PIX/ASA 7.x: пример настройки доступа к локальной сети для VPN-клиентов

Содержание

Введение

В этом документе представлены пошаговые инструкции по настройке доступа VPN-клиентов Cisco **только** к своей локальной сети при наличии туннеля к Cisco ASA 5500 Series Security Appliance или Cisco PIX 500 Series Security Appliance. Такая конфигурация предоставляет VPN-клиентам безопасный доступ к корпоративным ресурсам с помощью IPsec, а также позволяет клиенту выполнять такие действия, как печать, из любого местоположения. Если разрешено, трафик, предназначенный для Интернета, продолжает передаваться по туннелю к ASA или PIX.

Примечание: Эта конфигурация не является настройкой раздельного туннелирования, при которой клиент обладает нешифрованным доступом к Интернету, оставаясь подключенным к ASA или PIX. Информацию о настройке раздельного туннелирования в ASA или PIX см. в документе PIX/ASA 7.x: пример настройки раздельного туннелирования для VPN-клиентов на устройстве ASA.

Предварительные условия

Требования

В данном документе предполагается, что в устройстве ASA или PIX уже есть действующая конфигурация VPN удаленного доступа. Если устройство еще не настроено, см. документ Пример настройки PIX/ASA 7.x в качестве удаленного VPN-сервера с помощью ASDM.

Используемые компоненты

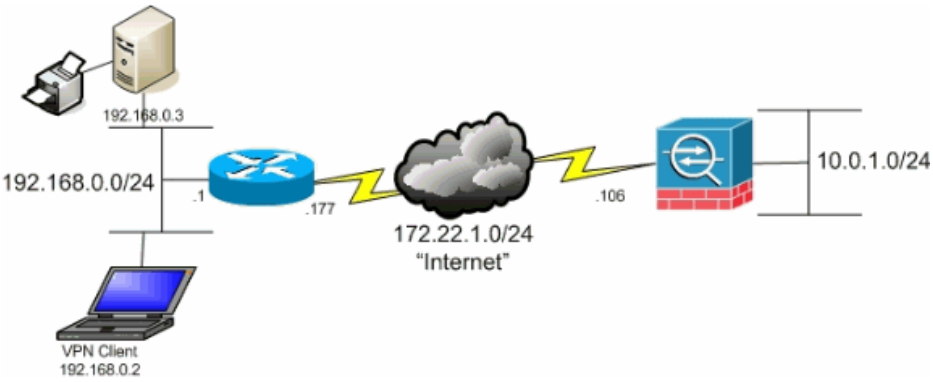
Сведения, содержащиеся в данном документе, приводятся для следующих версий программного и аппаратного обеспечения:

- Cisco ASA 5500 Series Security Appliance версии 7.2
- Cisco VPN Client версии 4.0.5

Сведения, приведенные в этом документе, были получены при тестировании устройств в специальной лабораторной среде. Все устройства, упоминаемые в этом документе, запускались с чистой конфигурацией (конфигурацией по умолчанию). Если сеть работает в реальных условиях, убедитесь в том, что понимаете потенциальное воздействие каждой команды.

Диаграмма сети

VPN-клиент расположен в типичной домашней сети или сети малого бизнеса и подключается к главному офису через Интернет.



Сопутствующие продукты

Эта конфигурация также может использоваться вместе с Cisco PIX 500 Series Security Appliance версии 7.x.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в статье Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Общие сведения

В отличие от классического сценария раздельного туннелирования, в котором весь трафик Интернета отправляется нешифрованным, при разрешении доступа к локальной сети для VPN-клиентов, таким клиентам разрешается обмениваться нешифрованными данными только с устройствами из сети клиента. Например, VPN-клиент, которому разрешен доступ к локальной сети при подключении к ASA из дома, может печатать на собственном принтере, но не имеет доступа к Интернету без предварительной отправки трафика через туннель.

Список доступа используется, чтобы разрешить доступ к локальной сети подобно тому, как в устройстве ASA настраивается раздельное туннелирование. Однако вместо определения сетей, которые *должны* шифроваться, в данном случае список доступа определяет сети, которые *не должны* шифроваться. Кроме того, в отличие от сценария раздельного туннелирования, в таком списке не требуется указывать действительные сети. Вместо этого устройство ASA предоставляет сеть по умолчанию 0.0.0.0/255.255.255.255, которая понимается как локальная сеть VPN-клиента.

Примечание: Когда VPN-клиент подключен и настроен для доступа к локальной сети, *печать или просмотр по имени* в данной сети невозможны. Однако имеется возможность просмотра или печати с помощью IP-адресов. Дополнительные сведения о такой ситуации, а также способы ее обхода см. в разделе Устранение неполадок данного документа.

Настройка доступа к локальной сети для VPN-клиентов

Выполните следующие две задачи, чтобы разрешить VPN-клиентам доступ к своей локальной сети при сохранении подключения к

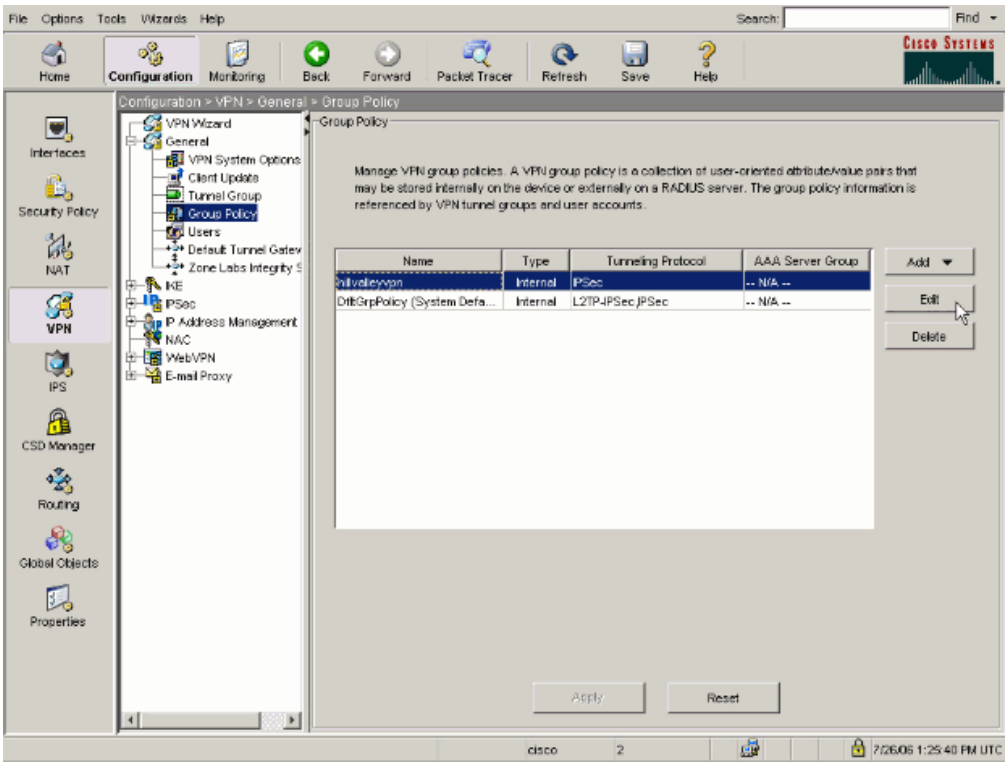
VPN-концентратору:

