ASAでのVPNクライアントのスプリットトンネリングの設定

内容

はじめに

このドキュメントでは、Cisco ASA 5500シリーズセキュリティアプライアンスにトンネリングしながら、VPN Clientがインターネットにアクセスできるようにするプロセスについて説明します。

前提条件

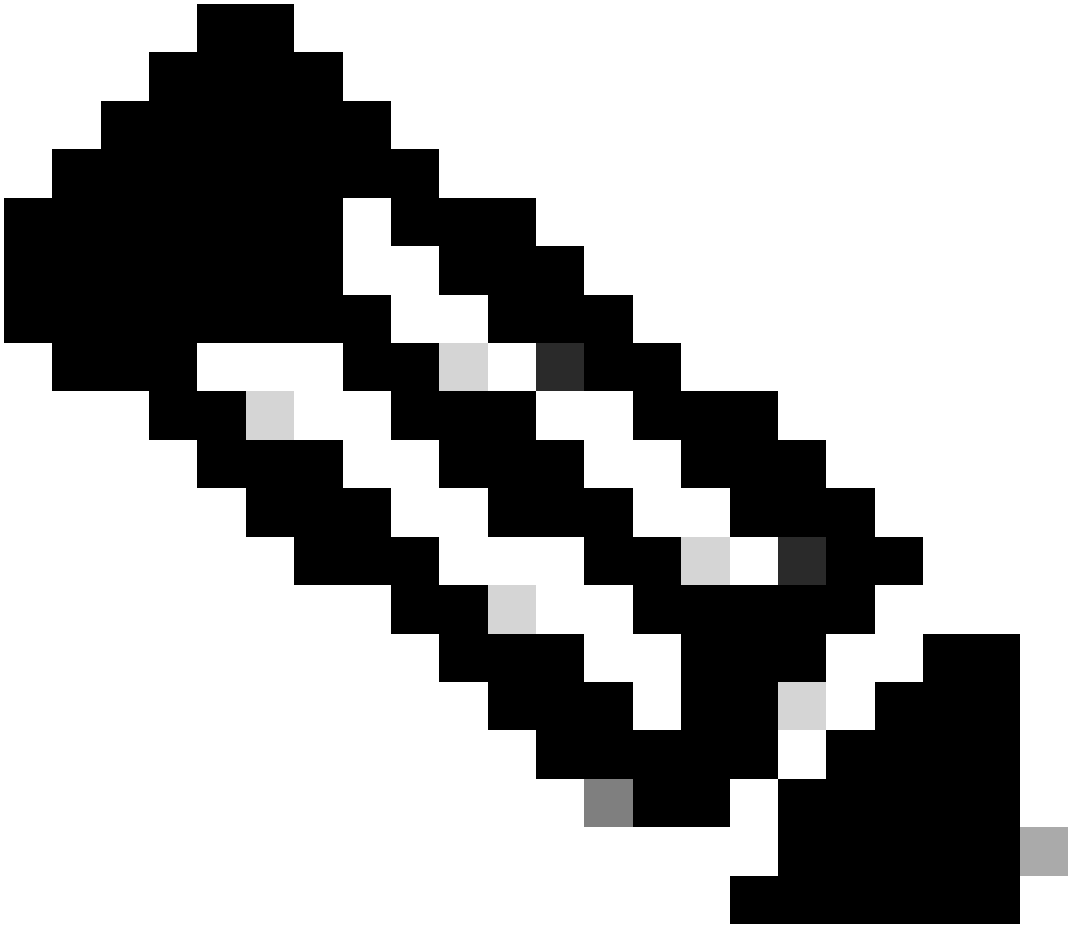
要件

このドキュメントは、動作しているリモート アクセス VPN 設定が ASA にすでに存在していることを前提としています。未設定の場合は、『ASDMを使用したリモートVPNサーバとしてのPIX/ASA 7.xの設定例』を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 5500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Cisco Systems VPN Client バージョン 4.0.5
- Adaptive Security Device Manager（ASDM）

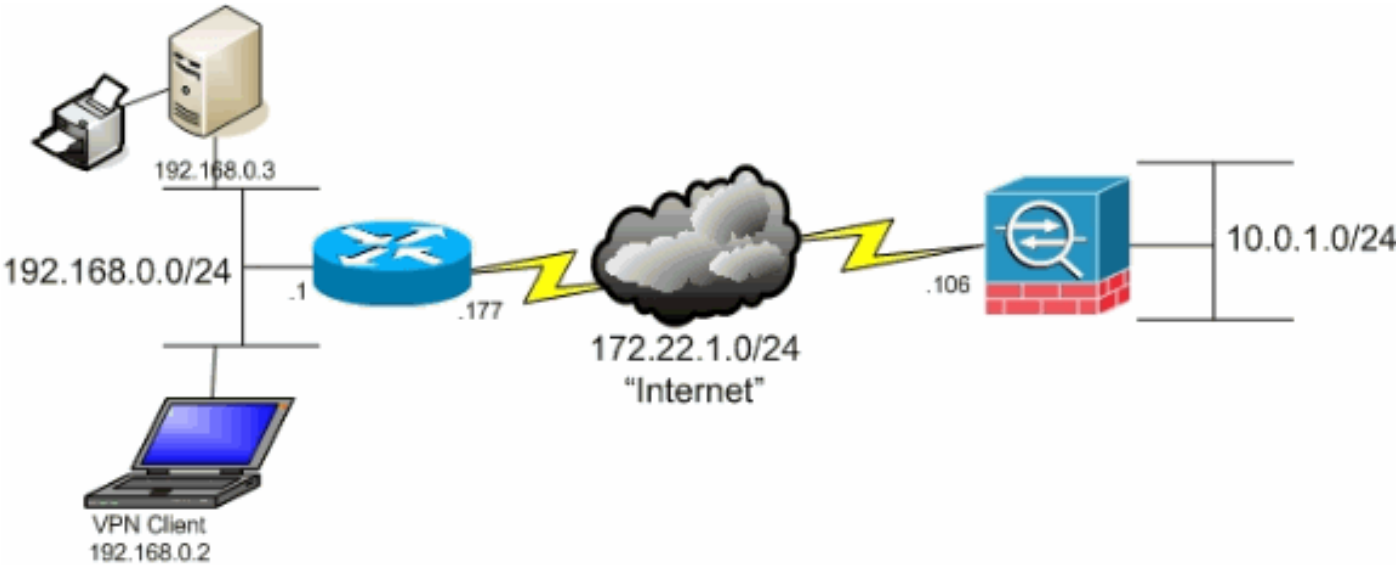


> 注：このドキュメントには、Cisco VPN Client 3.xと互換性のあるPIX 6.x CLI設定も含まれています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

ネットワーク図

VPN Client は一般的な SOHO ネットワーク上にあり、インターネット経由で本社に接続しています。



ネットワーク図

関連製品

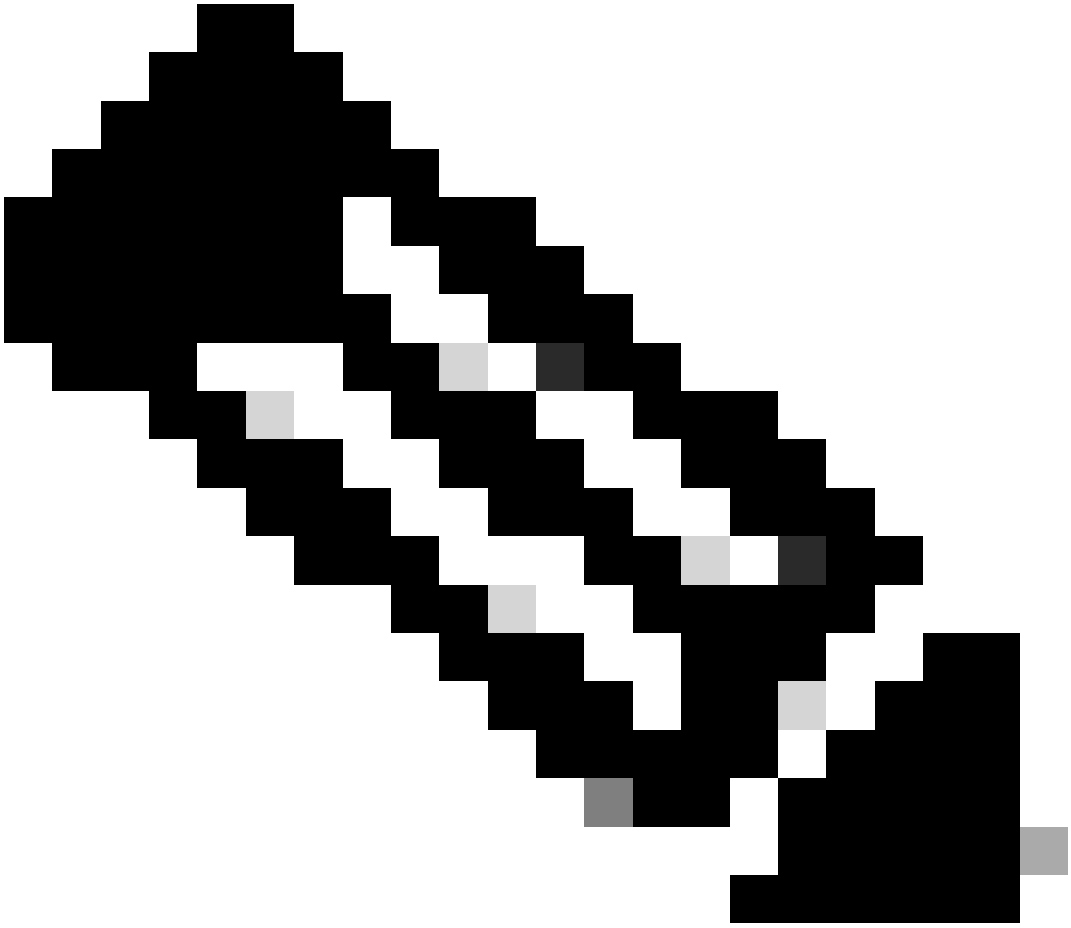
この設定は、Cisco PIX 500 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 7.x にも使用できます。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

このドキュメントでは、VPN Client が Cisco 適応型セキュリティ アプライアンス（ASA）5500 シリーズ セキュリティ アプライアンスにトンネリングされている間に、それにインターネットへのアクセスを許可する方法のステップごとの説明を提供します。この設定により、VPN Client は IPSec を使用した企業リソースへのセキュアなアクセスと、セキュリティ保護されていないインターネット アクセスの両方を実現できます。



注：フルトンネリングでは、インターネットと社内LANの両方へのデバイスアクセスが同時にイネーブルにされないため、最も安全な設定と見なされます。フル トンネリングとスプリット トンネリングの折衷案として、VPN Client にローカル LAN アクセスだけを許可することができます。詳細は、『PIX/ASA 7.x:VPNクライアントでローカルLANアクセスを許可するための設定例』を参照してください。

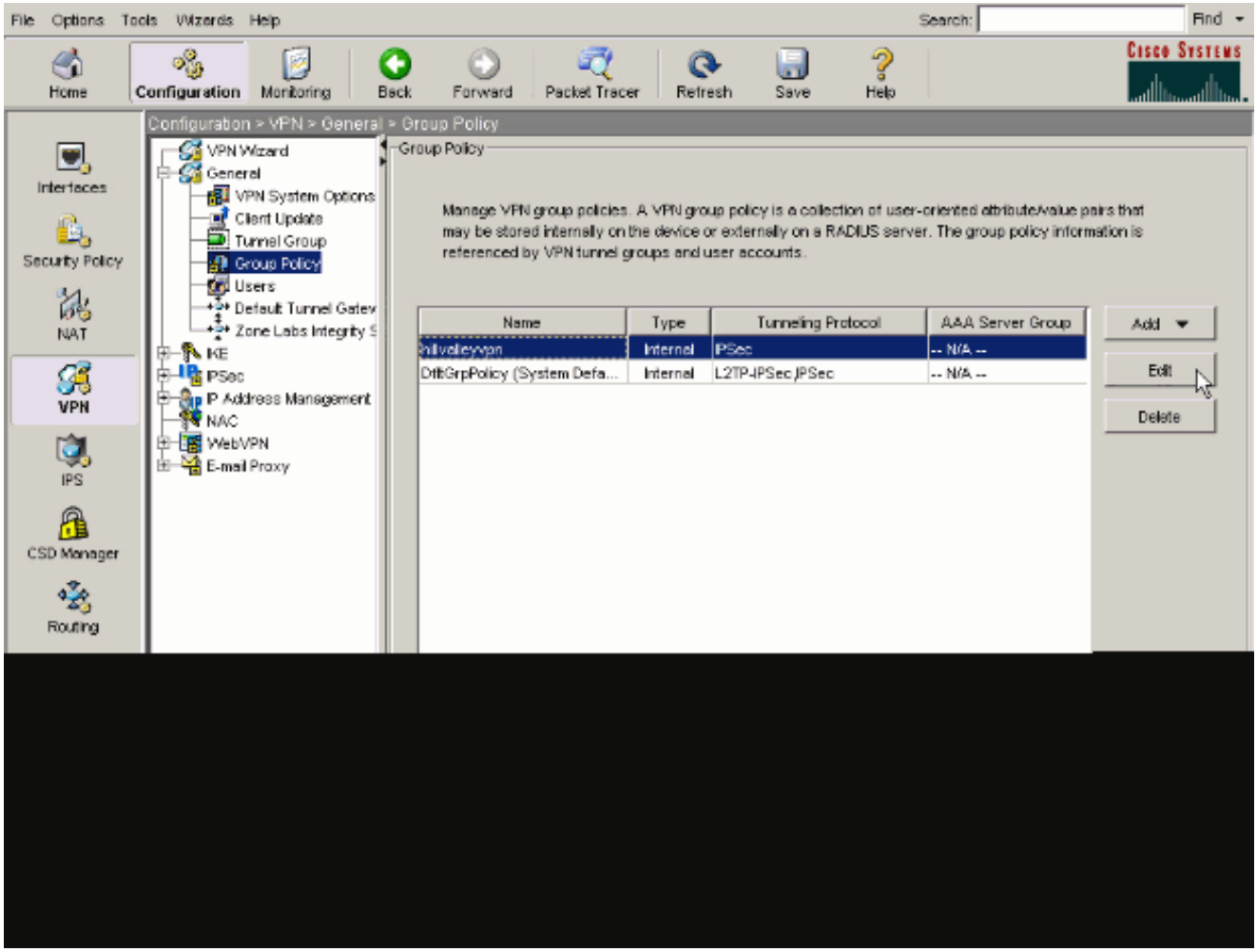
VPN Client と ASA の基本的な接続シナリオでは、宛先に関係なく、VPN Client からのすべてのトラフィックは暗号化されて ASA に送信されます。設定とサポートされるユーザ数によっては、このような設定は帯域幅を大量に消費する可能性があります。スプリット トンネリングでは、トンネル接続で、企業ネットワーク向けトラフィックの送信だけがユーザに許可されるため、この問題の軽減に役立ちます。インスタント メッセージ、電子メール、または通常の Web 閲覧など、その他すべてのトラフィックは、VPN Client のローカル LAN 経由でインターネットに送出されます。

