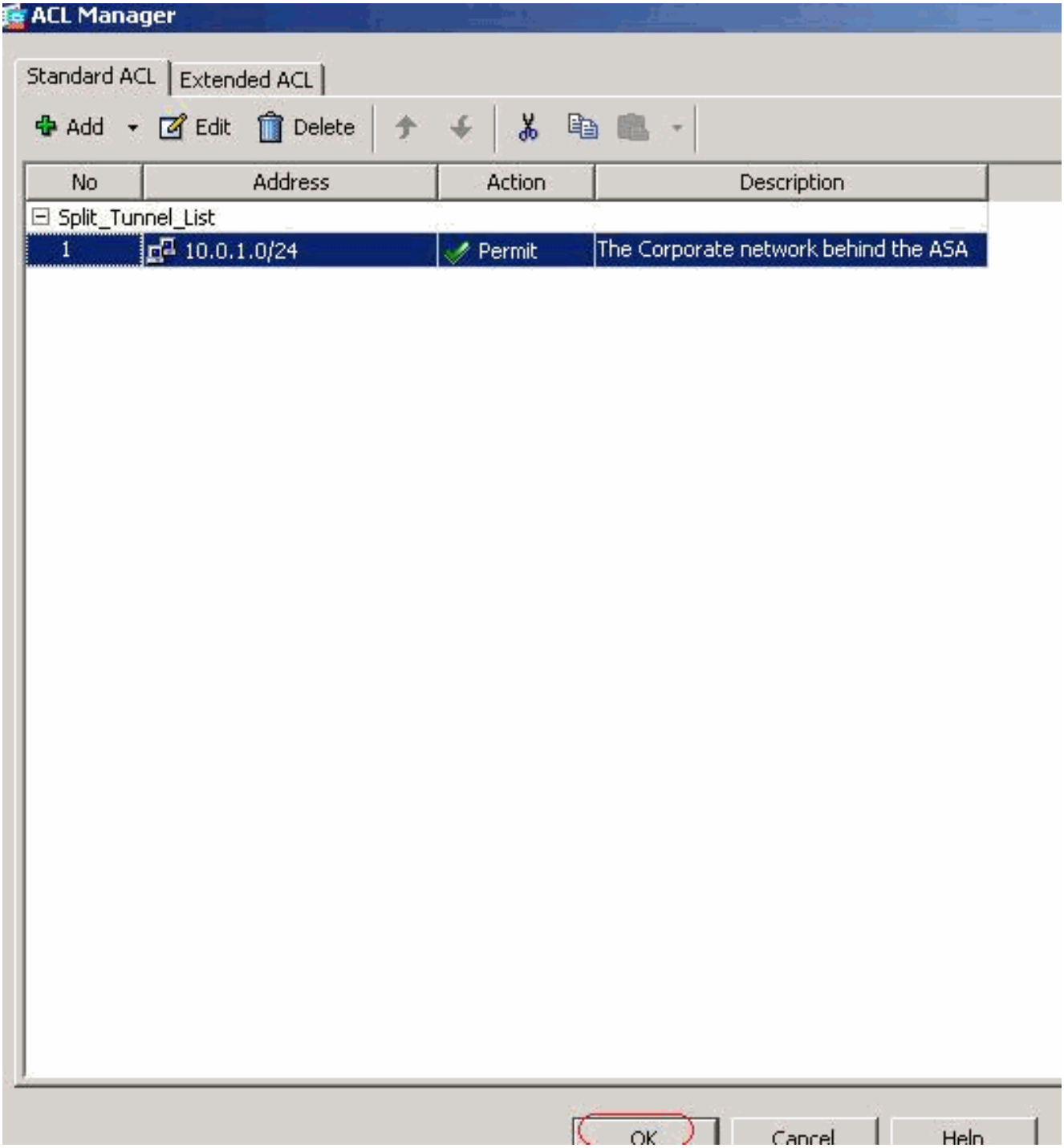


8. Definieren Sie den ACE, der dem LAN hinter der ASA entspricht. In diesem Fall ist das

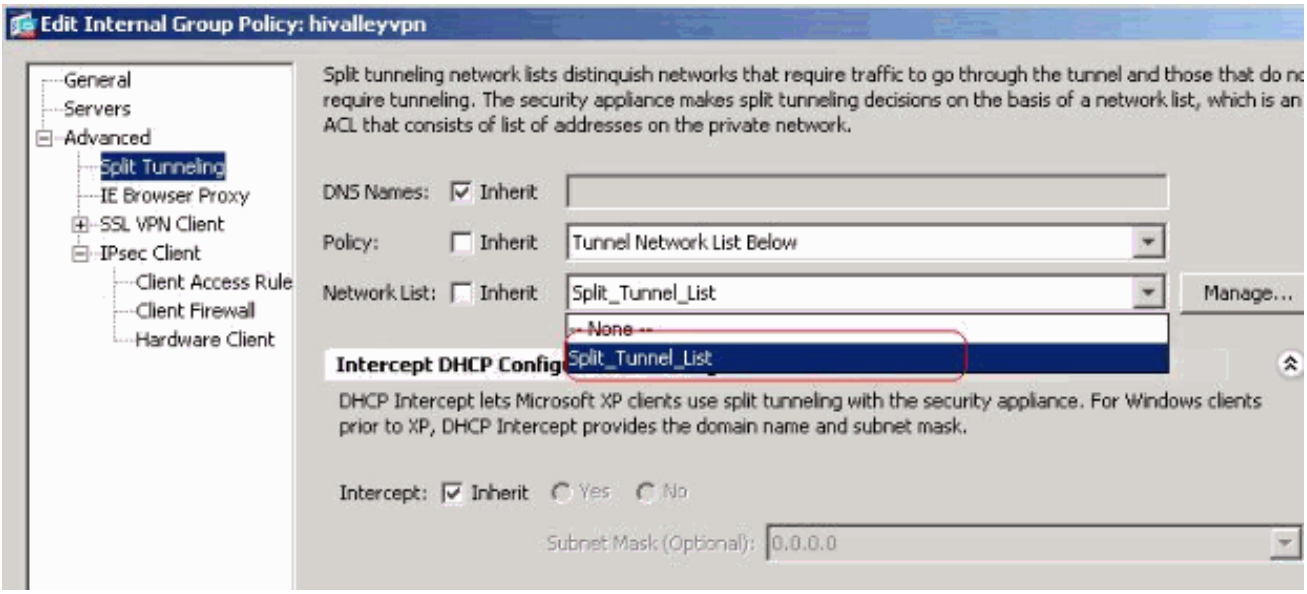
Netzwerk 10.0.1.0/24.Klicken Sie auf das Optionsfeld **Zulassen**.Wählen Sie die Netzwerkadresse mit der Maske **10.0.1.0/24 aus**.(Optional) Geben Sie eine Beschreibung an.Klicken Sie auf
OK.