- Настроить ASA с помощью приложения Adaptive Security Device Manager (ASDM) или Настроить ASA с помощью интерфейса командной строки
- Настройка VPN-клиента

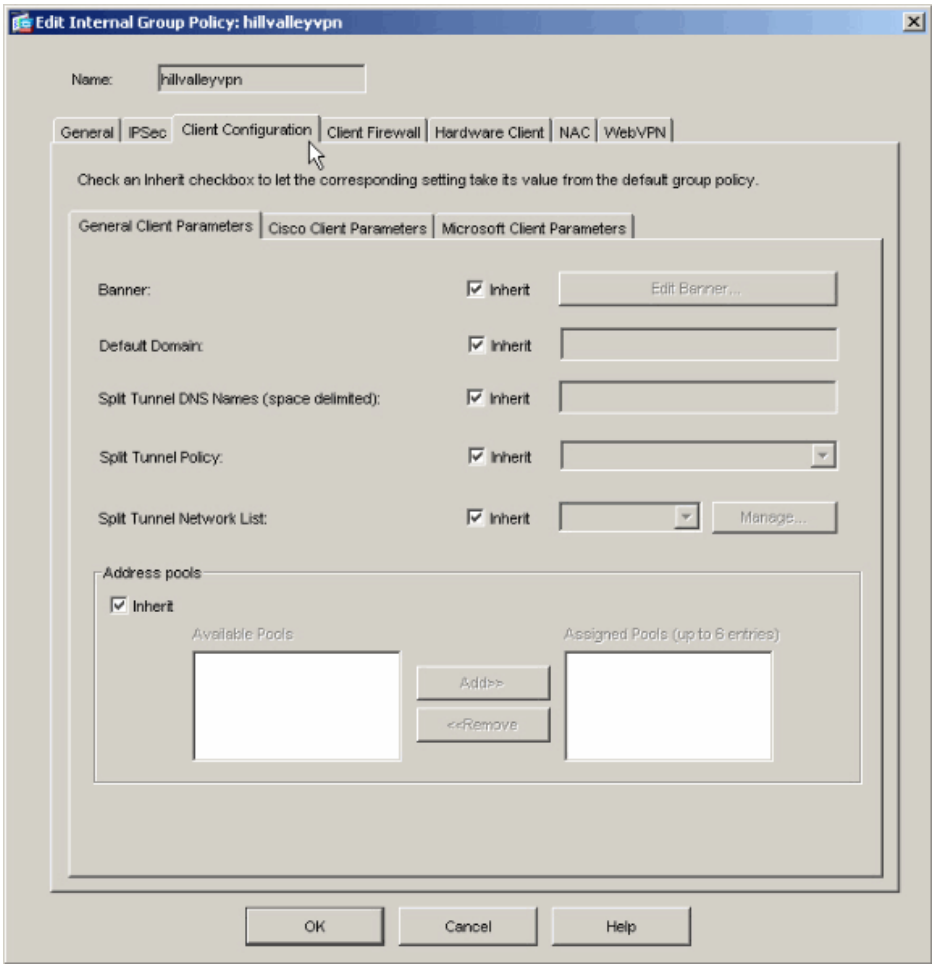
Настройка ASA с помощью ASDM

Выполните в ASDM следующие действия, чтобы разрешить VPN-клиентам доступ к локальной сети при наличии подключения к ASA.

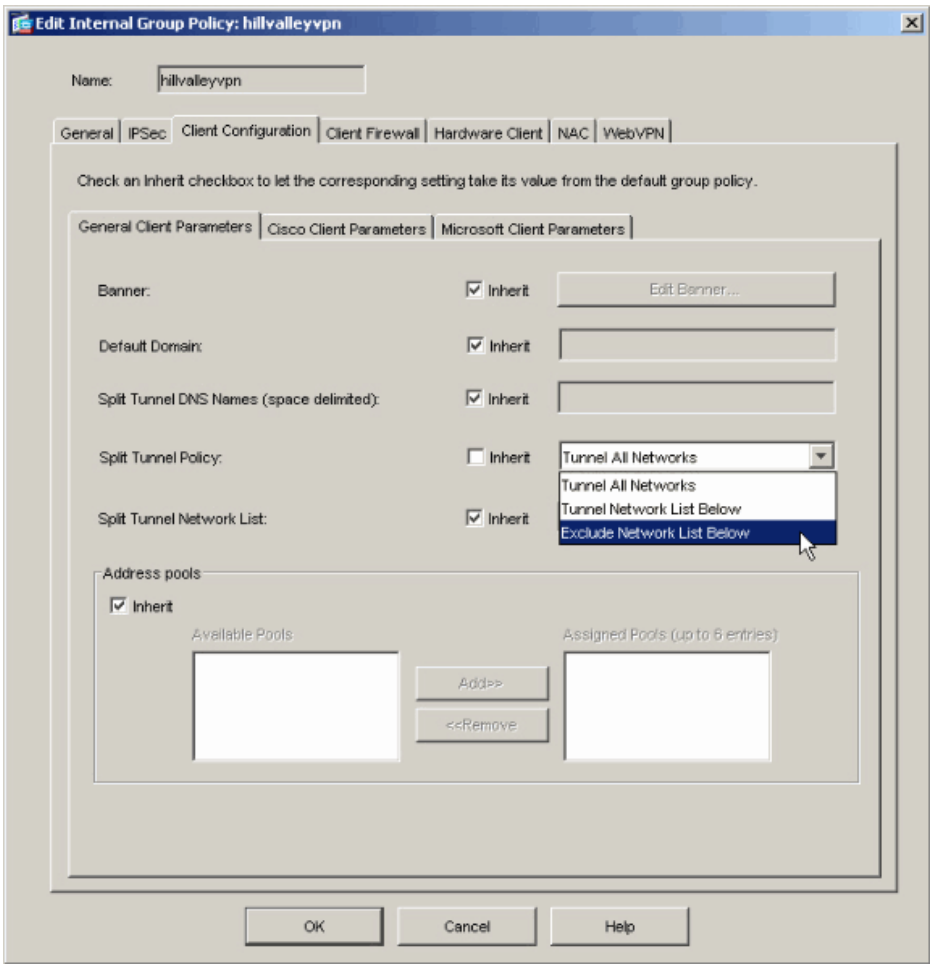
1. Выберите **Конфигурация > VPN > Общие > Групповая политика**, а затем — групповую политику, которая требуется для разрешения доступа к локальной сети. Затем нажмите кнопку **Изменить**.