ASA にスプリット トンネリングを設定する

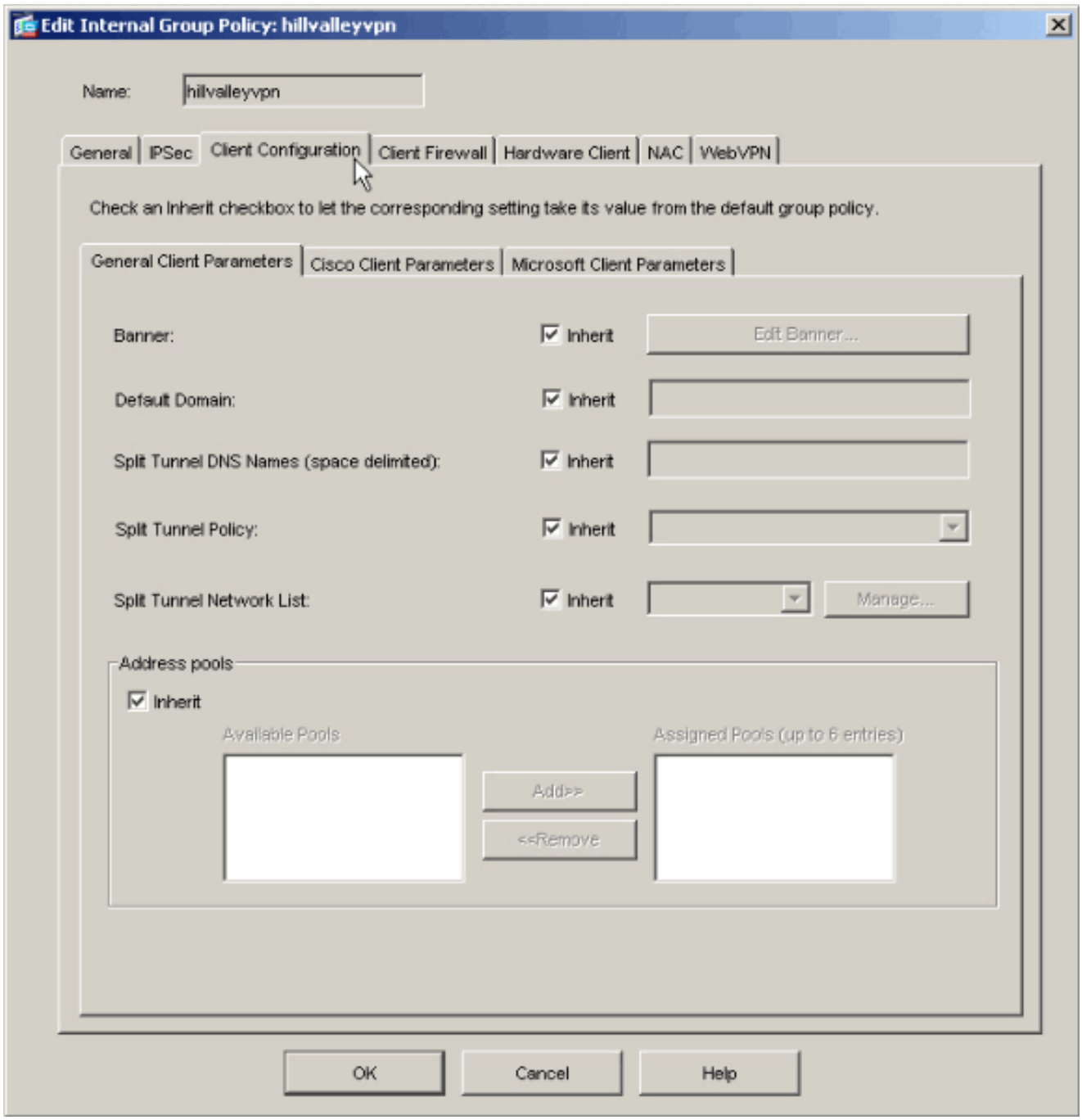
Adaptive Security Device Manager（ASDM）5.x で ASA 7.x を設定する

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。

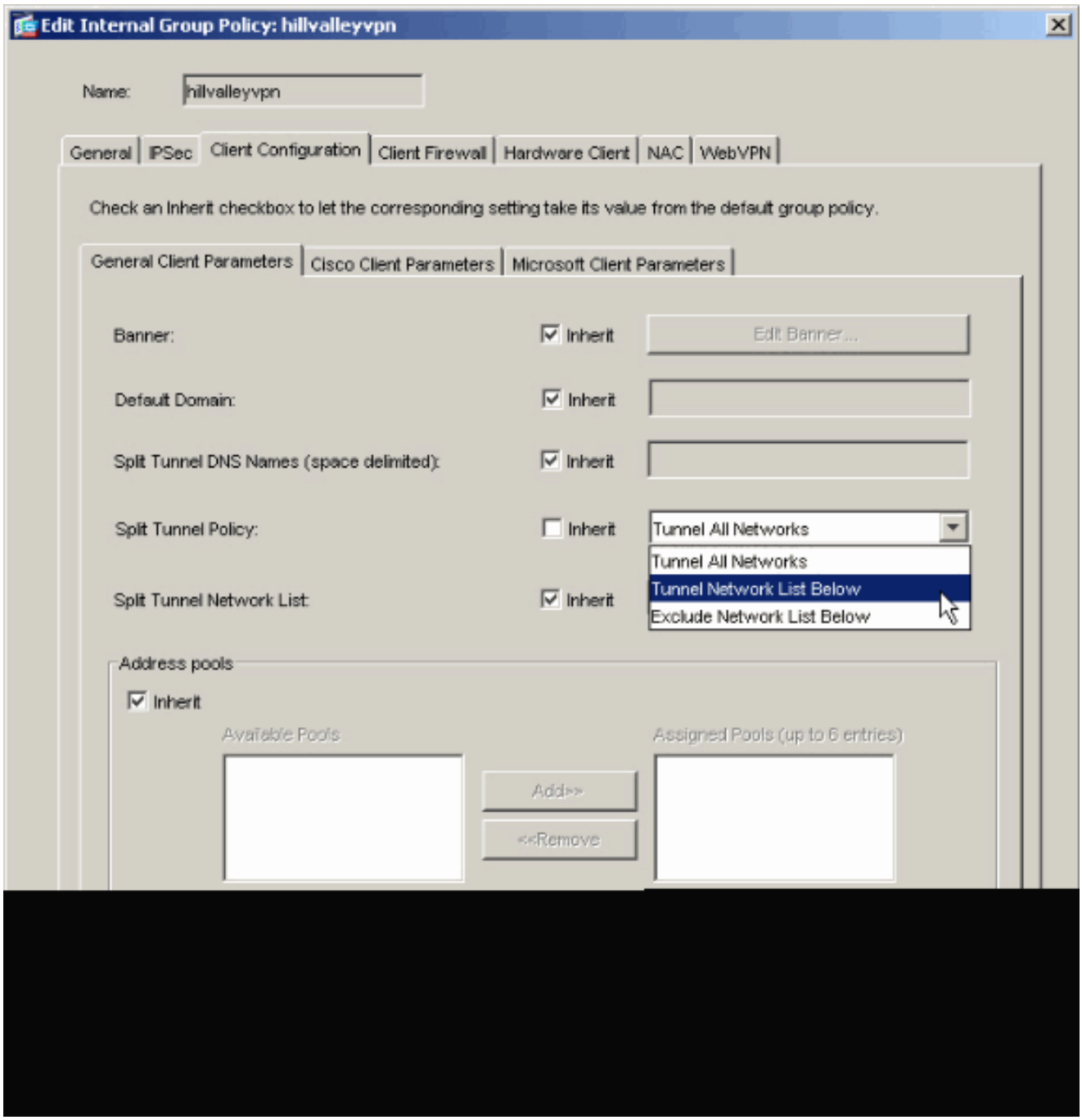
1. [Configuration] > [VPN] > [General] > [Group Policy] の順に選択し、ローカル LAN アクセスを有効にするグループ ポリシーを選択します。次に [Edit] をクリックします。