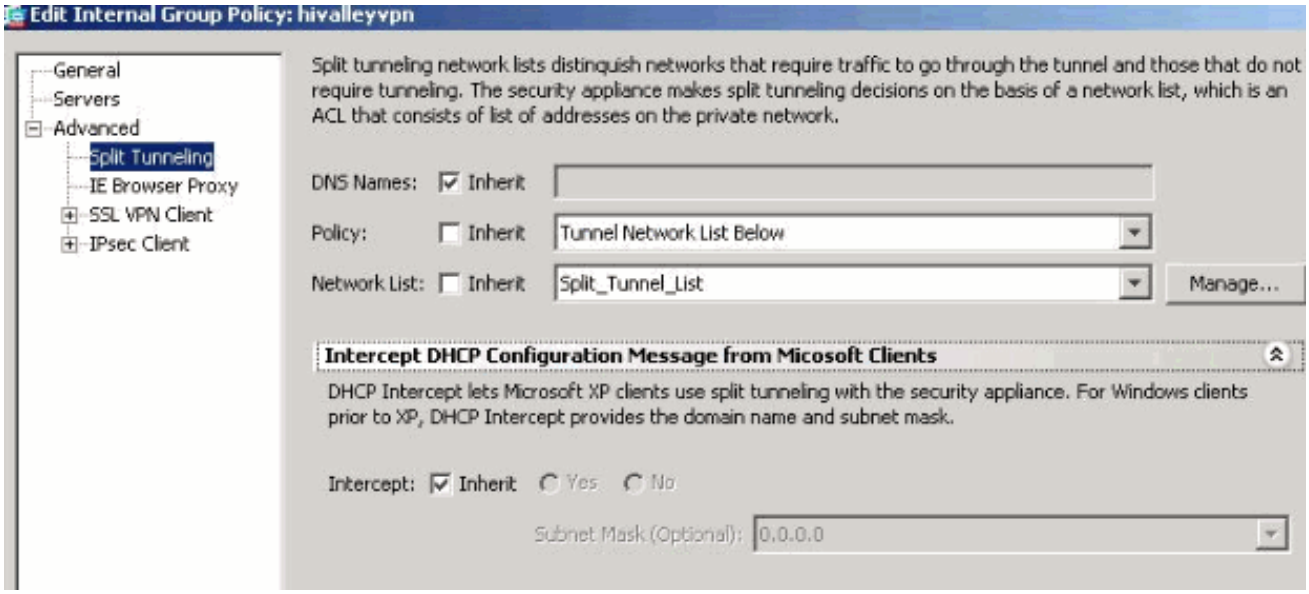
9. Klicken Sie auf **OK**, um den ACL Manager zu verlassen.



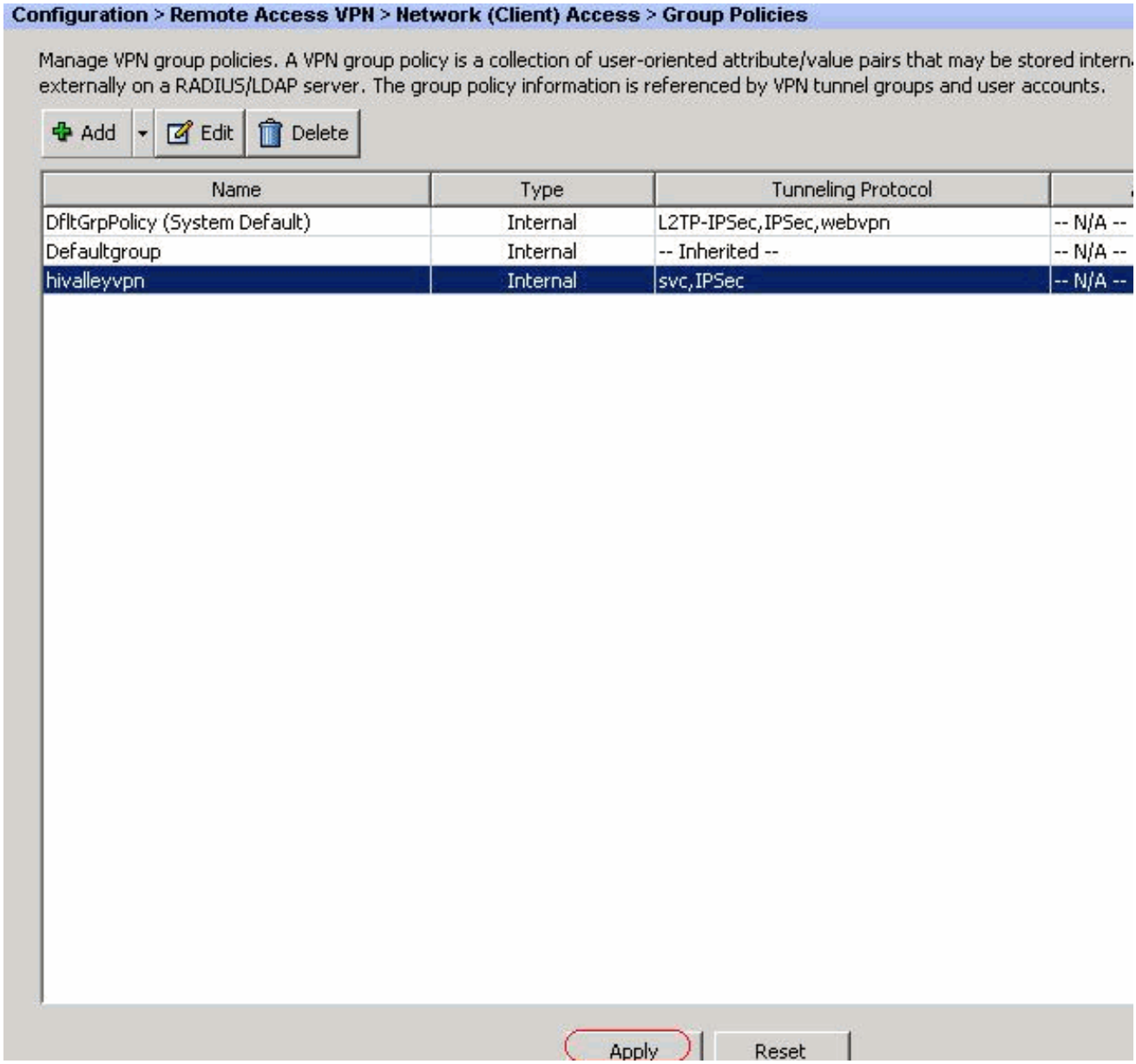
10. Stellen Sie sicher, dass die gerade erstellte ACL für die Split Tunnel Network List (Netzwerkliste des Split-Tunnels) ausgewählt ist.