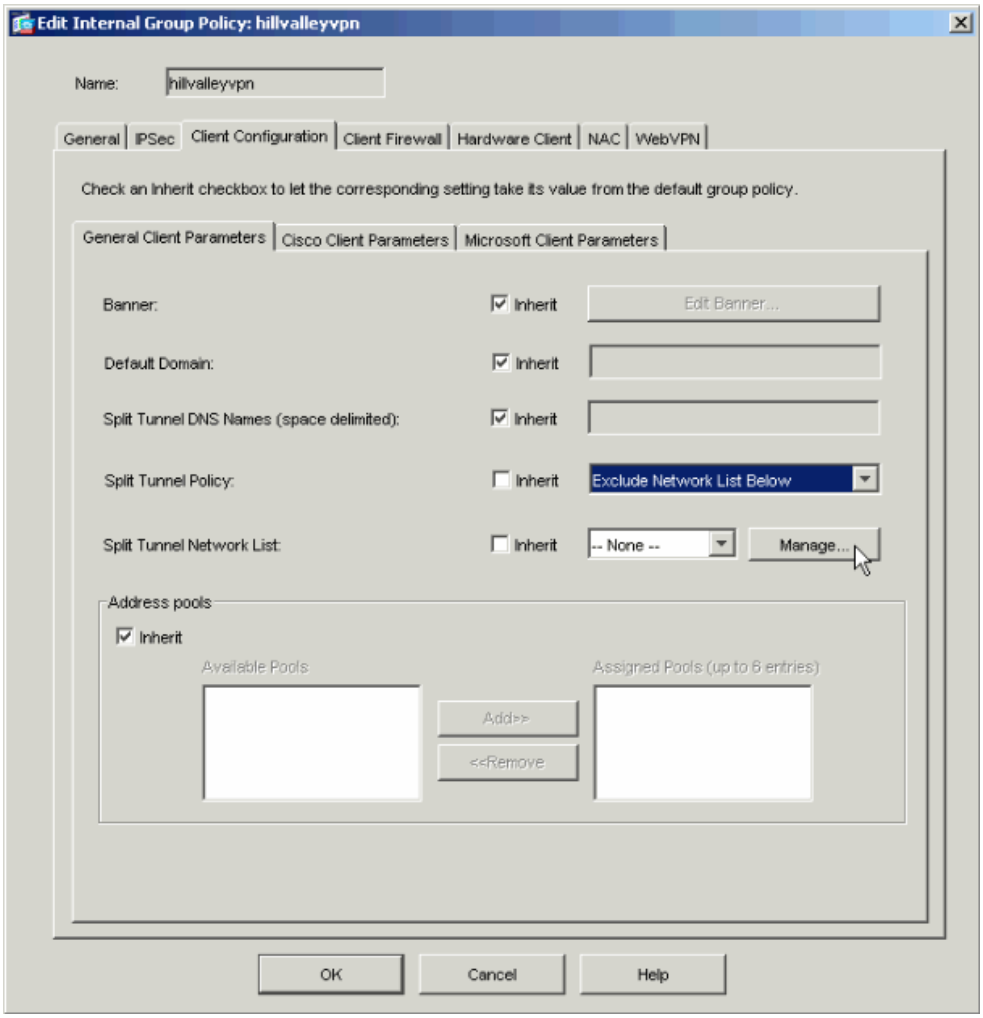
2. Перейдите на вкладку **Конфигурация клиента**.

2. 

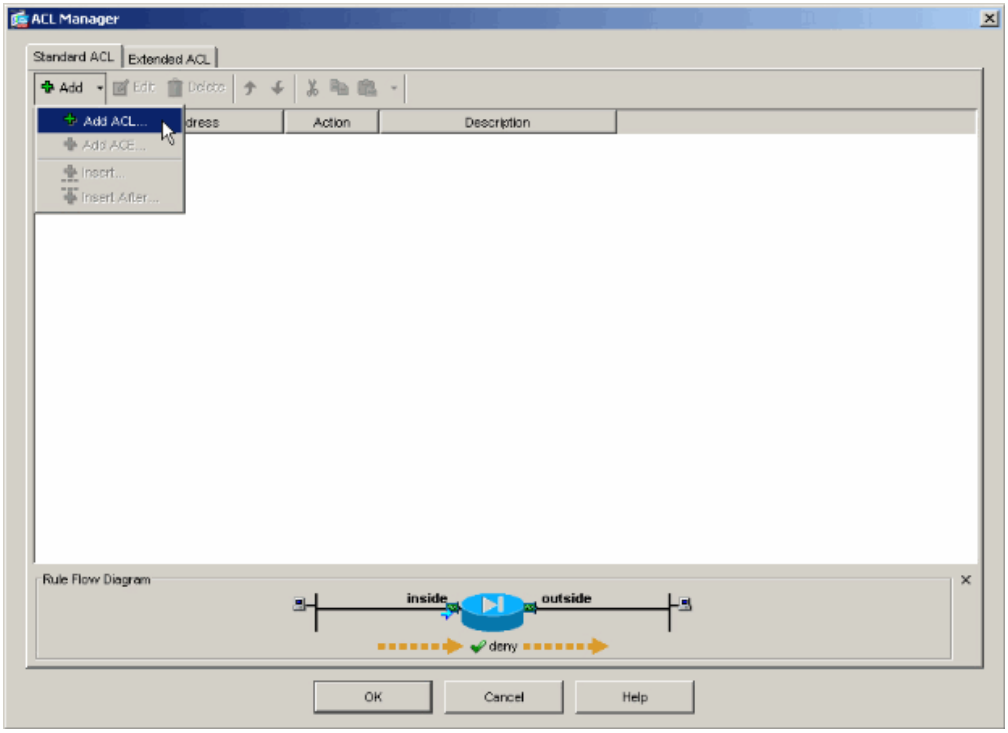
3. Снимите флажок **Наследование** для политики раздельного туннелирования и выберите **Исключить перечисленные ниже сети**.



