PIX/ASA 7.x: пример конфигурации модуля ASA, разрешающей раздельное туннелирование для клиентов VPN

Содержание

Введение

В этом документе приведены пошаговые инструкции, как разрешить клиентам VPN доступ в Интернет в то время, как их трафик туннелируется в модуль Cisco Adaptive Security Appliance (ASA) 5500. Эта конфигурация обеспечивает клиентам VPN безопасный доступ к корпоративным ресурсам по протоколу IPsec и небезопасный доступ в Интернет.

Предупреждение: Раздельное туннелирование может представлять угрозу безопасности. Поскольку клиенты VPN получают небезопасный доступ в Интернет, они могут подвергаться атакам. И в случае успешной атаки злоумышленник сможет получить доступ к корпоративной сети через туннель IPsec. В качестве компромисса между полным и раздельным туннелированием можно разрешить клиентам VPN только доступ к локальной сети. См. статью PIX/ASA 7.x: пример конфигурации, разрешающей клиентам VPN доступ к локальной сети, содержащую дополнительные сведения по этой теме.

Предварительные условия

Требования

В этом документе предполагается, что на устройстве ASA уже есть действующая конфигурация VPN для удаленного доступа. Если такой конфигурации еще нет, см. статью Пример настройки PIX/ASA 7.x в качестве удаленного сервера VPN с помощью ASDM.

Используемые компоненты

Сведения, представленные в этом документе, относятся к следующим версиям программного и аппаратного обеспечения.

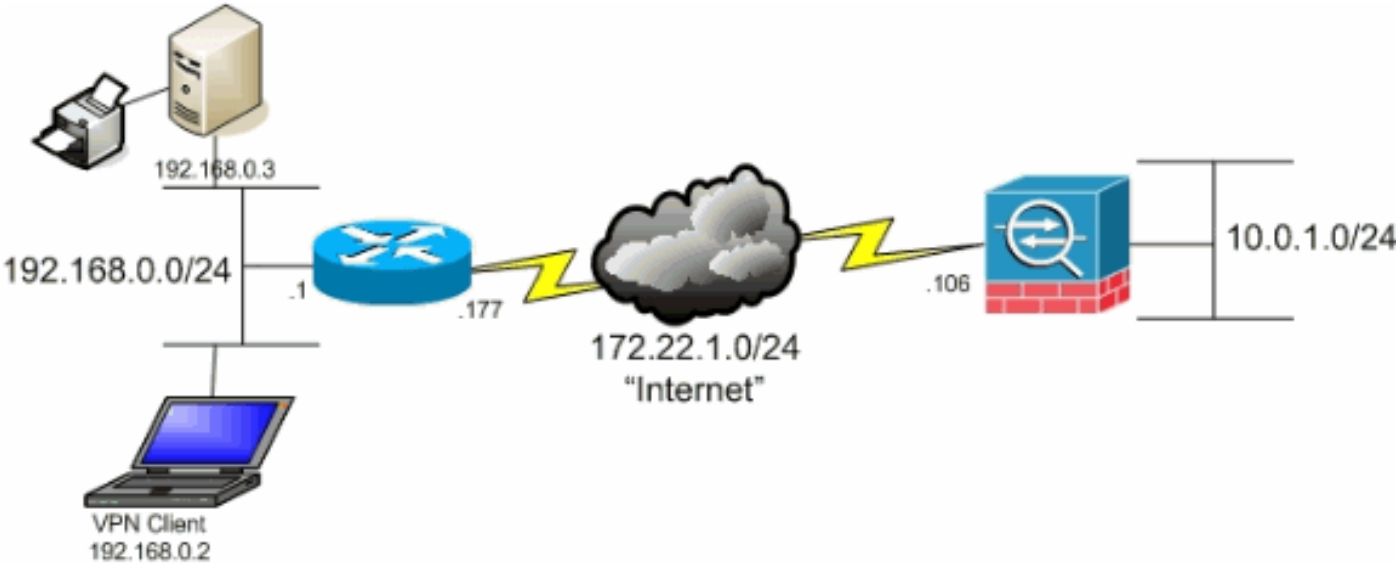
Программное обеспечение Cisco ASA 5500 Series Security Appliance версии 7.2

Cisco Systems VPN Client версии 4.0.5

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, начинали работу с чистой (стандартной) конфигурацией. При работе в действующей сети необходимо изучить все возможные последствия каждой команды.

Схема сети

Клиент VPN расположен в обычной сети SOHO и подключается через Интернет к главному офису.



Дополнительные продукты

Эту конфигурацию также можно использовать с ПО Cisco PIX 500 Series Security Appliance версии 7.x.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

В базовом сценарии "клиент VPN – ASA" весь трафик от клиента VPN шифруется и отправляется на устройство ASA независимо от конечного пункта назначения трафика. В зависимости от конфигурации и поддерживаемого количества пользователей, такая настройка может потреблять значительную пропускную способность. Раздельное

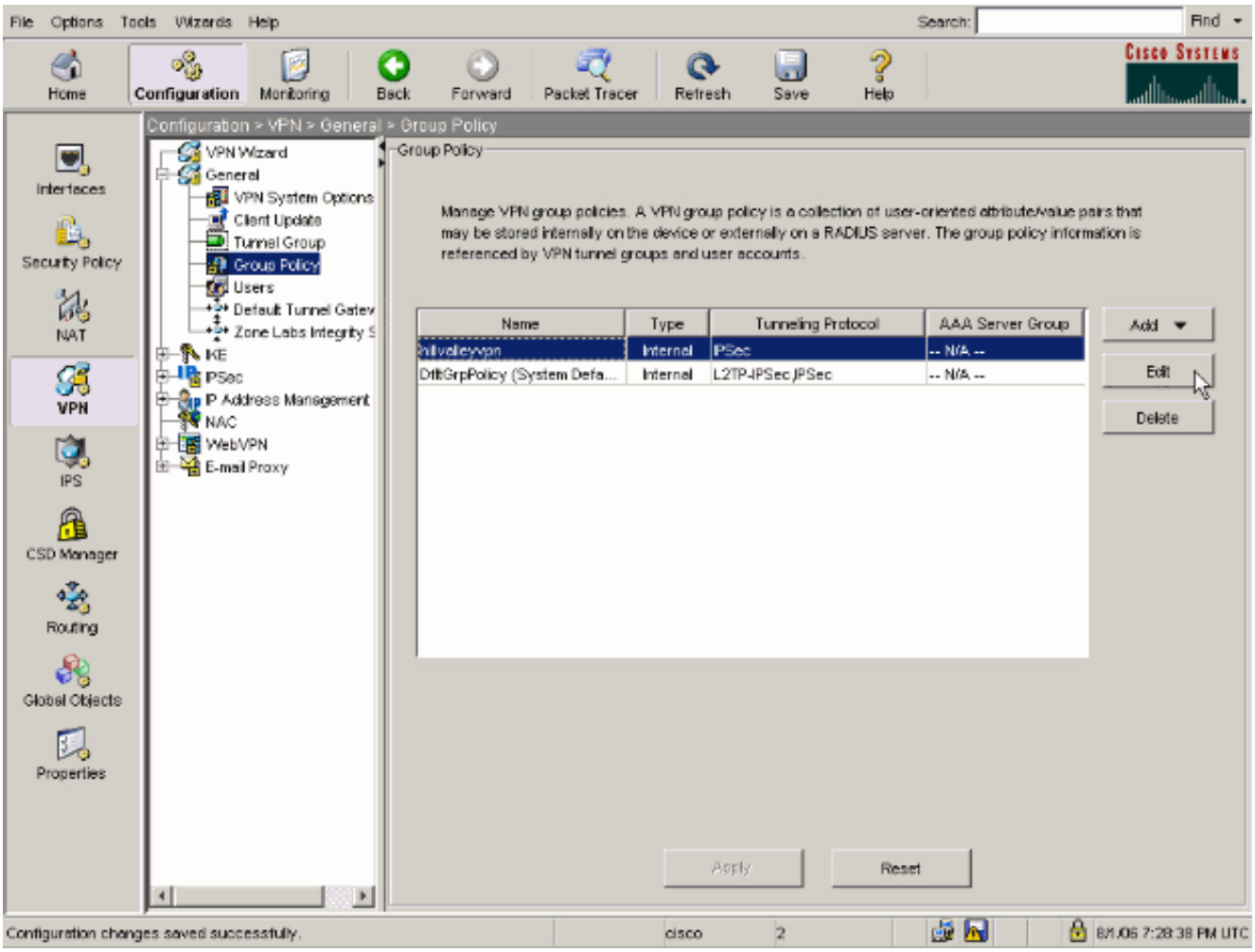
туннелирование может уменьшить эту проблему, так как оно позволяет пользователям отправлять по туннелю только трафик, предназначенный для корпоративной сети. Весь прочий трафик, например обмен мгновенными сообщениями, электронная почта и просмотр веб-страниц отправляется в Интернет через локальную сеть клиента VPN.