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 7.x und höher über die CLI

Anstatt das 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.

1. Wechseln in den Konfigurationsmodus
```
ciscoasa>enable
Password: ********
ciscoasa#configure terminal
ciscoasa(config)#
```
2. Erstellen Sie eine Zugriffsliste, die das Netzwerk hinter der ASA definiert.
```
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
```
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 wird die Richtlinie **tunnelspezifiziert**.

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

5. Geben Sie die Liste für den geteilten Tunnel-Zugriff an. In diesem Fall lautet die Liste **Split_Tunnel_List**.
   ```
   ciscoasa(config-group-policy)#split-tunnel-network-list value Split_Tunnel_List
   ```

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 von PIX 6.x über die CLI

Gehen Sie wie folgt vor:

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

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

2. Erstellen Sie eine VPN-Gruppe *vpn3000*, und geben Sie die Split-Tunnel-ACL wie folgt an:
   ```
   PIX(config)#vpngroup vpn3000 split-tunnel Split_Tunnel_List
   ```

   Hinweis: Weitere Informationen zur VPN-Konfiguration für den Remote-Zugriff 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 für PIX 6.x.

Überprüfen

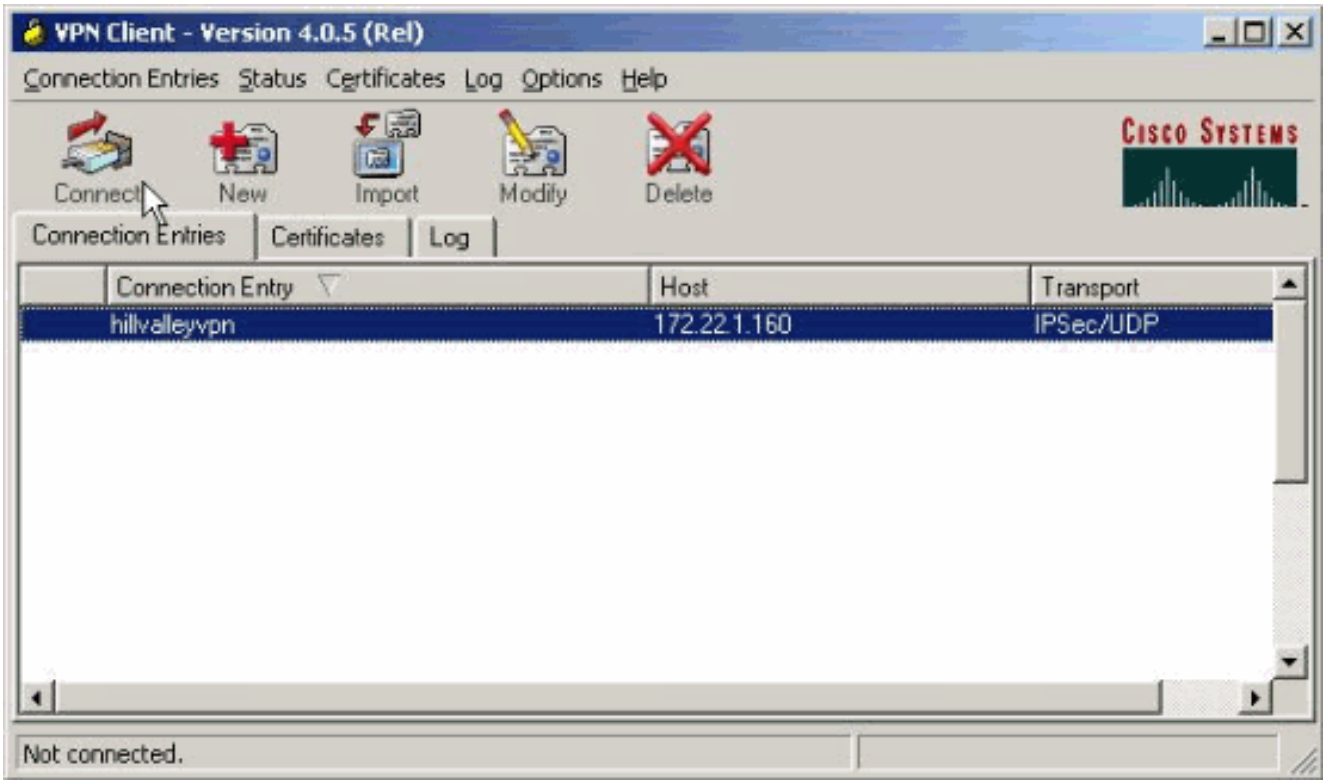
Befolgen Sie die Schritte in diesen Abschnitten, um Ihre Konfiguration zu überprüfen.

- Herstellen einer Verbindung mit dem VPN-Client
- VPN-Clientprotokoll anzeigen
- Testen des lokalen LAN-Zugriffs mit Ping