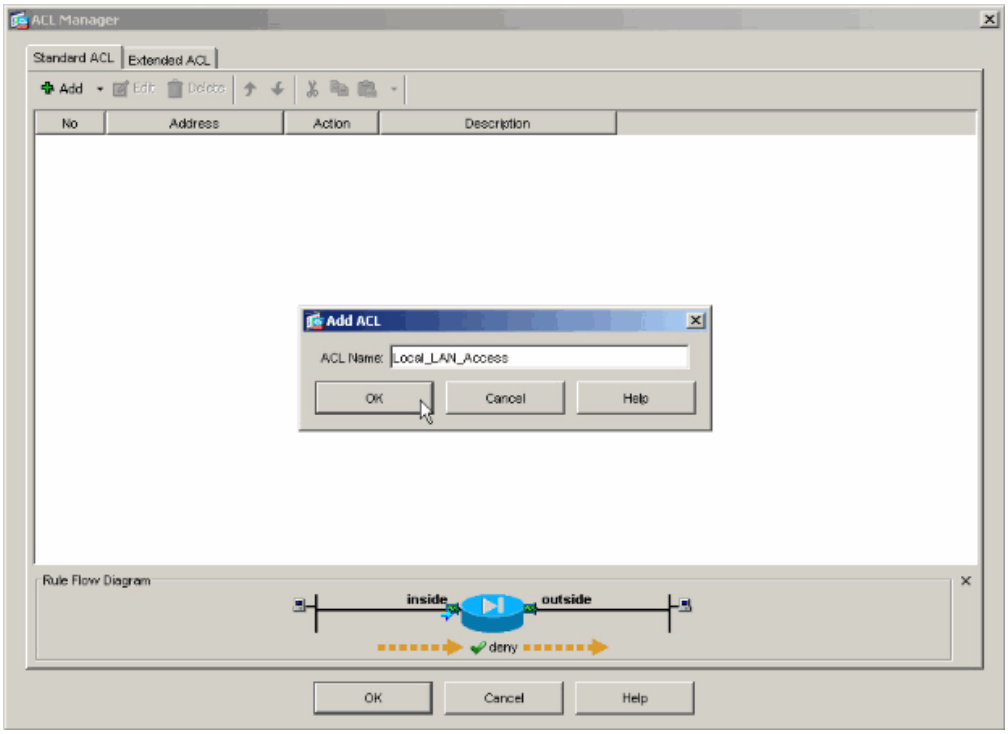
4. Снимите флажок **Наследование** для списка сетей с разделенными туннелями, затем нажмите кнопку **Контроль**, чтобы запустить диспетчер ACL.



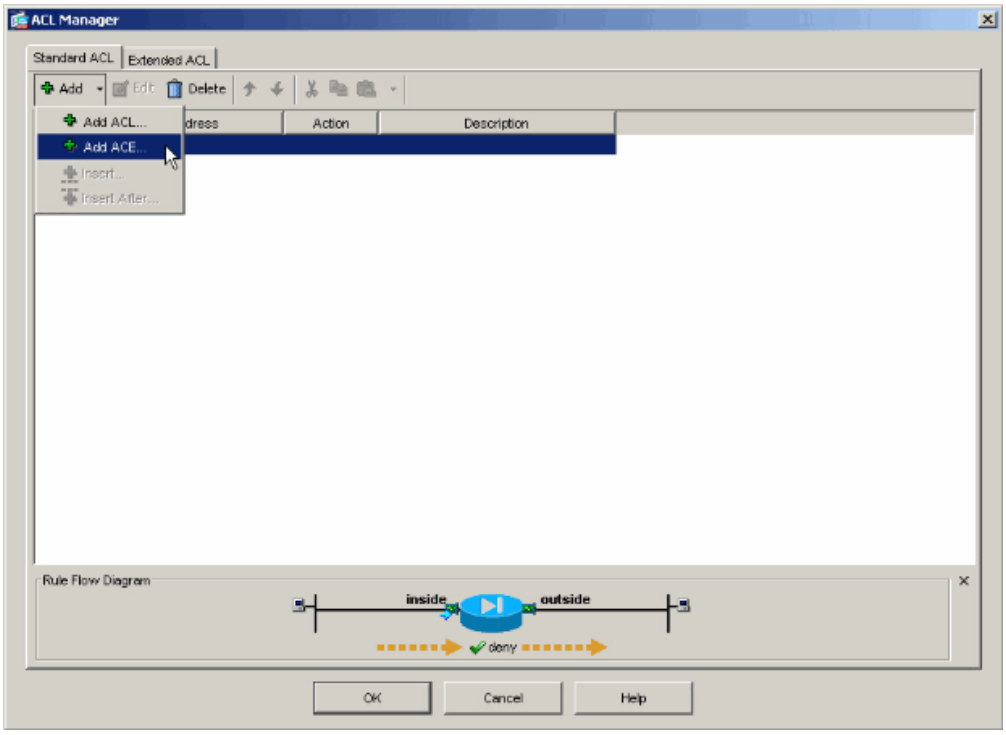
5. В данном диспетчере выберите **Добавить > Добавить список ACL...**, чтобы создать новый список контроля доступа.



6. Укажите имя для данного списка и нажмите кнопку **ОК**.

6. 

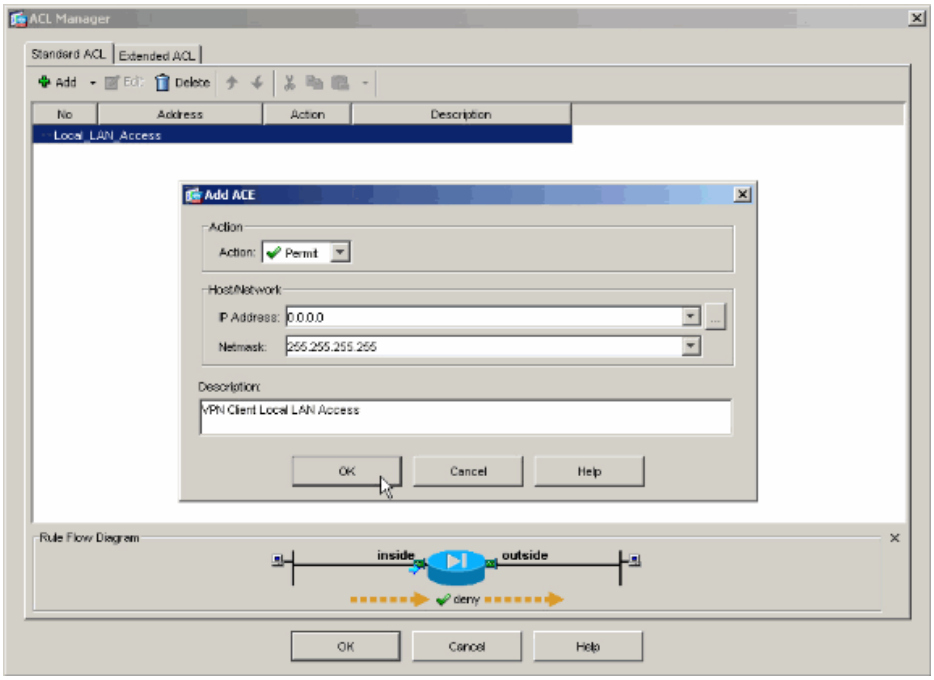
7. После создания списка ACL выберите **Добавить > Добавить ACE...**, чтобы добавить элемент контроля доступа (ACE).