Настройка раздельного туннелирования в ASA

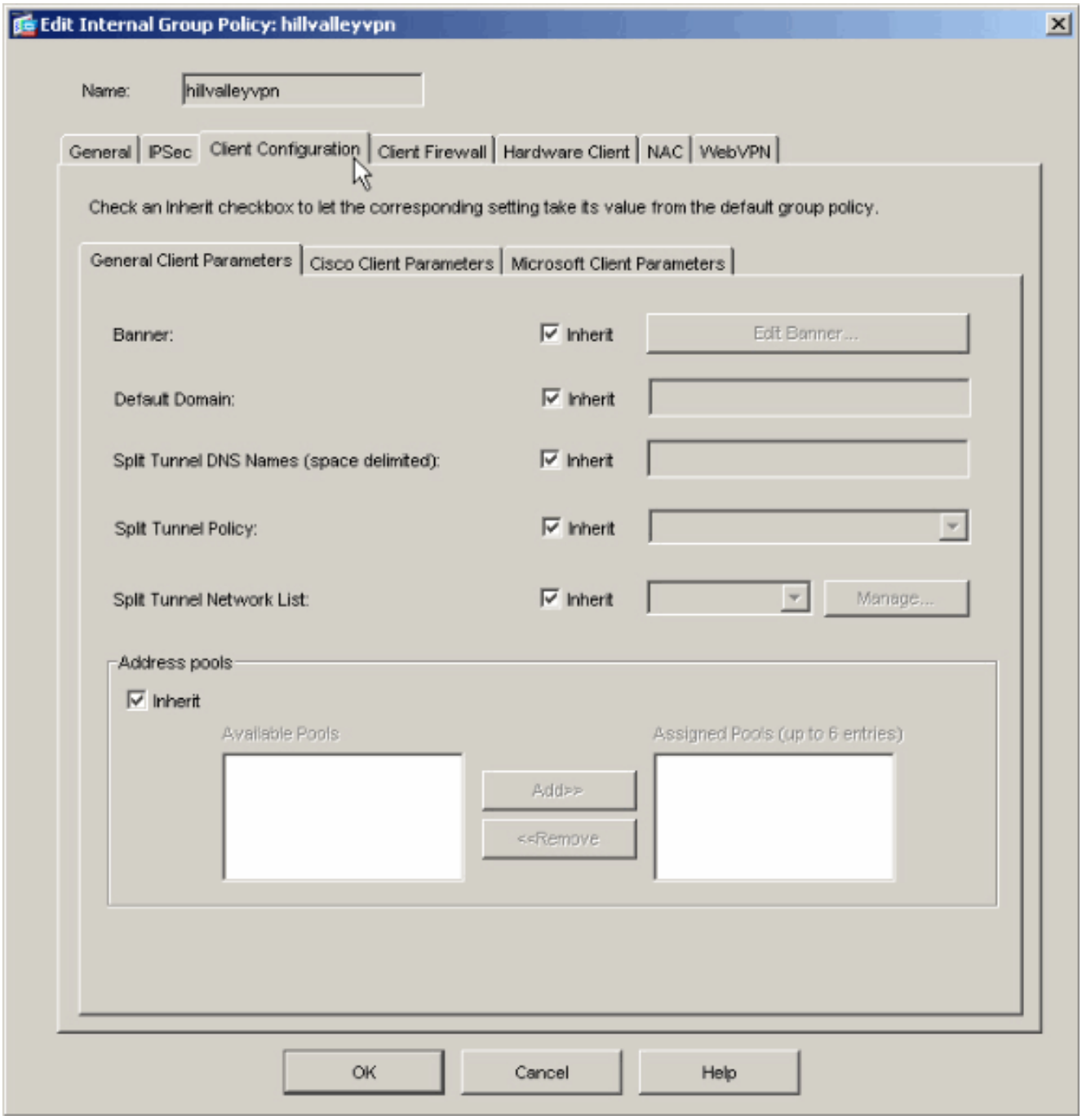
Настройка ASA с помощью Adaptive Security Device Manager (ASDM)

Выполните следующие действия для настройки туннельной группы, чтобы разрешить раздельное туннелирование пользователям в этой группе.

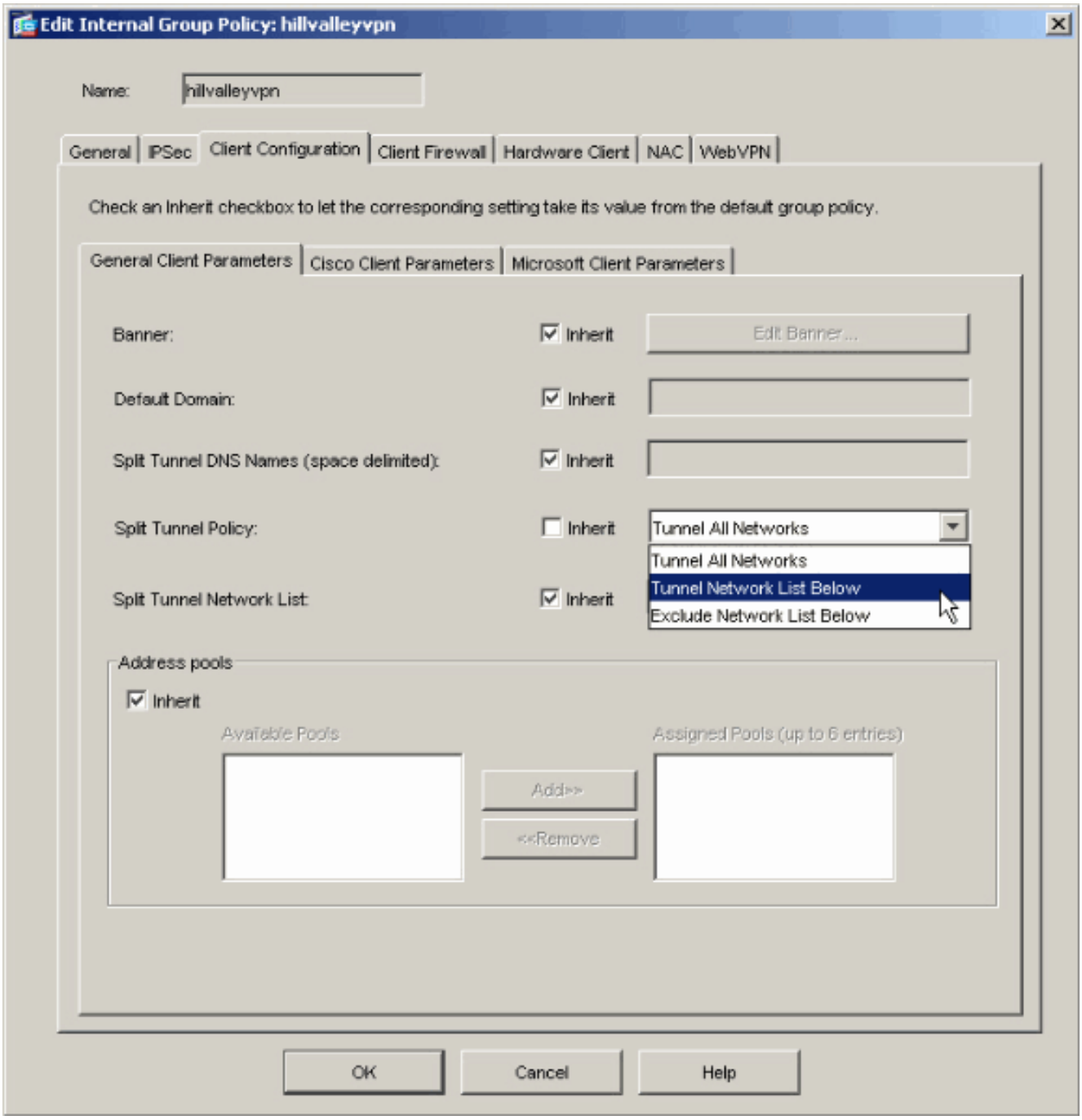
Щелкните **Configuration > VPN > General > Group Policy** и выберите групповую политику, в которой будет включен доступ к локальной сети. Затем нажмите кнопку **Edit**.



