Configurazione del tunneling ripartito per i client VPN sull'appliance ASA

Sommario

Introduzione

In questo documento viene descritto il processo per consentire ai client VPN di accedere a Internet durante il tunneling in un'appliance di sicurezza Cisco ASA serie 5500.

Prerequisiti

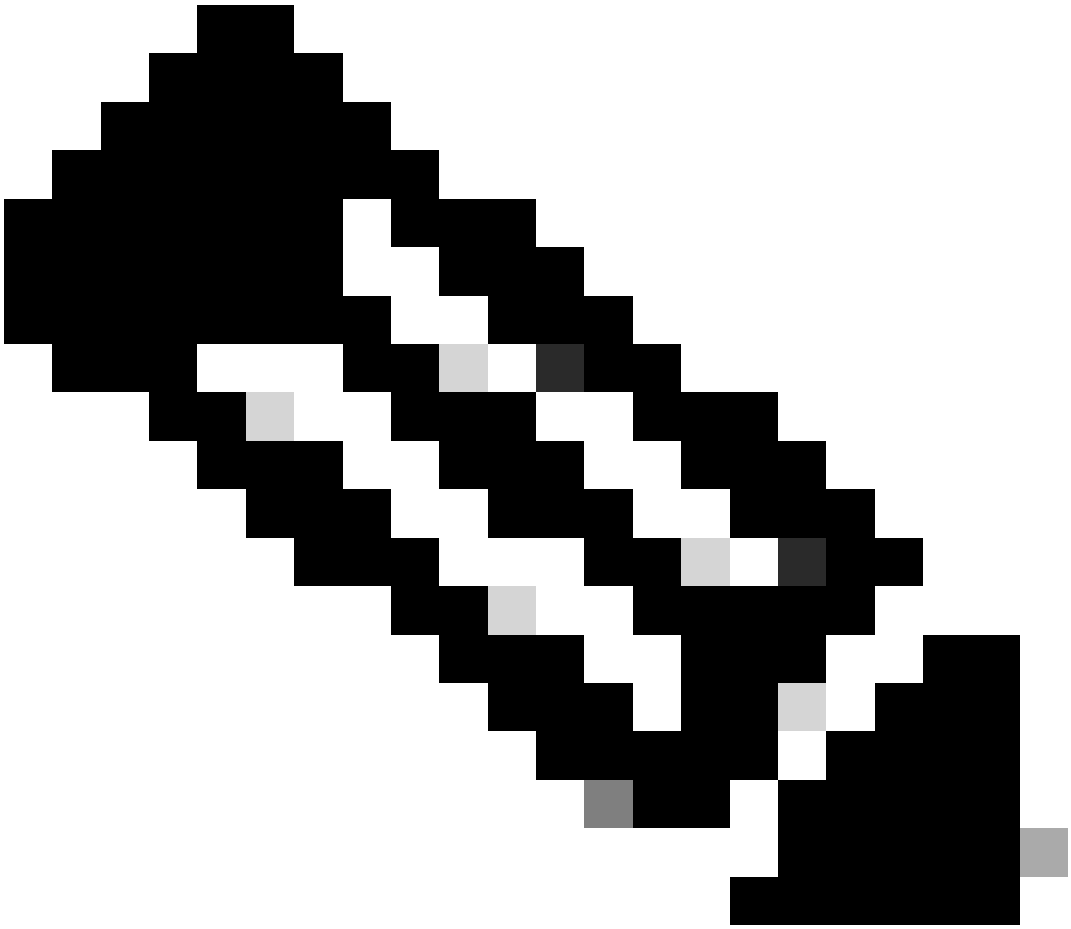
Requisiti

In questo documento si presume che sull'appliance ASA esista già una configurazione VPN ad accesso remoto funzionante. Fare riferimento a PIX/ASA 7.x come server VPN remoto usando l'esempio di configurazione ASDM, se non ne è già stato configurato uno.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ASA serie 5500 Security Appliance Software versione 7.x e successive
- Cisco Systems VPN Client versione 4.0.5
- Adaptive Security Device Manager (ASDM)

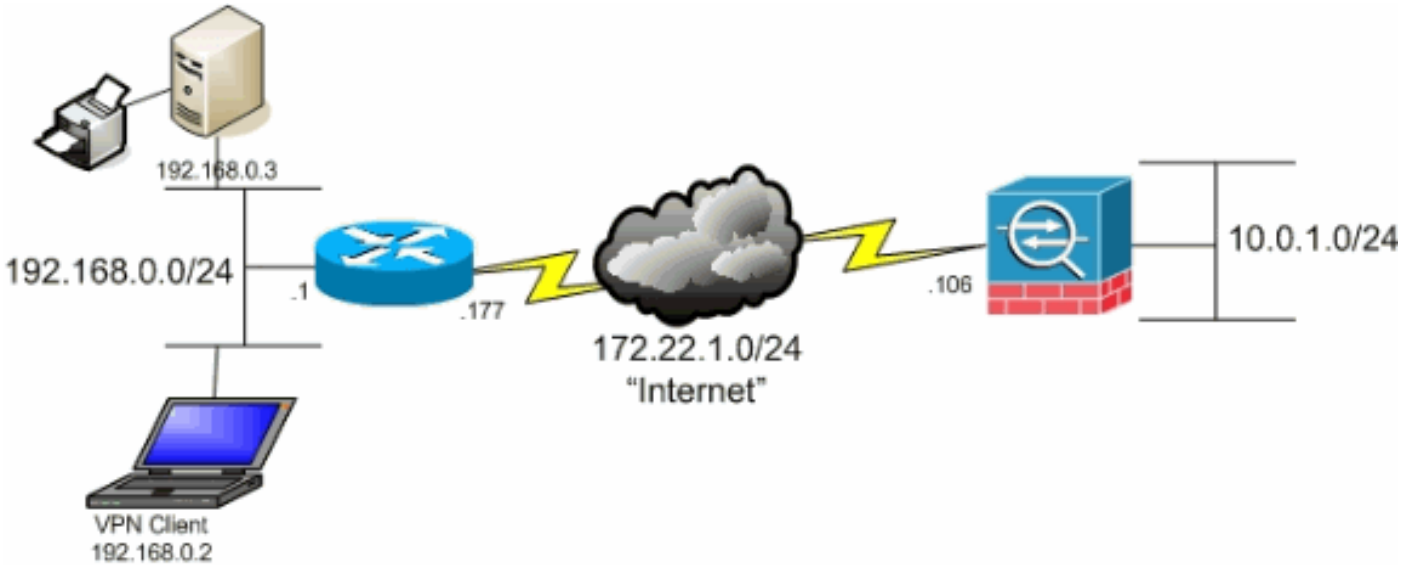


Nota: questo documento contiene anche la configurazione PIX 6.x CLI compatibile con Cisco VPN client 3.x.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Il client VPN si trova su una tipica rete SOHO e si connette tramite Internet all'ufficio principale.



Esempio di rete

Prodotti correlati

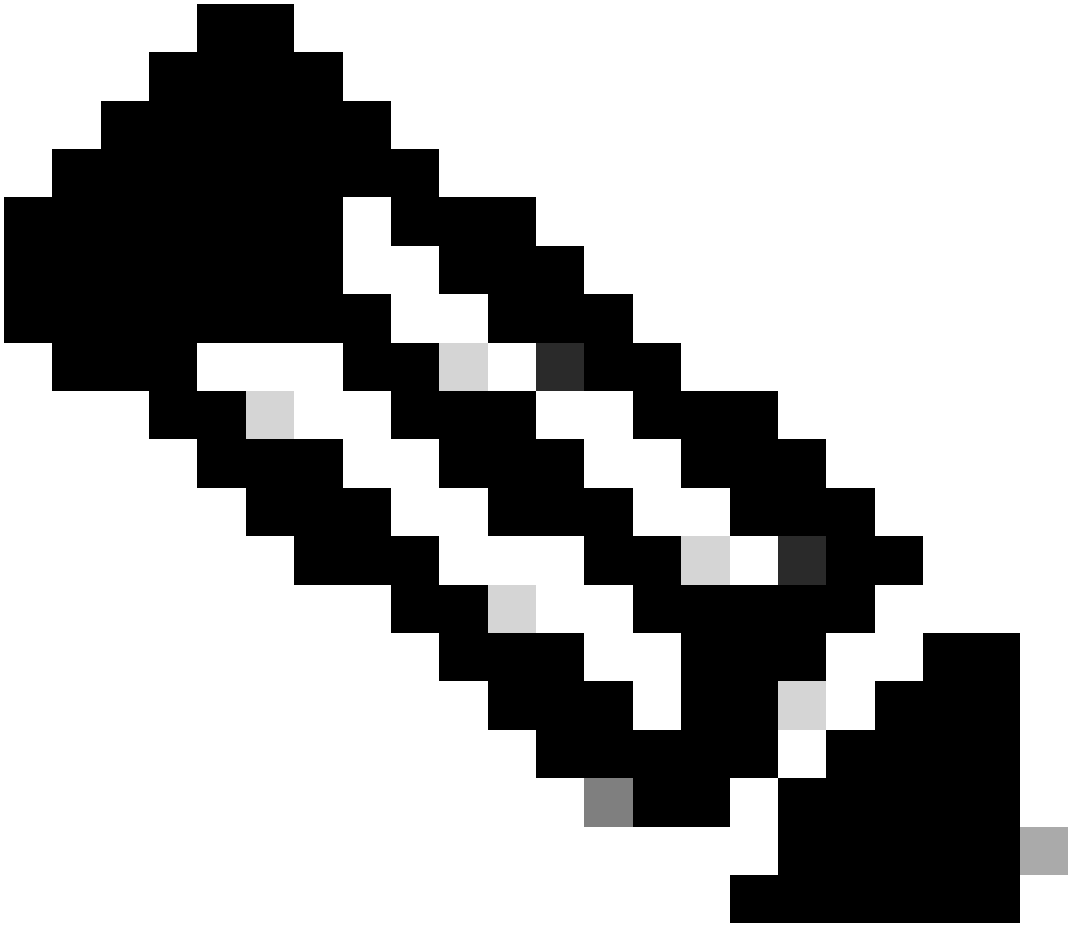
Questa configurazione può essere utilizzata anche con il software Cisco PIX serie 500 Security Appliance versione 7.x.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

In questo documento viene spiegato dettagliatamente come consentire ai client VPN di accedere a Internet mentre sono tunneling in un'appliance di sicurezza Cisco Adaptive Security Appliance (ASA) serie 5500. Questa configurazione consente ai client VPN di accedere in modo sicuro alle risorse aziendali tramite IPsec, garantendo al contempo l'accesso non protetto a Internet.



Nota: il tunneling completo è considerato la configurazione più sicura in quanto non consente l'accesso simultaneo del dispositivo a Internet e alla LAN aziendale. Un compromesso tra il tunneling completo e il tunneling suddiviso permette ai client VPN solo l'accesso alla LAN locale. Per ulteriori informazioni, fare riferimento all'esempio di configurazione PIX/ASA 7.x: Allow Local LAN Access for VPN Clients.

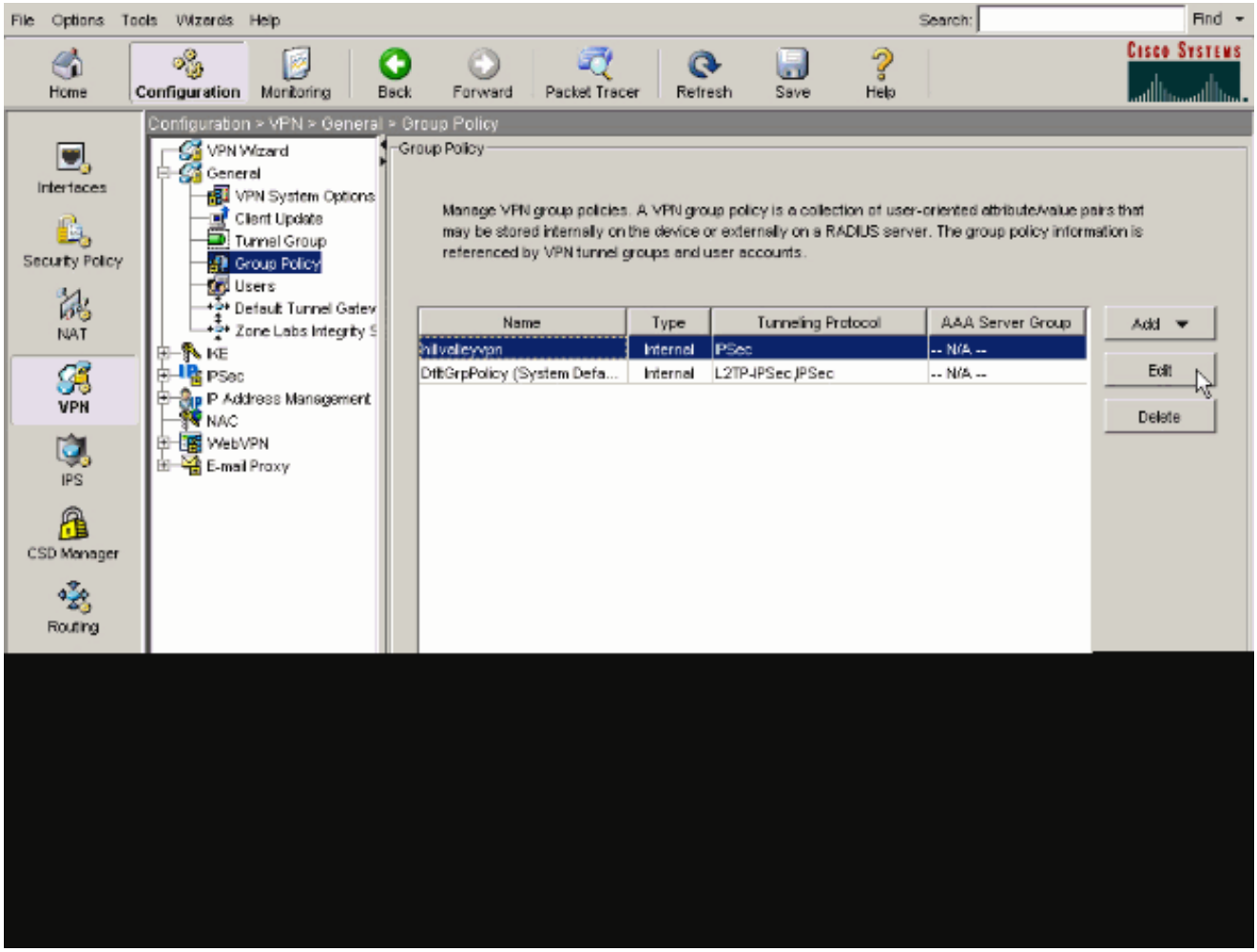
In uno scenario di base tra client VPN e ASA, tutto il traffico proveniente dal client VPN viene crittografato e inviato all'ASA, a prescindere dalla destinazione. In base alla configurazione e al numero di utenti supportati, tale configurazione può richiedere un uso intensivo della larghezza di banda. Il tunneling ripartito può ridurre questo problema in quanto consente agli utenti di inviare solo il traffico destinato alla rete aziendale attraverso il tunnel. Tutto il resto del traffico, come la messaggistica istantanea, la posta elettronica o la navigazione casuale, viene inviato a Internet tramite la LAN locale del client VPN.