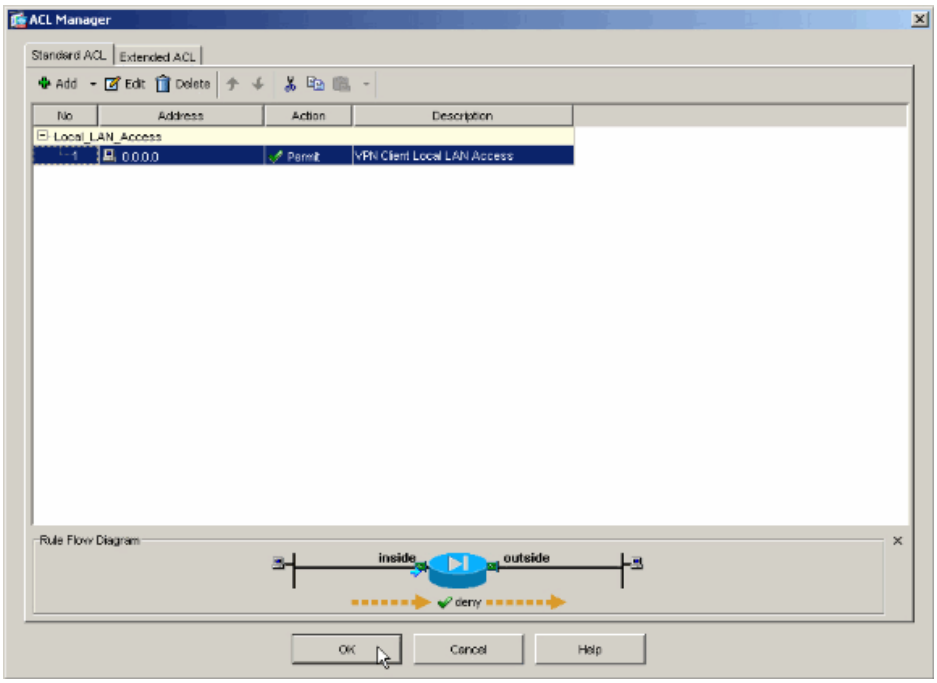
8. Определите элемент контроля доступа, соответствующий локальной сети клиента.

    1. Выберите **Разрешить**.
    2. Выберите IP-адрес **0.0.0.0**.
    3. Выберите маску сети **255.255.255.255**.
    4. Введите описание *(необязательно)*.
    5. Нажмите кнопку **ОК**.

5.

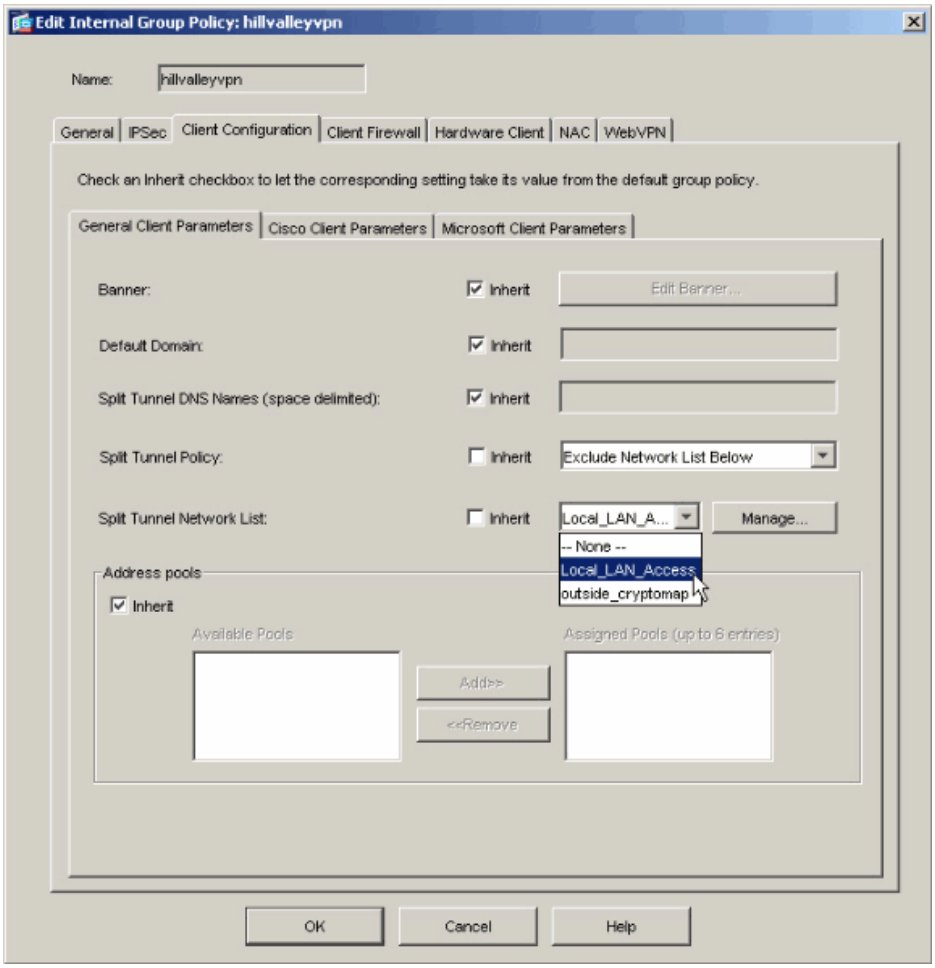


9. Нажмите кнопку **ОК**, чтобы завершить работу с диспетчером ACL.