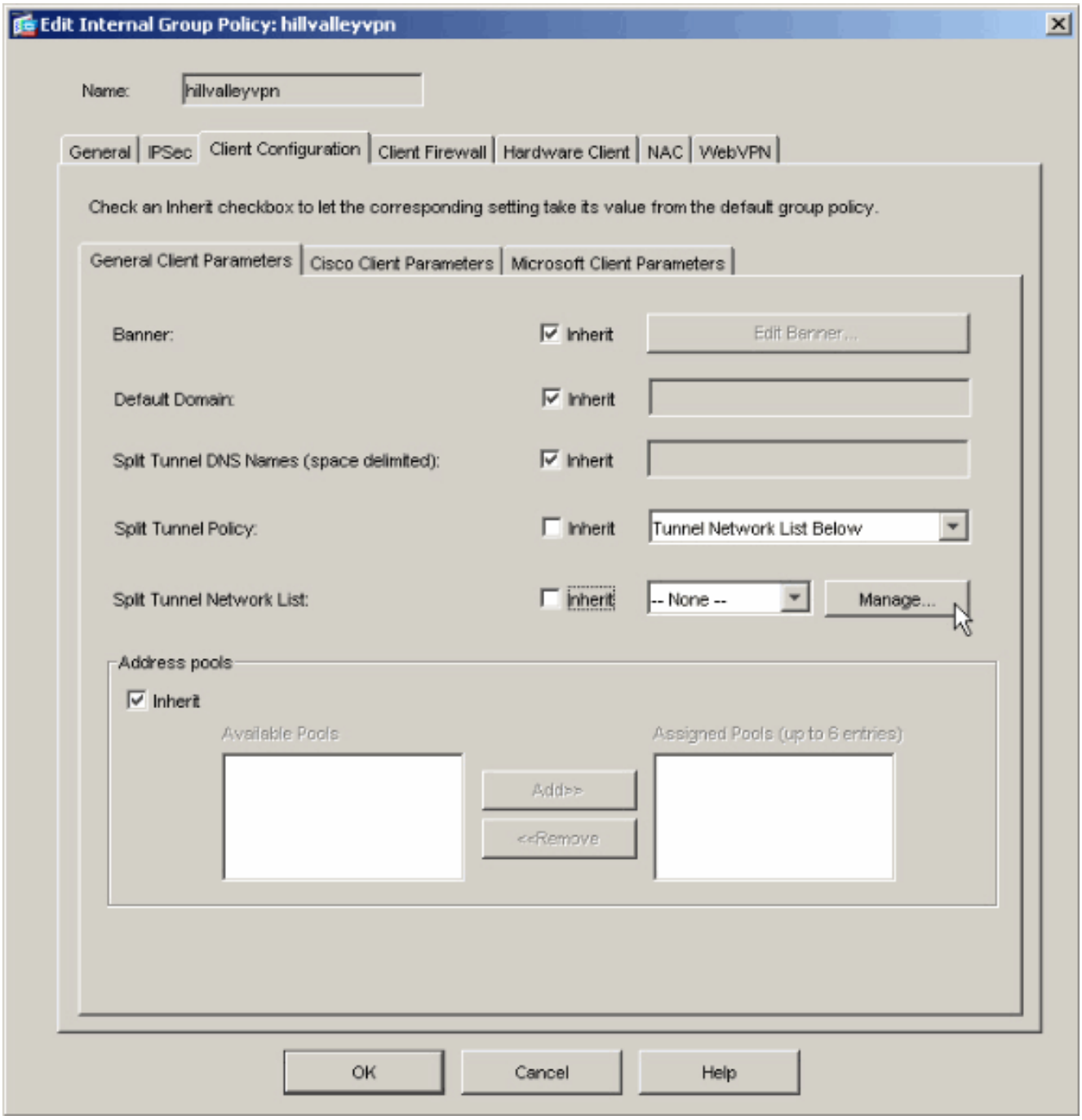
Перейдите на вкладку "Client Configuration".



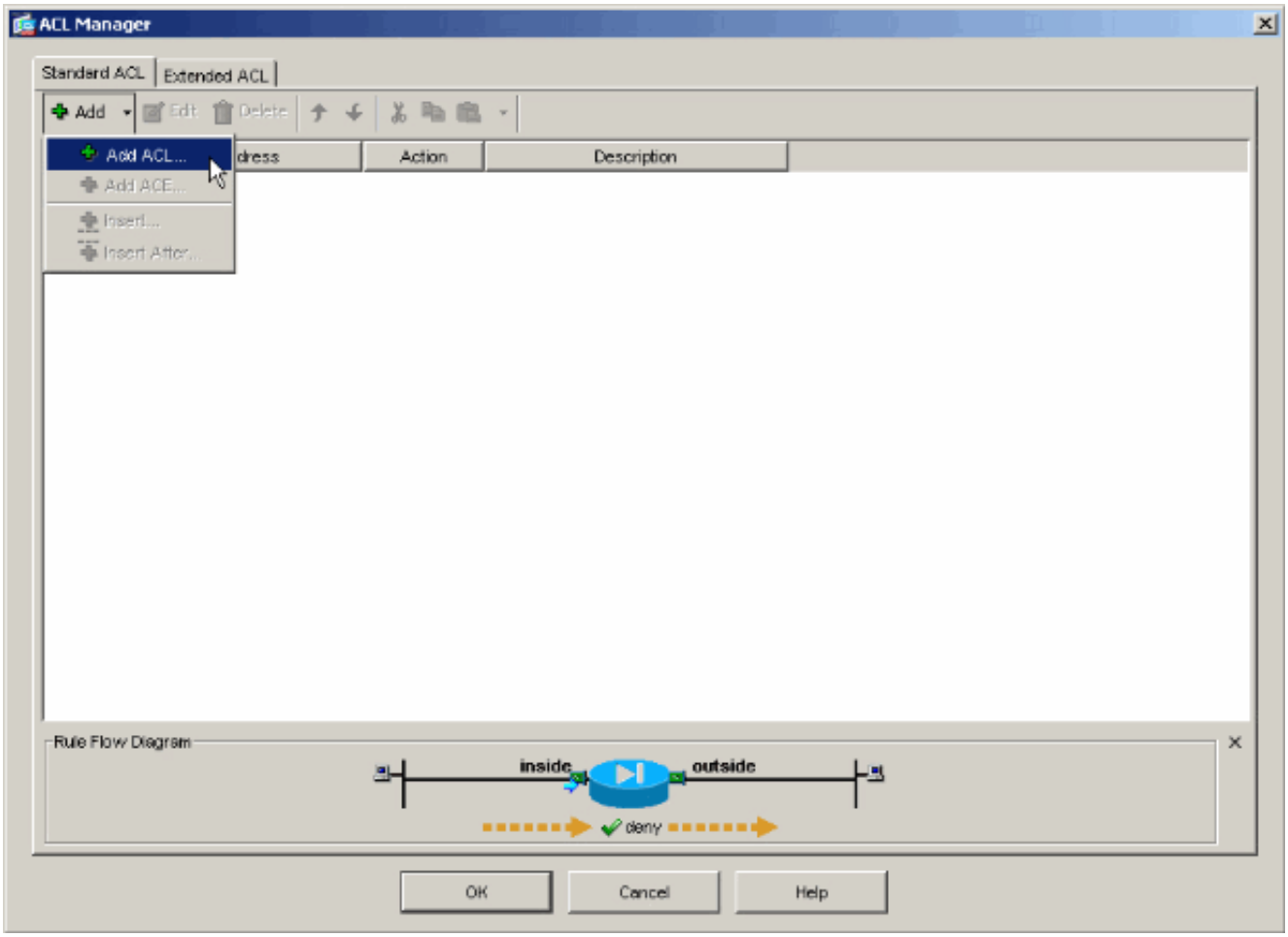
Снимите флажок **Inherit** для политики раздельных туннелей (Split Tunnel Policy) и выберите **Tunnel Network List Below**.