Configurazione del tunneling ripartito sull'appliance ASA

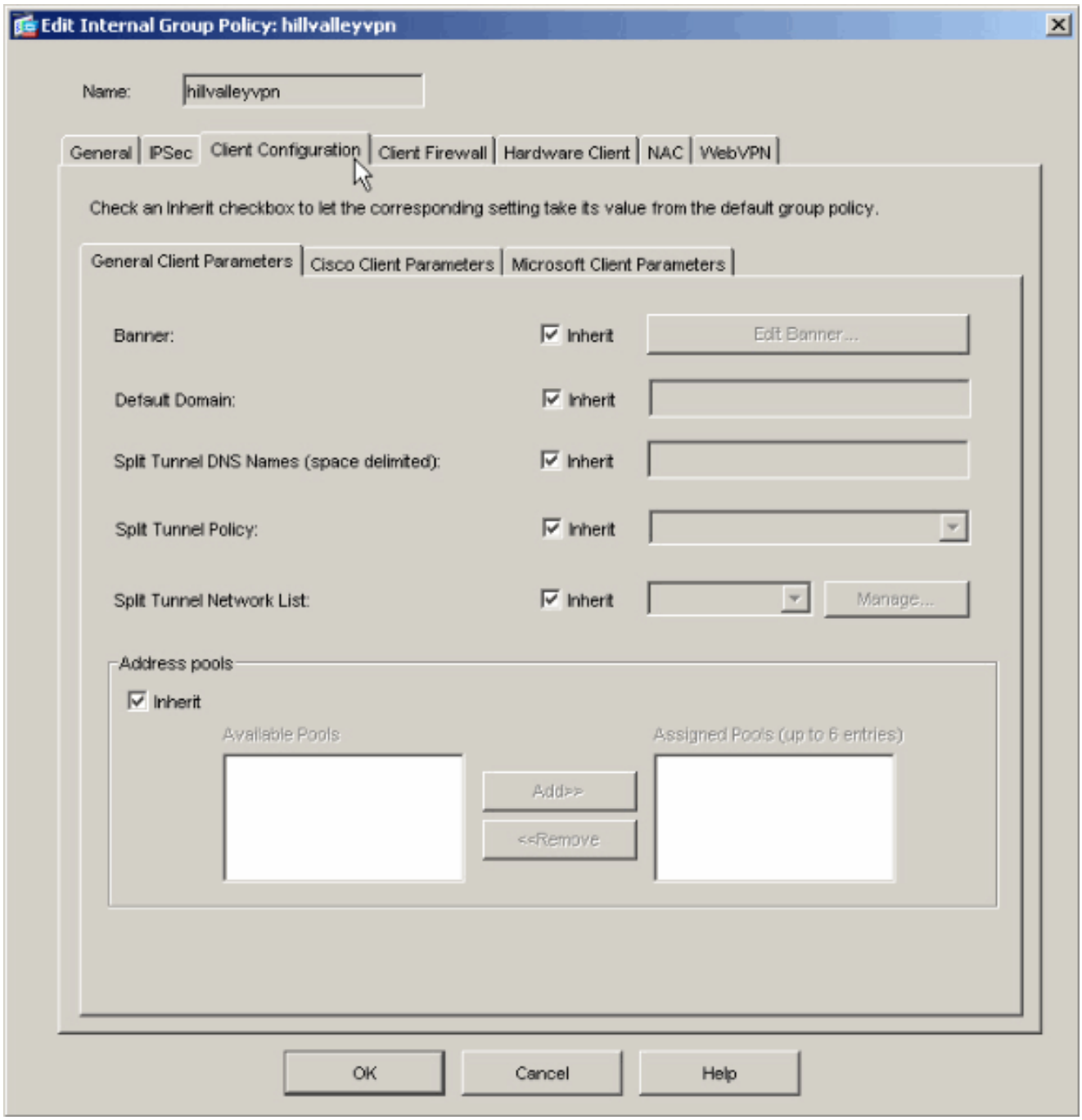
Configurare ASA 7.x con Adaptive Security Device Manager (ASDM) 5.x

Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling suddiviso per gli utenti del gruppo.

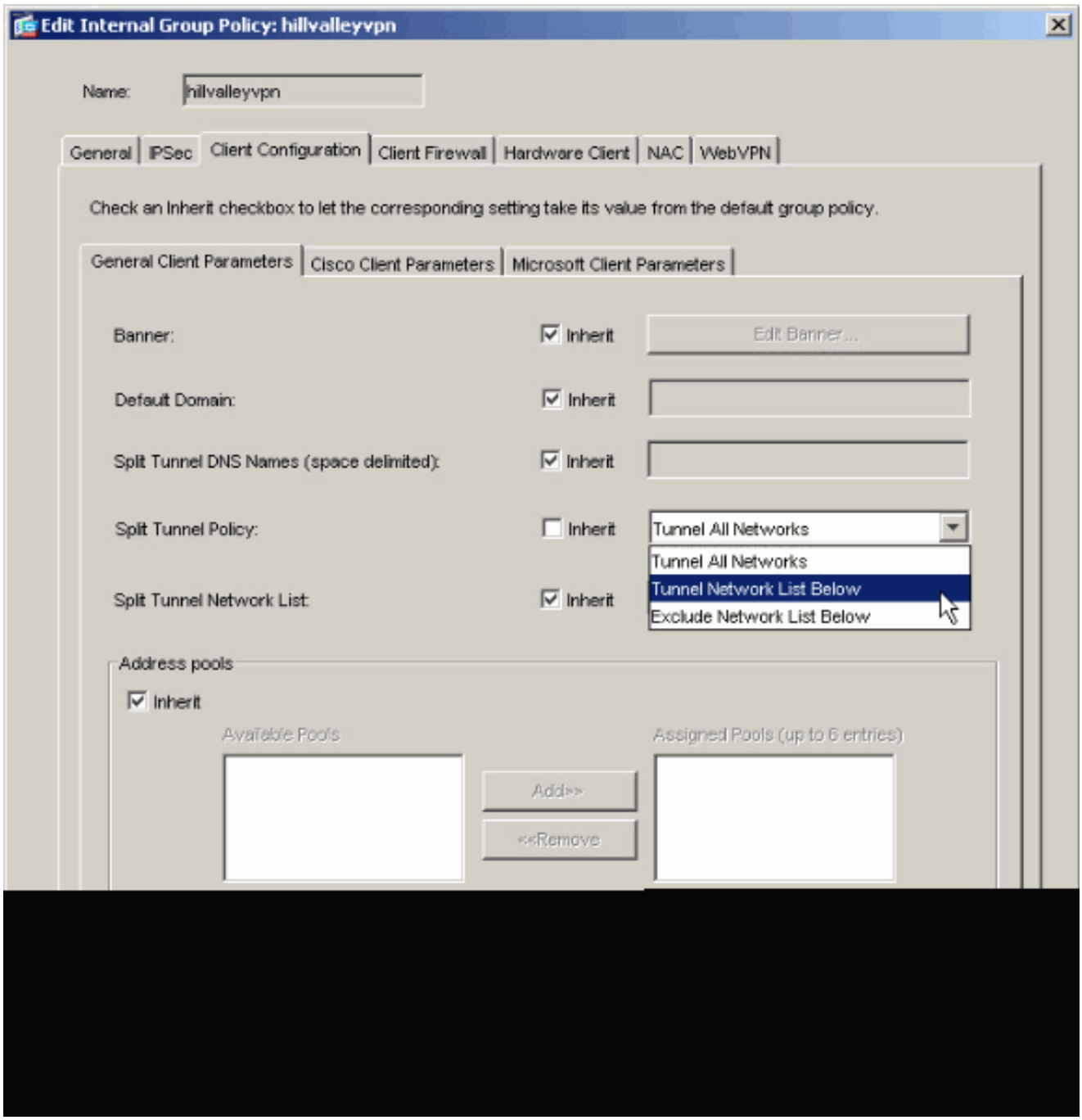
1. Scegliere Configurazione > VPN > Generale > Criteri di gruppo e selezionare i Criteri di gruppo in cui abilitare l'accesso LAN locale. Quindi fare clic su Modifica .



2. Andare alla scheda Configurazione client.

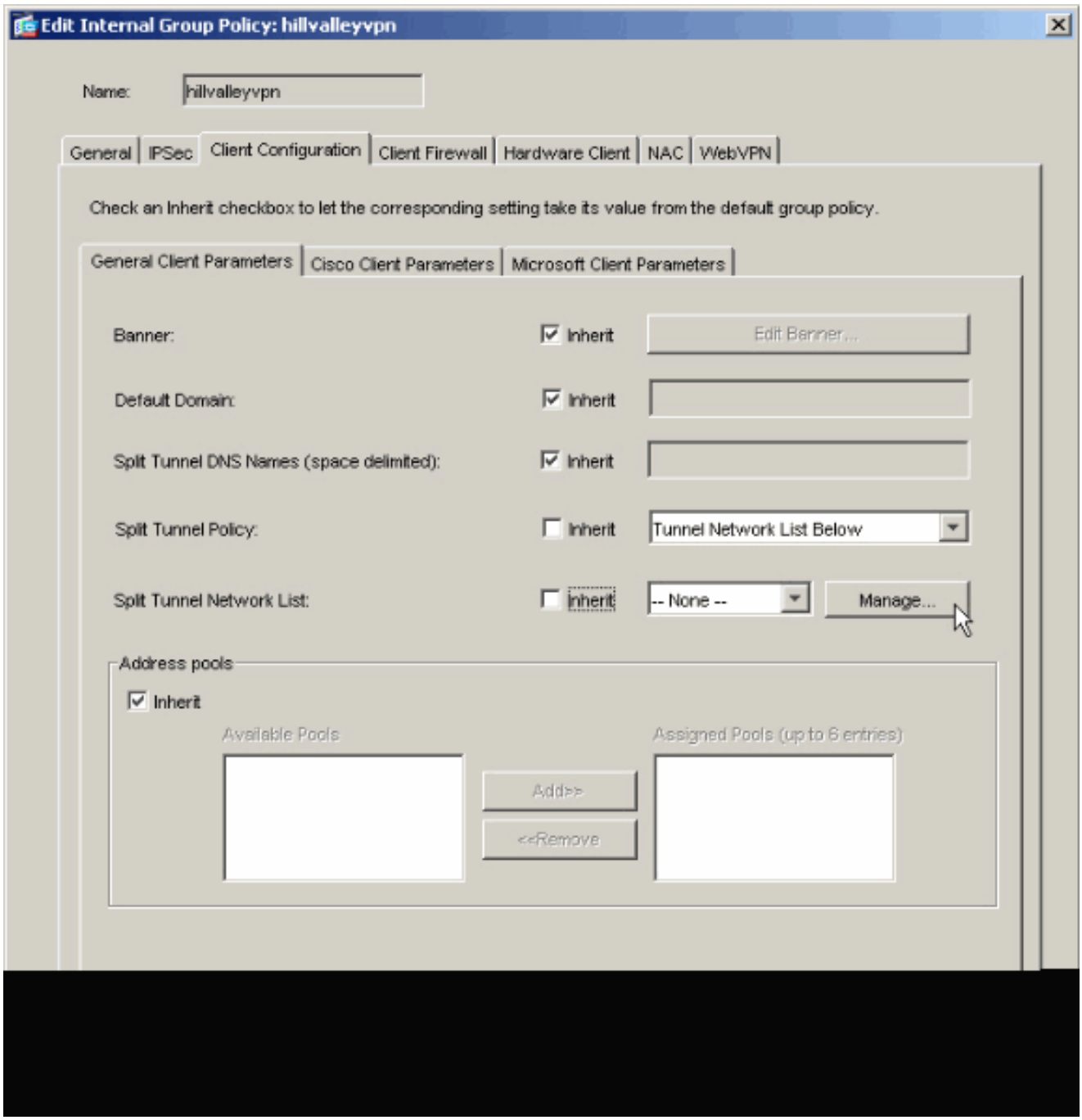


3. Deselezionare la casella Eredita per Criteri tunnel suddivisi e scegliere Tunnel Network List Below.



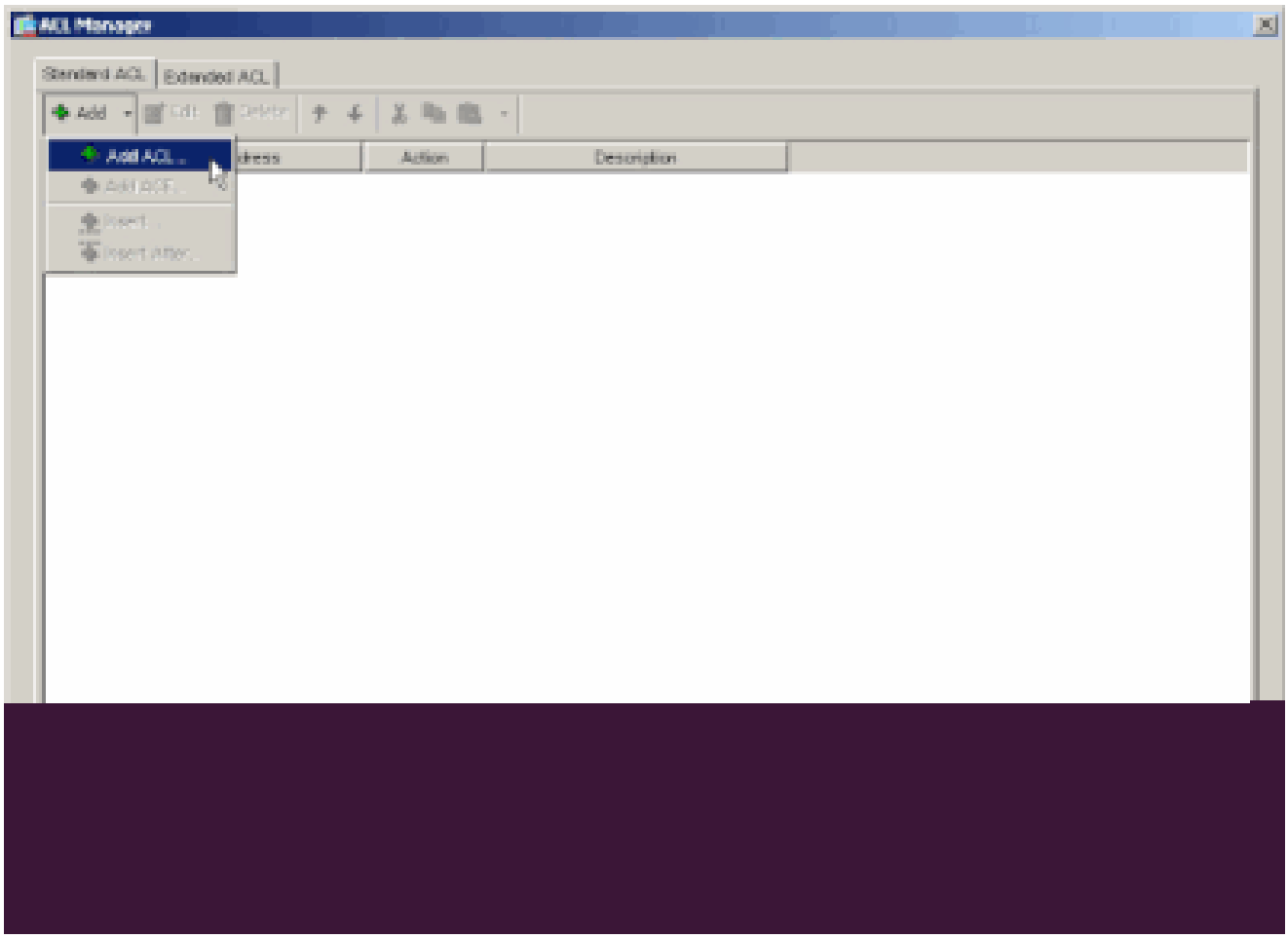
•

Deselezionare la casella di controllo **Eredita** per Elenco reti tunnel suddivise, quindi fare clic su **Gestisci** per avviare Gestione ACL.