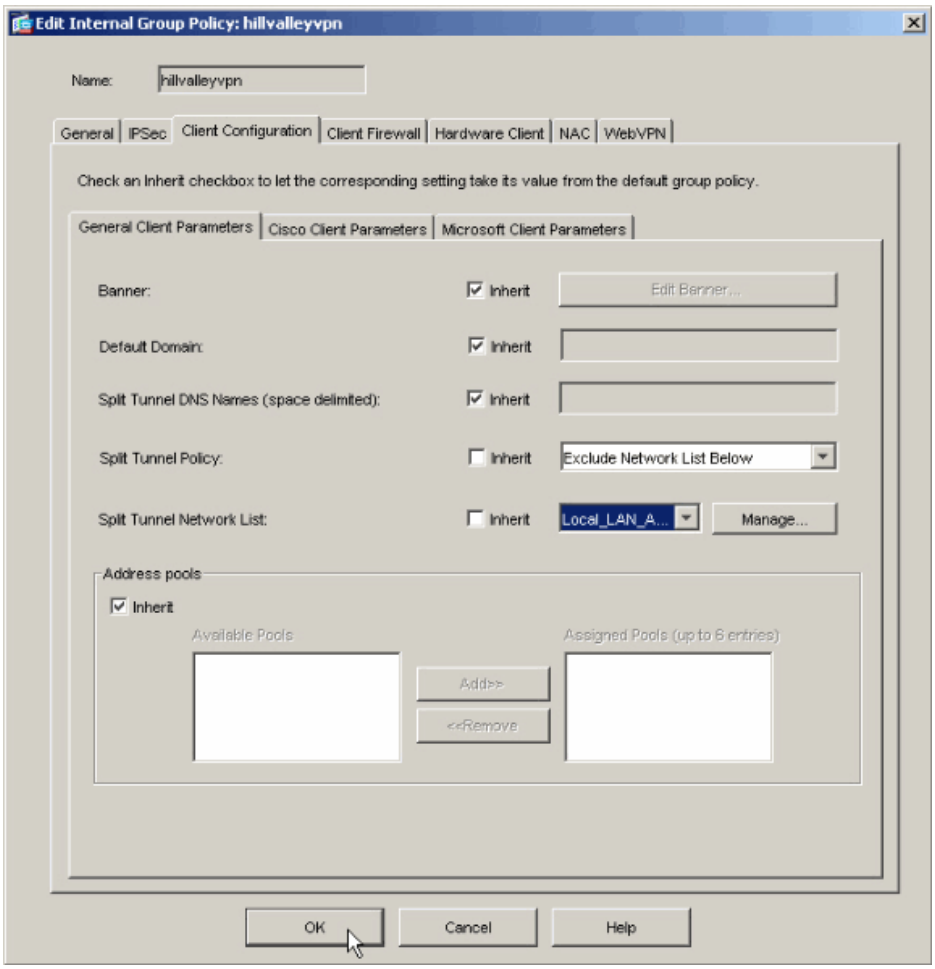


10. Убедитесь, что только что созданный ACL выбран для списка сетей с разделенными туннелями.

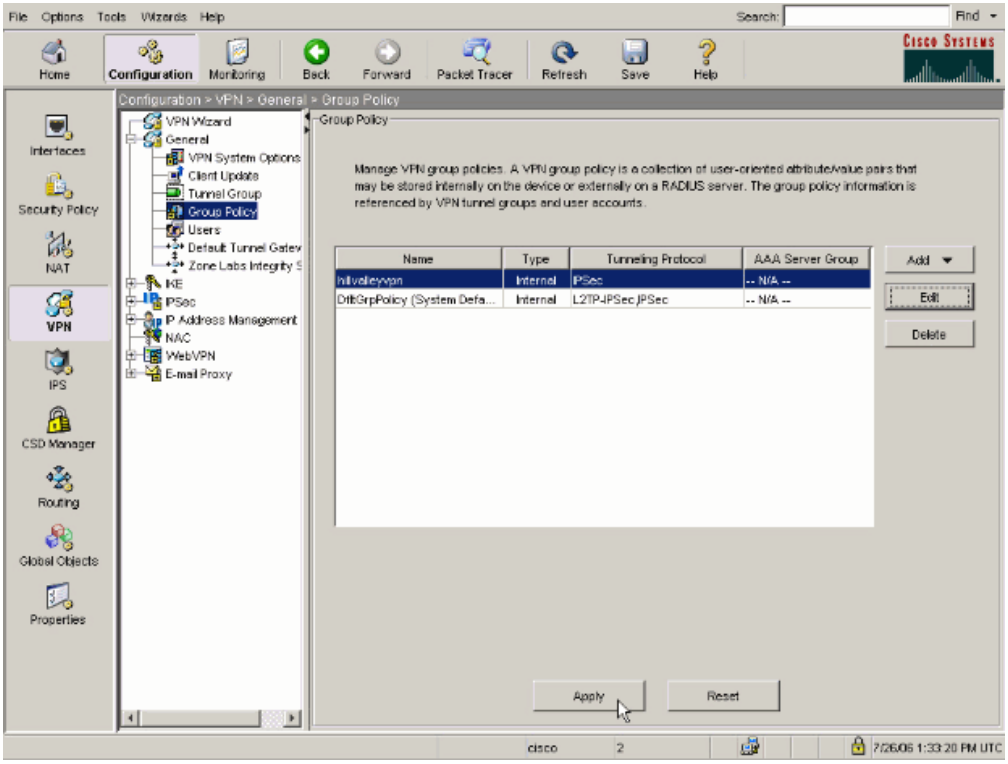
10.



11. Нажмите кнопку **ОК**, чтобы вернуться к настройке групповой политики.



12. Нажмите кнопку **Применить**, а затем — **Отправить** (при необходимости), чтобы отправить команды устройству ASA.

12. 

Настройка ASA с помощью интерфейса командной строки

Разрешить VPN-клиентам доступ к локальной сети при наличии подключения к ASA можно не только при помощи ASDM, но и посредством интерфейса командной строки устройства ASA.

1. Перейдите в режим конфигурирования.

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

2. Создайте список доступа, чтобы разрешить доступ к локальной сети.

```
ciscoasa(config)#access-list Local_LAN_Access remark VPN Client Local LAN Access
ciscoasa(config)#access-list Local_LAN_Access standard permit host 0.0.0.0
```

3. Перейдите в режим конфигурирования групповой политики, которую необходимо изменить.

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

4. Укажите политику раздельного туннелирования. В данном случае это политика **excludespecified**.

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

5. Укажите список доступа к разделенным туннелям. В данном случае это список **Local_LAN_Access**.

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

6. Выйдите из обоих режимов конфигурирования.

