Пример конфигурации PIX/ASA 7.x с тремя внутренними сетями

Содержание

Общие сведения

В данном документе приведен пример конфигурации для PIX Security Appliance версии 7.x или Adaptive Security Appliance (ASA) 5500 с тремя внутренними сетями при помощи интерфейса командной строки (CLI) или Adaptive Security Device Manager (ASDM) версии 5.x. Для упрощения используются статические маршруты.

Примечание. Некоторые параметры в ASDM начиная с версии 5.2 могут отличаться от параметров ASDM 5.1. Дополнительные сведения см. в документе Документация ASDM.

Предварительные условия

Требования

При добавлении более одной внутренней сети, которые находятся за брандмауэром PIX, необходимо помнить следующее:

- PIX не может маршрутизировать пакеты;
- PIX не поддерживает вторичную адресацию;
- За PIX необходимо использовать маршрутизатор, который будет обеспечивать маршрутизацию между имеющейся сетью и вновь добавляемой сетью;
- Шлюзом по умолчанию для всех узлов должен быть внутренний маршрутизатор;
- На внутреннем маршрутизаторе добавьте маршрут по умолчанию, который указывает на PIX;
- Удалите кэш протокола разрешения адресов (ARP) на внутреннем маршрутизаторе.

Чтобы позволить ASDM настроить устройство, см. Разрешение ASDM доступа по HTTPS.

Используемые компоненты

Сведения, содержащиеся в данном документе, приведены на основе следующих версий программного и аппаратного обеспечения:

- PIX Security Appliance 515E с ПО версии 7.1;
- ASDM 5.1;
- Маршрутизаторы Cisco с программным обеспечением Cisco IOS® Release 12.3(7)T.

Примечание. Хотя конфигурация, описанная в данном документе, проверялась на PIX Security Appliance, она также совместима с ASA 5500.

Данные для документа были получены в специально созданных лабораторных условиях. При написании данного документа использовались только устройства с пустой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд.

Другая продукция этого типа

Данную конфигурацию также можно использовать с Cisco ASA Security Appliance версии 7.x.

Условные обозначения

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

Настройка

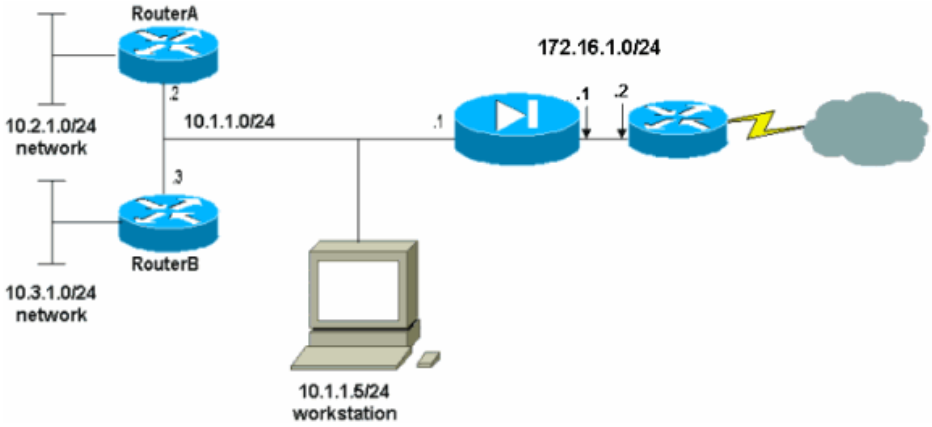
В этом разделе приводятся сведения о настройке функций, описанных в данном документе.

Примечание. Для поиска дополнительной информации о командах в данном документе используйте служебную программу. Command Lookup (только для зарегистрированных пользователей).

Схемы IP-адресации, которые использованы в данной конфигурации, не допускаются для законной маршрутизации в Интернете. Это адреса RFC 1918 , которые использовались в лабораторной среде.

Схема сети

В данном документе используется следующая конфигурация сети:



Шлюзом по умолчанию для узлов сети 10.1.1.0 является маршрутизатор RouterA. В маршрутизаторе RouterB добавлен маршрут по умолчанию, который указывает на RouterA. У маршрутизатора RouterA есть маршрут по умолчанию, который указывает на внутренний интерфейс PIX.