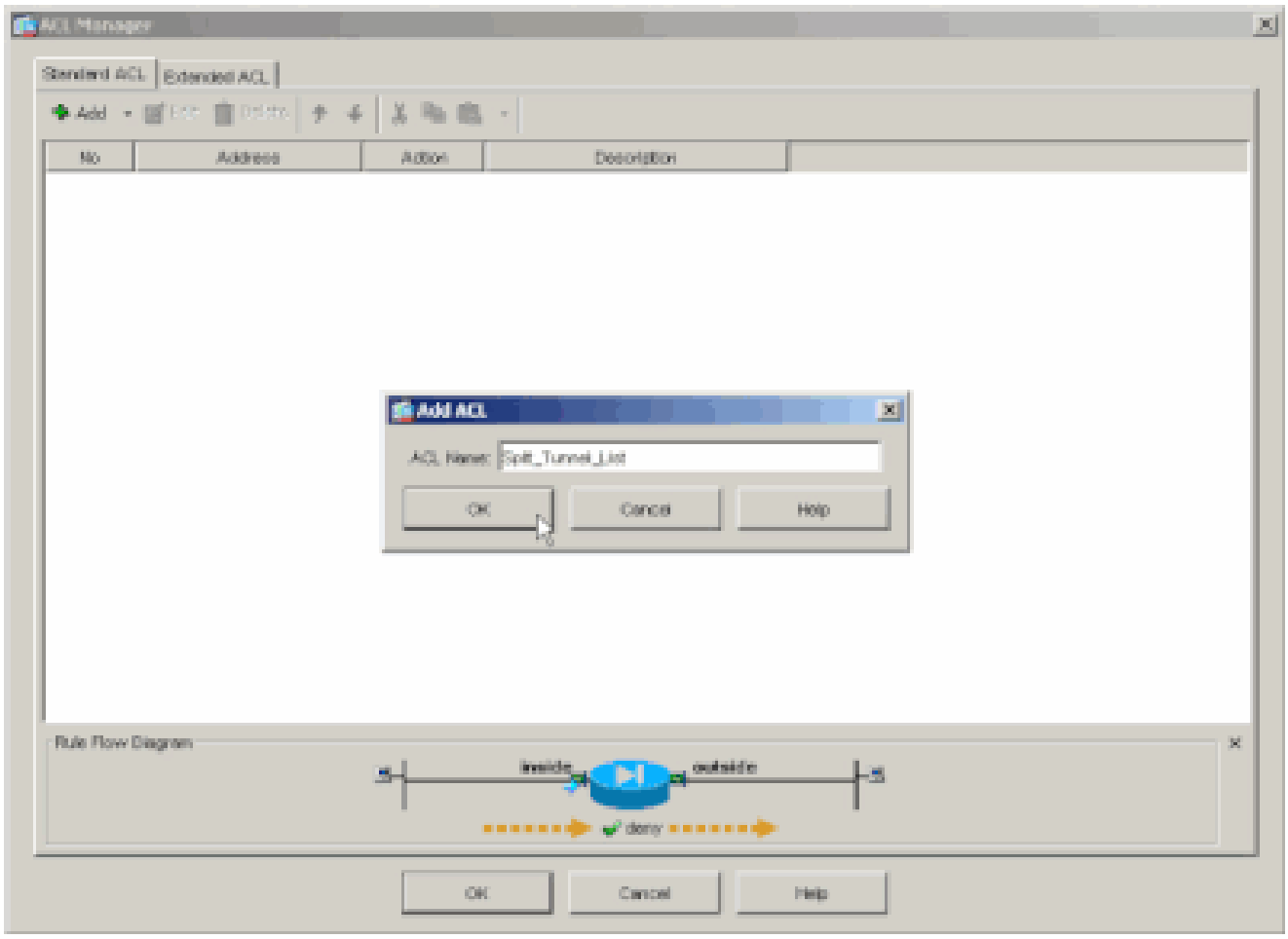
•

In Gestione ACL, selezionare **Aggiungi > Aggiungi ACL...** per creare un nuovo elenco degli accessi.



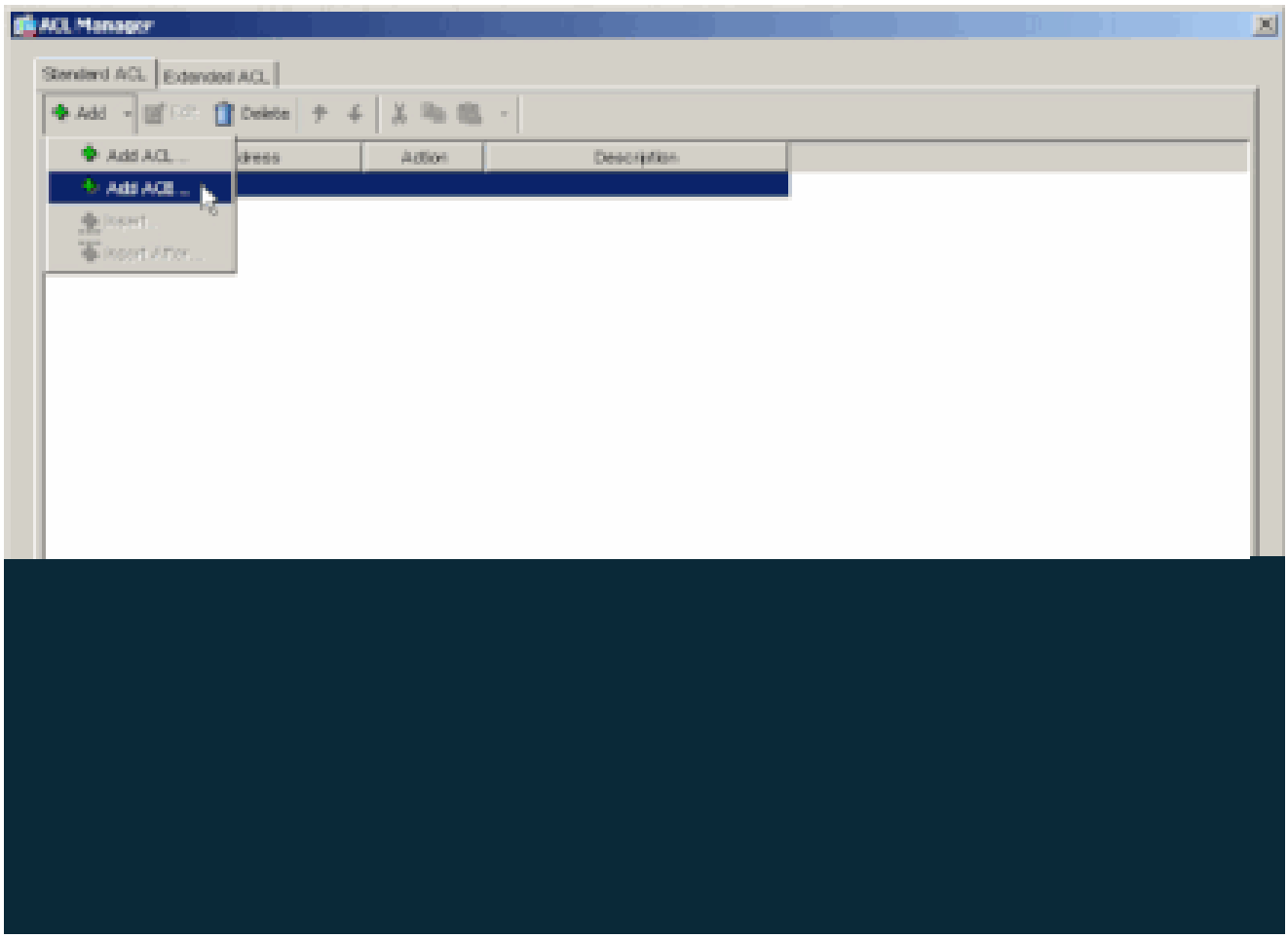
•

Specificare un nome per l'ACL e fare clic su **OK**.



•

Dopo aver creato l'ACL, selezionare **Add > Add ACE. .**per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).



•

Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.0.1.0/24.

a.

Scegliere **Autorizza** .

b.

Scegliere un indirizzo IP di **10.0.1.0**

c.

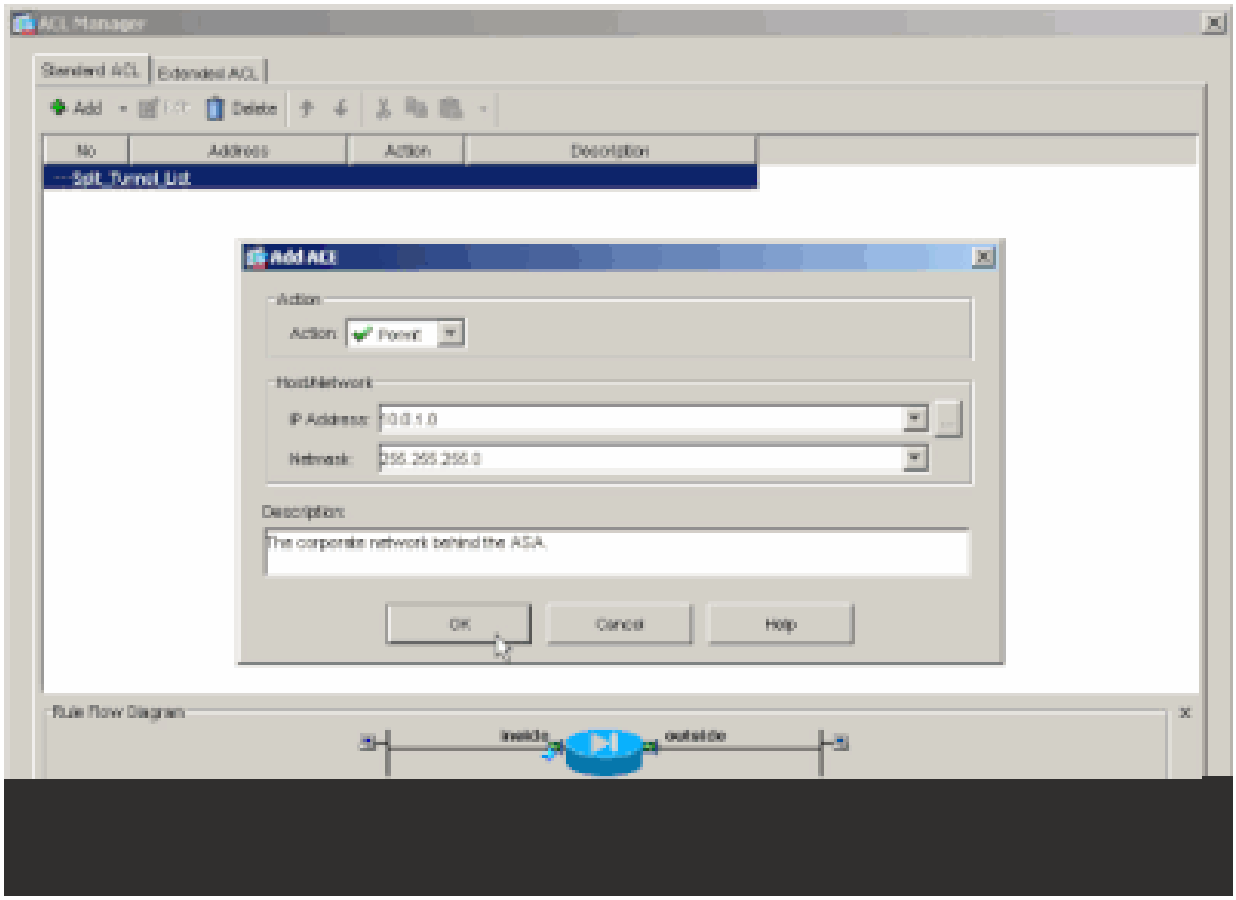
Selezionare una maschera di rete di **255.255.255.0**.

d.

(Facoltativo) Fornire una descrizione.

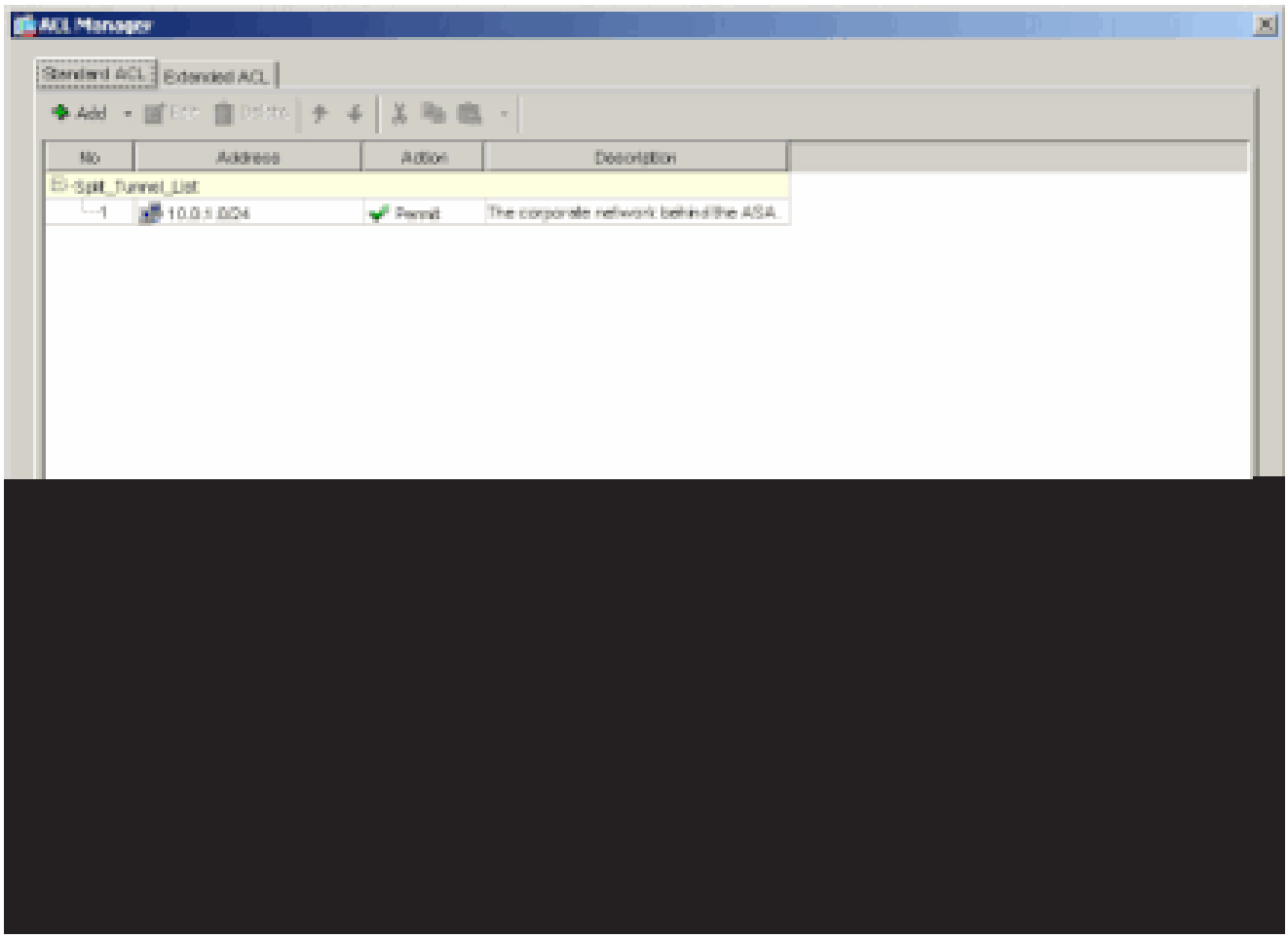
e.

Fate clic su > **OK**.