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

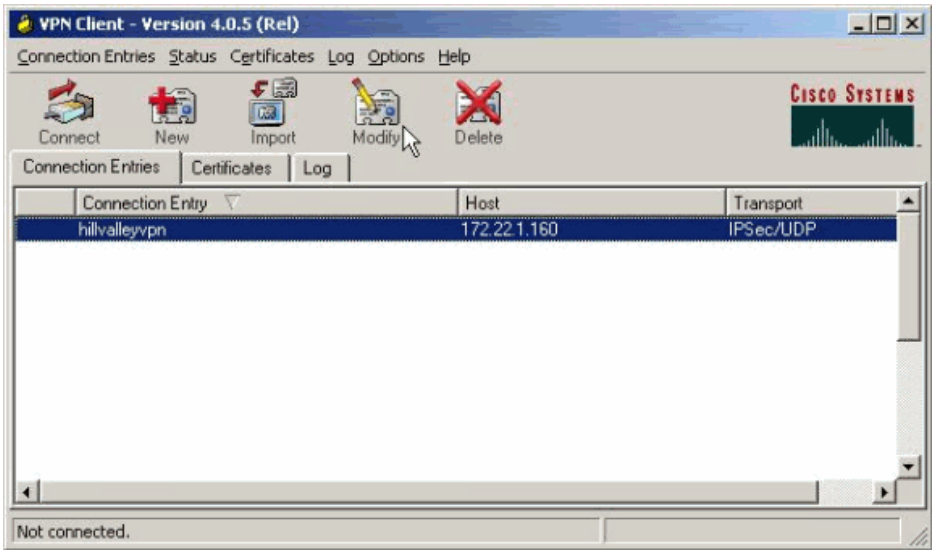
7. Сохраните конфигурацию в энергонезависимой ОЗУ (NVRAM) и нажмите клавишу **Ввод** при запросе ввода имени исходного файла.

```
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#
```

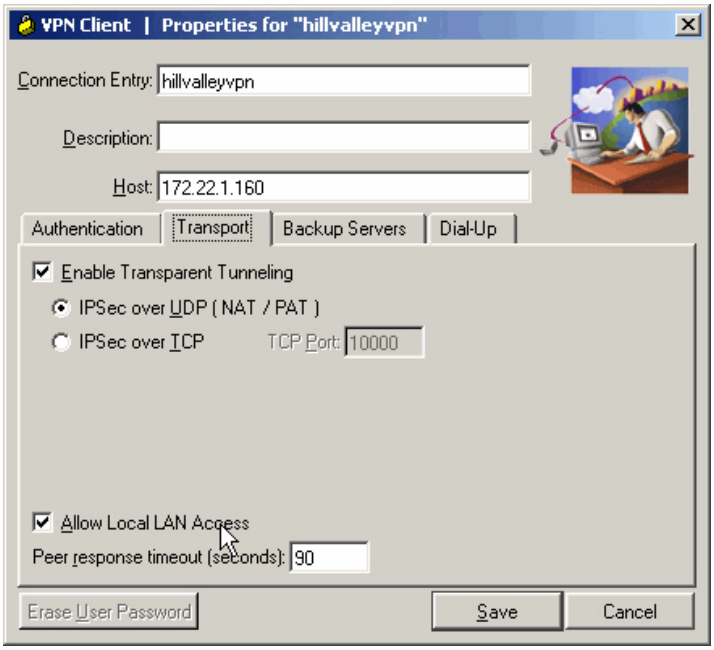
Настройка VPN-клиента

Для разрешения клиенту доступа к локальной сети при наличии подключения к ASA выполните в VPN-клиенте следующие действия.

1. Выберите запись существующего подключения и нажмите кнопку **Изменить**.



2. Перейдите на вкладку "Transport" (Транспорт) и установите флажок **Allow Local LAN Access** (Разрешить доступ к локальной сети). Затем нажмите кнопку **Сохранить**.



Проверка

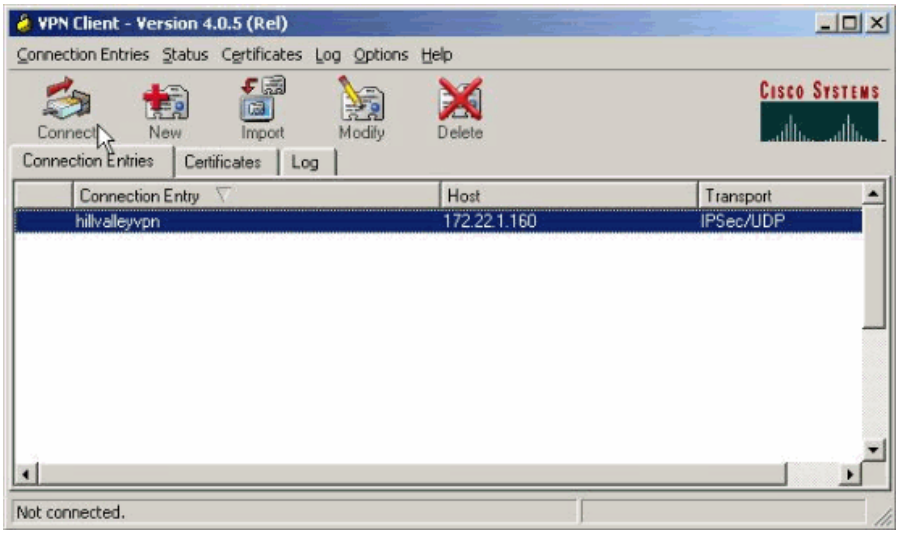
Выполните описанные в следующих разделах действия, чтобы проверить конфигурацию.

- Подключение с помощью VPN-клиента
- Просмотр журнала VPN-клиента
- Проверка доступа к локальной сети с помощью эхо-запроса

Подключение с помощью VPN-клиента

Для проверки своей конфигурации подключите VPN-клиент к VPN-концентратору.

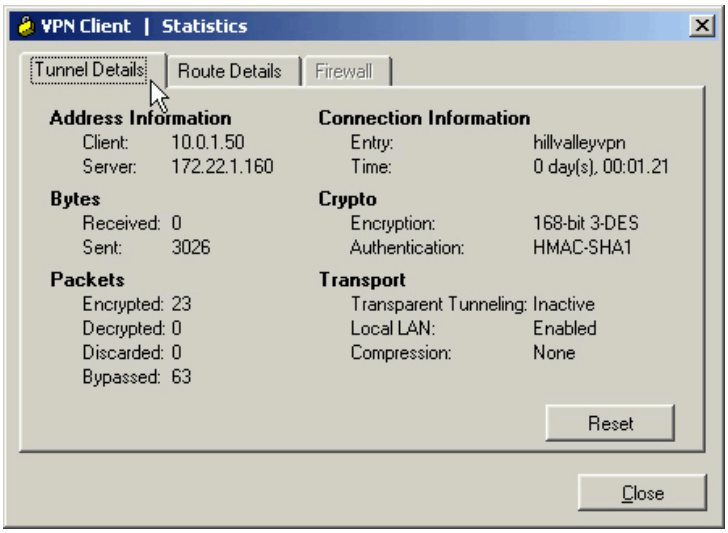
1. Выберите из списка запись своего соединения и нажмите кнопку **Подключиться**.