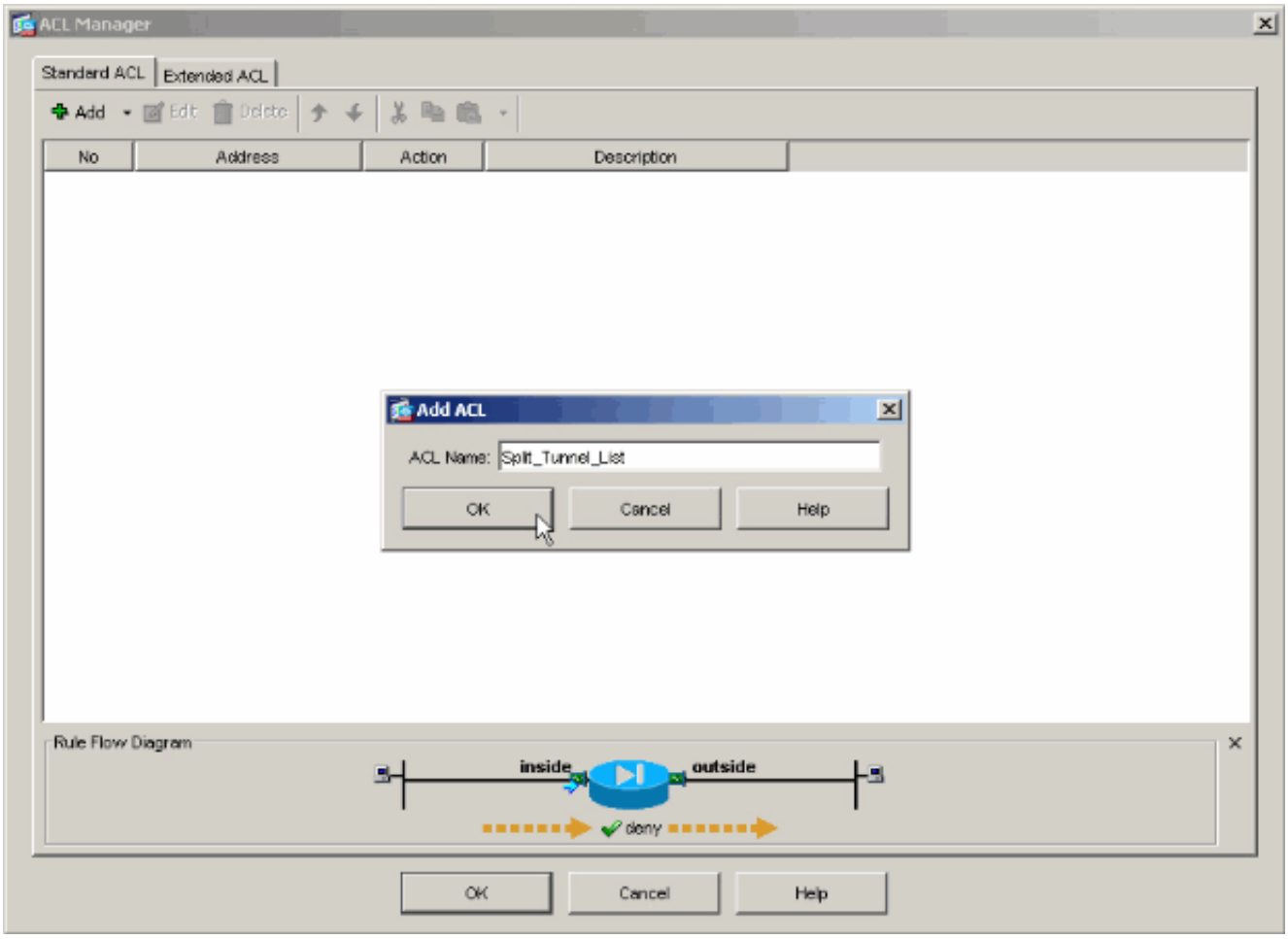
Снимите флажок **Inherit** для списка сетей для раздельного туннелирования (Split Tunnel Network List) и нажмите кнопку **Manage**, чтобы запустить ACL Manager.



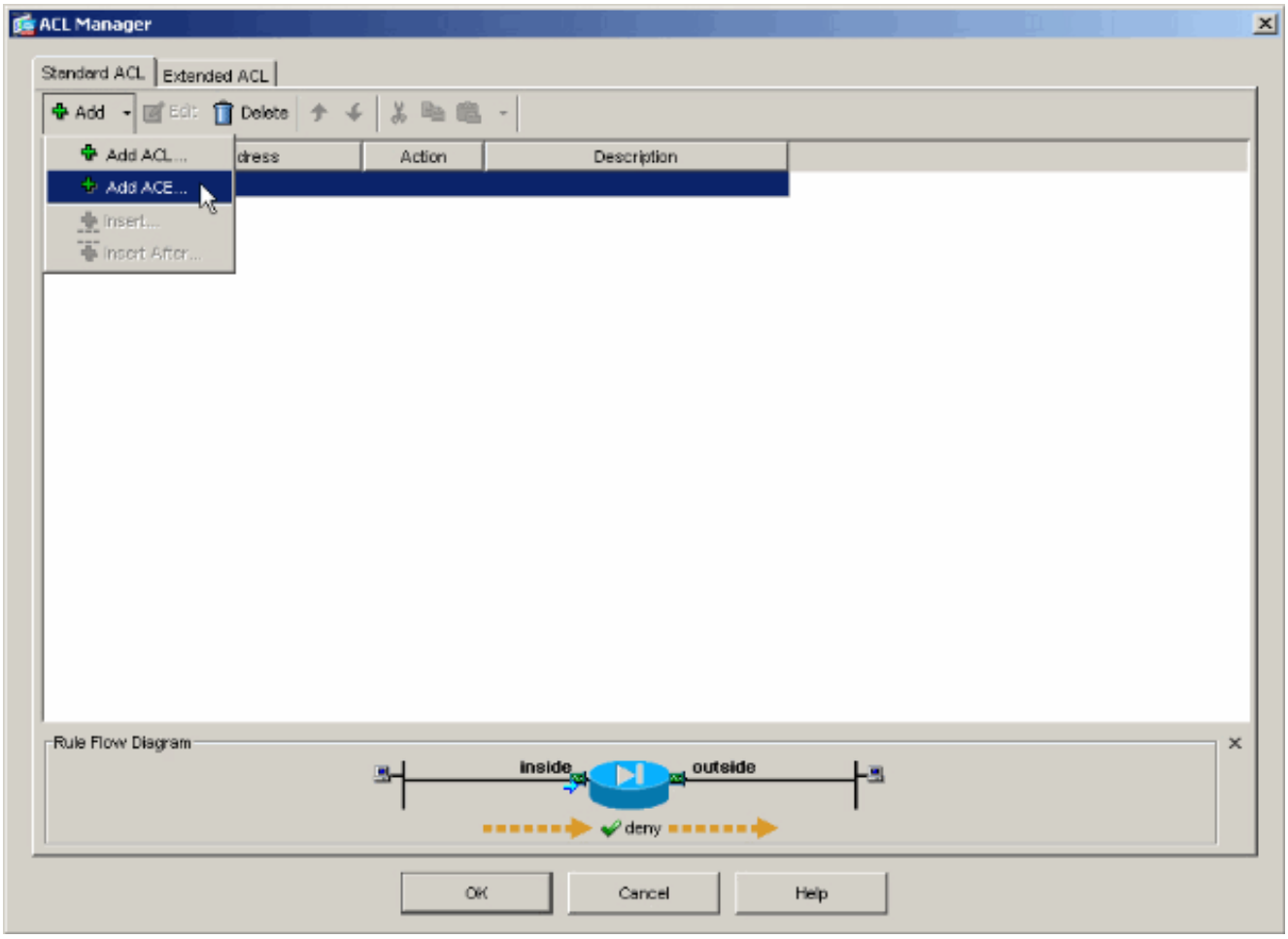
В ACL Manager выберите **Add > Add ACL...**, чтобы создать новый список доступа.



Введите имя ACL и нажмите кнопку **OK**.



Создав ACL, выберите **Add > Add ACE...**, чтобы добавить запись управления доступом (Access Control Entry, ACE).



Задайте запись ACE, соответствующую локальной сети, расположенной за модулем ASA. В нашем случае это сеть 10.0.1.0/24.