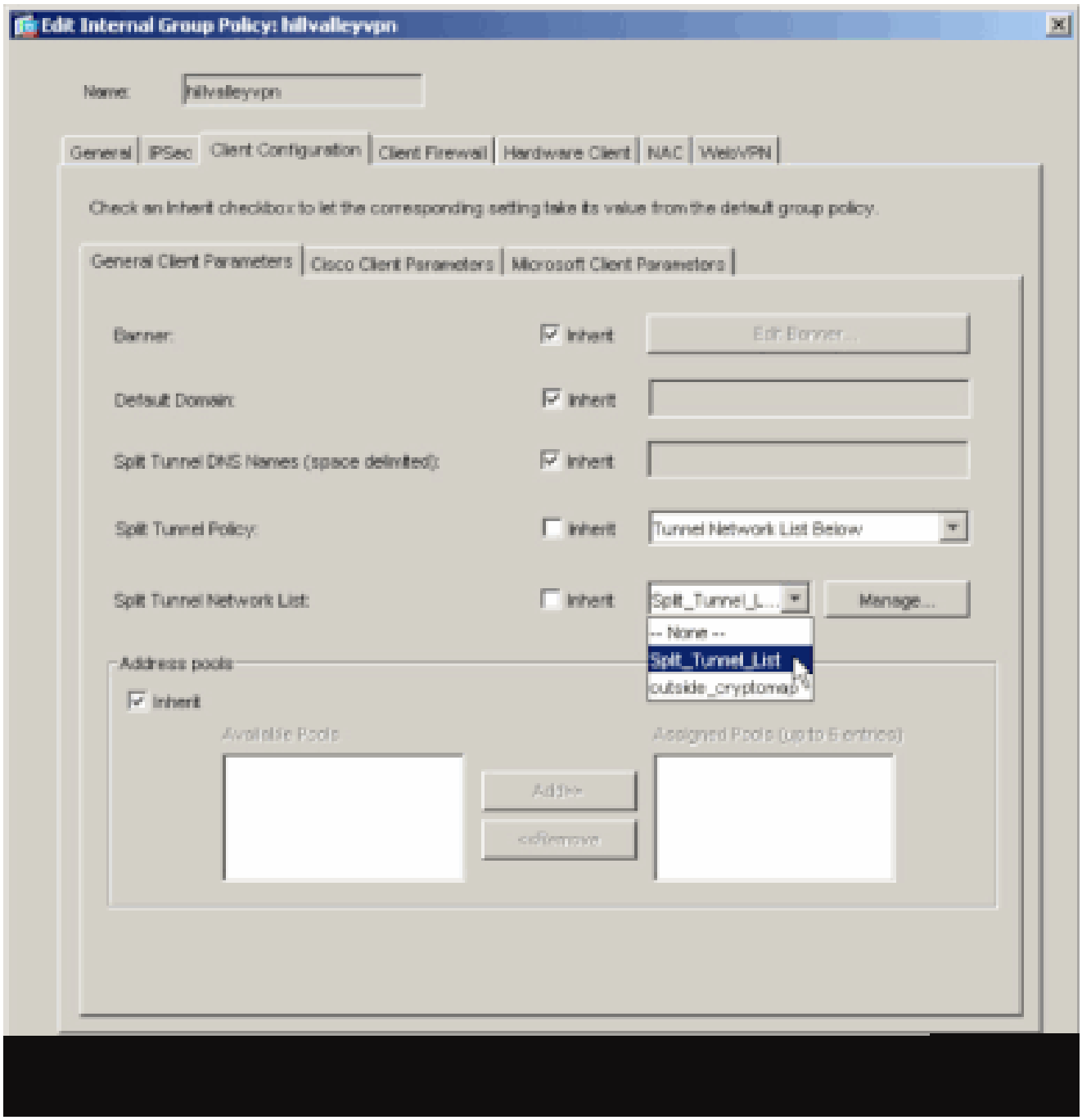
•

Per uscire da Gestione ACL, fare clic su **OK**.



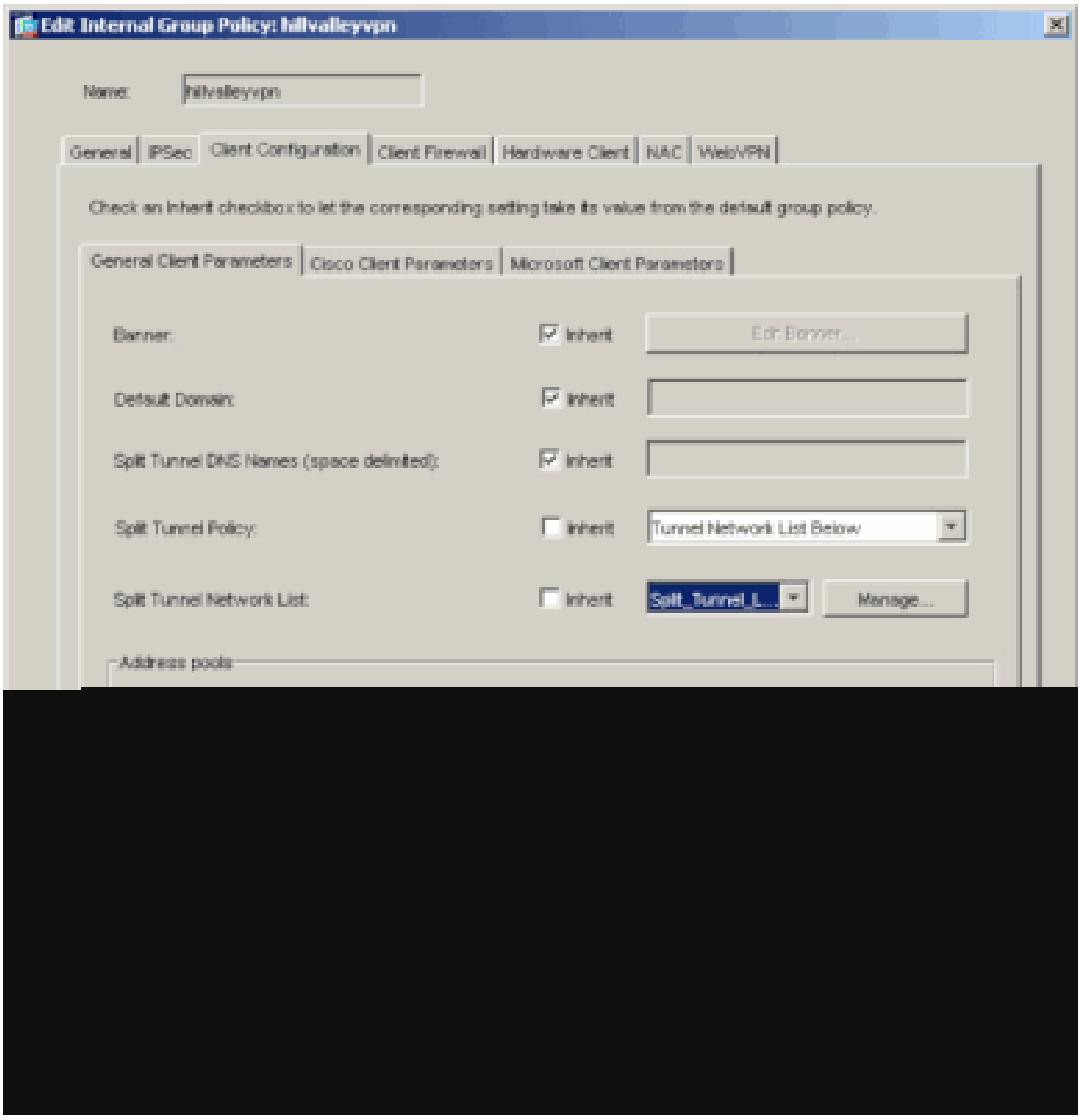
•

Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.



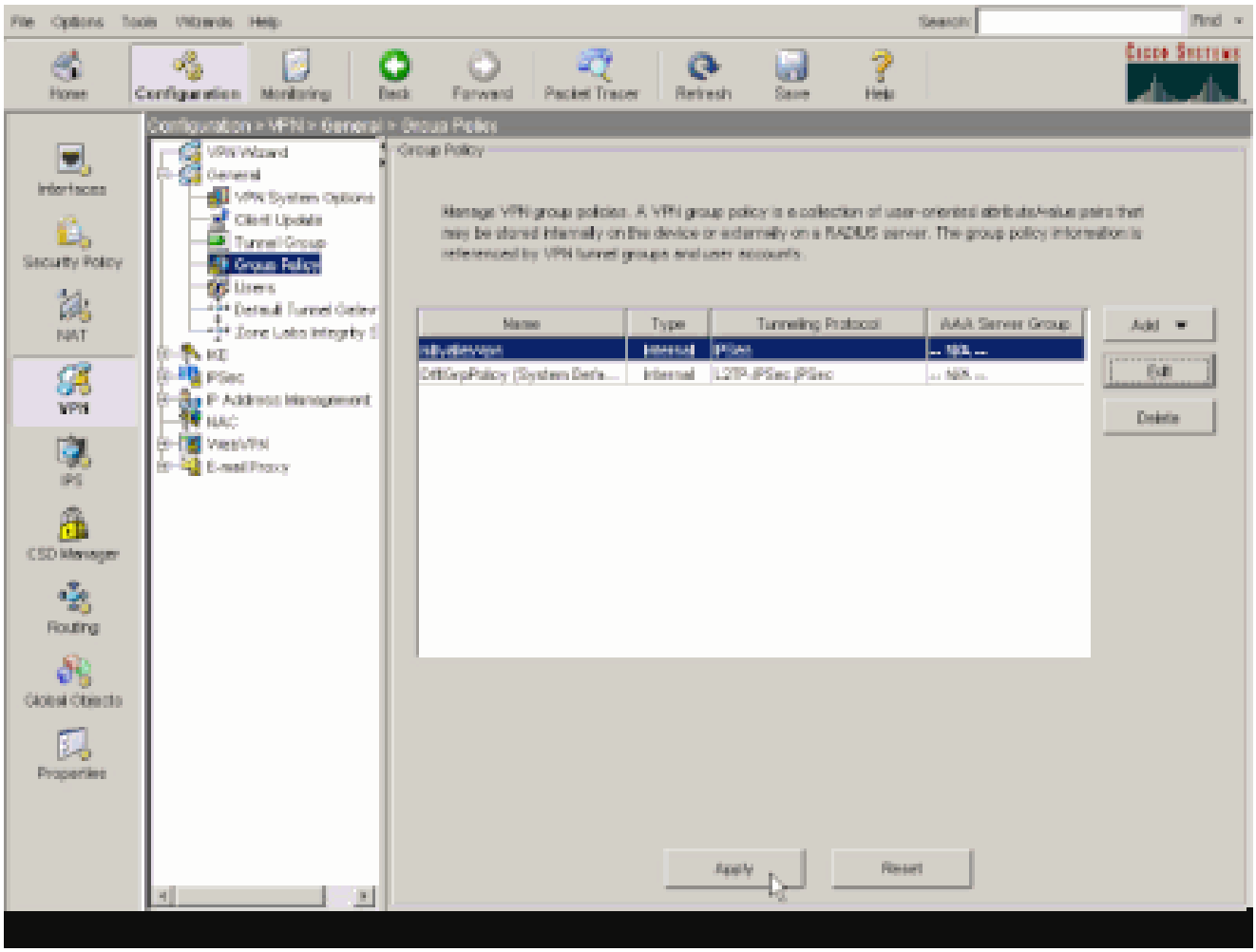
•

Per tornare alla configurazione di Criteri di gruppo, fare clic su **OK**.



•

Per inviare i comandi all'appliance ASA, fare clic su **Apply** e quindi su **Send** (se necessario).

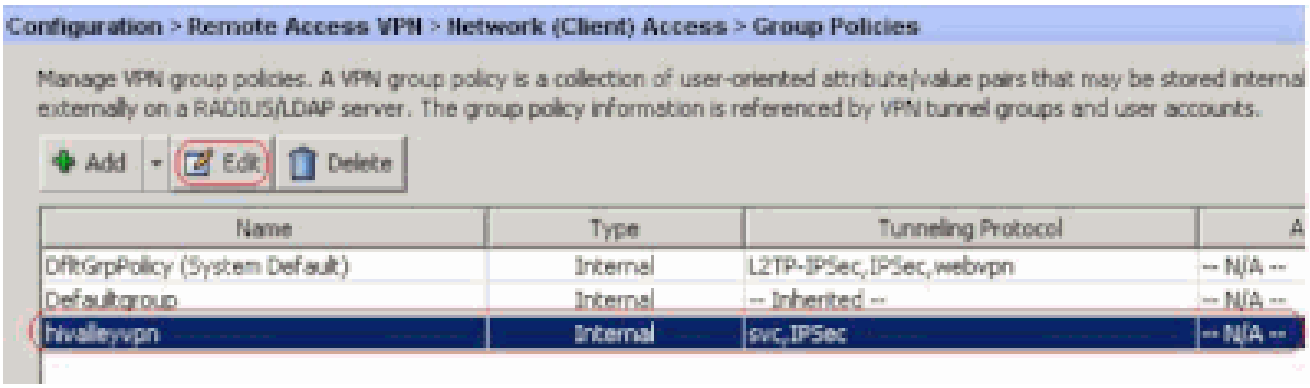


Configurare ASA 8.x con ASDM 6.x

Completare questa procedura per configurare il gruppo di tunnel in modo da consentire il tunneling suddiviso per gli utenti del gruppo.

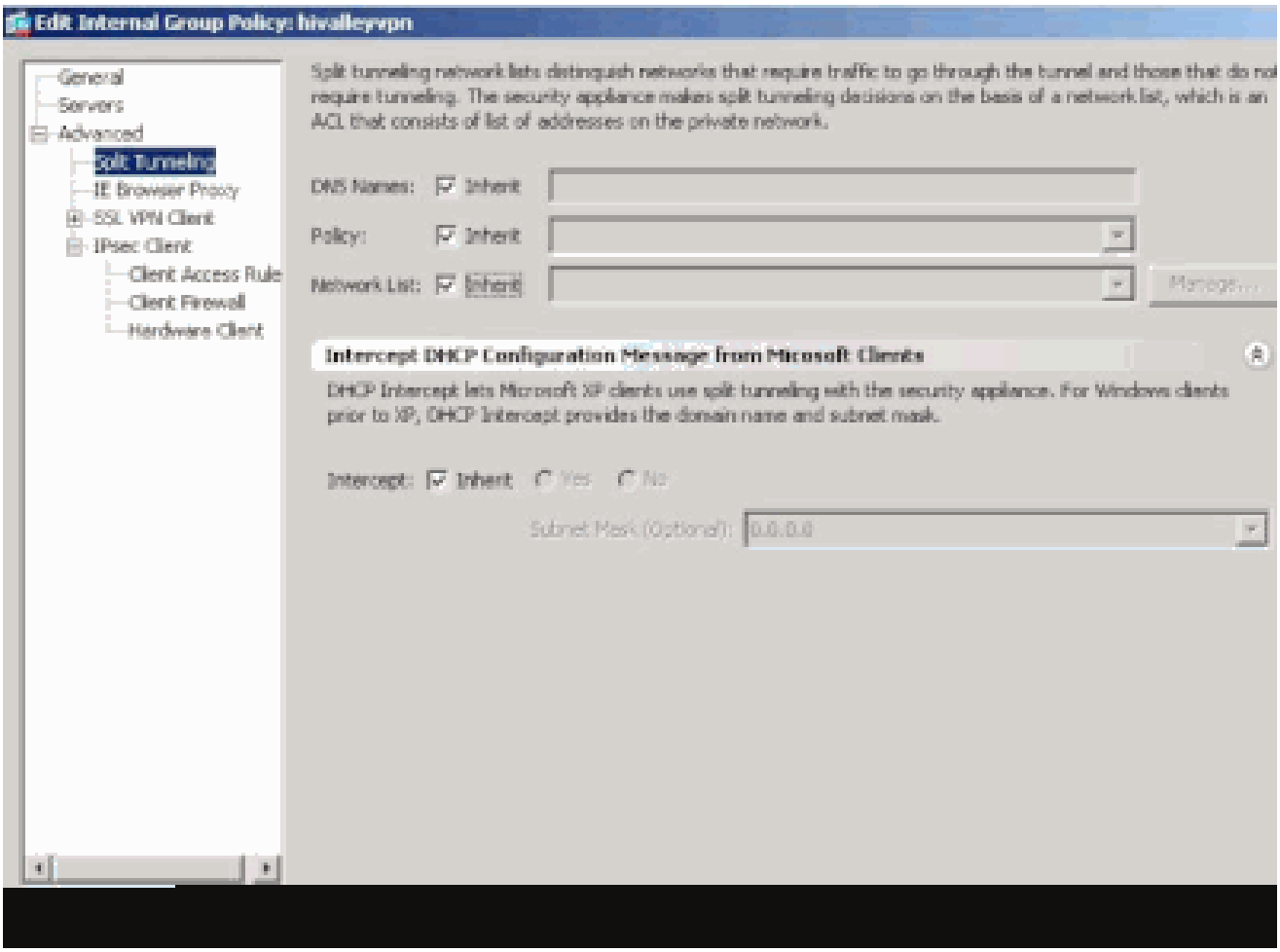
-

Scegliere **Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Criteri di gruppo** e scegliere i Criteri di gruppo in cui abilitare l'accesso LAN locale. Quindi fare clic su **Modifica**.