2. [Client Configuration] タブに移動します。

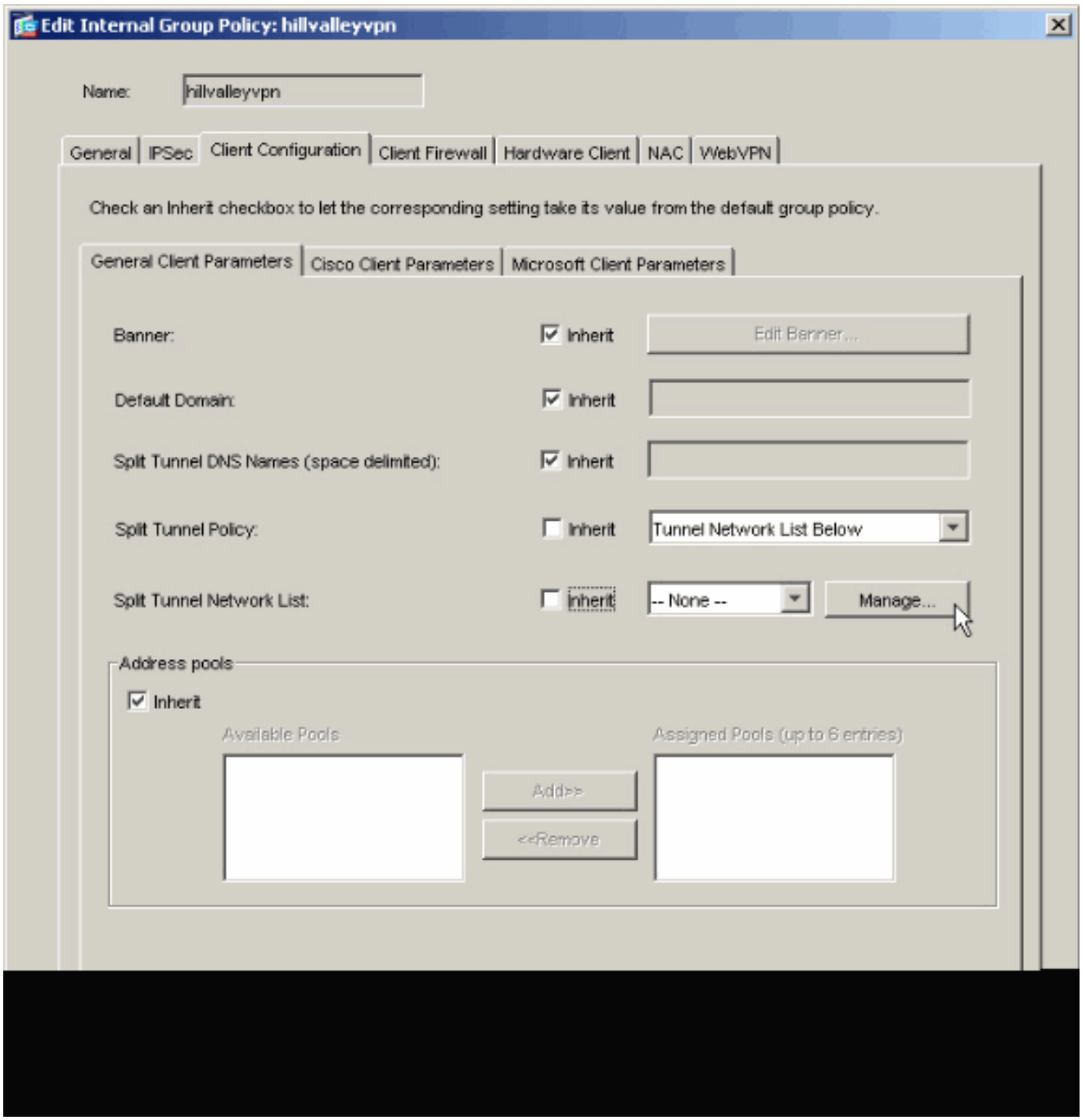


3. Split Tunnel PolicyのInheritボックスのチェックマークを外し、Tunnel Network List Belowを選択する。



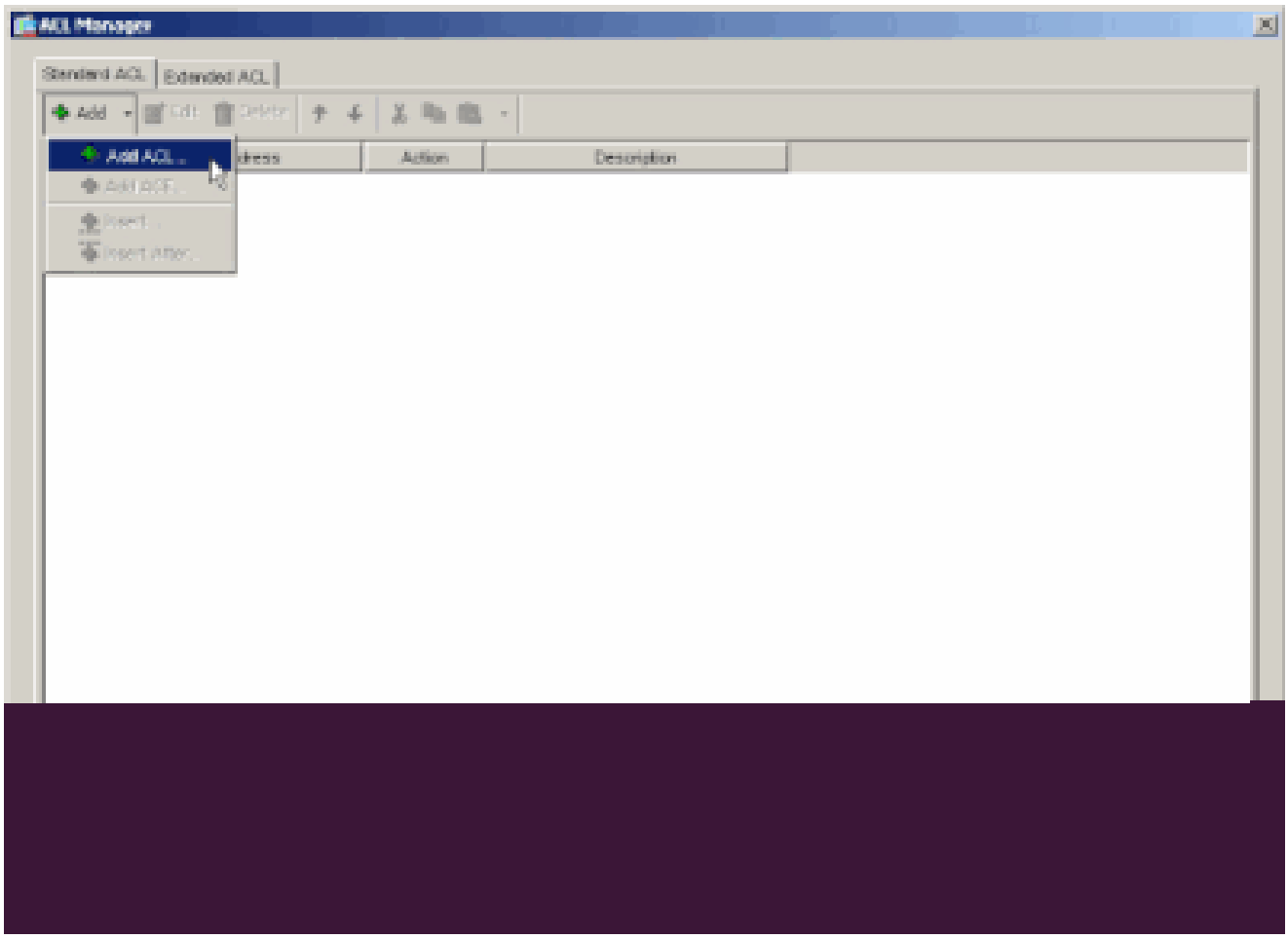
•

[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。



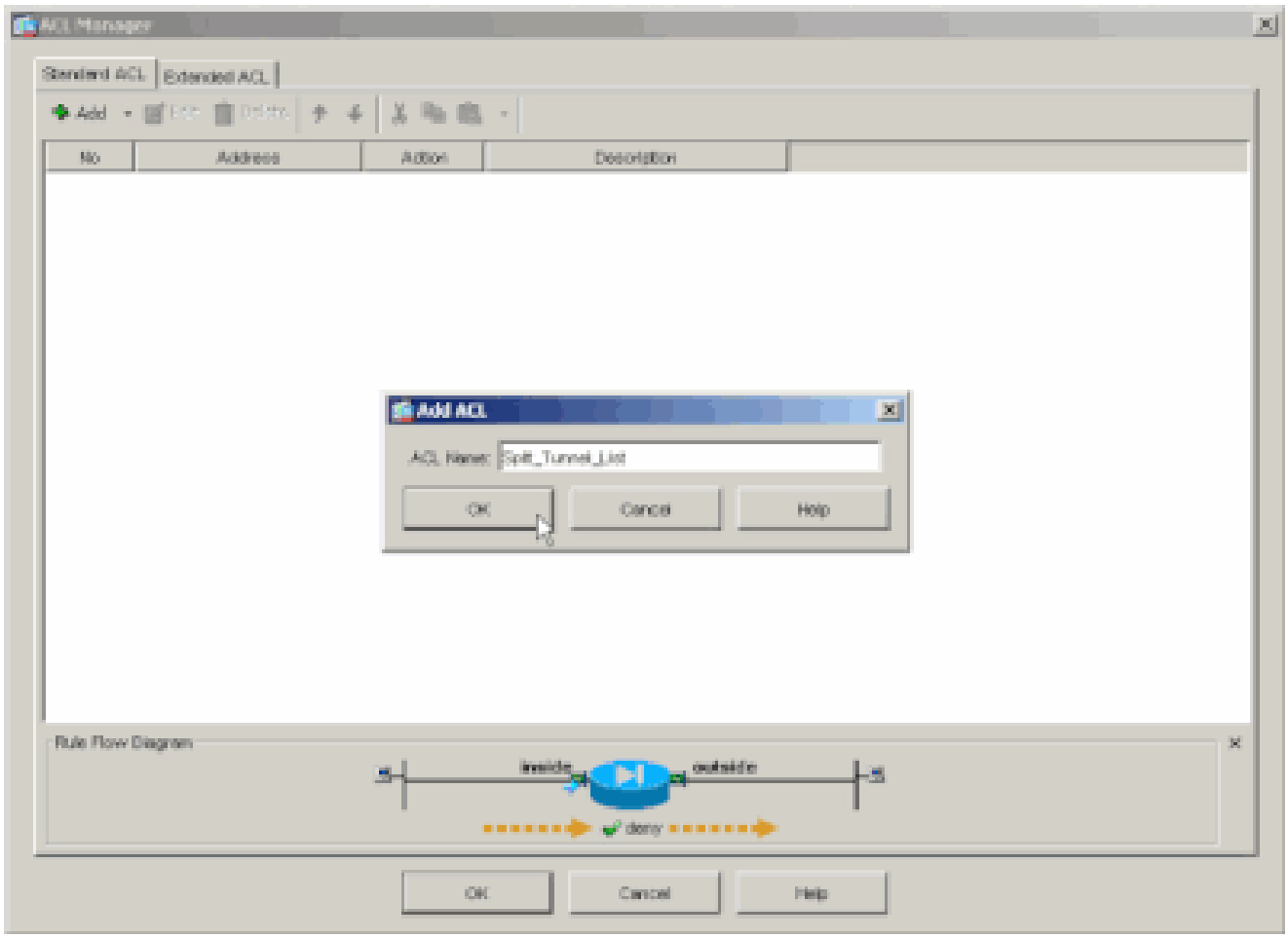
•

[ACL Manager] で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。



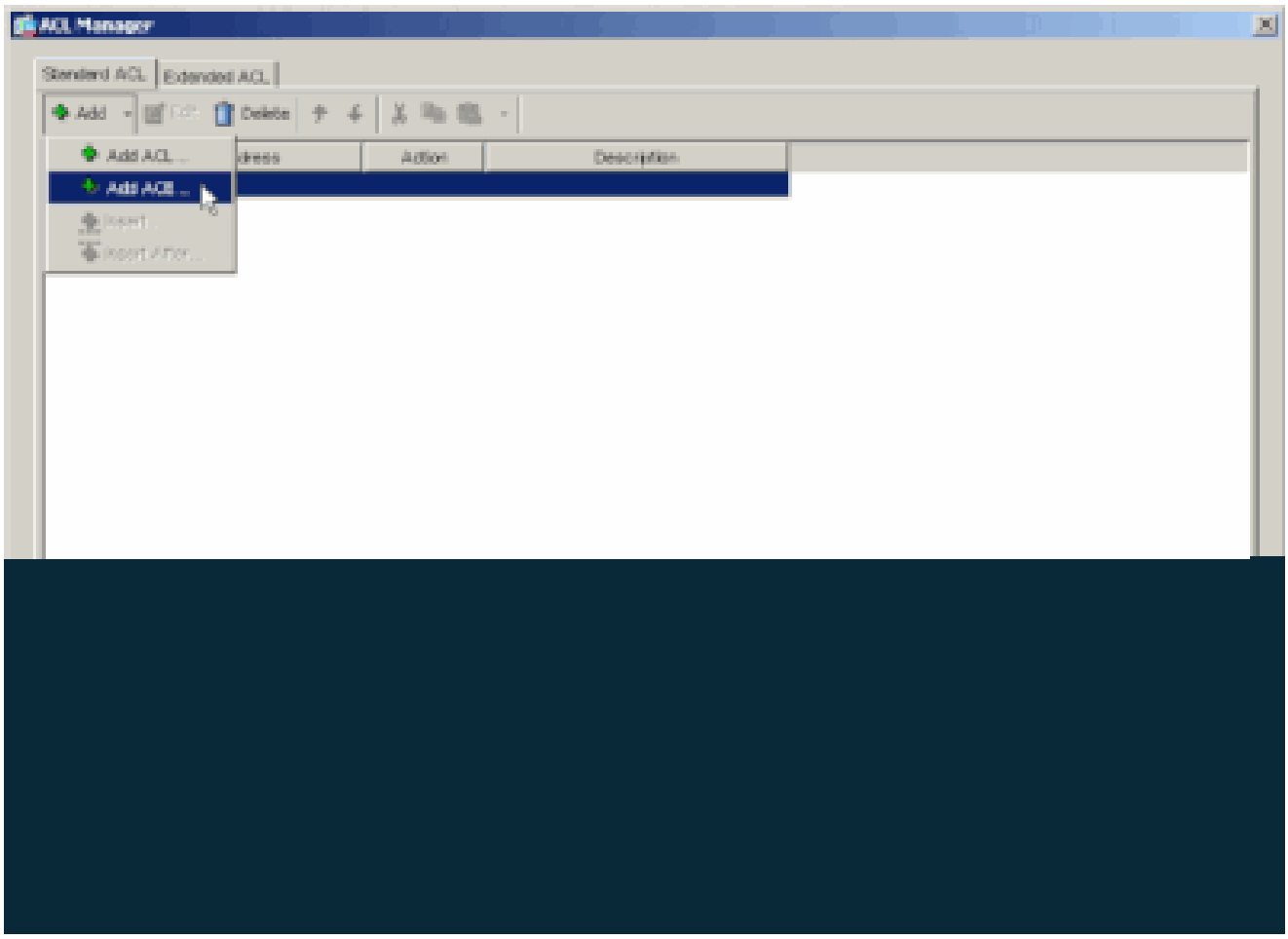
-

ACL に名前を指定して [OK] をクリックします。



-

ACLを作成したら、**Add** > **Add ACEの順に選択します。.**コマンドを入力して、アクセスコントロールエントリ(ACE)を追加します。



- ASA の背後にある LAN に対応する ACE を定義します。この場合、ネットワークは 10.0.1.0/24 です。

  a. [Permit] を選択します。

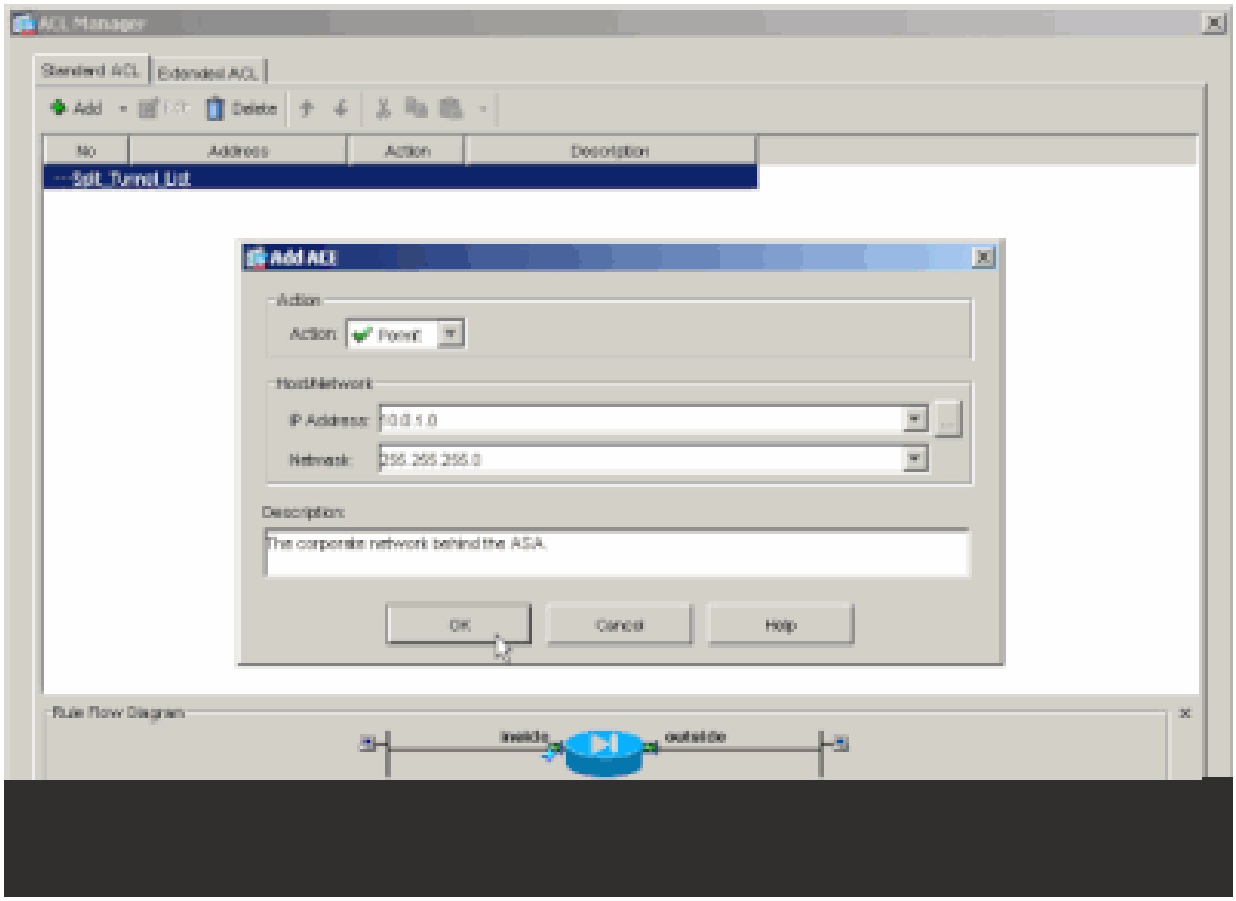
  b. [IP Address] で [10.0.1.0] を選択します。

  c. [Netmask] で [255.255.255.0] を選択します。

  d. （任意）説明を入力します。

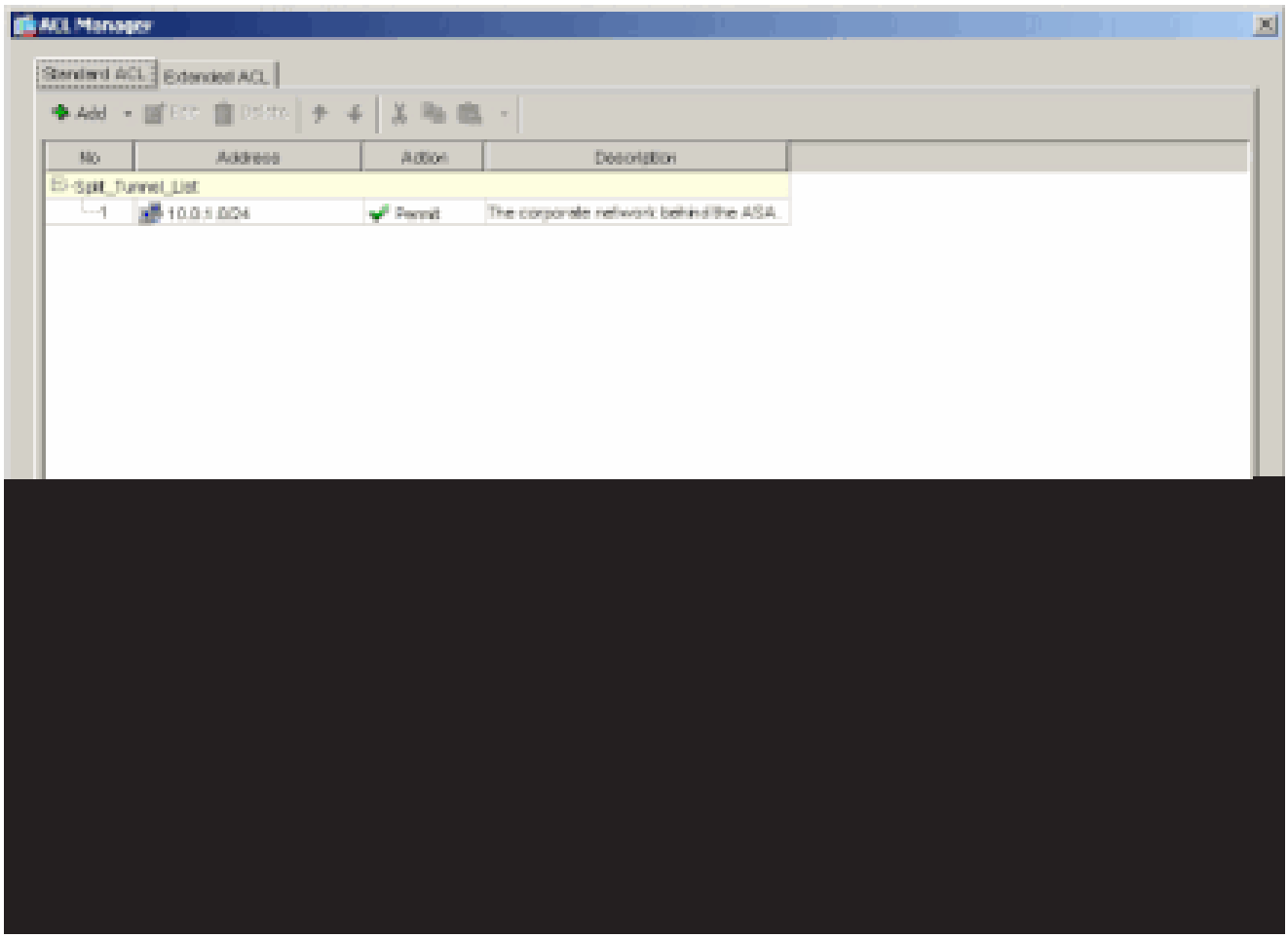
e.