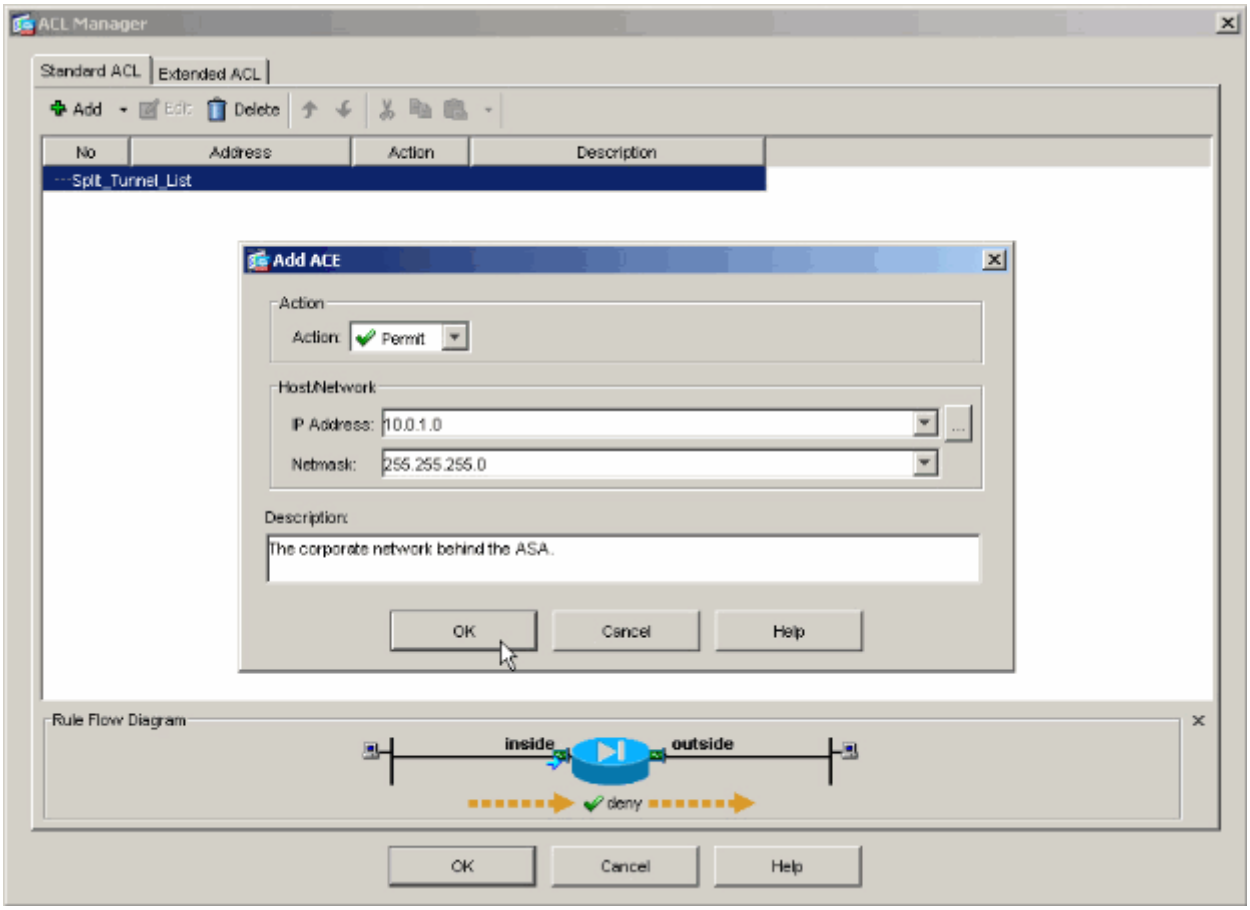
Выберите **Permit**.

Выберите IP-адрес **10.0.1.0**

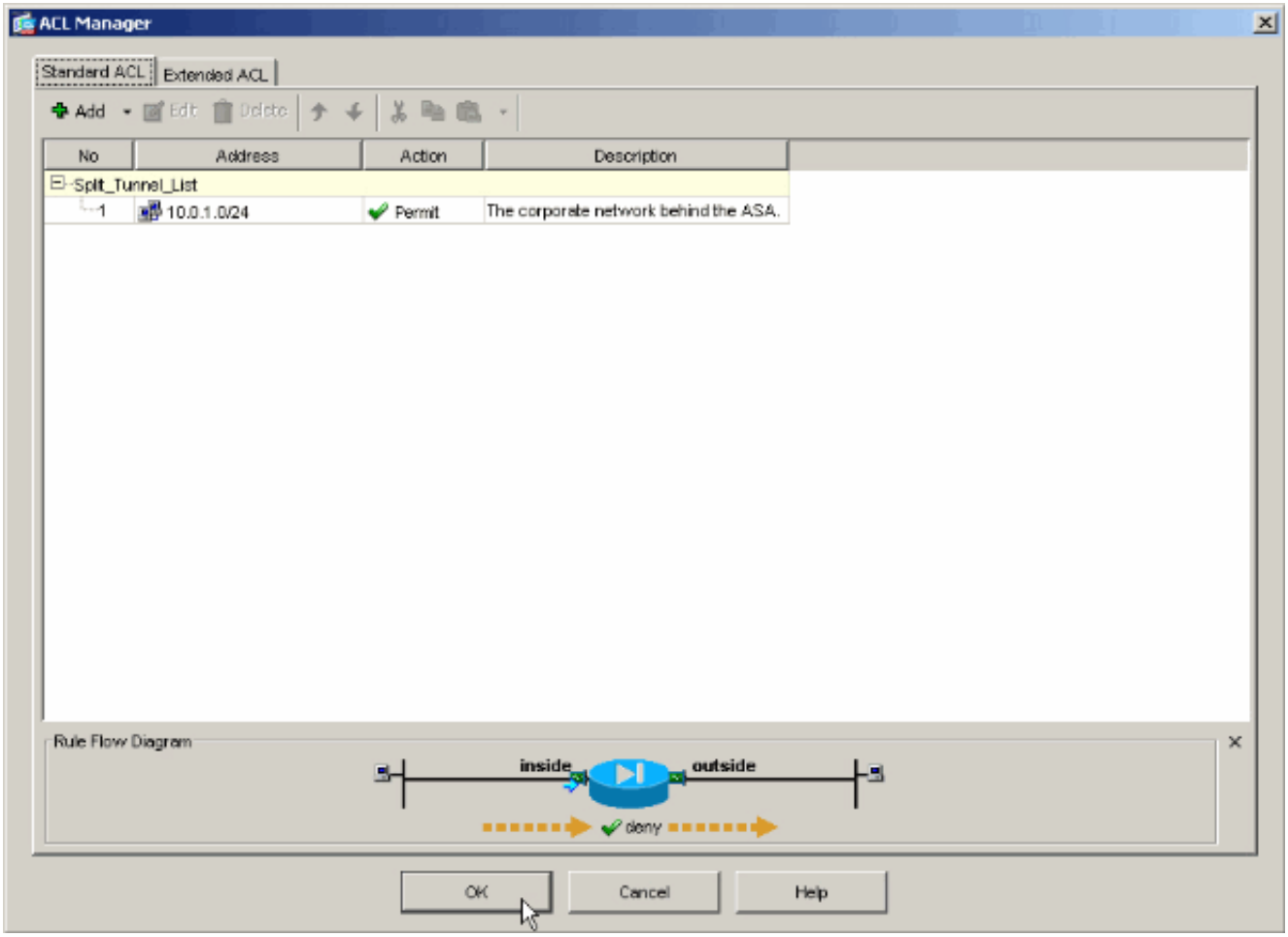
Выберите сетевую маску **255.255.255.0**.

Укажите описание *(необязательно)*

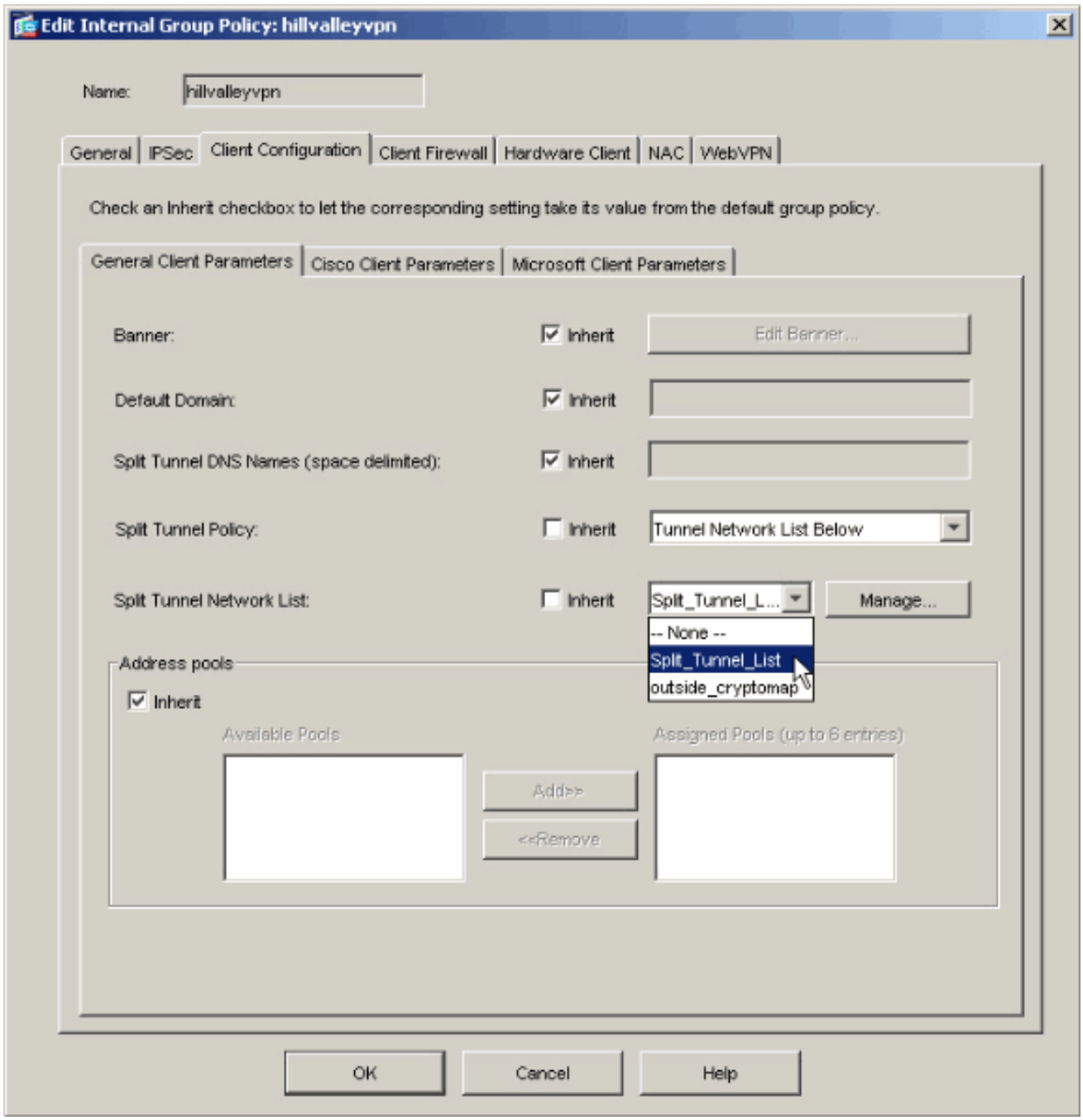
Нажмите кнопку **OK**.