Конфигурации

В данном документе используются следующие конфигурации:

- Конфигурация RouterA;
- Конфигурация RouterB;
- Конфигурация PIX Security Appliance 7.1.
    - Начальная загрузка и настройка PIX Security Appliance ASDM 5.1 посредством графического интерфейса пользователя
    - Настройка PIX Security Appliance посредством интерфейса командной строки

Конфигурация RouterA

```
RouterA#show running-config
Building configuration...

Current configuration : 1151 bytes
!
version 12.3
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname RouterA
!

interface Ethernet2/0
ip address 10.2.1.1 255.255.255.0
half-duplex
!

interface Ethernet2/1
ip address 10.1.1.2 255.255.255.0
half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.1
ip route 10.3.1.0 255.255.255.0 10.1.1.3
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterA#
```

Конфигурация RouterB

```
RouterB#show running-configBuilding configuration...Current configuration : 1132 bytes
!
version 12.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!
hostname RouterB
!

interface FastEthernet0/0
ip address 10.1.1.3 255.255.255.0
speed auto
!

interface Ethernet1/0
ip address 10.3.1.1 255.255.255.0
half-duplex
!
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
RouterB#
```

Если для настройки PIX Security Appliance необходимо использовать ASDM, но начальная загрузка устройства не произведена, выполните следующие действия.

1. Войдите в консоль PIX.
2. Из очищенной конфигурации используйте интерактивные запросы, позволяющие включить ASDM для управления PIX с рабочей станции 10.1.1.5.

Конфигурация PIX Security Appliance 7.1

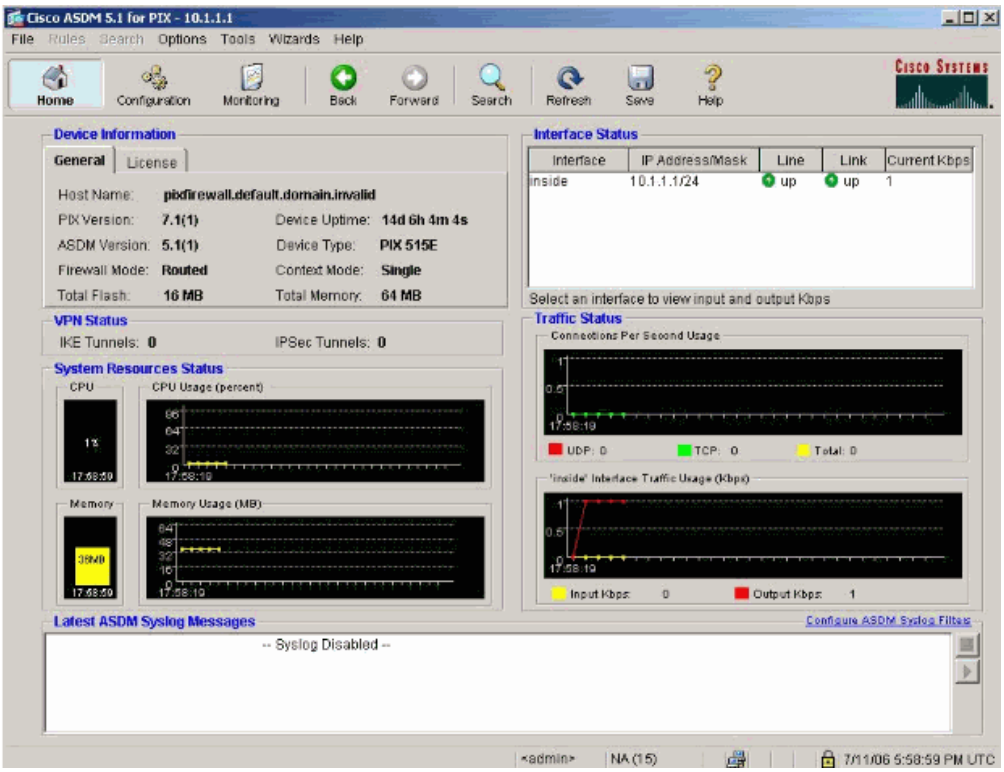
```
Pre-configure Firewall now through interactive prompts [yes]? yesFirewall Mode [Routed]:
Enable password [<use current password>]: cisco
Allow password recovery [yes]?
Clock (UTC):
 Year [2005]:
 Month [Mar]:
 Day [15]:
 Time [05:40:35]: 14:45:00
Inside IP address: 10.1.1.1
Inside network mask: 255.255.255.0
Host name: OZ-PIX
Domain name: cisco.com
IP address of host running Device Manager: 10.1.1.5

The following configuration will be used:
        Enable password: cisco
        Allow password recovery: yes
        Clock (UTC): 14:45:00 Mar 15 2005
        Firewall Mode: Routed
        Inside IP address: 10.1.1.1
        Inside network mask: 255.255.255.0
        Host name: OZ-PIX
        Domain name: cisco.com
        IP address of host running Device Manager: 10.1.1.5

Use this configuration and write to flash? yes
        INFO: Security level for "inside" set to 100 by default.
        Cryptochecksum: a0bff9bb aa3d815f c9fd269a 3f67fef5

965 bytes copied in 0.880 secs
        INFO: converting 'fixup protocol dns maximum-length 512' to MPF commands
        INFO: converting 'fixup protocol ftp 21' to MPF commands
        INFO: converting 'fixup protocol h323_h225 1720' to MPF commands
        INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands
        INFO: converting 'fixup protocol netbios 137-138' to MPF commands
        INFO: converting 'fixup protocol rsh 514' to MPF commands
        INFO: converting 'fixup protocol rtsp 554' to MPF commands
```

```
        INFO: converting 'fixup protocol sip 5060' to MPF commands
        INFO: converting 'fixup protocol skinny 2000' to MPF commands
        INFO: converting 'fixup protocol smtp 25' to MPF commands
        INFO: converting 'fixup protocol sqlnet 1521' to MPF commands
        INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands
        INFO: converting 'fixup protocol tftp 69' to MPF commands
        INFO: converting 'fixup protocol sip udp 5060' to MPF commands
        INFO: converting 'fixup protocol xdmcp 177' to MPF commands

Type help or '?' for a list of available commands.
        OZ-PIX>
```