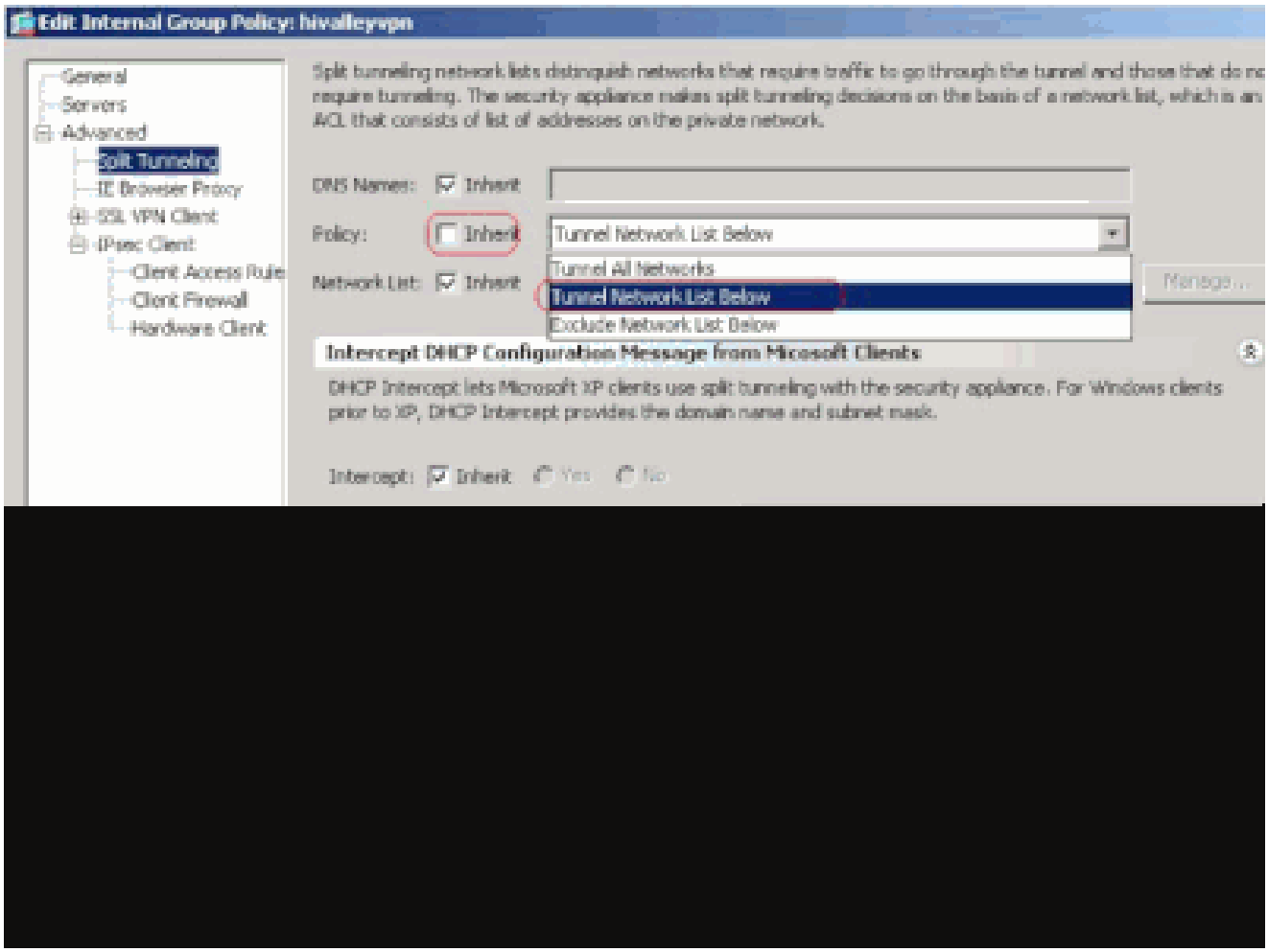
-

Fare clic su **Tunneling ripartito**.



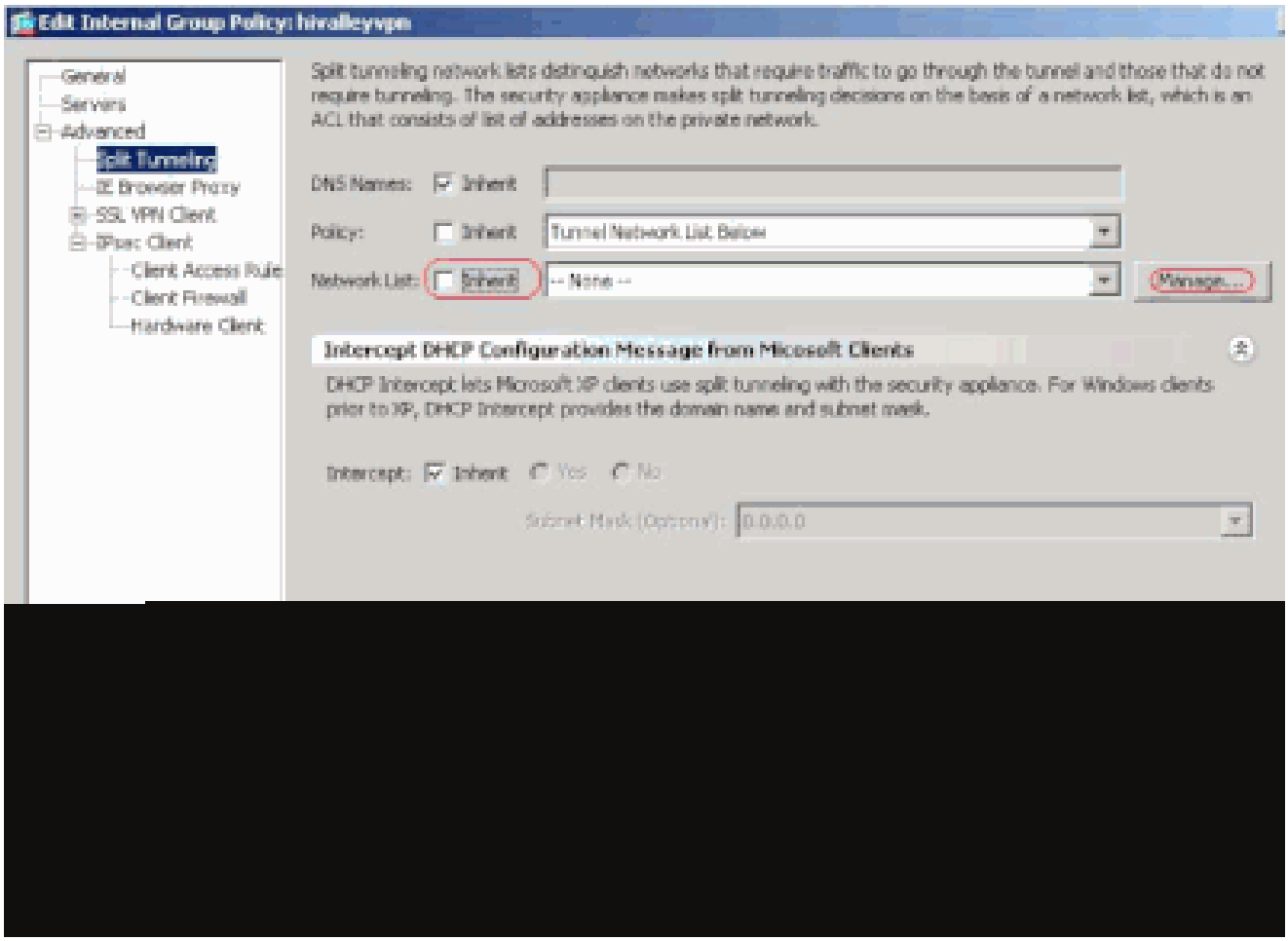
•

Deselezionare la casella **Eredita** per Criteri tunnel suddivisi e scegliere **Elenco reti tunnel di seguito**.



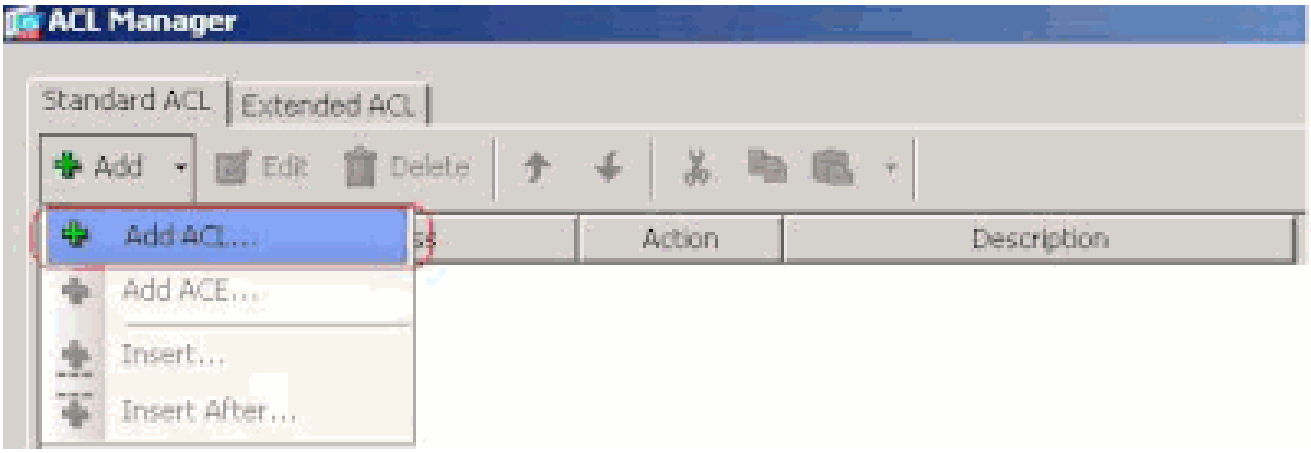
•

Deselezionare la casella di controllo **Eredita** per Elenco reti tunnel suddivise, quindi fare clic su **Gestisci** per avviare Gestione ACL.



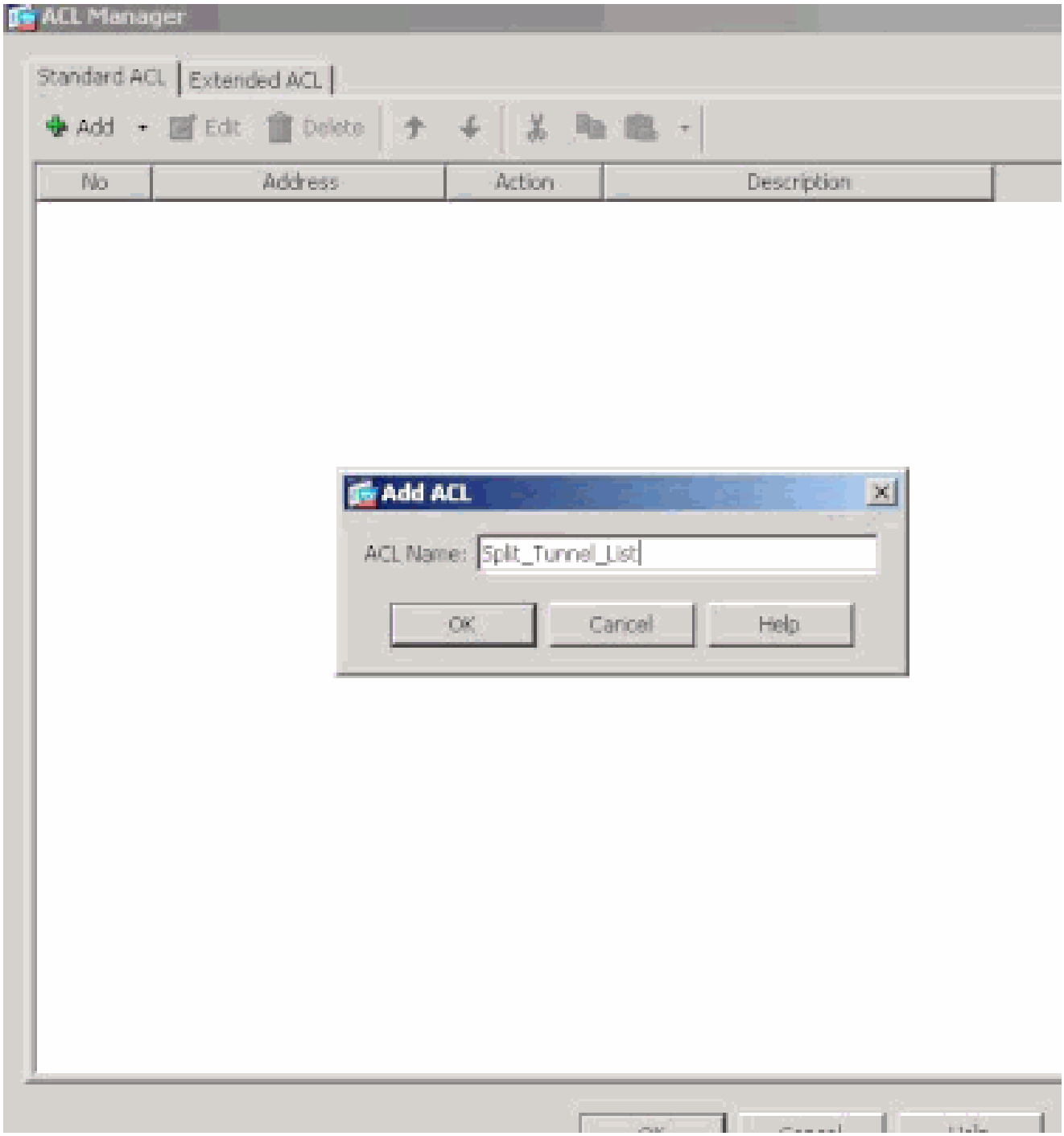
-

In Gestione ACL, selezionare **Aggiungi > Aggiungi ACL...** per creare un nuovo elenco degli accessi.