> **OK**をクリックします。



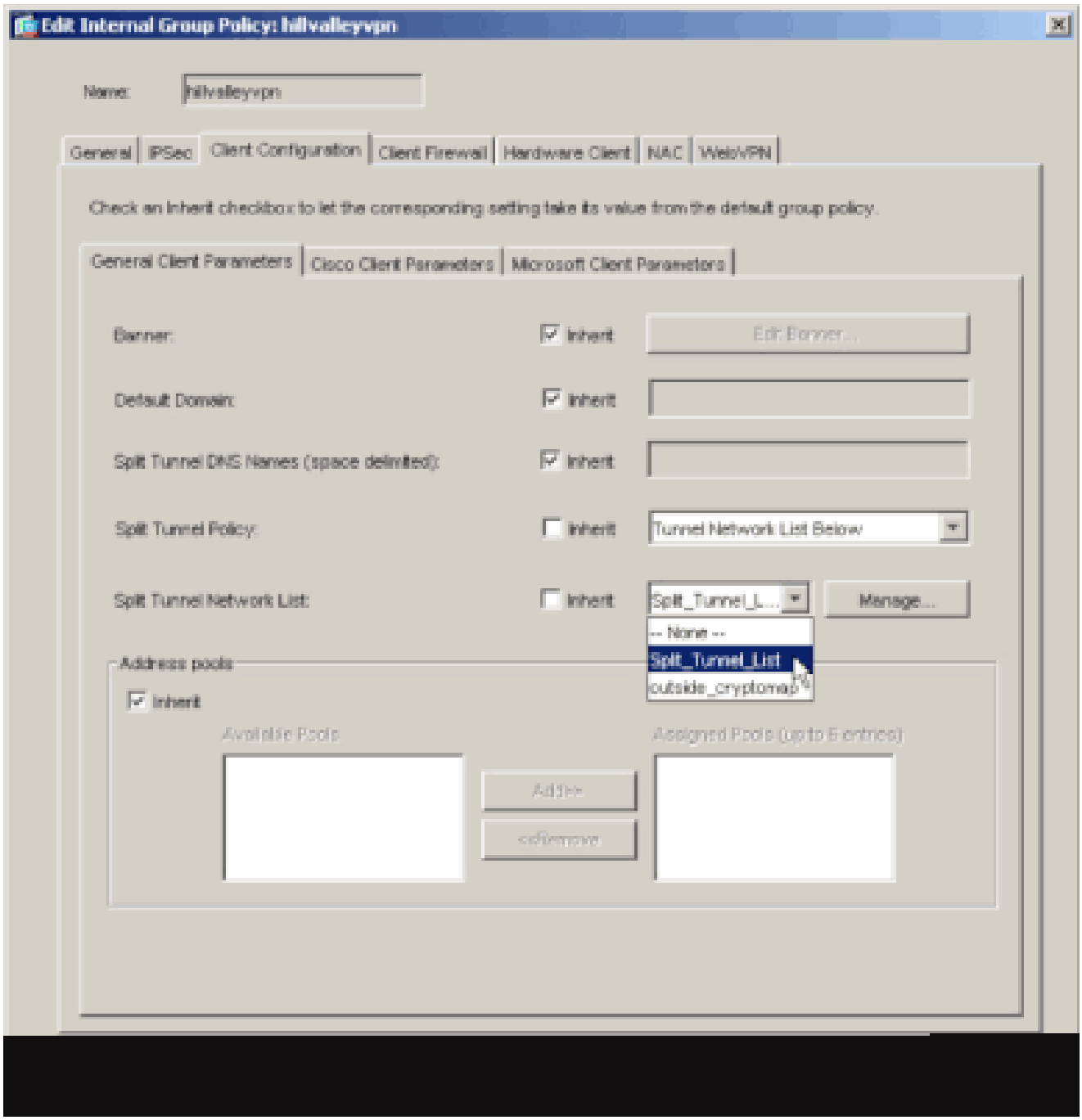
•

[OK] をクリックして [ACL Manager] を終了します。



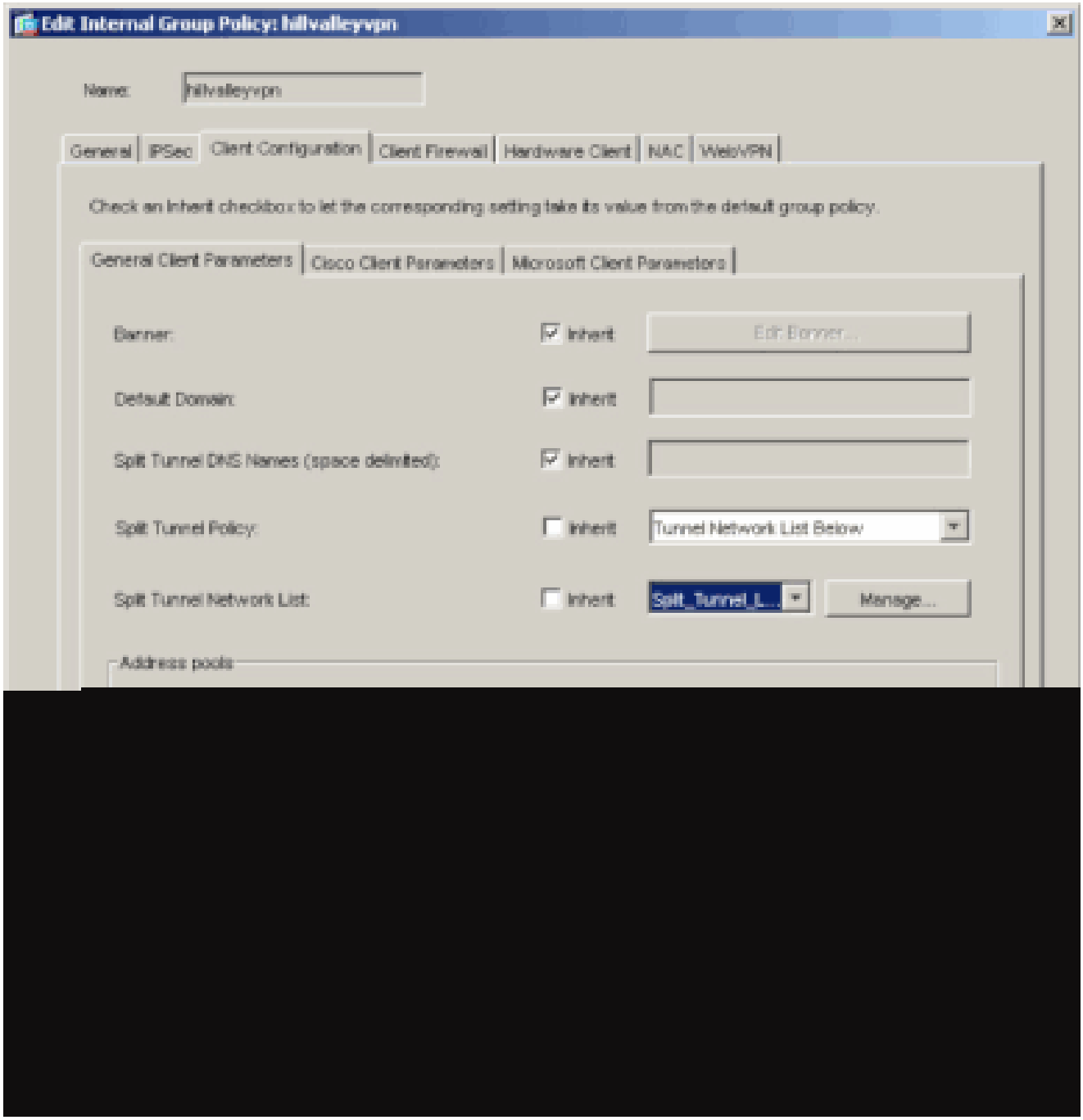
•

Split Tunnel Network List で、作成した ACL が選択されていることを確認します。



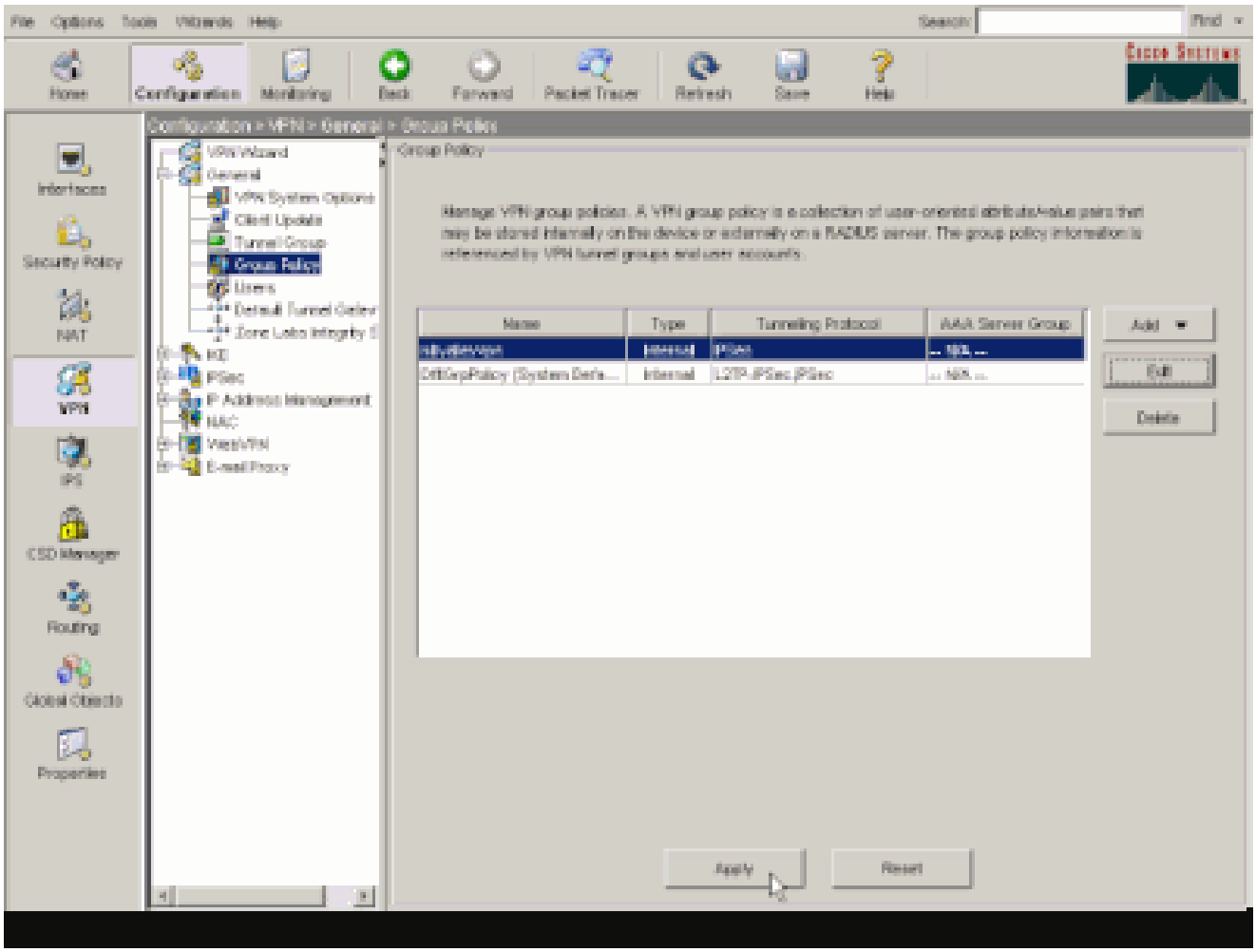
•

[OK] をクリックして、グループ ポリシー設定に戻ります。



•

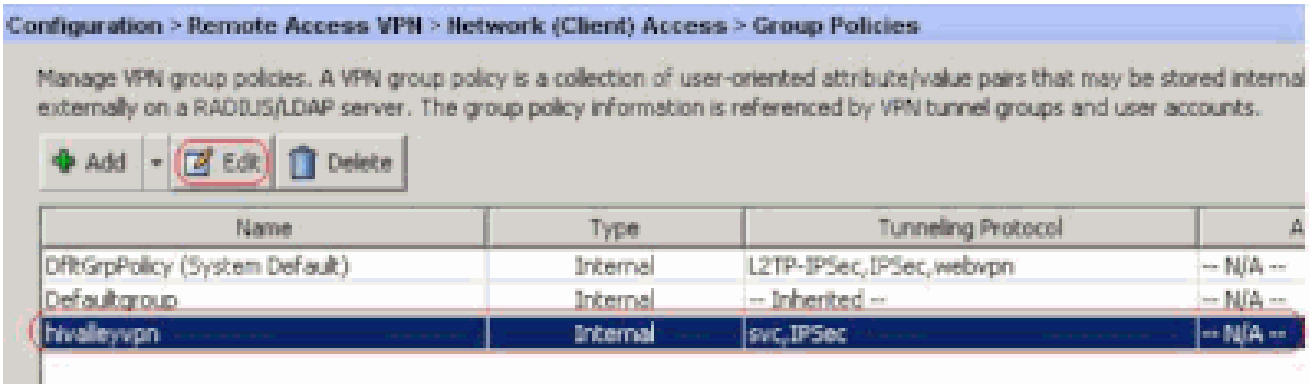
[Apply] をクリックしてから [Send]（必要な場合）をクリックして、コマンドを ASA に送信します。



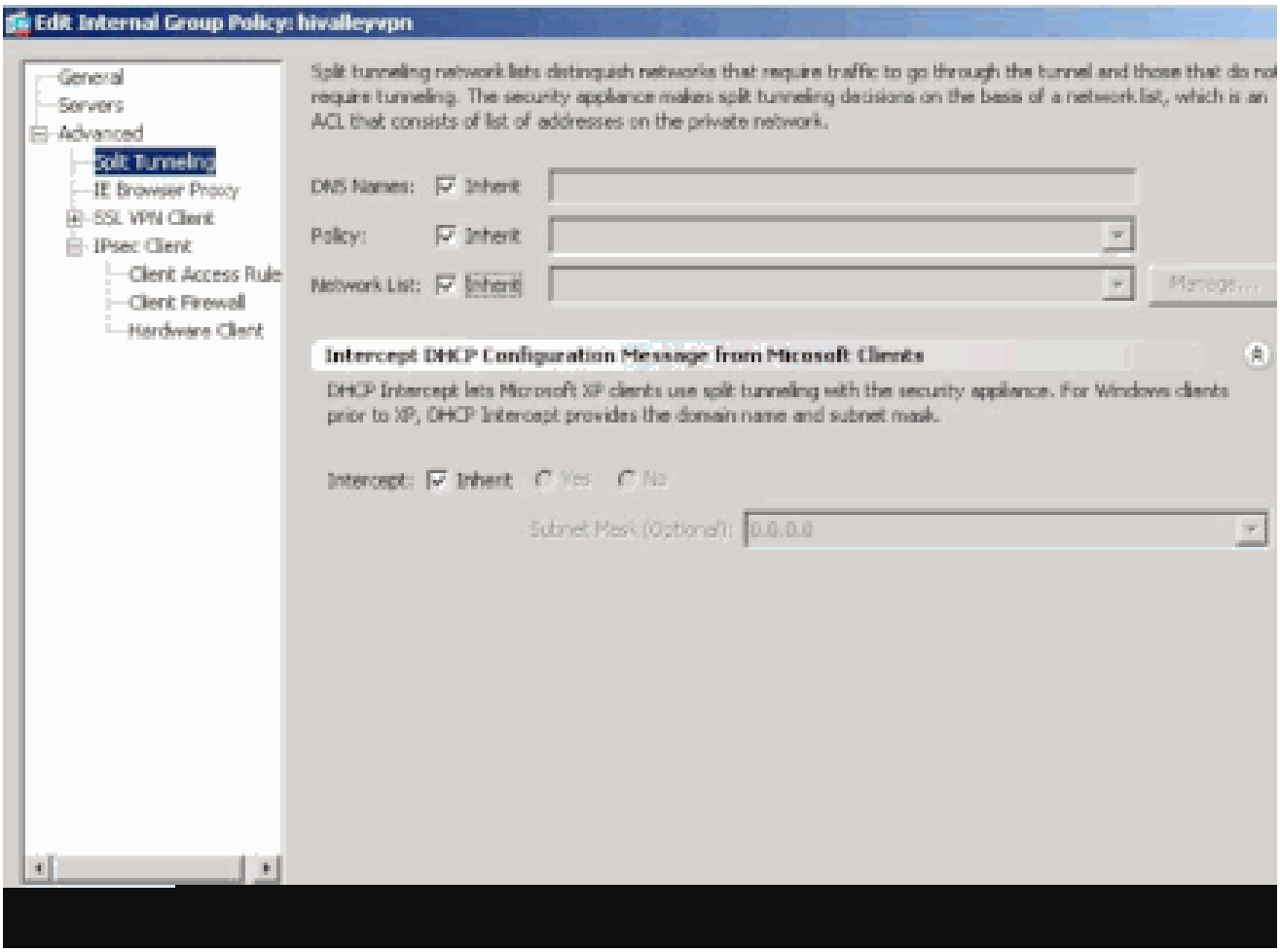
ASDM 6.xによるASA 8.xの設定

次の手順を実施して、グループのユーザにスプリット トンネリングを許可するトンネル グループを設定します。

- [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、ローカル LAN アクセスを有効にするグループ ポリシーを選択します。次に [Edit] をクリックします。