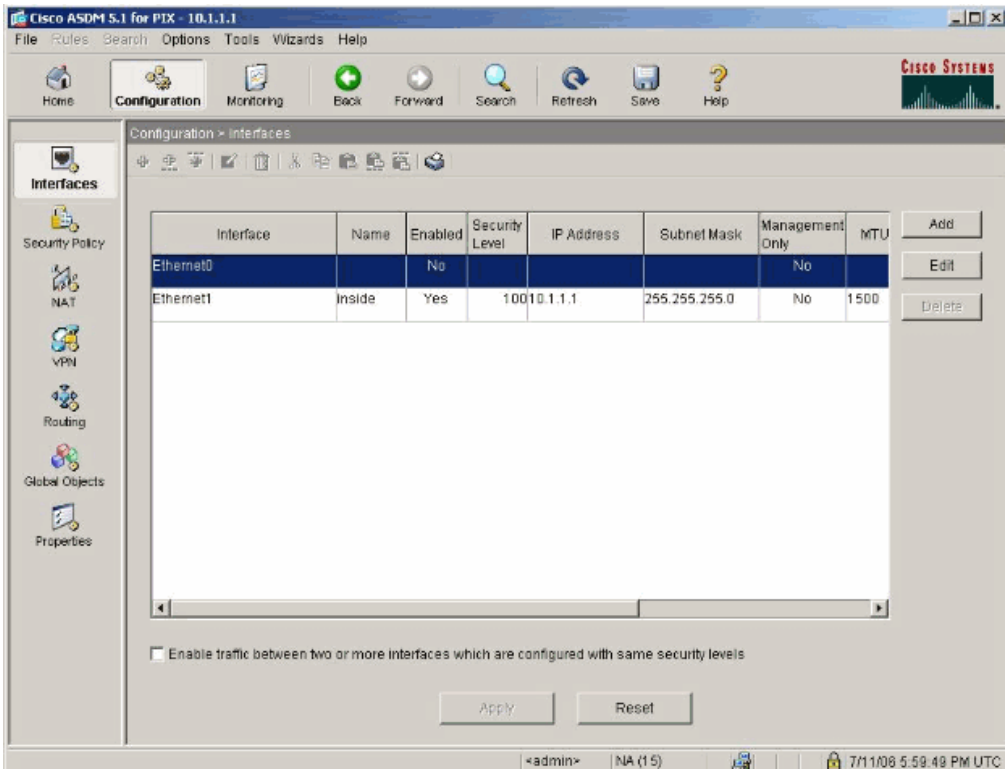
Начальная загрузка и настройка PIX Security Appliance ASDM 5.1 посредством графического интерфейса пользователя

Для настройки при помощи графического интерфейса пользователя ASDM выполните следующие действия.