Herstellen einer Verbindung mit dem VPN-Client

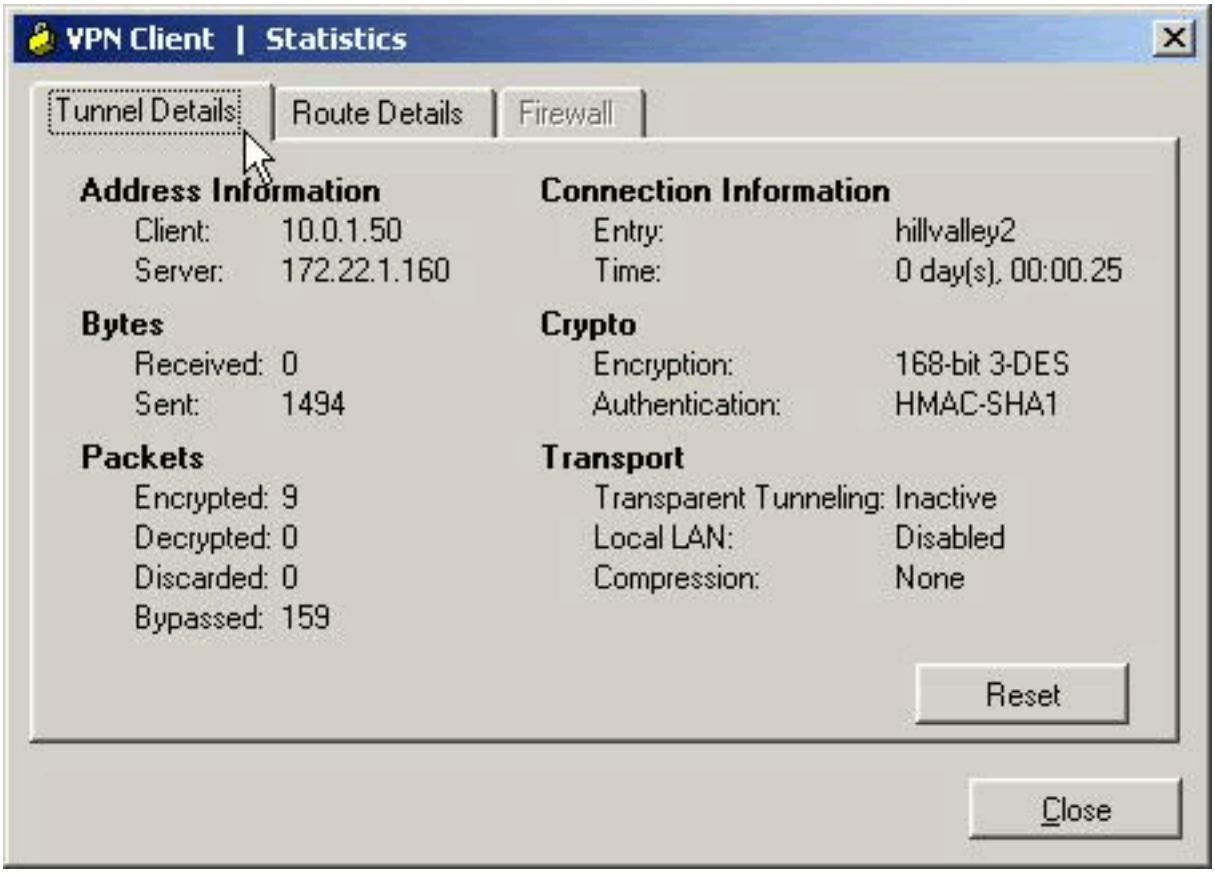
Verbinden Sie den VPN-Client mit dem VPN-Konzentrator, um Ihre Konfiguration zu überprüfen.