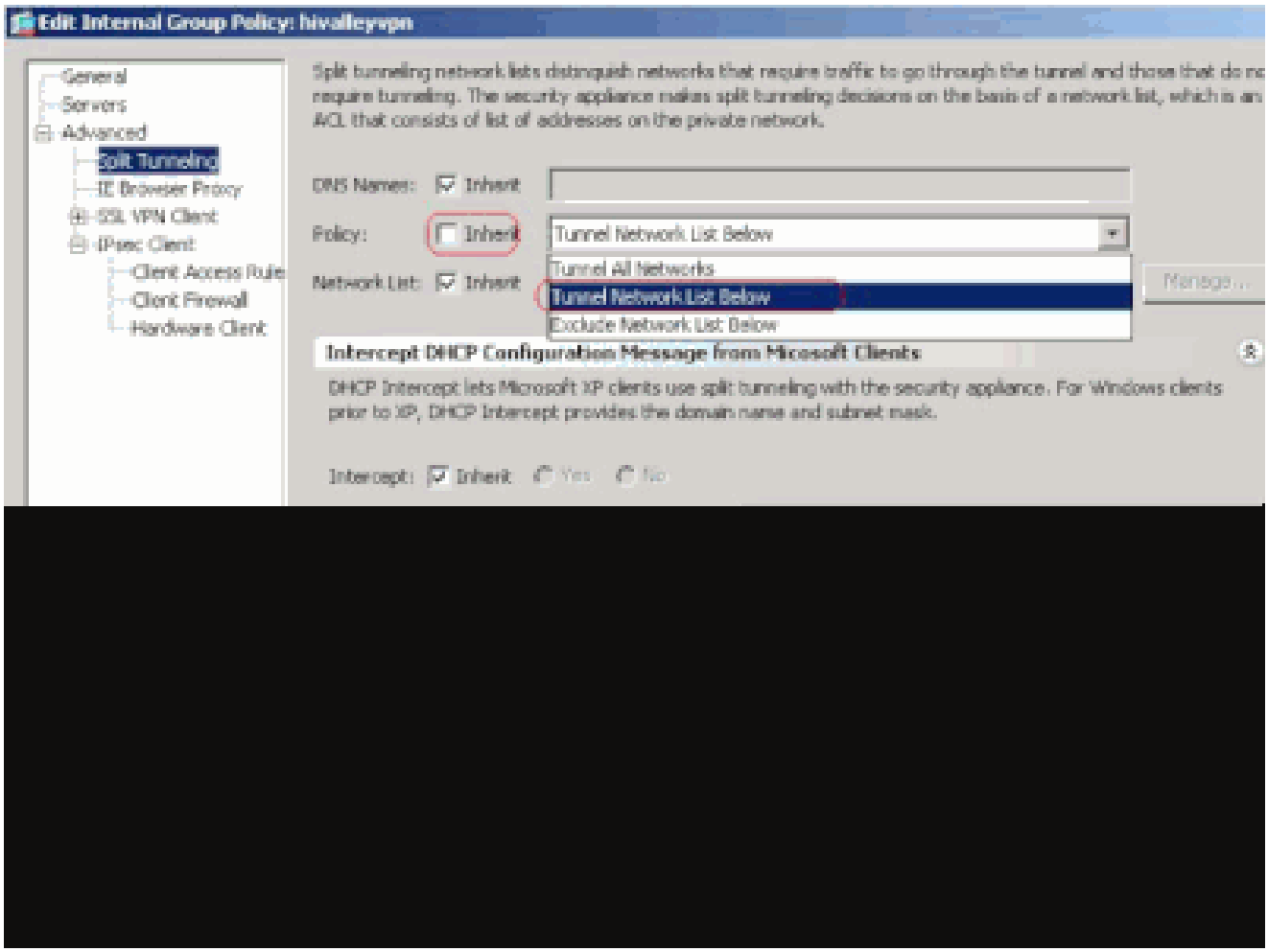


- [Split Tunneling] をクリックします。



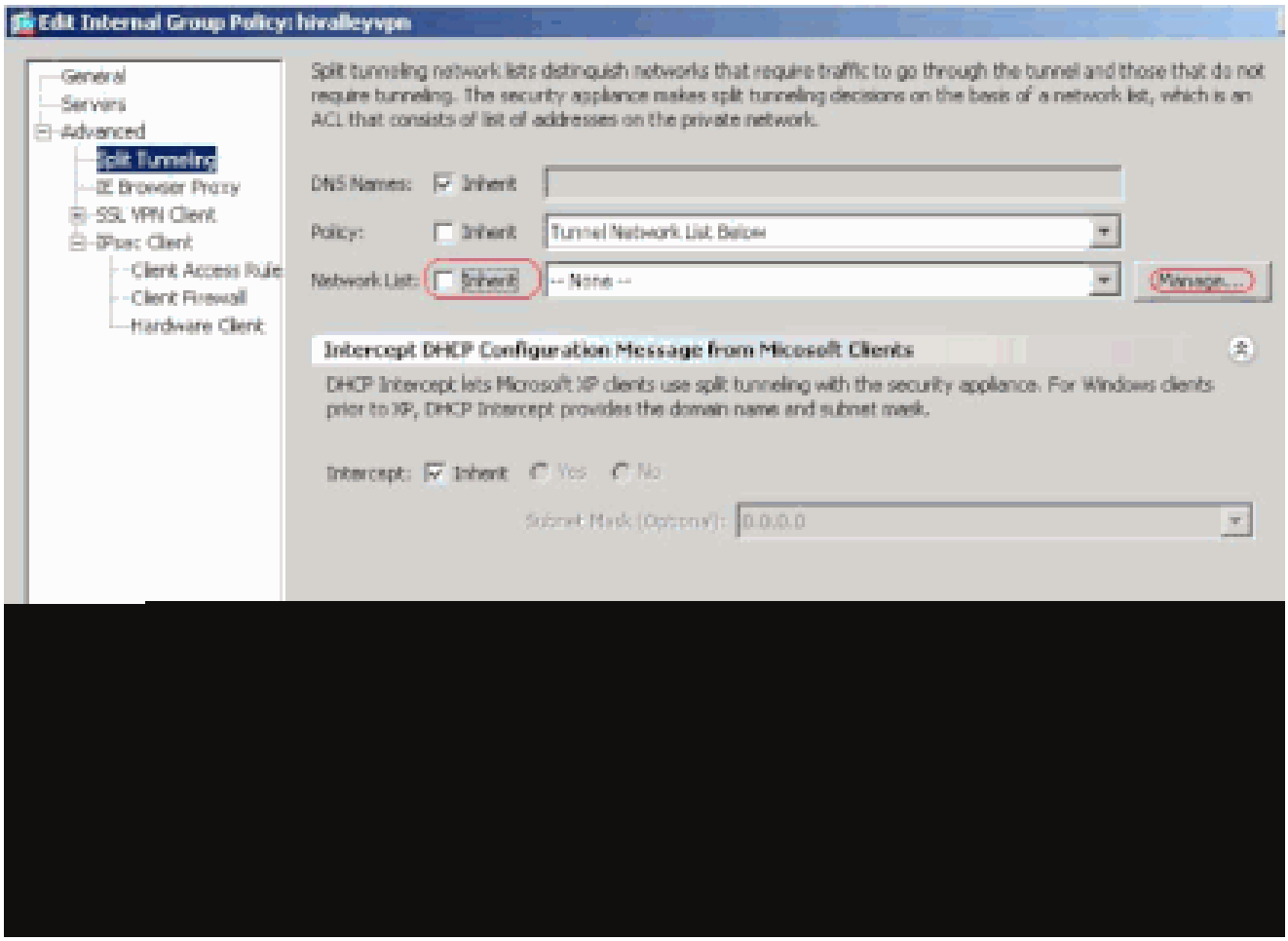
-

[Split Tunnel Policy] の [Inherit] ボックスをオフにし、[Tunnel Network List Below] を選択します。



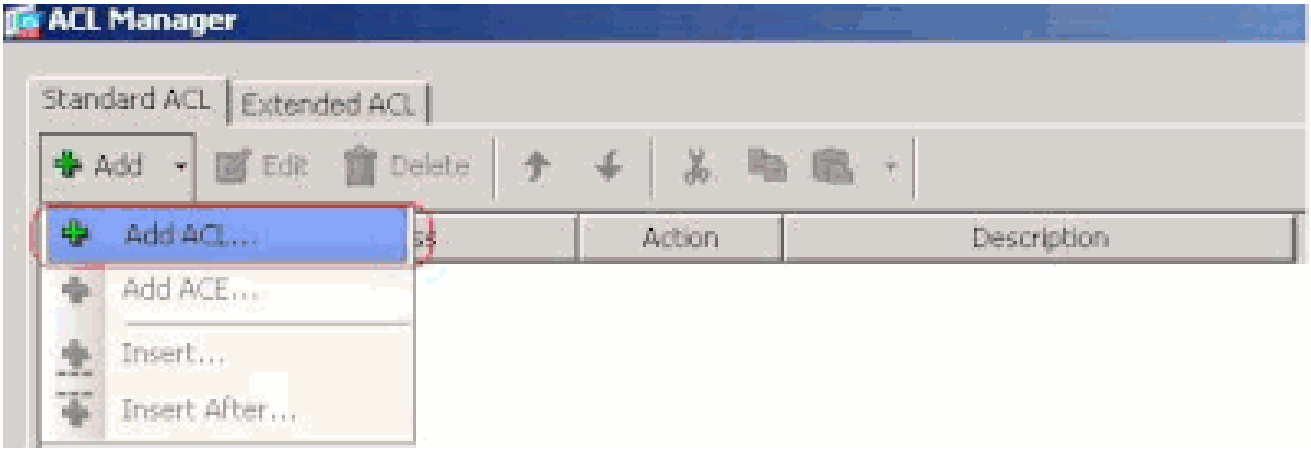
•

[Split Tunnel Network List] の [Inherit] ボックスをオフにし、[Manage] をクリックして ACL Manager を起動します。



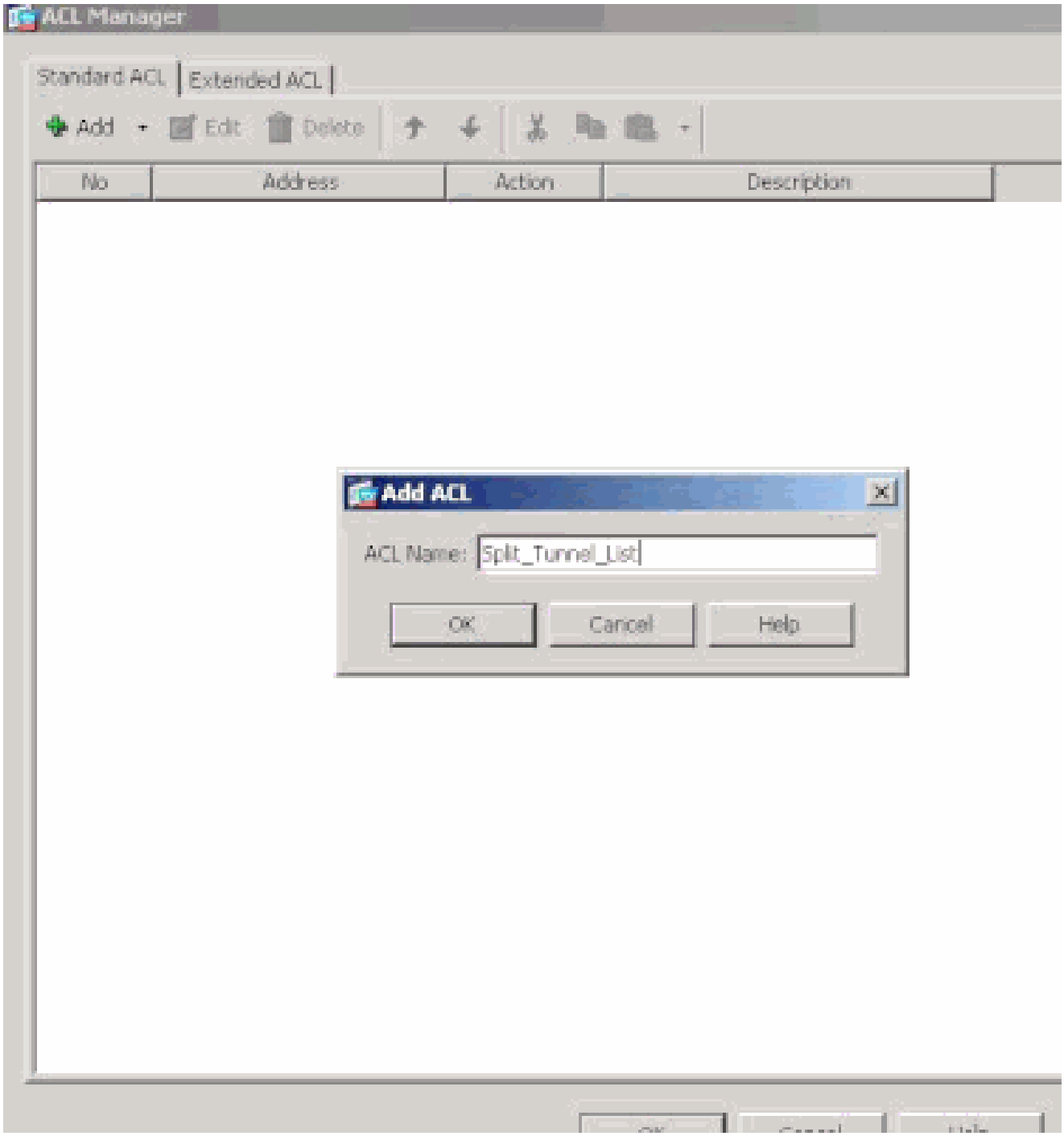
•

[ACL Manager] で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。



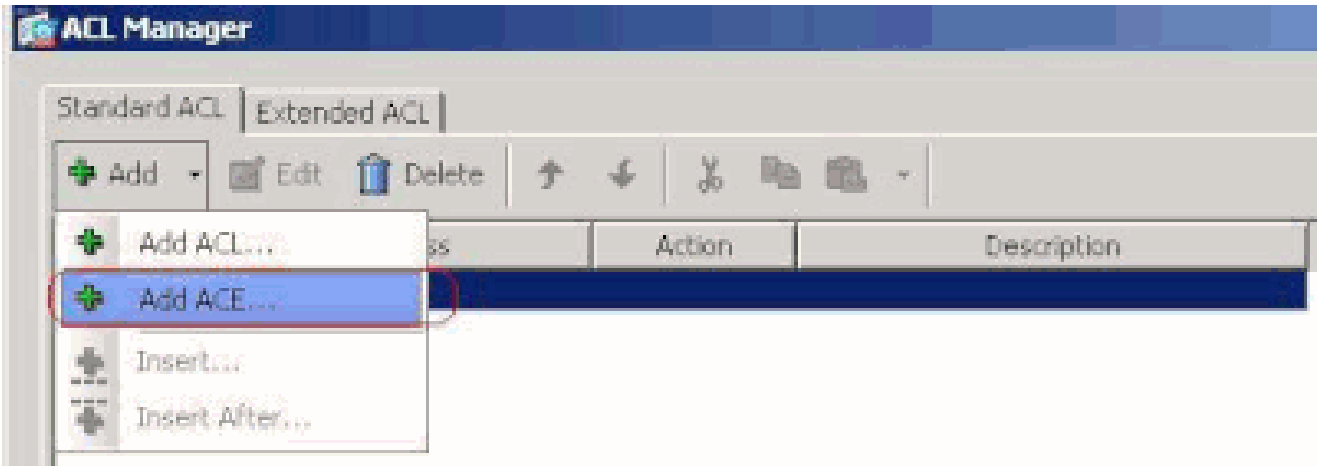
•

ACL の名前を指定して [OK] をクリックします。



-

ACL が作成された後、[Add] > [Add ACE...] を選択して、アクセス コントロール エントリ（ ACE ）を追加します。



•

ASA の背後にある LAN に対応する ACE を定義します。この場合、ネットワークは 10.0.1.0/24 です。

a.