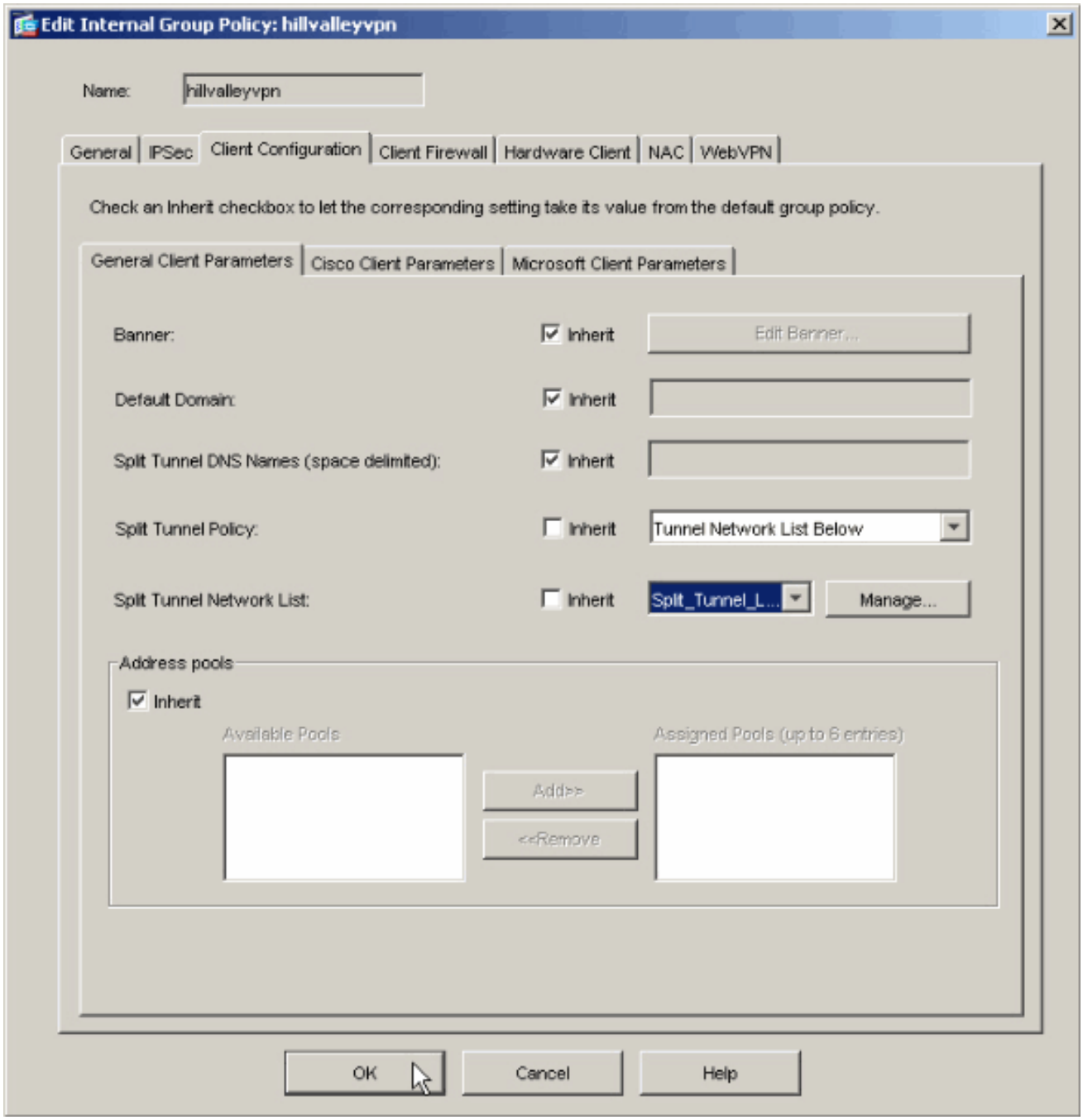
Нажмите кнопку **OK**, чтобы выйти из ACL Manager.



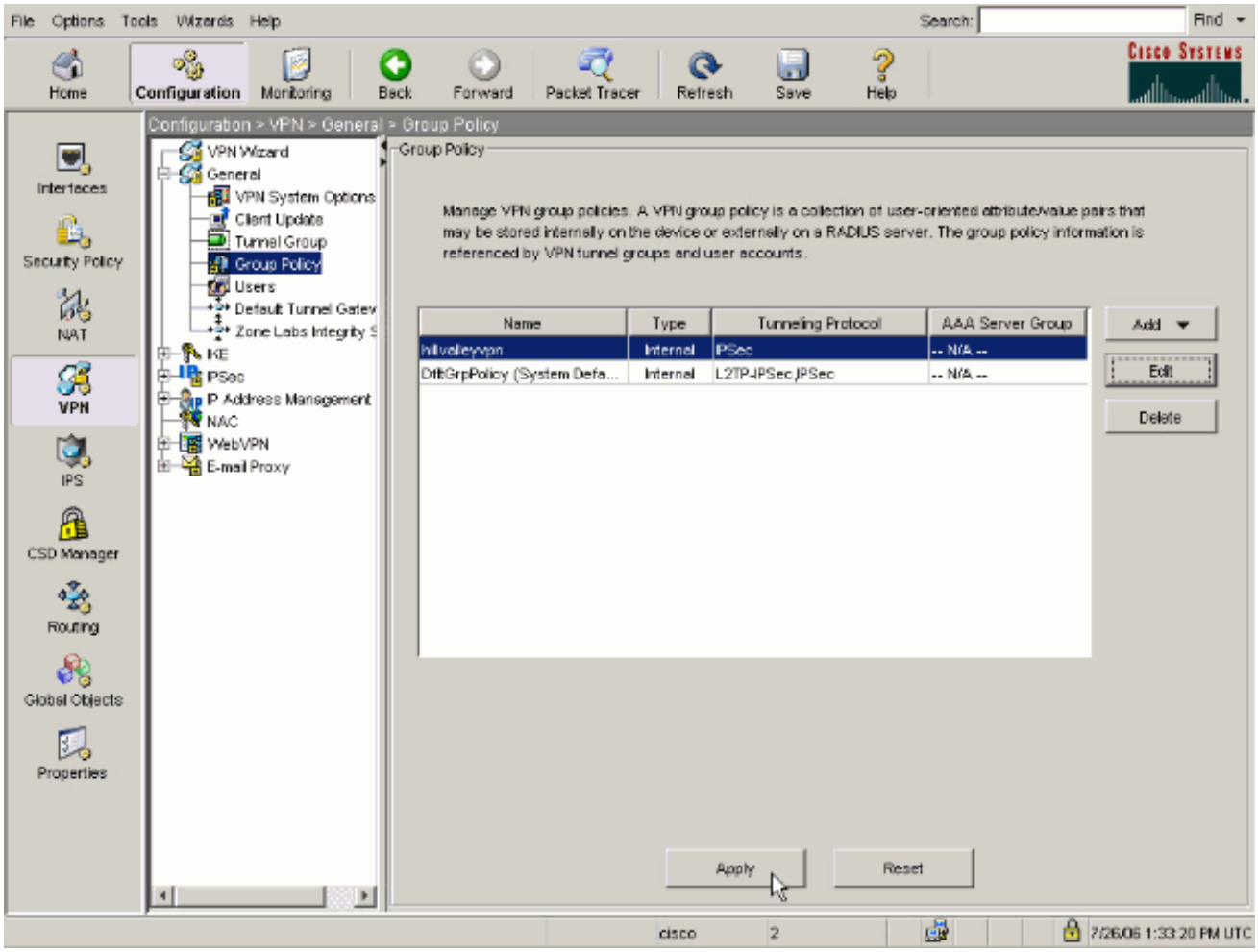
Убедитесь, что только что созданный список ACL выбран в списке сетей для раздельного туннелирования.