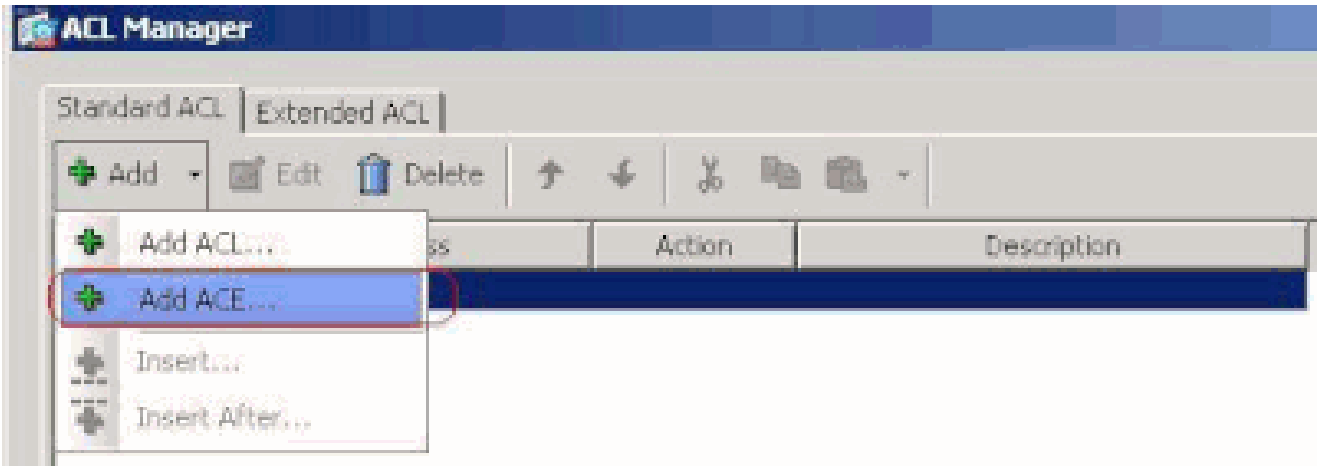
-

Specificare un nome per l'ACL e fare clic su **OK**.



•

Una volta creato l'ACL, scegliere **Aggiungi > Aggiungi ACE...** per aggiungere una voce di controllo di accesso (ACE, Access Control Entry).



-

Definire l'ACE che corrisponde alla LAN dietro l'ASA. In questo caso, la rete è 10.0.1.0/24.

a.

Fare clic sul pulsante di opzione **Autorizza**.

b.

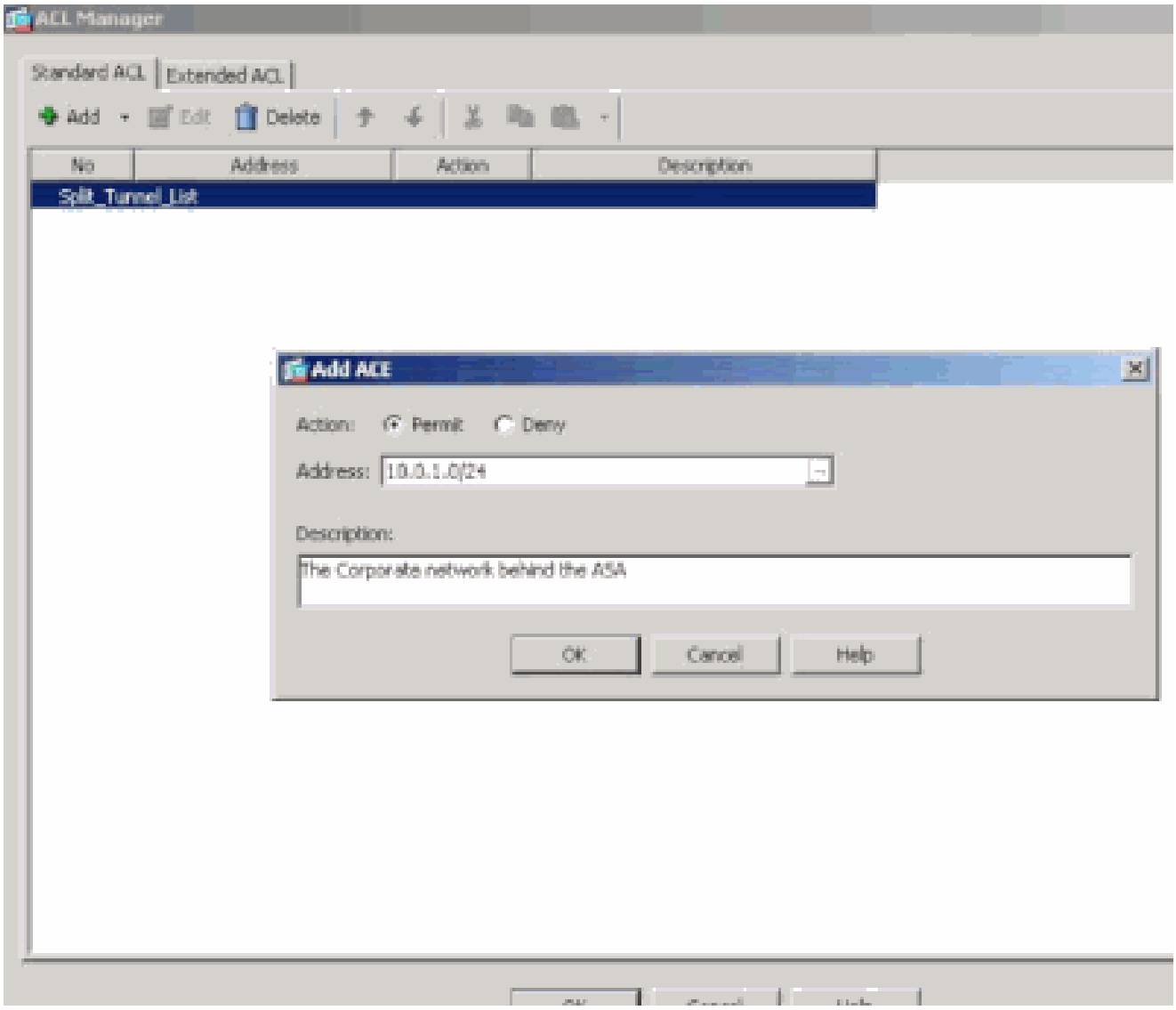
Scegliere l'indirizzo di rete con maschera **10.0.1.0/24**.

c.

(Facoltativo) Fornire una descrizione.

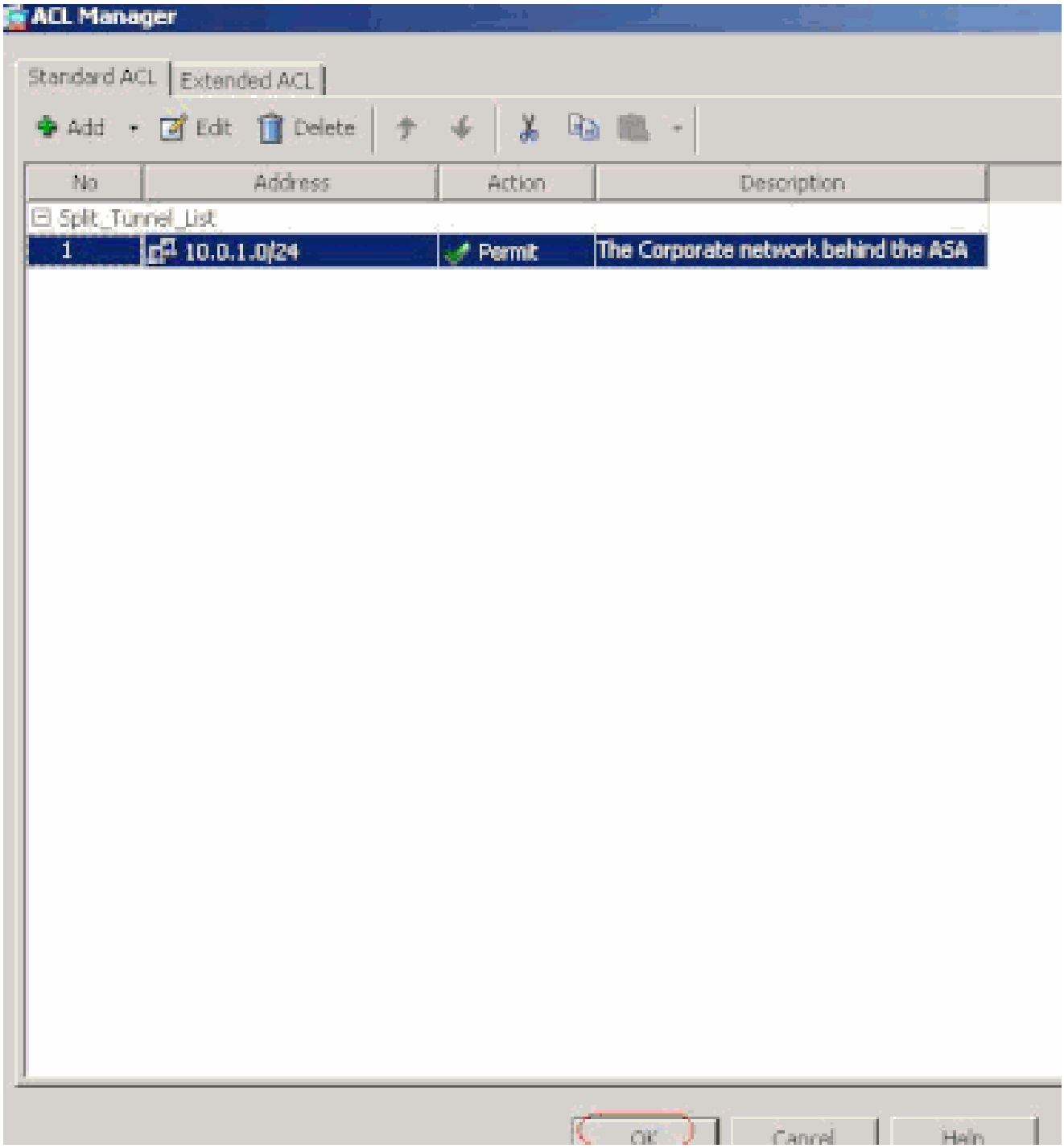
d.

Fare clic su OK.



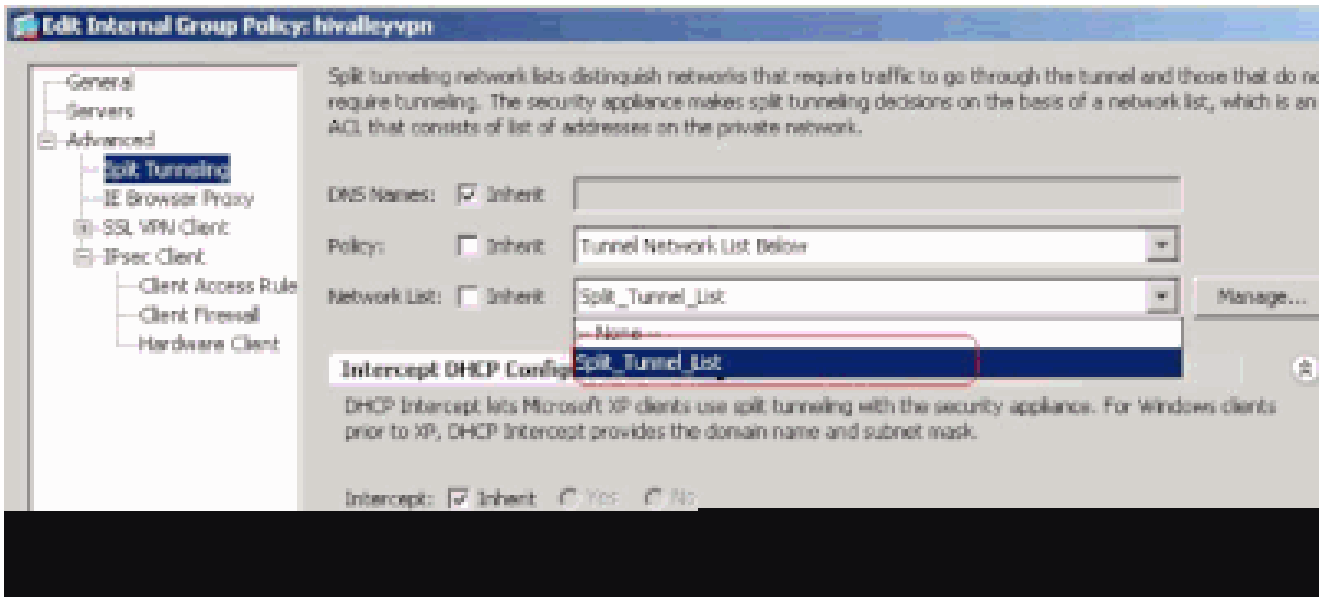
•

Per uscire da Gestione ACL, fare clic su **OK**.



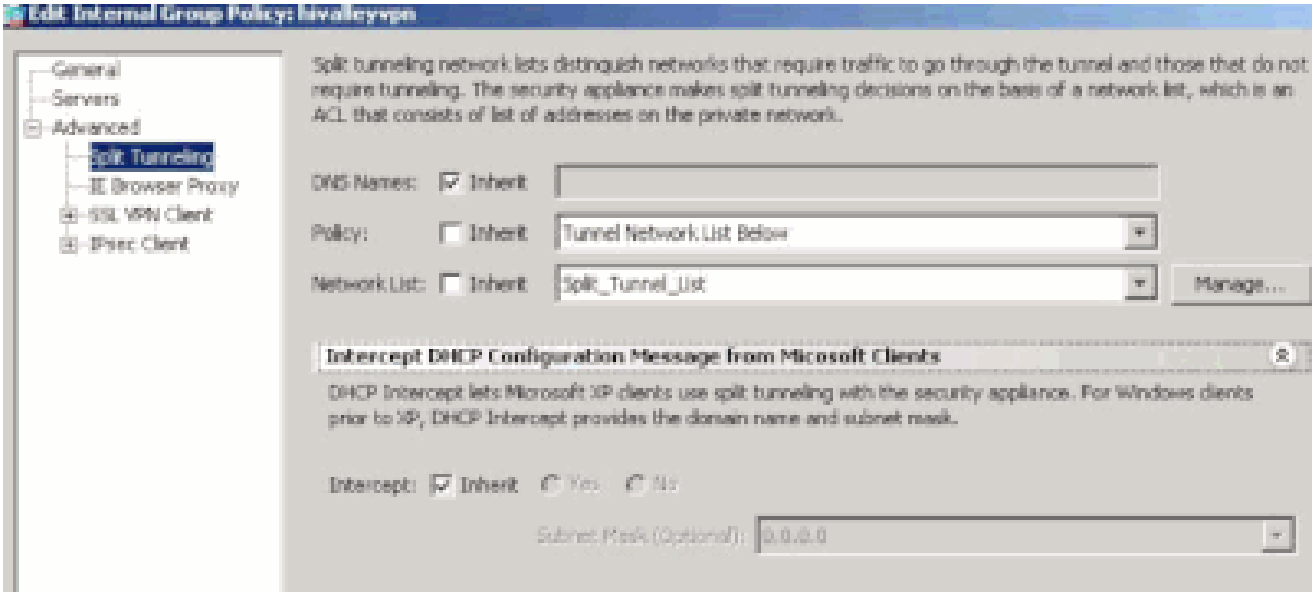
•

Accertarsi quindi che l'ACL appena creato sia selezionato per l'elenco delle reti a tunnel suddiviso.