[Permit] オプション ボタンをクリックします。

b.

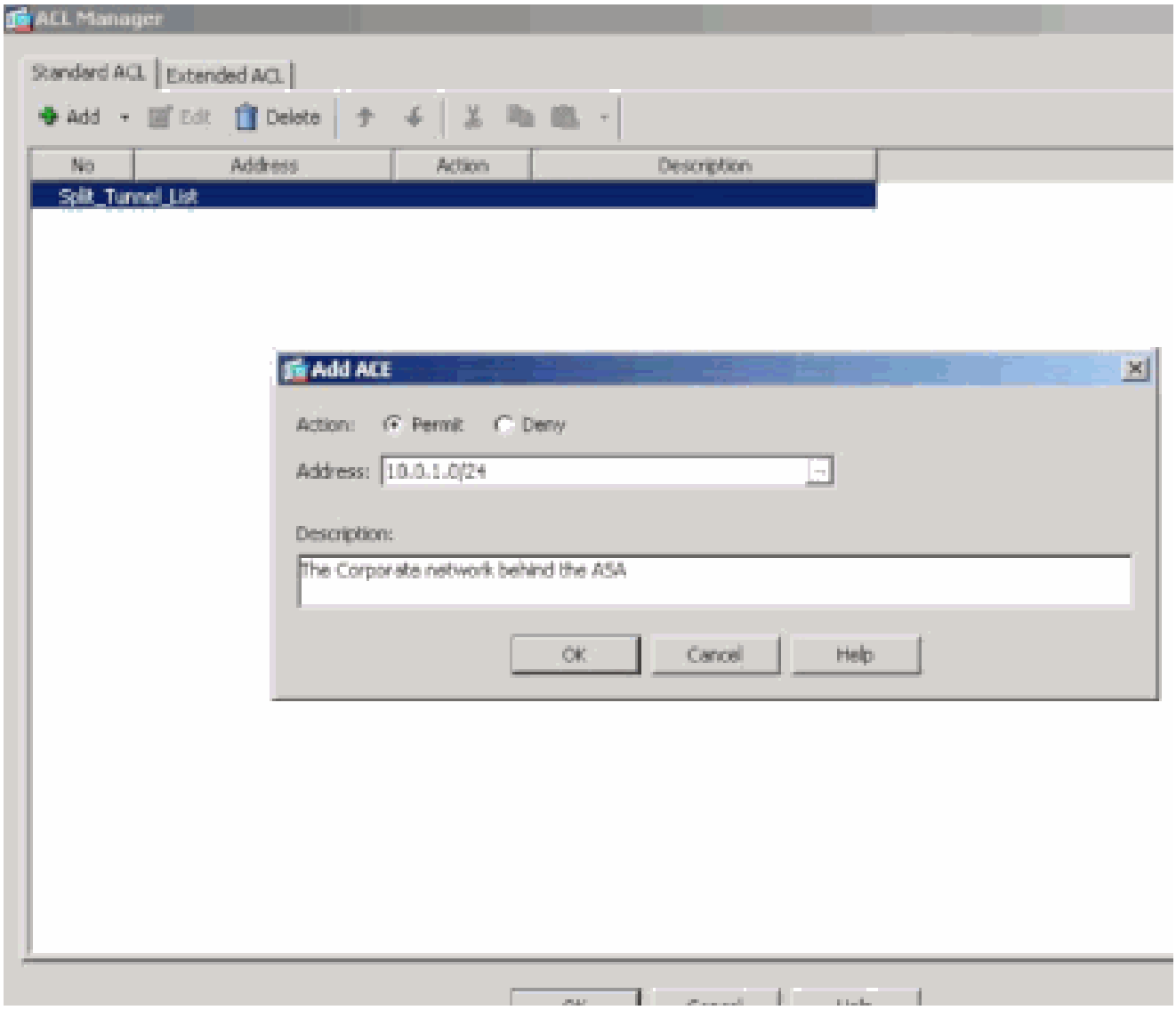
マスク 10.0.1.0/24 のネットワーク アドレスを選択します。

c.

（任意）説明を入力します。

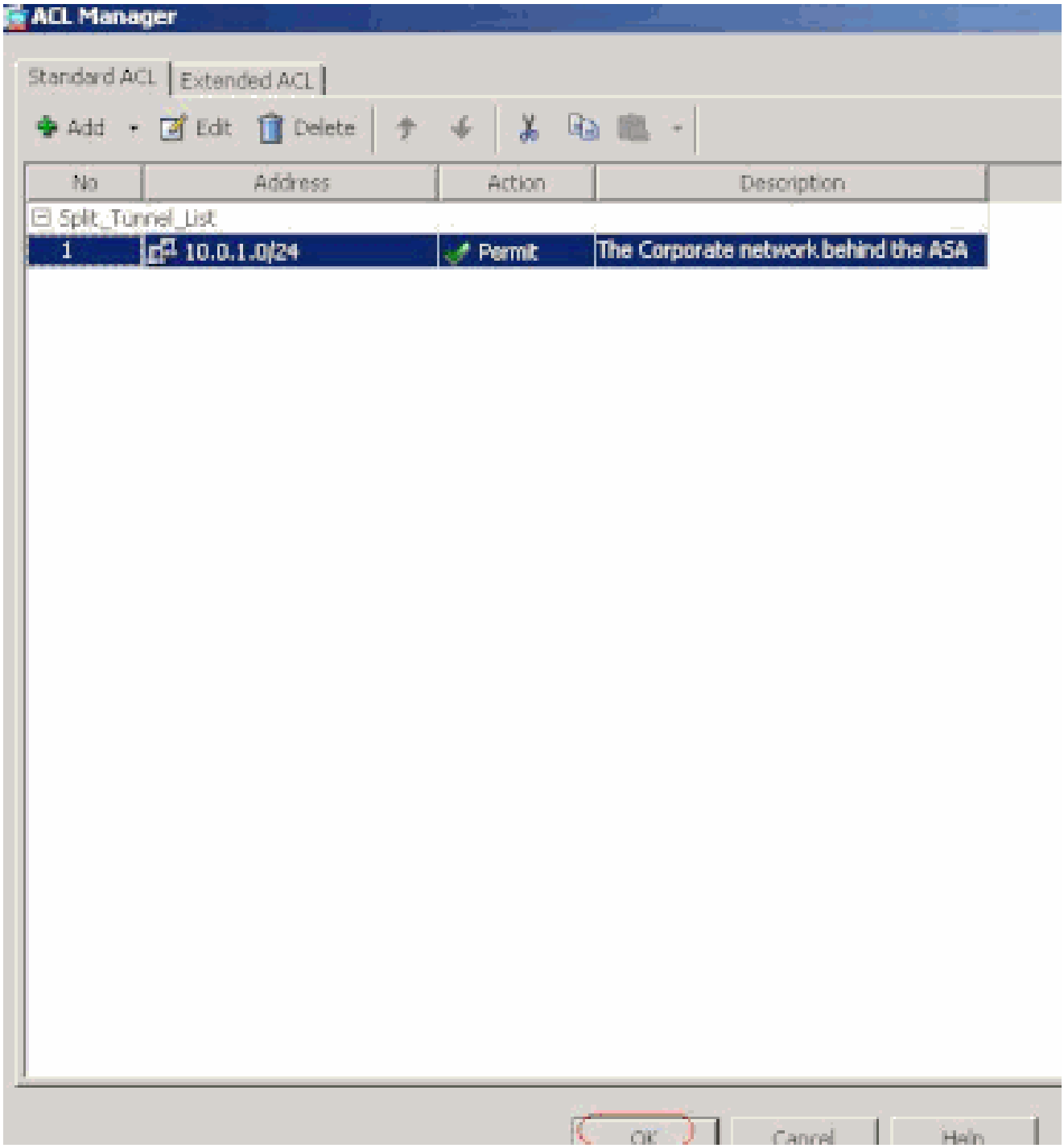
d.