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

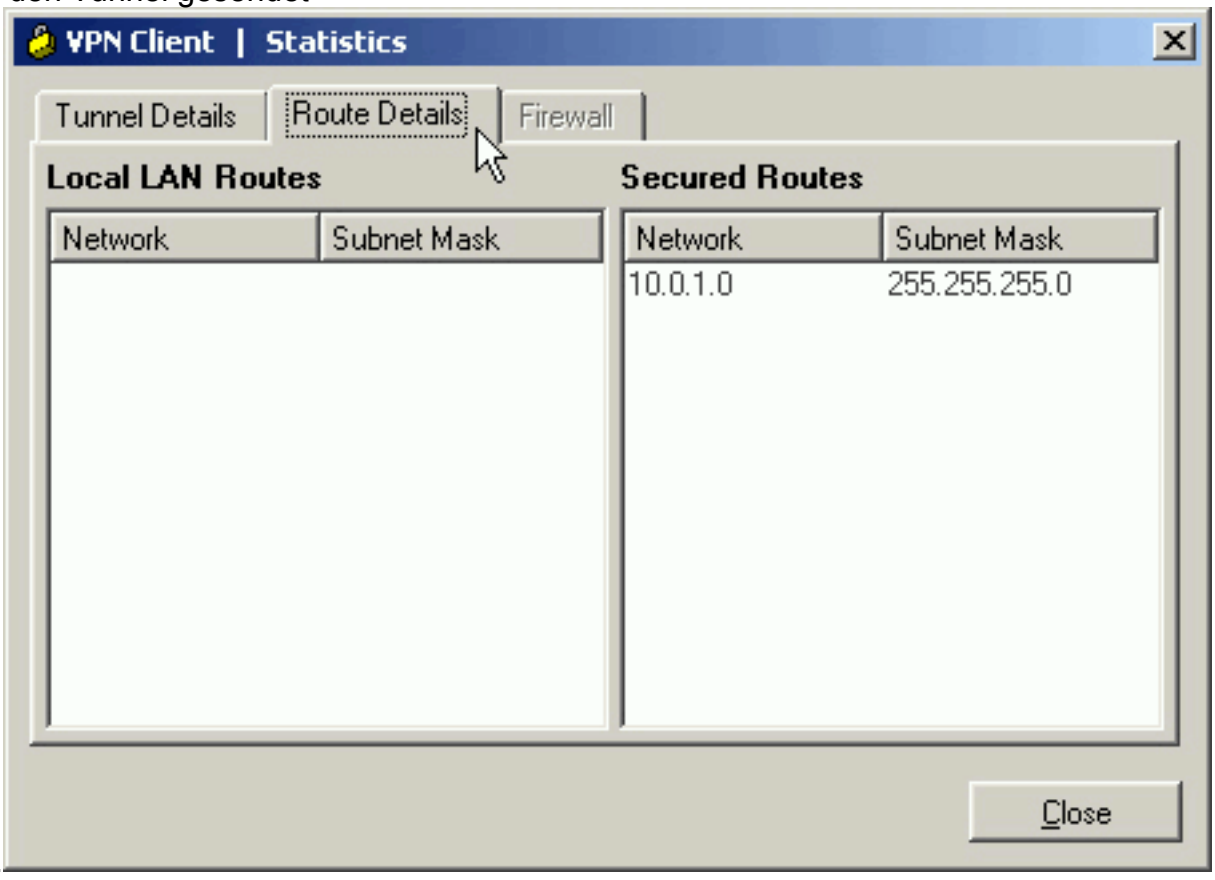


2. Geben Sie Ihre Anmeldeinformationen ein.

3. Wählen Sie **Status > Statistics.. (Status > Statistik) aus.** um das Fenster Tunneldetails anzuzeigen, in dem Sie die Einzelheiten des Tunnels überprüfen und den Verkehrsfluss sehen
können.