Нажмите кнопку **OK**, чтобы вернуться к конфигурации групповой политики.



Нажмите кнопку **Apply** и затем (если потребуется) **Send**, чтобы отправить эти команды в модуль ASA.



Настройка ASA с помощью CLI

Чтобы разрешить раздельное туннелирование в ASA, можно не использовать приложение ASDM, а воспользоваться интерфейсом командной строки (CLI) модуля ASA, выполнив следующие действия:

Войдите в режим конфигурации.

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

Создайте список доступа, определяющий сеть за модулем ASA.

```
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
```

Войдите в режим конфигурации групповой политики, которую нужно изменить.

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

Укажите политику раздельных туннелей. В этом случае политика указывается как **tunnelspecified**.

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

Укажите список доступа для раздельных туннелей. В этом случае список указывается как **Split_Tunnel_List**.

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

Выйдите из обоих режимов конфигурации.

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

Сохраните конфигурацию в энергонезависимой памяти (NVRAM) и нажмите клавишу **ВВОД**, когда будет предложено указать имя файла источника.

```
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#
```

Проверка

Выполните шаги, описанные в следующих разделах, чтобы проверить конфигурацию.

Подключение с помощью клиента VPN

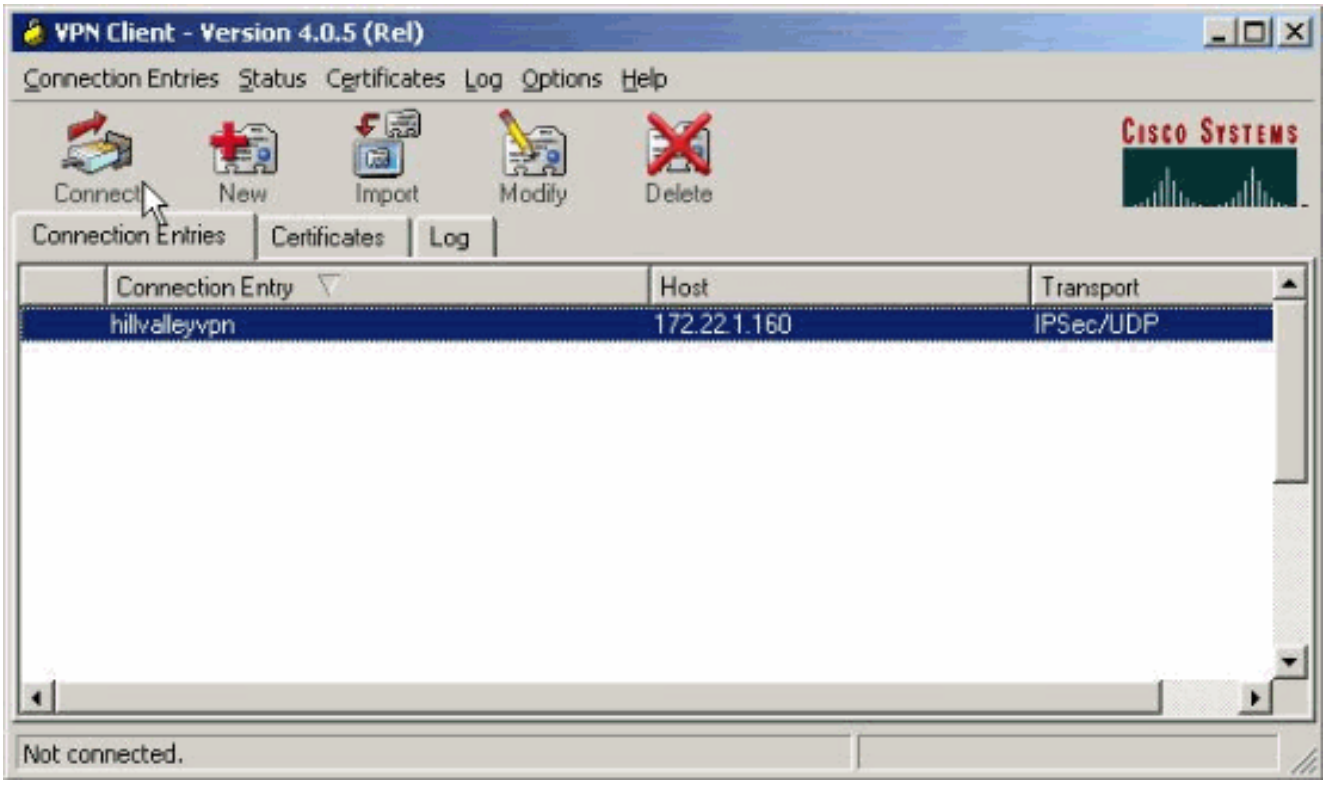
Просмотр журнала клиента VPN

Проверка доступа к локальной сети с помощью эхо-запроса

Подключение с помощью клиента VPN

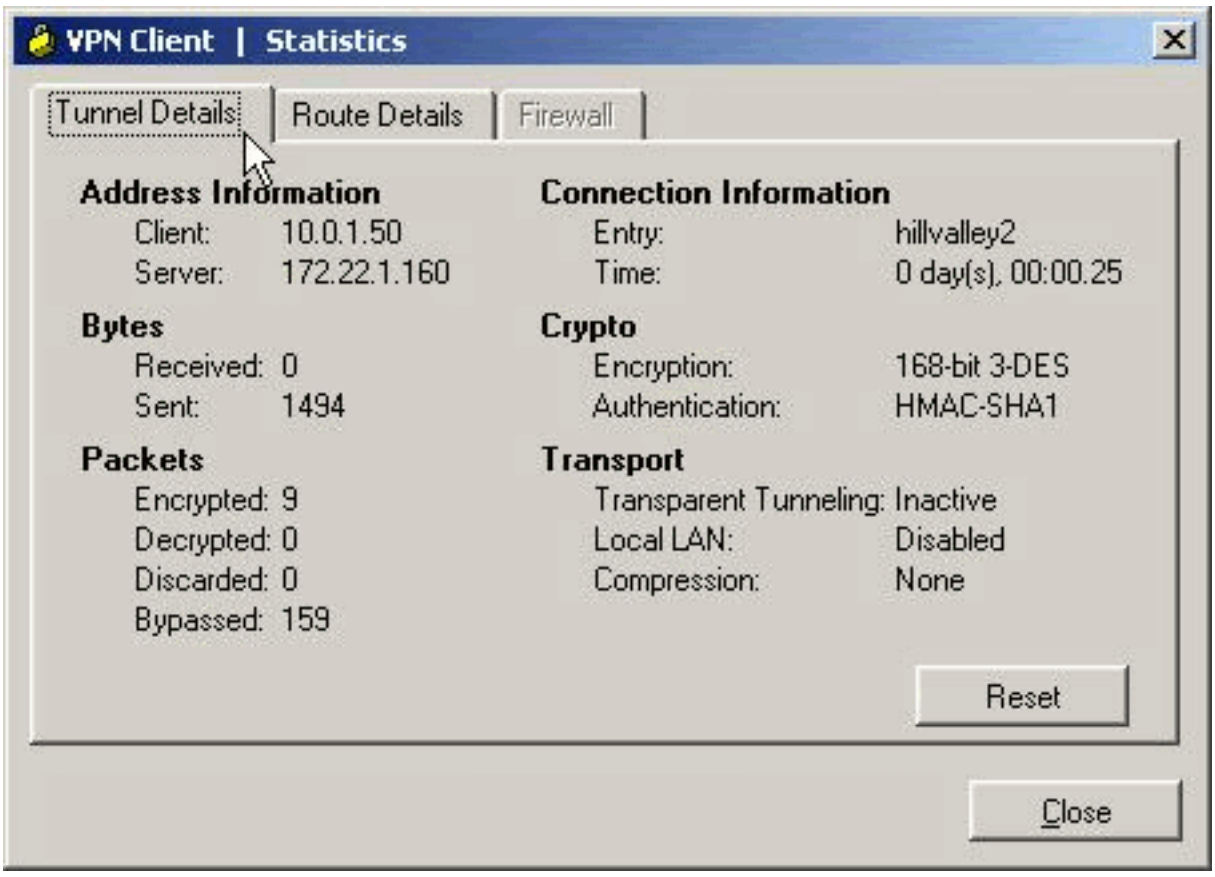
Подключите клиент VPN к концентратору VPN, чтобы проверить конфигурацию.

Выберите подключение из списка и нажмите кнопку **Connect**.