[OK] をクリックします。



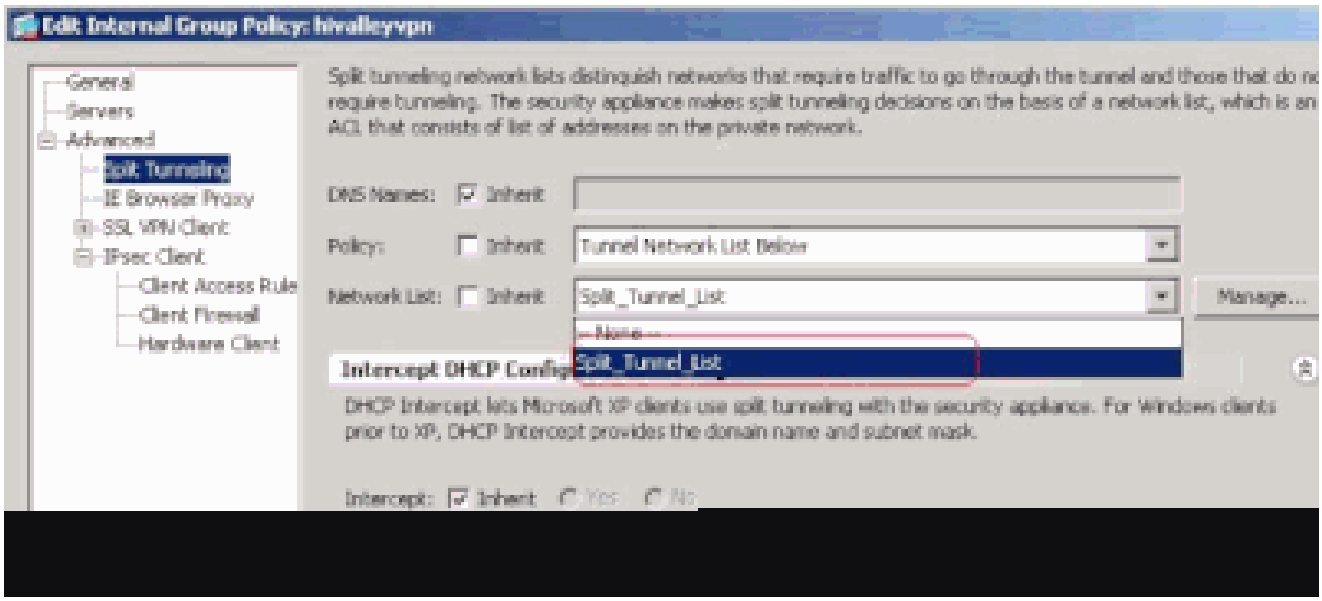
•

[OK] をクリックして [ACL Manager] を終了します。



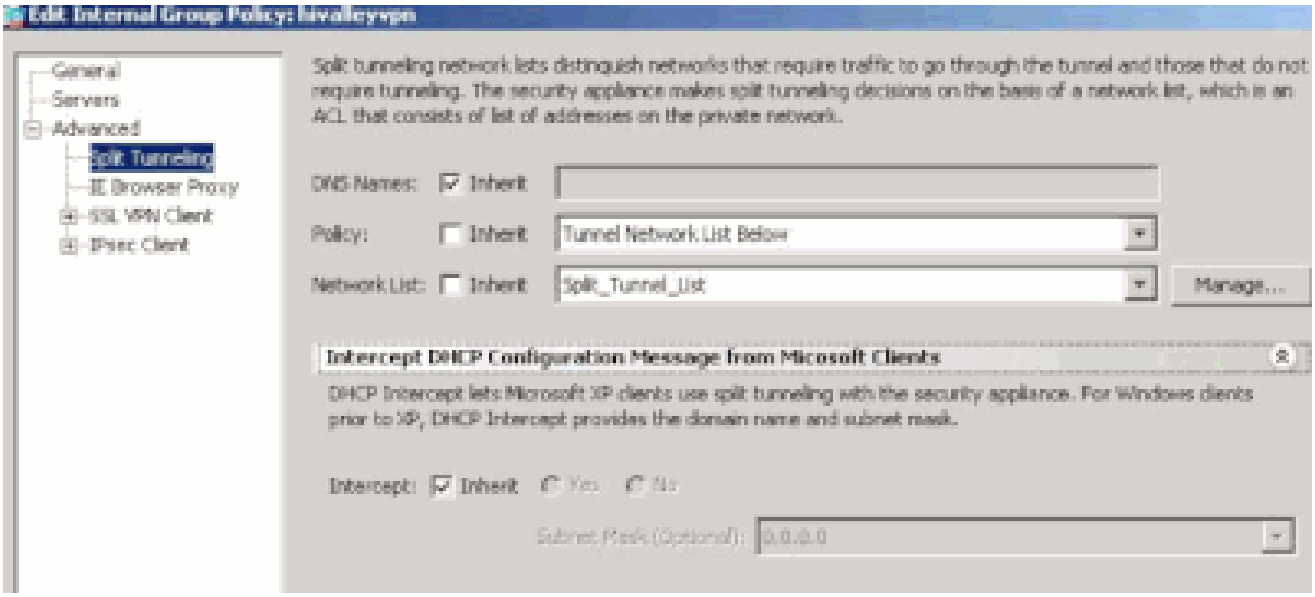
•

Split Tunnel Network List で、作成した ACL が選択されていることを確認します。



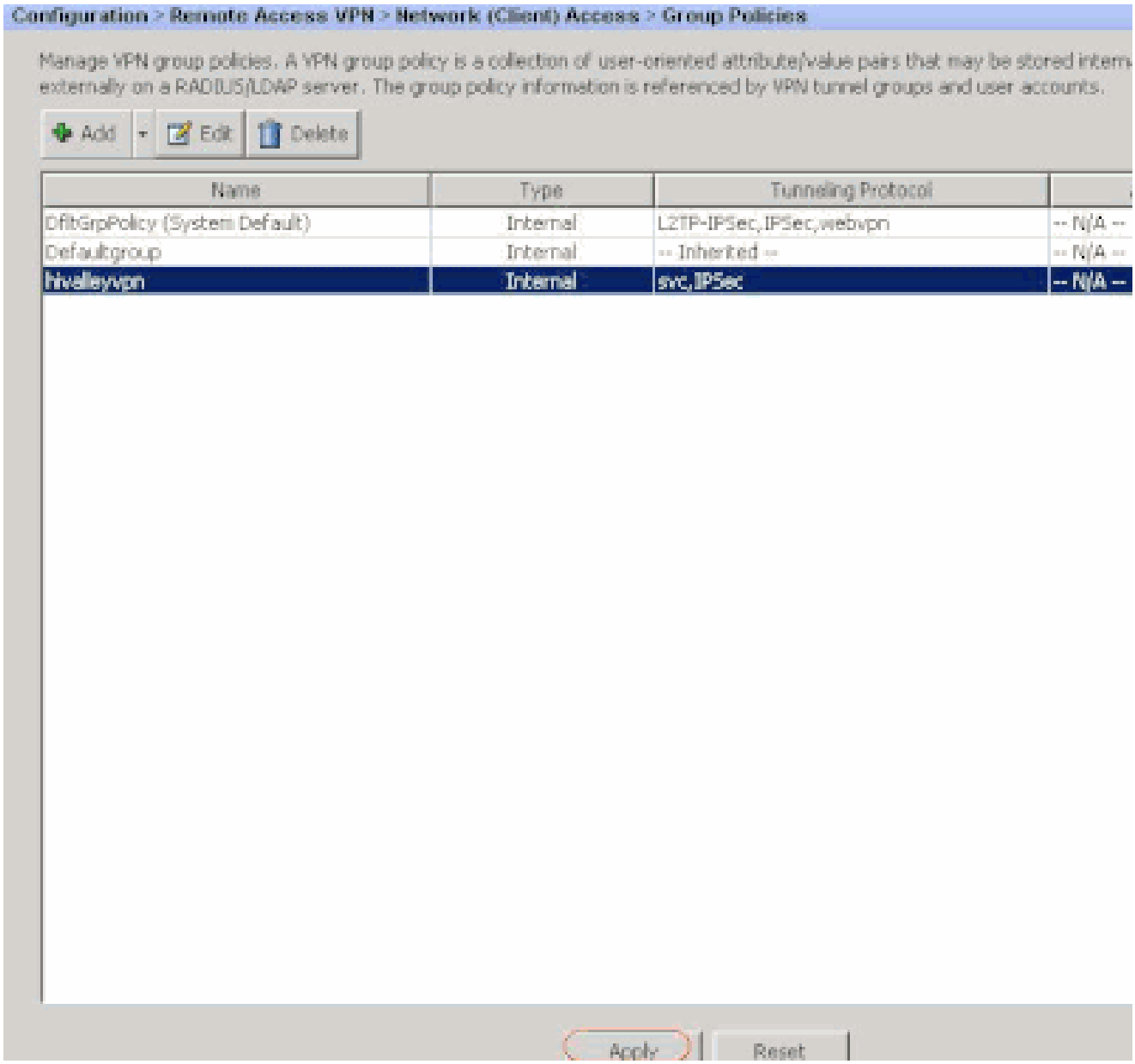
•

[OK] をクリックして、グループ ポリシー設定に戻ります。



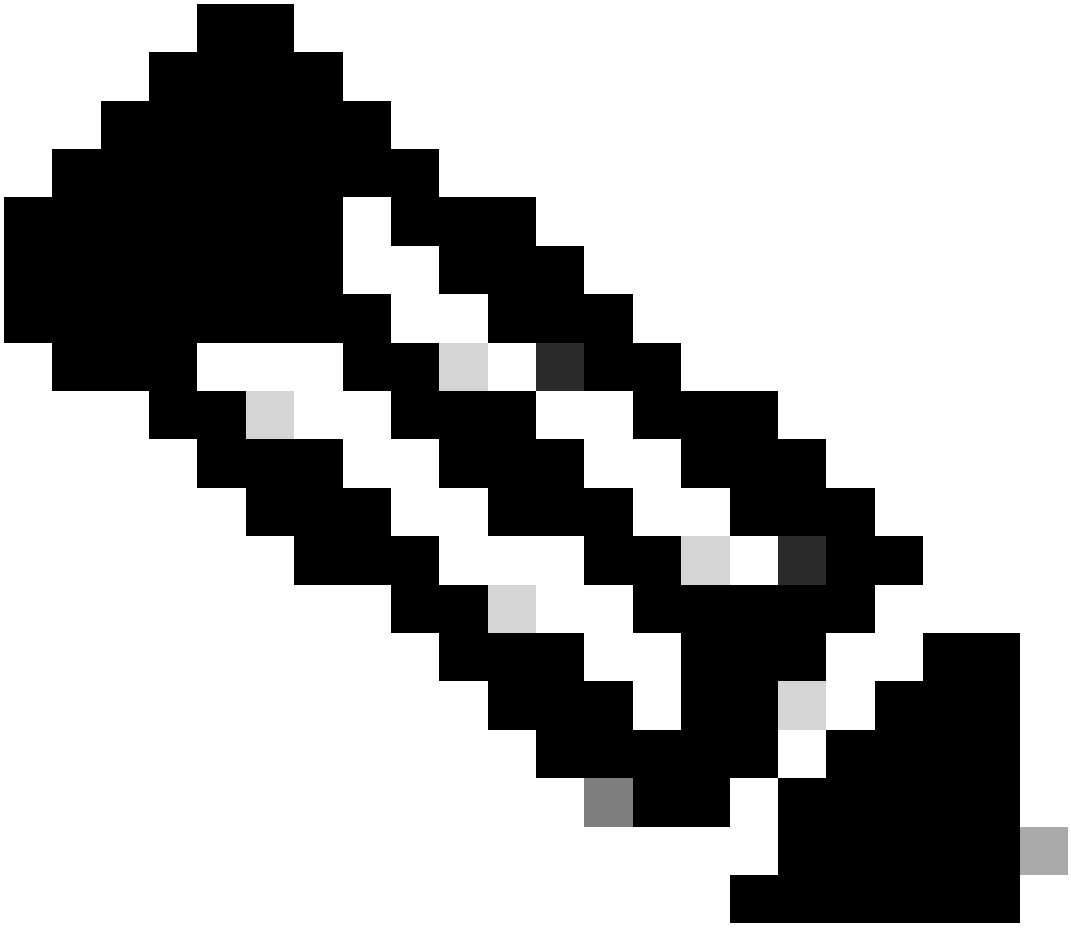
•

[Apply] をクリックしてから [Send]（必要な場合）をクリックして、コマンドを ASA に送信します。



CLI で ASA 7.x 以降を設定する

ASDM を使用する代わりに、ASA CLI で次の手順を実行して、ASA のスプリット トンネリングを許可することもできます。



注:CLIスプリットトンネリングの設定は、ASA 7.xと8.xの両方で同じです。

- コンフィギュレーション モードに切り替えます。

```
<#root>

ciscoasa>
```

```
enable


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


configure terminal


ciscoasa(config)#
```

- ASA の背後にあるネットワークを定義するアクセス リストを作成します。

```
    <#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
```

- 修正するポリシーのグループ ポリシー コンフィギュレーション モードに入ります。

```
    <#root>
```

```
ciscoasa(config)#
```

```
 group-policy hillvalleyvpn attributes
```

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

- スプリット トンネル ポリシーを指定します。この例では、ポリシーは tunnelspecified です。

```
    <#root>

ciscoasa(config-group-policy)#

 split-tunnel-policy tunnelspecified
```

- スプリット トンネル アクセス リストを指定します。この例では、リストは Split_Tunnel_List です。

```
    <#root>

ciscoasa(config-group-policy)#

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

- 次のコマンドを実行します。

<#root>

ciscoasa(config)#

tunnel-group hillvalleyvpn general-attributes

- グループ ポリシーとトンネル グループを関連付けます。

<#root>

ciscoasa(config-tunnel-ipsec)#

default-group-policy hillvalleyvpn

- 2 つのコンフィギュレーション モードを終了します。

<#root>

ciscoasa(config-group-policy)#

exit

ciscoasa(config)#

```
exit
```

```
ciscoasa#
```

- この設定を不揮発性 RAM（NVRAM）に保存して、ソース ファイル名を指定するようにプロンプトが表示されたら、Enter キーを押します。

```
<#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#
```

CLI で PIX 6.x を設定する

次のステップを実行します。

- PIX の背後にあるネットワークを定義するアクセス リストを作成します。