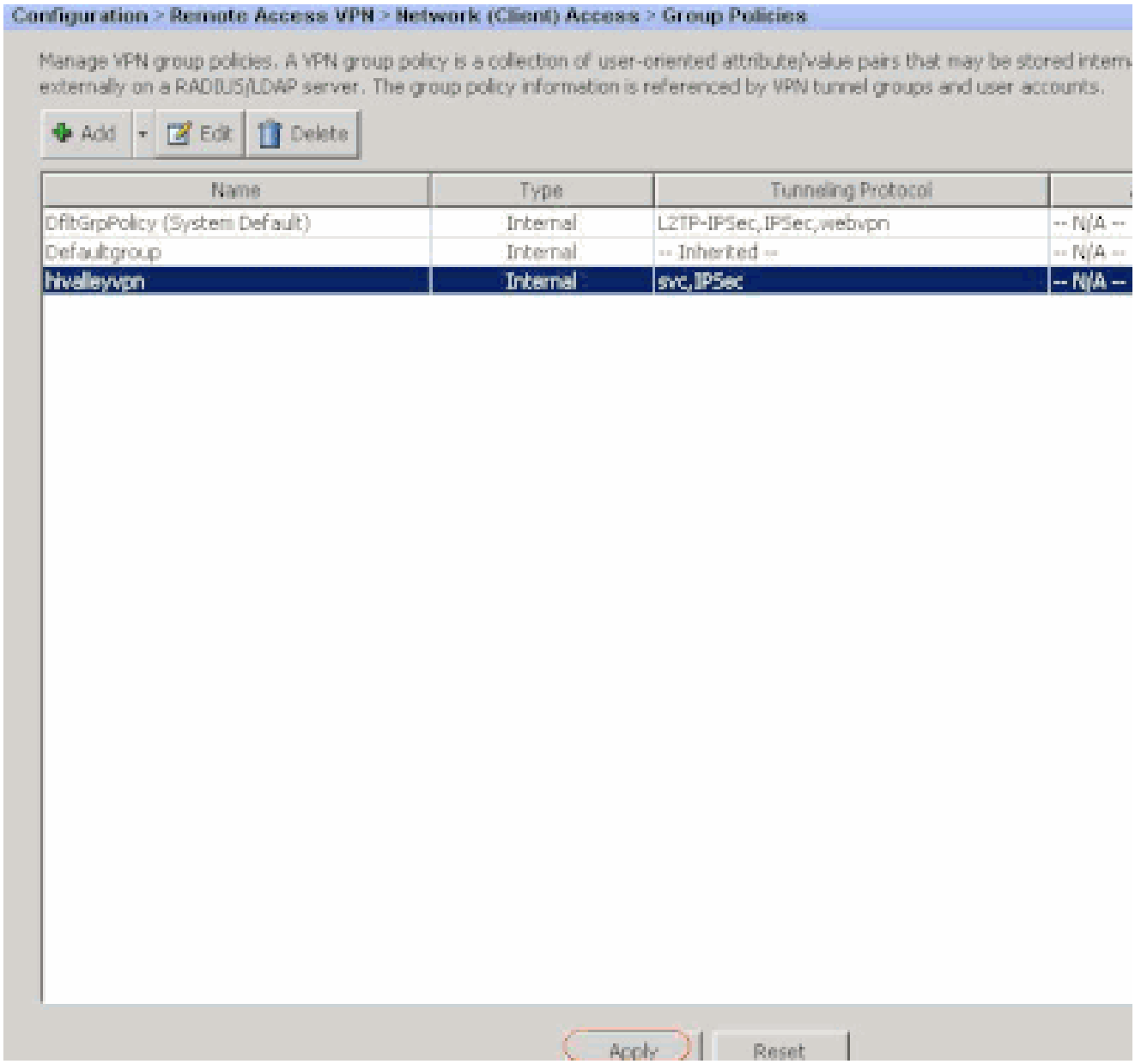
•

Per tornare alla configurazione di Criteri di gruppo, fare clic su **OK**.



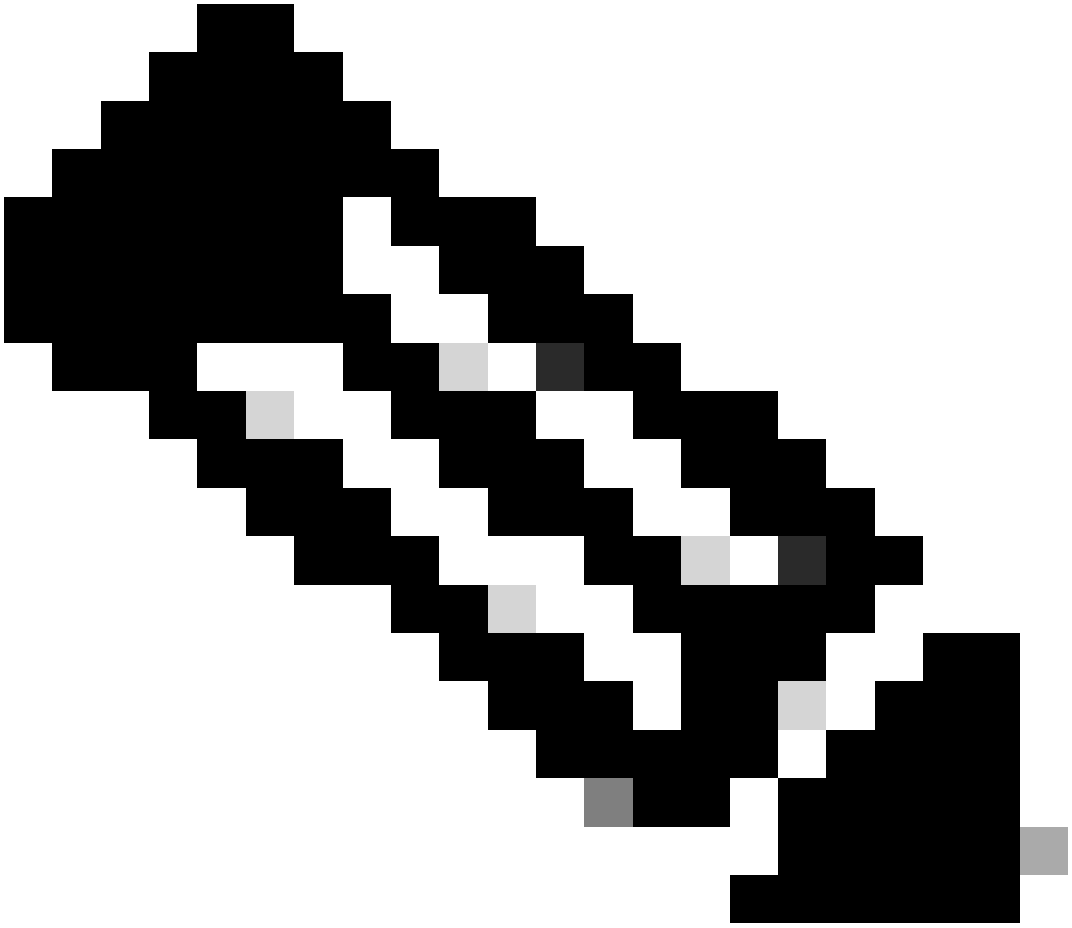
•

Per inviare i comandi all'appliance ASA, fare clic su **Apply** e quindi su **Send** (se necessario).



Configurazione di ASA 7.x e versioni successive tramite CLI

Anziché utilizzare ASDM, è possibile completare i seguenti passaggi nella CLI dell'ASA per consentire il tunneling suddiviso sull'appliance ASA:



Nota: la configurazione del tunneling con split CLI è la stessa per entrambe le appliance ASA 7.x e 8.x.

-

Accedere alla modalità di configurazione.

```
<#root>

ciscoasa>
```

```
enable
```

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

```
configure terminal
```

```
ciscoasa(config)#
```

-

Creare l'elenco degli accessi che definisce la rete dietro l'appliance ASA.

```
    <#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
```

-

Accedere alla modalità di configurazione di Criteri di gruppo per il criterio che si desidera modificare.

```
    <#root>

ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

-

Specificare i criteri per il tunnel suddiviso. In questo caso il criterio è **specificato tramite tunneling**.

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

-

Specificare l'elenco degli accessi al tunnel suddiviso. In questo caso, l'elenco è **Split_Tunnel_List**.

```
    <#root>

ciscoasa(config-group-policy)#

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

-

Immettere questo comando

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

-

Associare i Criteri di gruppo al gruppo di tunnel

<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

-

Uscire dalle due modalità di configurazione.

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

exit

```
ciscoasa#
```

- Salvare la configurazione nella memoria RAM non volatile (NVRAM) e premere **Invio** quando richiesto per specificare il nome del file di origine.

```
<#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#
```

Configurazione di PIX 6.x tramite la CLI

Attenersi alla seguente procedura:

- Creare l'elenco degli accessi che definisce la rete dietro al PIX.