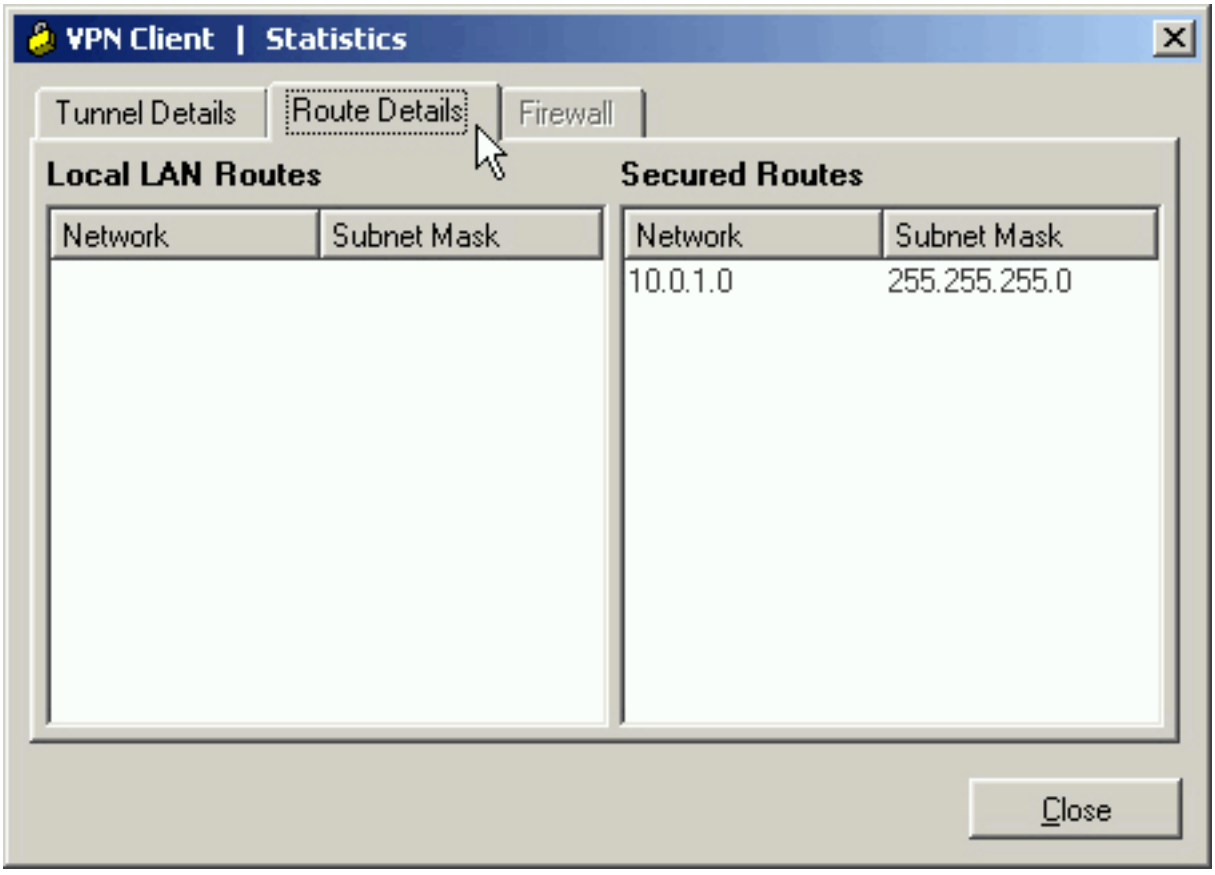
Введите учетные данные.

Выберите **Status > Statistics...**, чтобы отобразить окно "Tunnel Details", в котором можно узнать подробные данные о туннеле и увидеть потоки трафика.



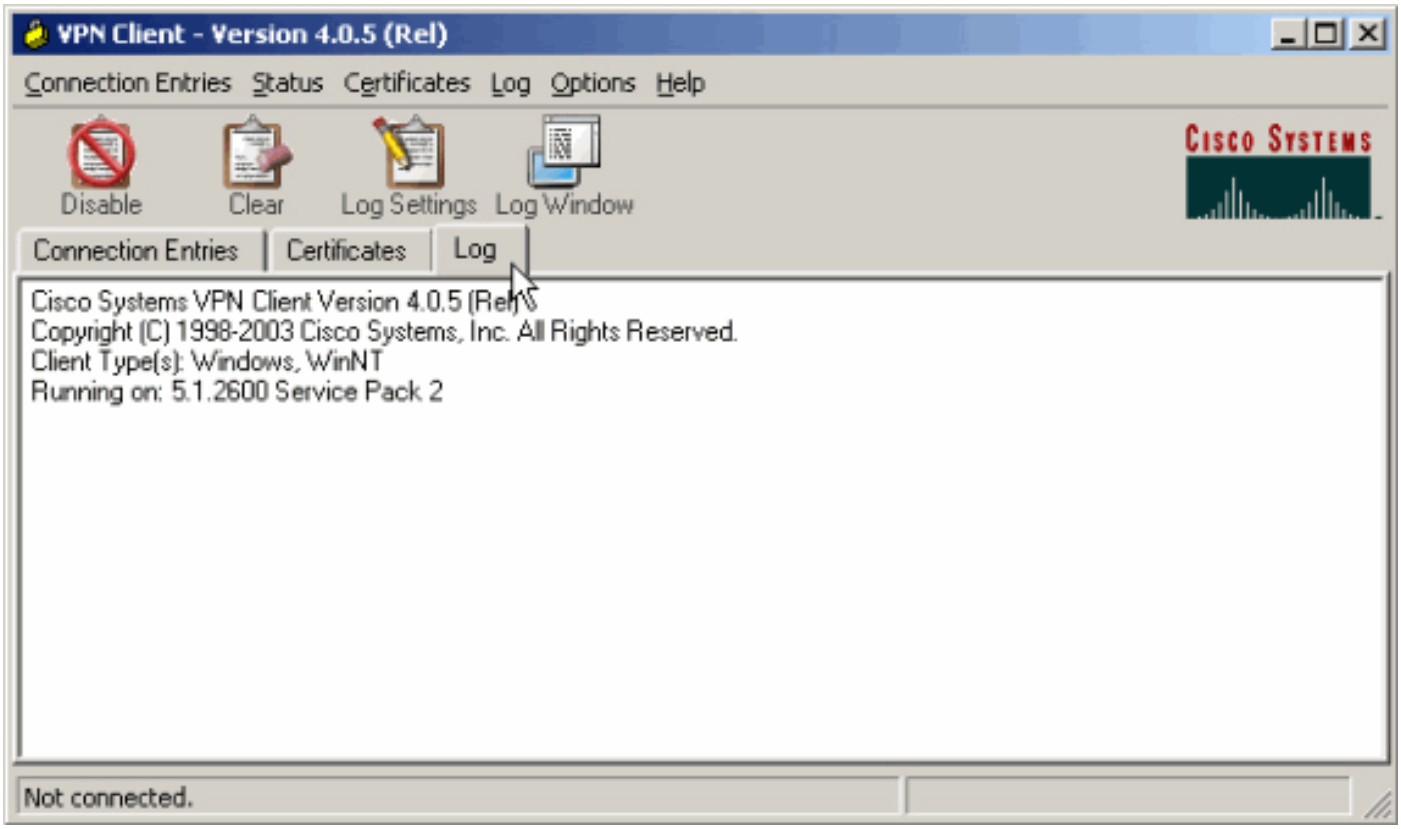
Перейдите на вкладку "Route Details", чтобы увидеть маршруты к ASA, защищенные клиентом VPN.

В этом примере клиент VPN защищает доступ к сети 10.0.1.0/24, а весь остальной трафик не шифруется и не отправляется по туннелю.



Просмотр журнала клиента VPN

В журнале клиента VPN, можно увидеть, задан параметр, определяющий раздельное туннелирование, или нет. Чтобы просмотреть журнал, перейдите на вкладку "Log" в клиенте VPN. Затем щелкните **Настройки журнала** , чтобы определить, какие событиях регистрируются в журнале. В этом примере для IKE задано значение **3 - High**, а для других элементов журнала – значение **1 - Low**.




```
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#
```

Проверка доступа к локальной сети с помощью эхо-запроса

Дополнительный способ убедиться, что клиент VPN настроен для раздельного туннелирования в то время, как его трафик туннелируется в ASA, — использовать команду **ping** в командной строке Windows. Локальная сеть клиента VPN — 192.168.0.0/24, и в сети присутствует другой узел с IP-адресом 192.168.0.3.

```
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
```

Устранение неполадок

Для этой конфигурации отсутствуют сведения об устранении неполадок.

Дополнительные сведения

- Пример настройки PIX/ASA 7.x в режиме удаленного сервера VPN с помощью ASDM
- Модули Cisco ASA 5500
- Техническая поддержка и документация — Cisco Systems