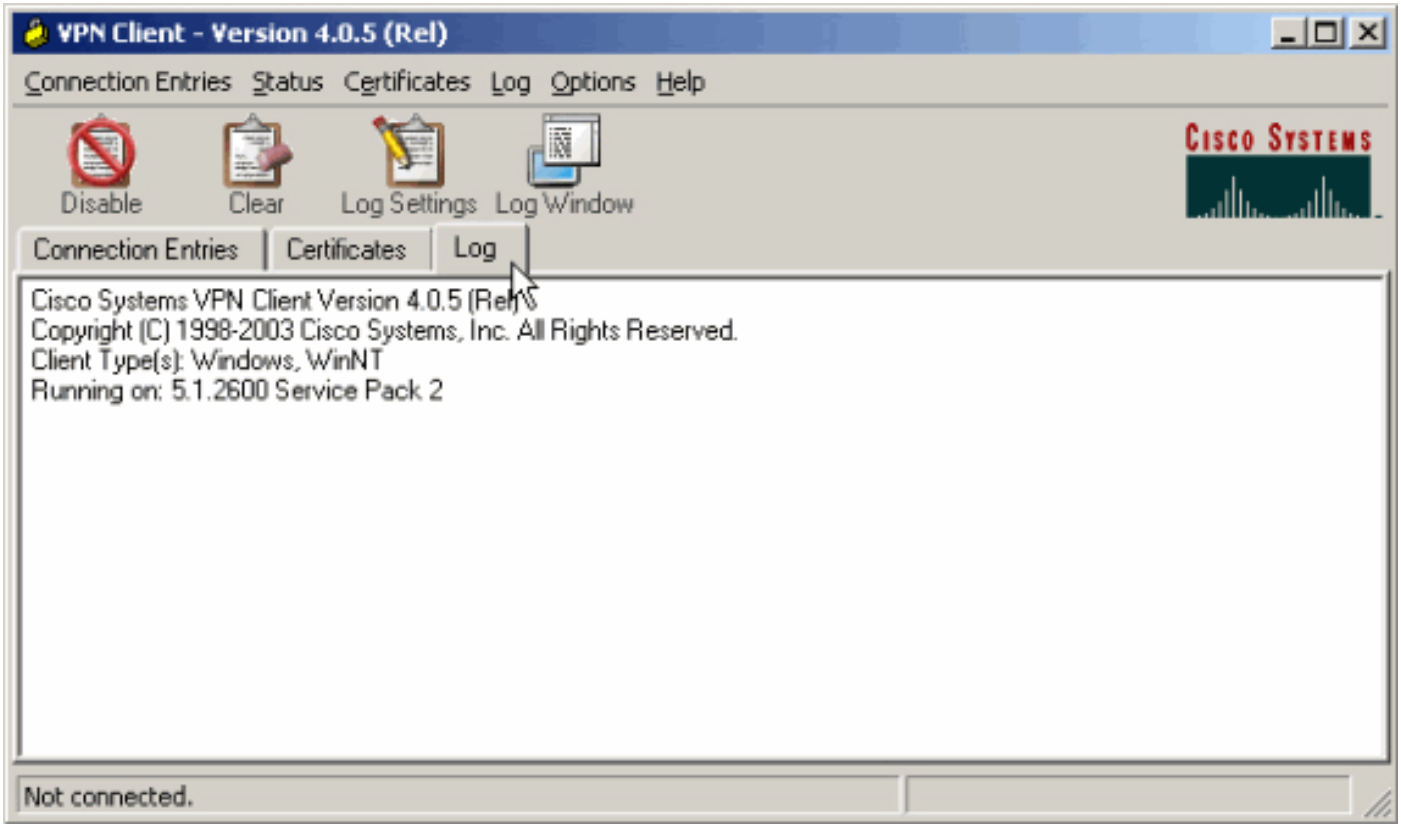
4. Wechseln Sie zur Registerkarte Route Details (Routendetails), um die Routen anzuzeigen, die der VPN-Client für die ASA sichert.In diesem Beispiel sichert der VPN-Client den Zugriff auf 10.0.1.0/24, während der gesamte andere Datenverkehr nicht verschlüsselt und nicht über den Tunnel gesendet



wird.

[VPN-Clientprotokoll anzeigen]

Beim Überprüfen des VPN-Clientprotokolls können Sie bestimmen, ob der Parameter für das Split-Tunneling festgelegt ist. Um das Protokoll anzuzeigen, gehen Sie zur Registerkarte Log (Protokoll) im VPN-Client. Klicken Sie dann auf **Protokolleinstellungen**, um die protokollierten Einstellungen anzupassen. In diesem Beispiel ist IKE auf **3 - High (3 - Hoch)** festgelegt, während alle anderen Protokollelemente auf **1 - Low (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/6IKE/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 zum Testen, dass der VPN-Client für Split-Tunneling konfiguriert ist, während er für die ASA getunnelt wird, besteht in der Verwendung des **Ping-**Befehls in der Windows-Befehlszeile. 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.

```
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 durch die Anzahl der Einträge in einer Split-Tunnel-ACL

Die Anzahl der Einträge in einer für Split-Tunnel verwendeten Zugriffskontrollliste ist beschränkt. Es wird empfohlen, nicht mehr als 50-60 ACE-Einträge zu verwenden, um eine zufriedenstellende Funktionalität zu gewährleisten. 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 Dokumentation - Cisco Systems