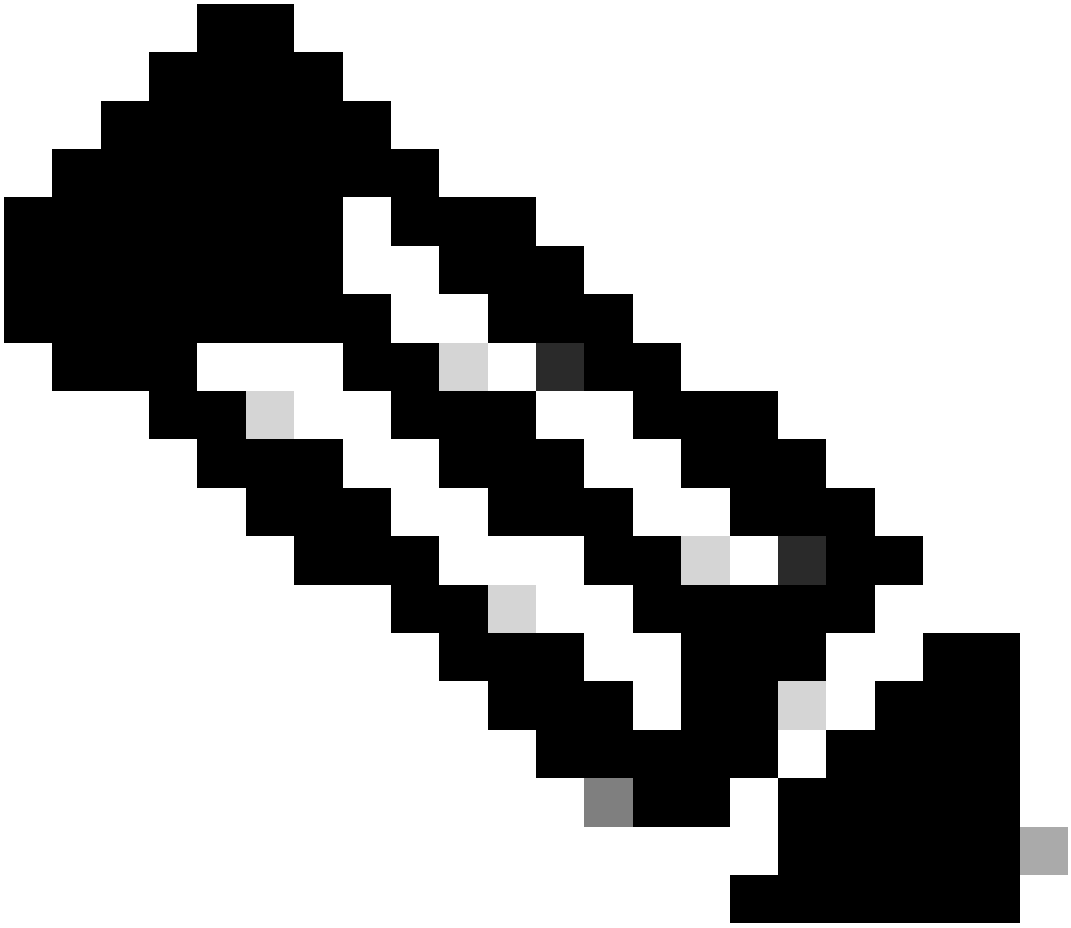
```
<#root>

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

- Creare un gruppo vpn **vpn3000** e specificare l'ACL del tunnel suddiviso come mostrato:

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



Nota: per ulteriori informazioni sulla configurazione della VPN di accesso remoto per PIX 6.x, fare riferimento a Cisco Secure PIX Firewall 6.x e Cisco VPN Client 3.5 per Windows con autenticazione RADIUS IAS Microsoft Windows 2000 e 2003.

Verifica

Per verificare la configurazione, completare la procedura descritta in queste sezioni.

- Connessione con il client VPN

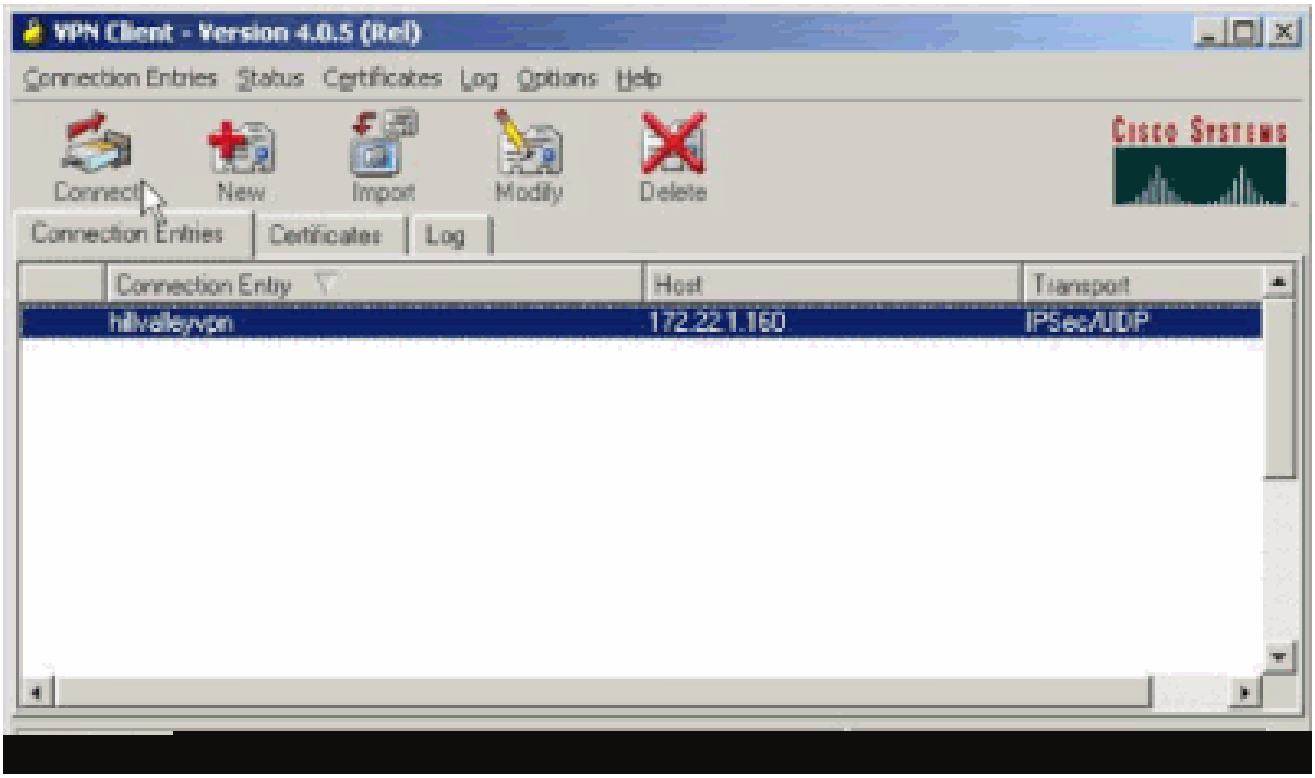
- Visualizza registro client VPN

- Test dell'accesso LAN locale con ping

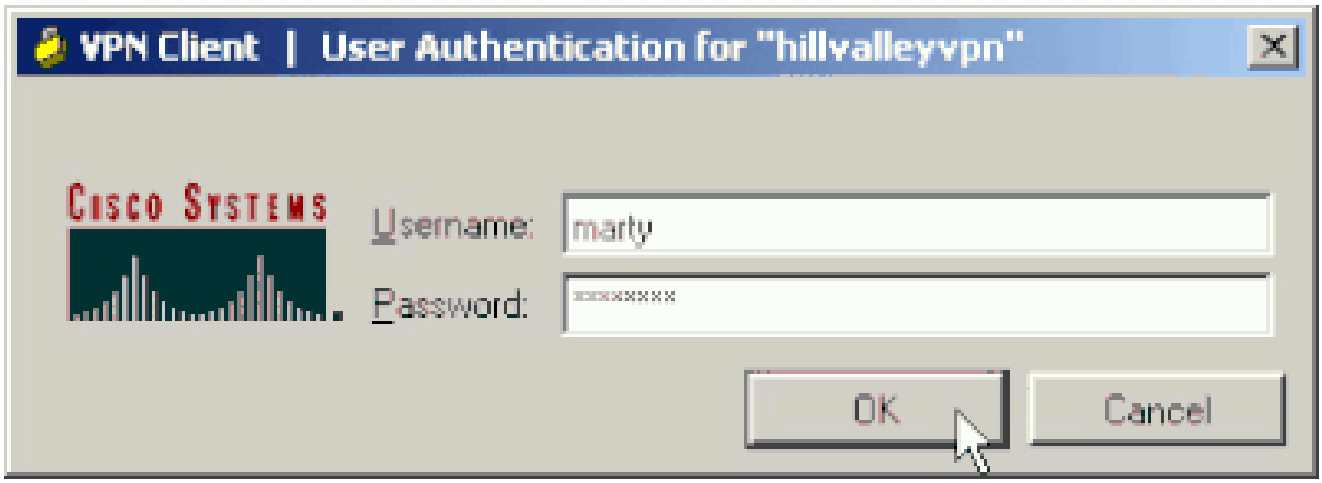
Connessione con il client VPN

Connettere il client VPN a VPN Concentrator per verificare la configurazione.

- Selezionare la voce di connessione dall'elenco e fare clic su **Connetti**.

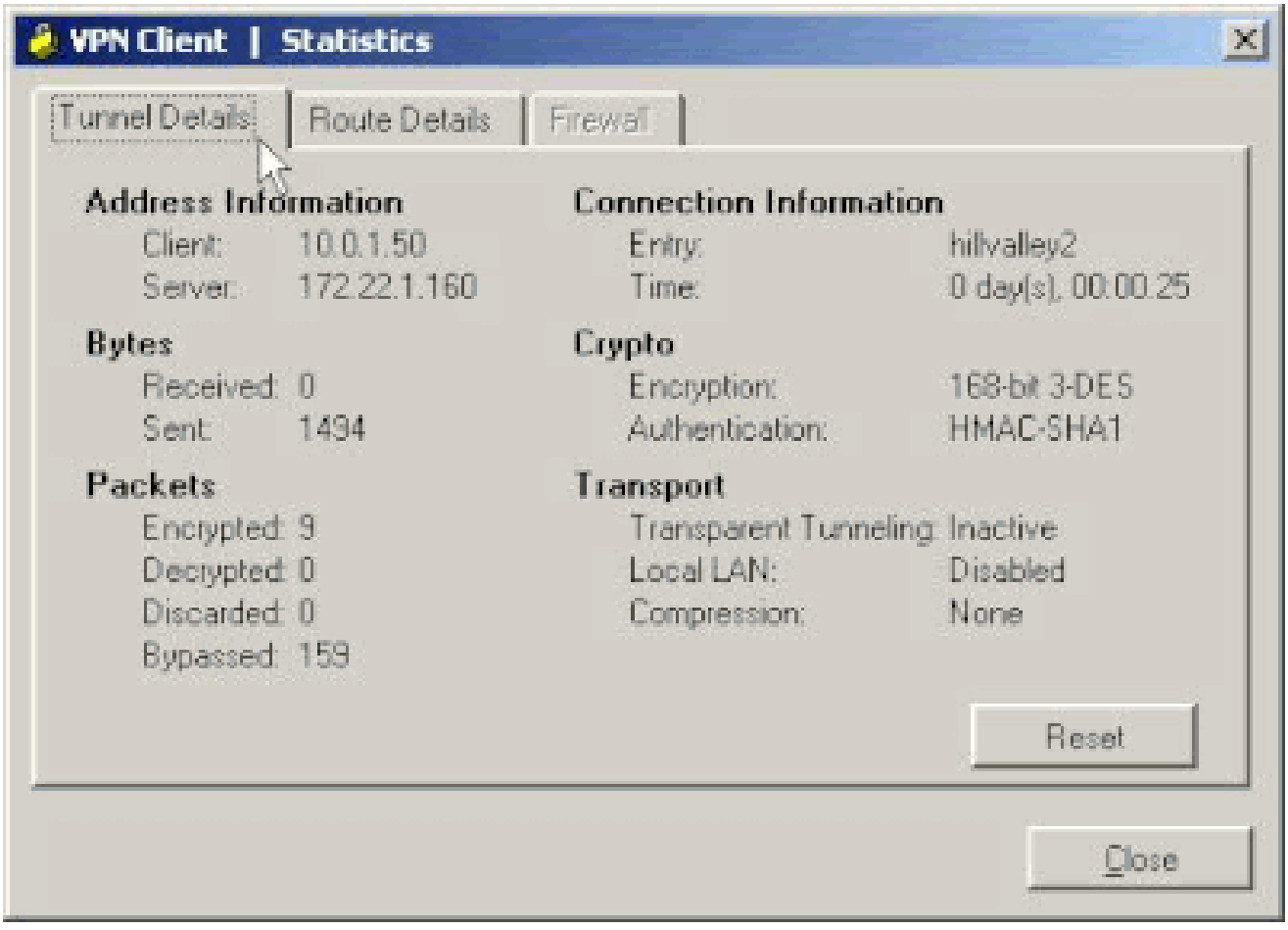


- Immettere le credenziali.



•

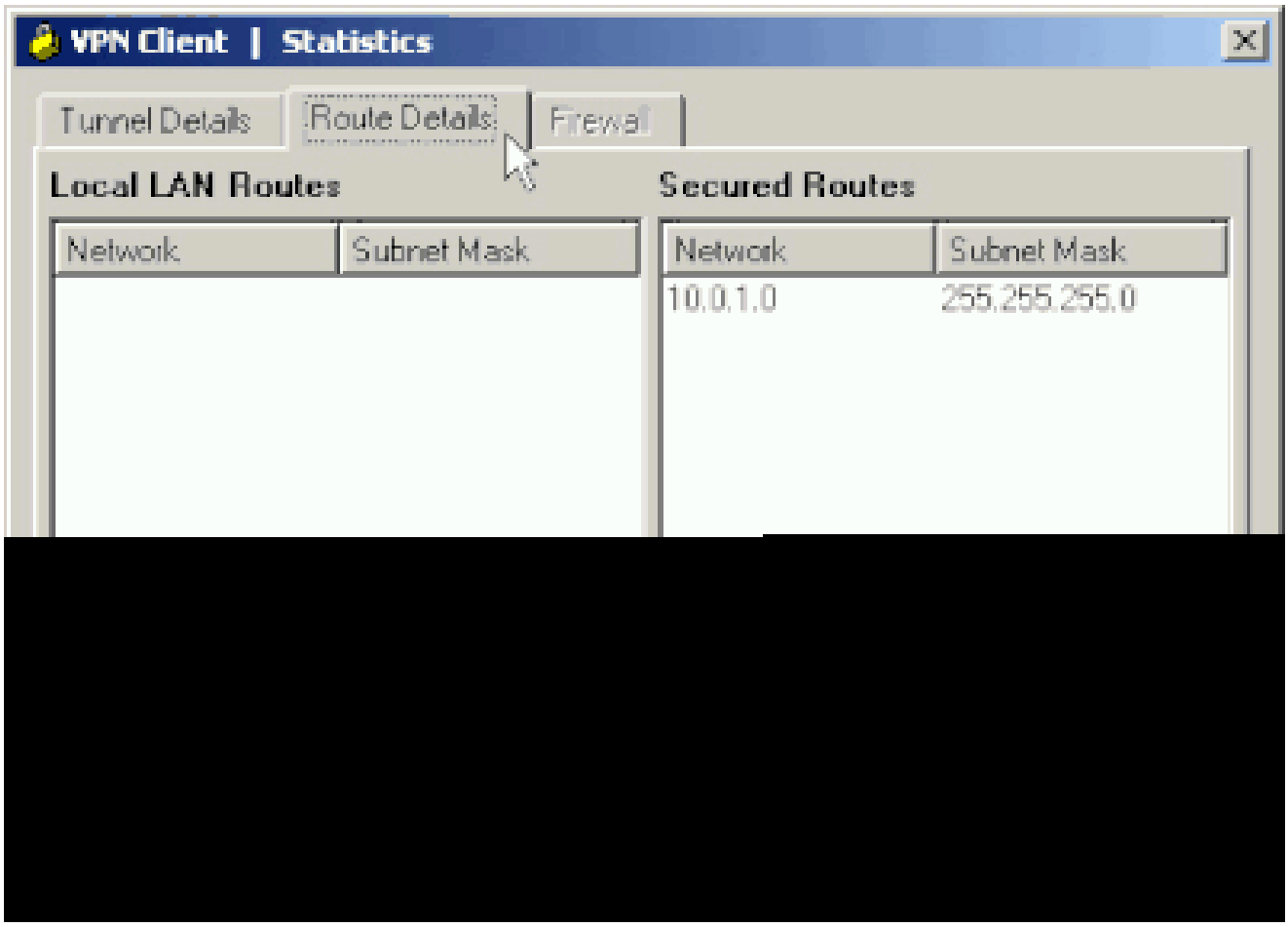
Scegliere **Stato > Statistiche...** per visualizzare la finestra Dettagli tunnel, in cui è possibile esaminare i dettagli del tunnel e verificare il flusso del traffico.



•

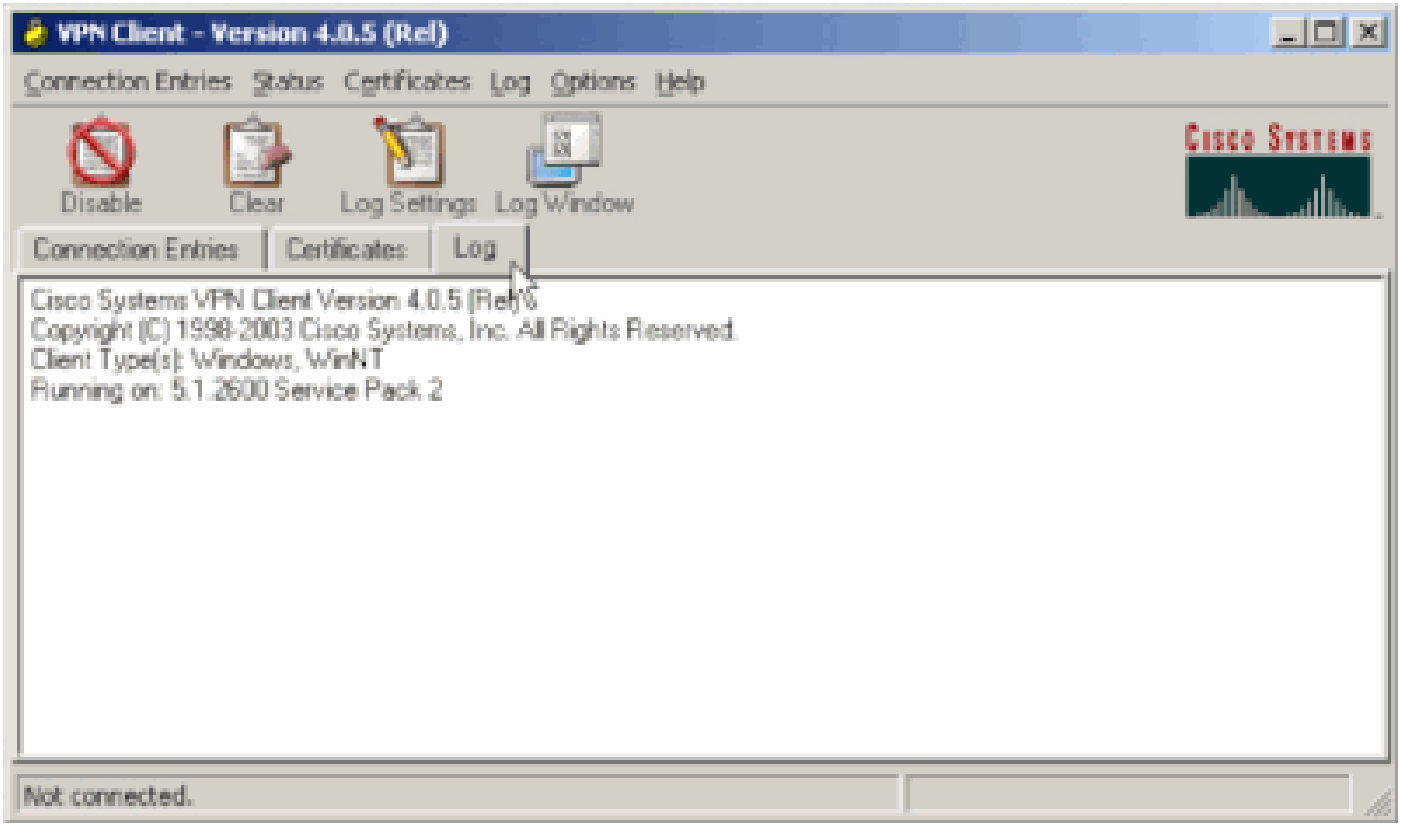
Per visualizzare le route che il client VPN sta proteggendo verso l'appliance ASA, andare alla scheda Dettagli route.

Nell'esempio, il client VPN sta proteggendo l'accesso a 10.0.1.0/24, mentre tutto il resto del traffico non è crittografato e non viene inviato attraverso il tunnel.



Visualizza registro client VPN

Quando si esamina il registro del client VPN, è possibile determinare se è impostato o meno il parametro che specifica la suddivisione del tunneling. Per visualizzare il log, andare alla scheda Log nel client VPN. Quindi fare clic su **Log Settings** (Impostazioni registro) per regolare i dati registrati. Nell'esempio, IKE è impostato su **3 - Alta** mentre tutti gli altri elementi del log sono impostati su **1 - Bassa**.




```
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.
```

Test dell'accesso LAN locale con ping

Per verificare che il client VPN sia configurato per il tunneling suddiviso quando è tunneling all'ASA, è possibile usare anche il comando **ping** sulla riga di comando di Windows. La LAN locale del client VPN è 192.168.0.0/24 e sulla rete è presente un altro host con indirizzo IP 192.168.0.3.

```
   <#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
```

Risoluzione dei problemi

Limitazione del numero di voci in un ACL con tunnel suddiviso

È presente una restrizione relativa al numero di voci in un ACL usato per il tunnel suddiviso. Si consiglia di non utilizzare più di 50-60 voci ACE per una funzionalità soddisfacente. È consigliabile implementare la funzionalità di subnet per coprire un intervallo di indirizzi IP.

Informazioni correlate

- **PIX/ASA 7.x come server VPN remoto con configurazione ASDM**
- **Cisco ASA serie 5500 Adaptive Security Appliance**
- **Supporto tecnico Cisco e download**

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).