```
<#root>
```

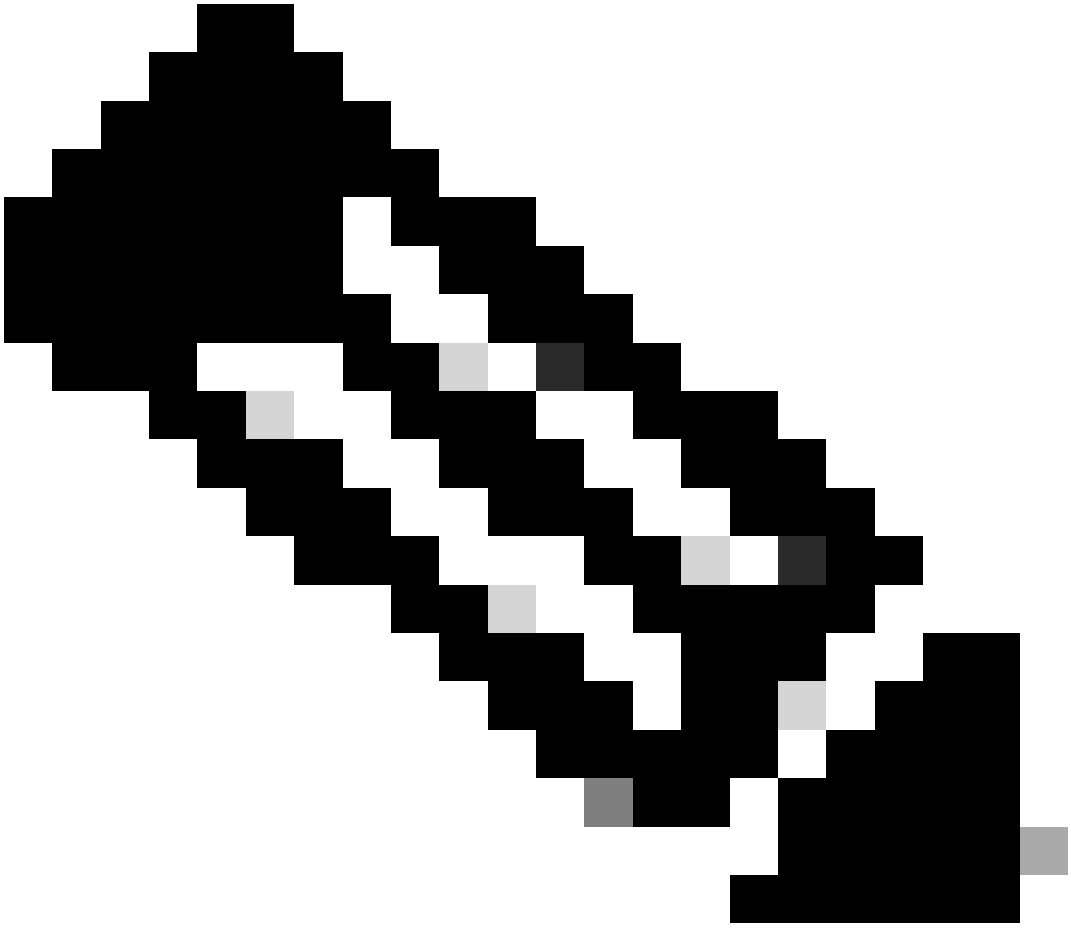
```
PIX(config)#access-list Split_Tunnel_List standard permit 10.0.1.0 255.255.255.0
```

- VPN グループ vpn3000 を作成して、次のようにスプリット トンネル ACL を指定します。

<#root>

PIX(config)#

vpngroup vpn3000 split-tunnel Split_Tunnel_List



注：PIX 6.xのリモートアクセスVPN設定の詳細は、『Cisco Secure PIX Firewall 6.xおよびCisco VPN Client 3.5 for WindowsでMicrosoft Windows 2000/2003 IAS RADIUS認証を使用するための設定』を参照してください。

確認

次に示すセクションの手順を実行して、設定を確認します。

- VPN Client で接続する

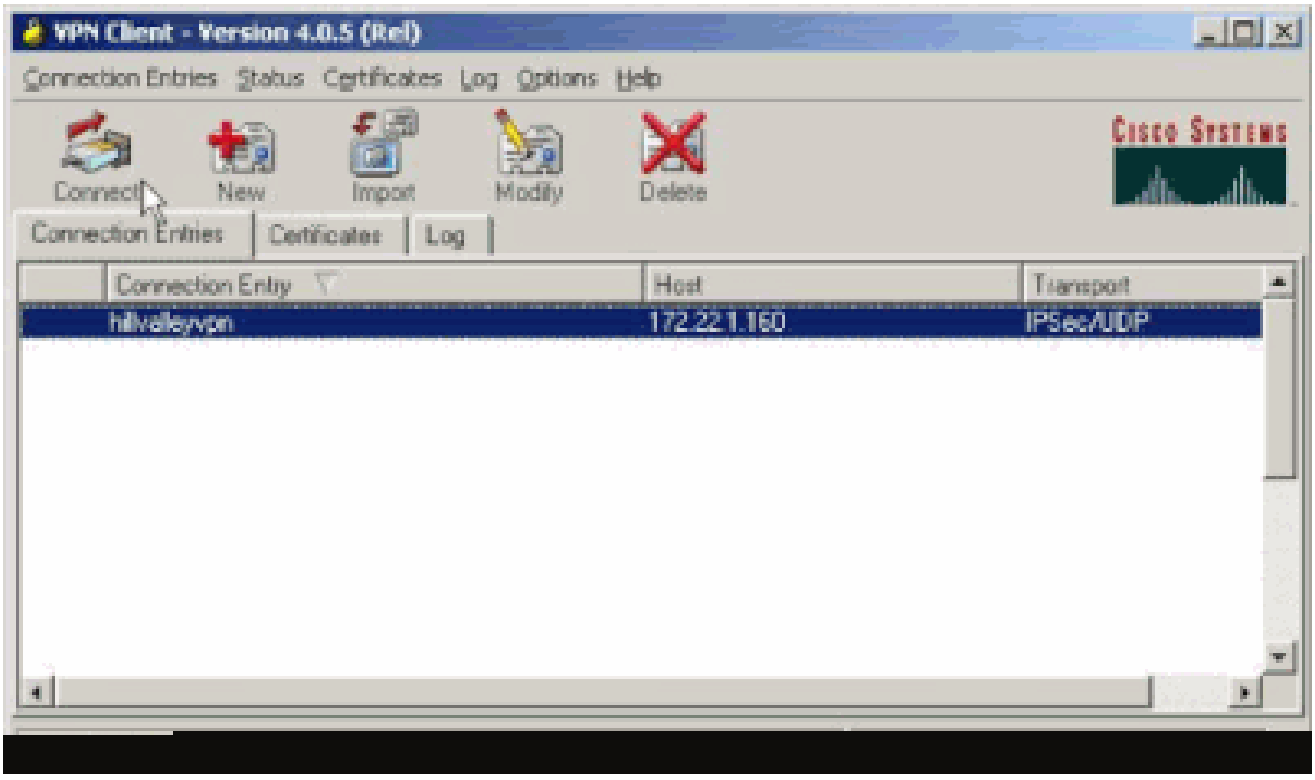
- VPN Client ログの表示

- Ping でローカル LAN アクセスをテストする

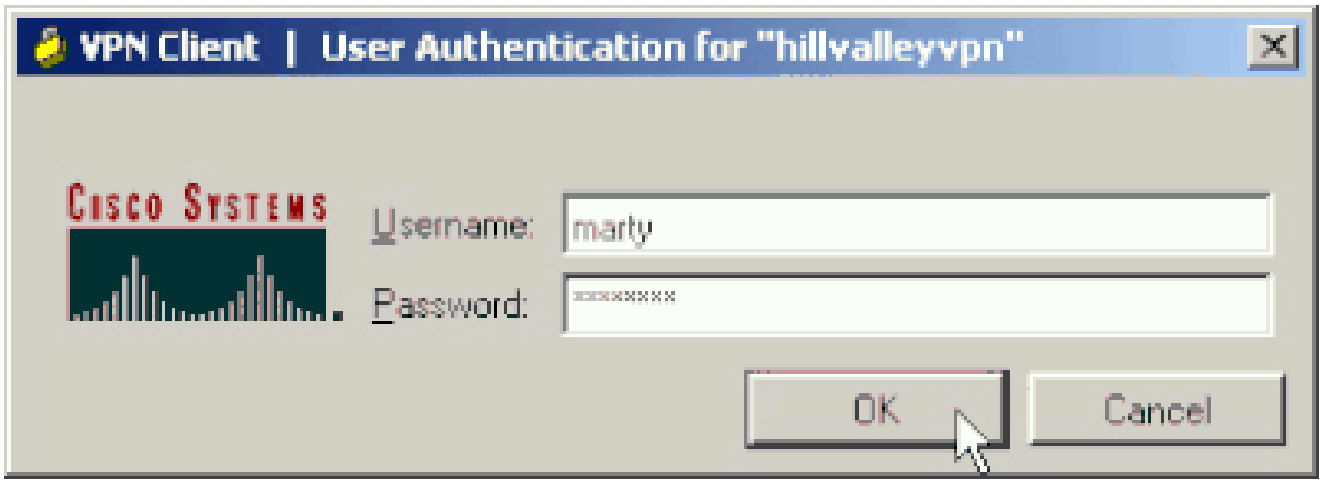
VPN Client で接続する

VPN Client を VPN コンセントレータに接続して、設定を確認します。

- リストから接続エントリを選択して [Connect] をクリックします。

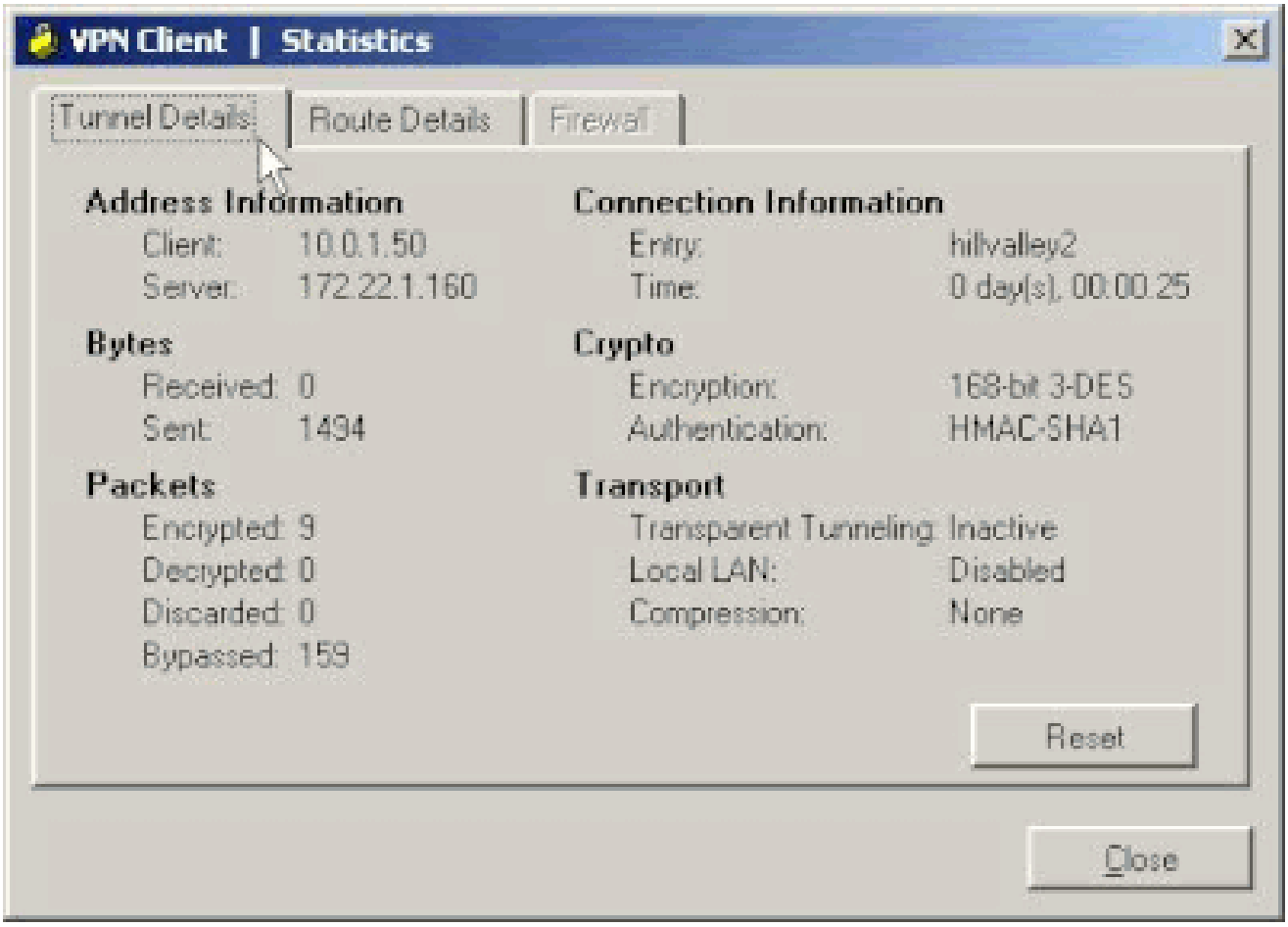


- 認証情報を入力してください。



-

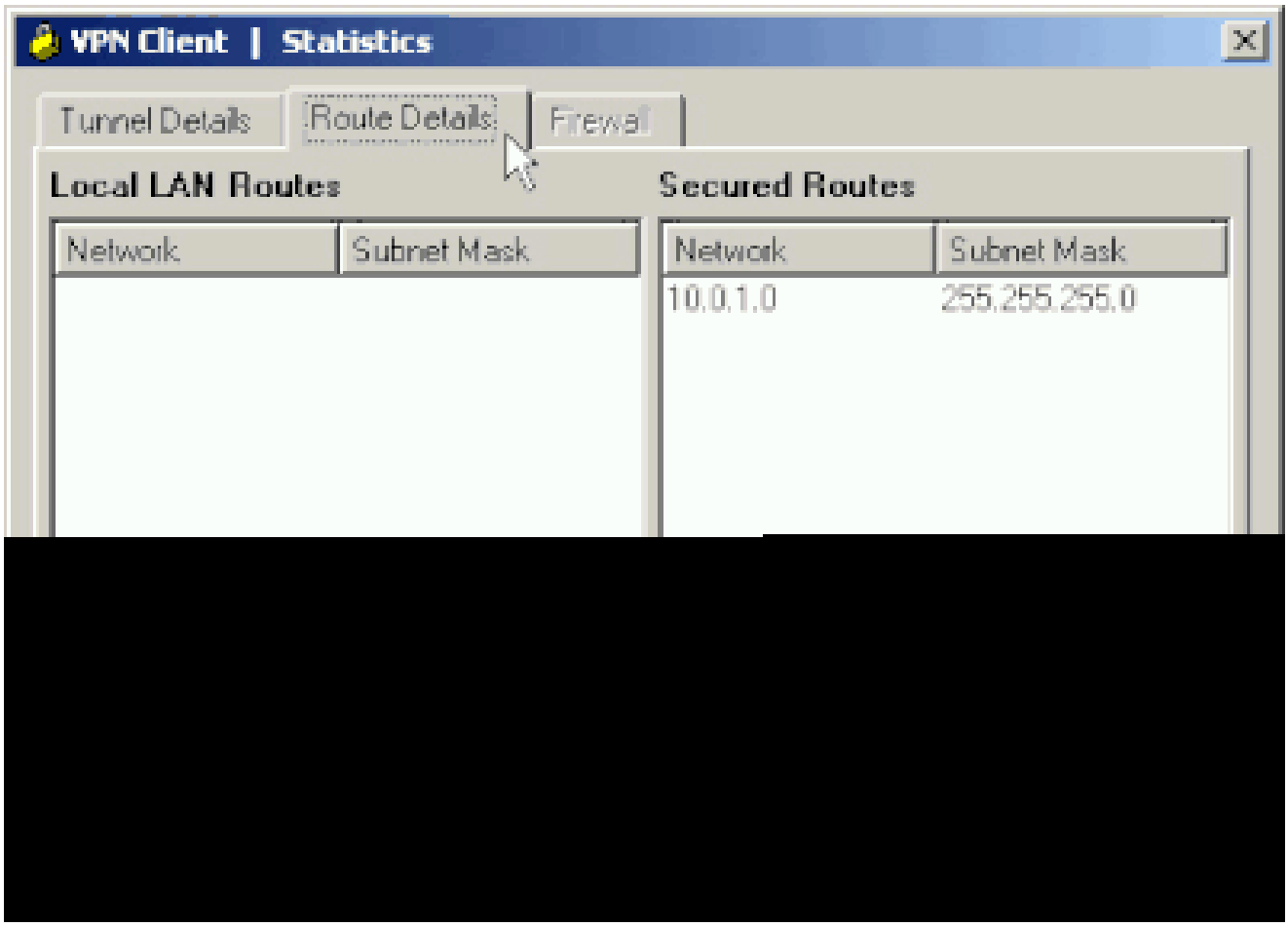
[Status] > [Statistics...] の順に選択して、[Tunnel Details] ウィンドウを表示します。ここでトンネルの詳細を調べ、トラフィックの流れを確認できます。



-

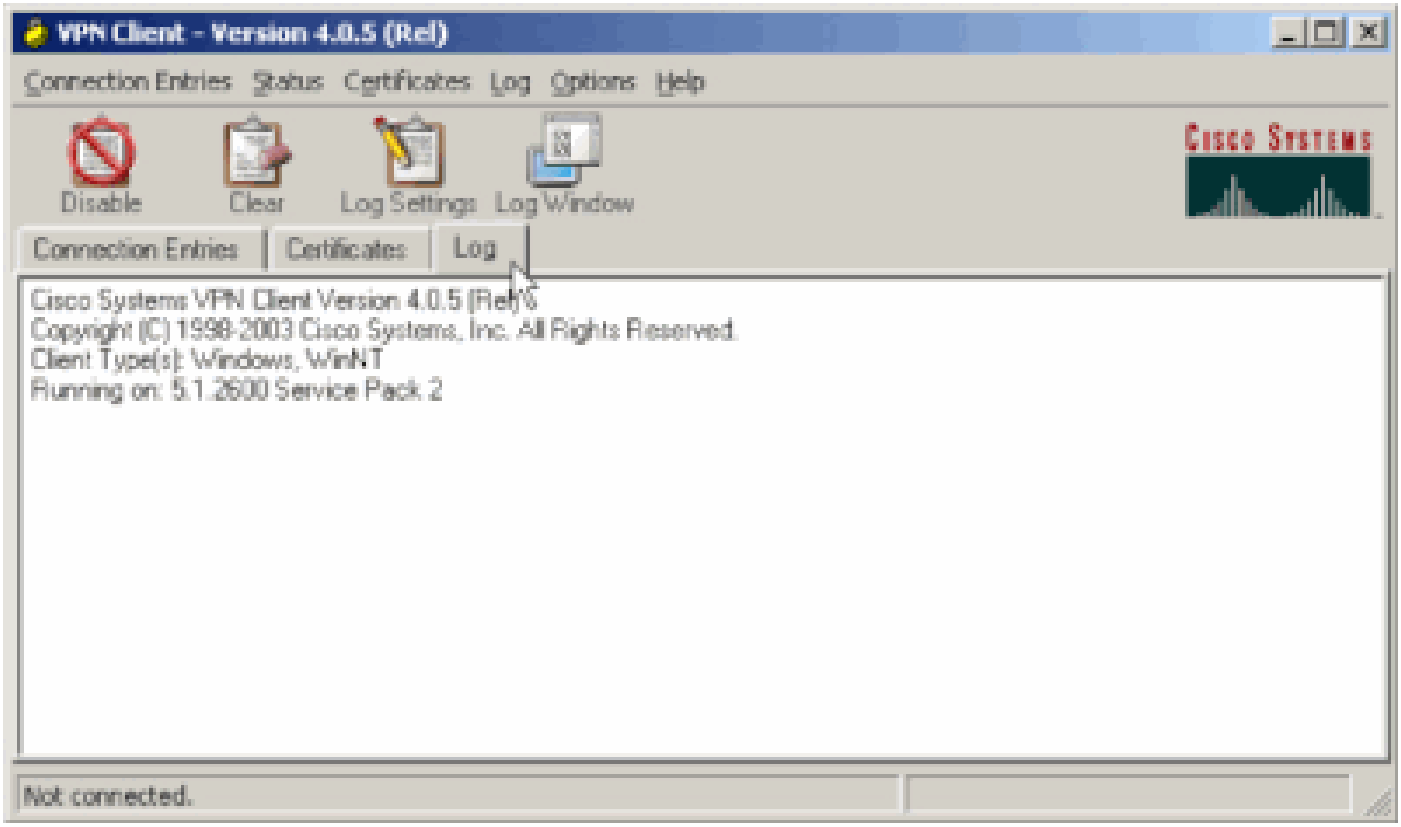
VPN Client が ASA に対して保護しているルートを確認するには、[Route Details] タブに移動します。

この例では、VPN Client は 10.0.1.0/24 へのアクセスを保護していますが、一方で、他のすべてのトラフィックは暗号化されず、トンネルを経由しては送信されません。



VPN Client ログの表示

VPN Client ログを調査すると、スプリット トンネリングを指定するパラメータが設定されているかどうかを確認できます。ログを表示するには、VPN Client の [Log] タブに移動します。その後、[Log Settings] をクリックして、記録される内容を調整します。この例では、IKE は **3- High** に設定されており、他のすべてのログ要素は 1 - Low に設定されています。




```
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.
```

Ping でローカル LAN アクセスをテストする

VPN Client が ASA へのトンネル時にスプリット トンネリングを使用するように設定されているかどうかは、Windows コマンド ラインで ping コマンドを使用してテストすることもできます。VPN Client のローカル LAN は 192.168.0.0/24 で、もう一方のホストは同じネットワーク上に IP アドレス 192.168.0.3 で存在しています。

```
   <#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
```

トラブルシュート

スプリット トンネル ACL でのエントリの数に関する制限

スプリット トンネルに使用される ACL のエントリの数には制限があります。機能を適切に動作させるためには、ACE のエントリを 50 ~ 60 以下にすることをお勧めします。サブネット化機能を実装して IP アドレスの範囲をカバーすることをお勧めします。

関連情報

- **ASDM の設定例を使用したリモート VPN サーバとしての PIX/ASA 7.x**
- **Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス**
- **シスコのテクニカルサポートとダウンロード**

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。