2. Введите учетные данные.

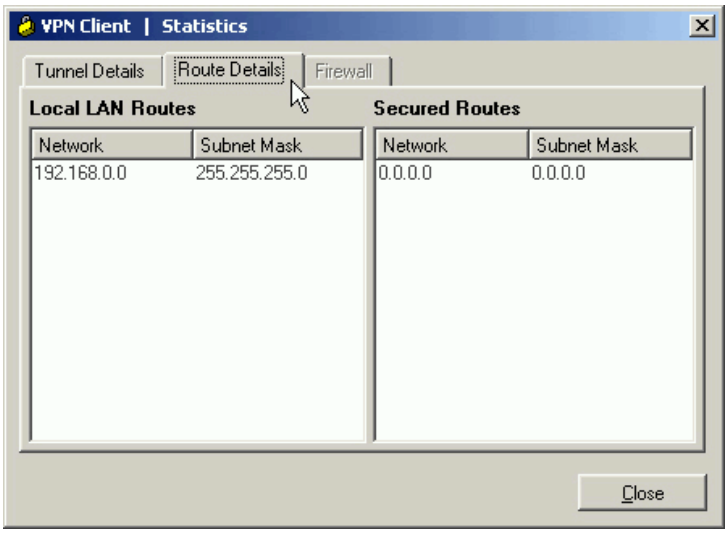
2. 

3. Выберите **Состояние > Статистика...**, чтобы открыть окно "Tunnel Details" (Сведения о туннелях), в котором отображаются подробные данные о туннеле и потоках трафика. Также в разделе "Transport" (Транспорт) можно увидеть, что локальная сеть включена.



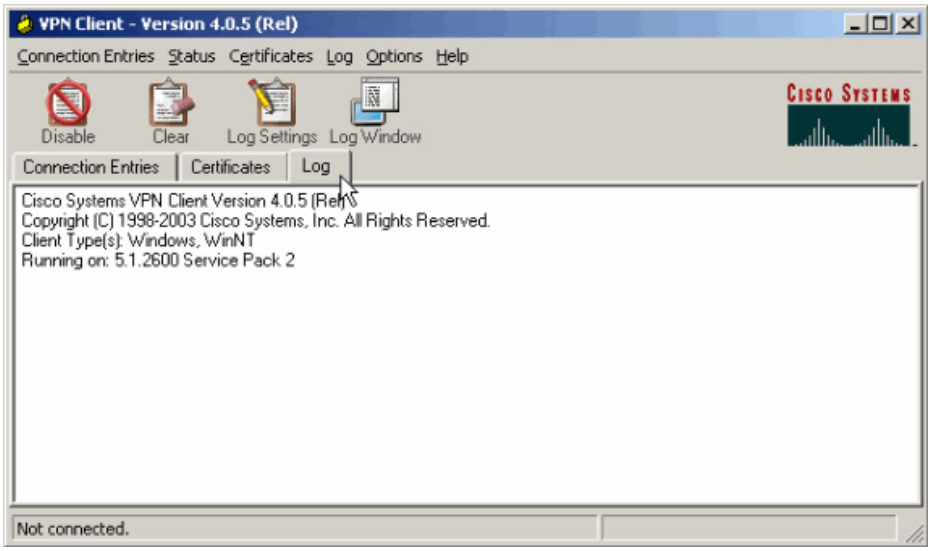
4. Перейдите на вкладку "Route Details" (Сведения о маршрутах), чтобы просмотреть маршруты, к которым у VPN-клиента сохраняется локальный доступ.

   В данном примере VPN-клиенту разрешен доступ к локальной сети по адресу 192.168.0.0/24, тогда как весь остальной трафик шифруется и отправляется через туннель.



Просмотр журнала VPN-клиента

При просмотре журнала VPN-клиента можно определить, установлен ли параметр, разрешающий доступ к локальной сети. Для просмотра журнала перейдите на вкладку "Log" (Журнал) в VPN-клиенте. Щелкните **Параметры журнала,** чтобы настроить элементы, регистрируемые в журнале. В данном примере параметру IKE задано значение **3- High** (3- высокий), всем остальным элементам журнала — **1 - Low** (1- низкий).




```
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
!--- Local LAN access is permitted and the local LAN is defined.

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

30     14:20:14.238  07/27/06  Sev=Info/5 IKE/0x6300000F
LOCAL_NET #1
subnet = 192.168.0.0
mask = 255.255.255.0
protocol = 0
src port = 0
dest port=0
!--- Output is supressed.
```

Проверка доступа к локальной сети с помощью эхо-запроса

Дополнительный способ проверки сохранения доступа VPN-клиента к локальной сети, при наличии туннеля к VPN-концентратору, состоит в использовании команды **ping** в командной строке Windows. Адрес локальной сети VPN-клиента — 192.168.0.0/24, в данной сети также 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

Невозможны печать или просмотр по имени

Когда VPN-клиент подключен и настроен для доступа к локальной сети, *распечатка или просмотр по имени* в данной сети невозможны. Имеется два пути обхода такой ситуации:

- Просмотреть или распечатать данные по IP-адресам.
  - Для просмотра вместо синтаксиса **\\общее_имя** используйте синтаксис **\\x.x.x.x**, где *x.x.x.x* — IP-адрес компьютера хоста.
  - Для печати настройте параметры сетевого принтера на использование IP-адреса вместо имени. Например, вместо синтаксиса **\\общее_имя\имя_принтера** укажите **\\x.x.x.x\имя_принтера**, где *x.x.x.x* — IP-адрес.
- Создайте или измените файл LMHOSTS VPN-клиента. Файл LMHOSTS на ПК Windows позволяет создавать статические сопоставления между именами узлов и IP-адресами. Например, файл LMHOSTS может иметь следующее содержание.

  ```
  192.168.0.3 SERVER1
  192.168.0.4 SERVER2
  192.168.0.5 SERVER3
  ```

  В Windows XP Professional Edition файл LMHOSTS находится в папке **%SystemRoot%\System32\Drivers\Etc**. Дополнительные сведения см. в документации Microsoft или в статье базы знаний Microsoft 314108 .

Дополнительные сведения

- **Пример настройки PIX/ASA7.x в качестве удаленного VPN-сервера с помощью ASDM**
- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/105413/local-lan-pix-asa.shtml