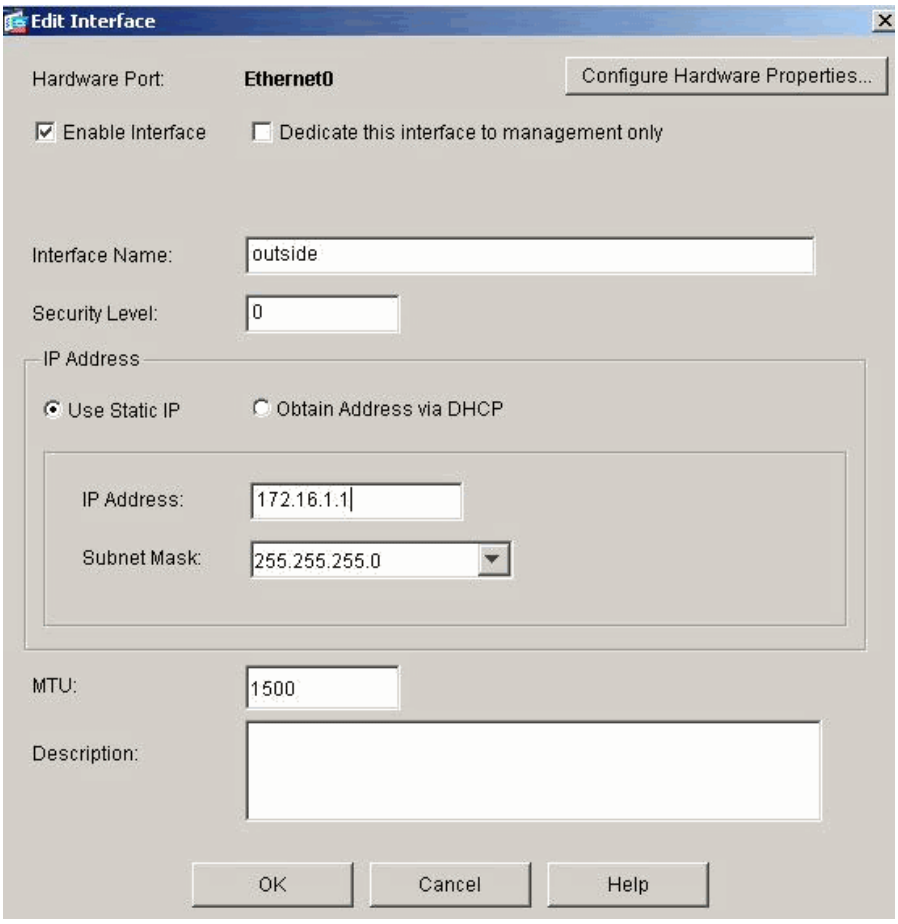
1. На рабочей станции 10.1.1.5 откройте веб-браузер, чтобы воспользоваться ADSM (в данном примере https://10.1.1.1).
2. При запросе сертификата нажмите кнопку **yes**.
3. Войдите с настроенным ранее паролем режима включения.
4. Если это первый запуск ASDM на ПК, будет выдан запрос на использование ASDM Launcher или использование ASDM в качестве Java-приложения. В данном примере выбирается и устанавливается ASDM Launcher.
5. Перейдите на страницу Home ASDM и нажмите кнопку **Configuration**.



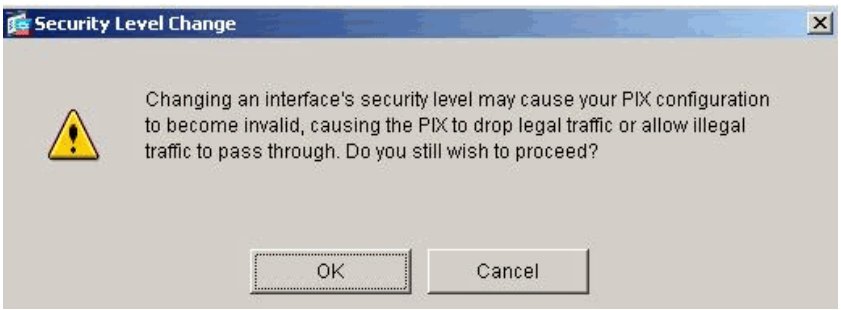
6. Чтобы настроить внешний интерфейс, выберите **Interface > Edit**.



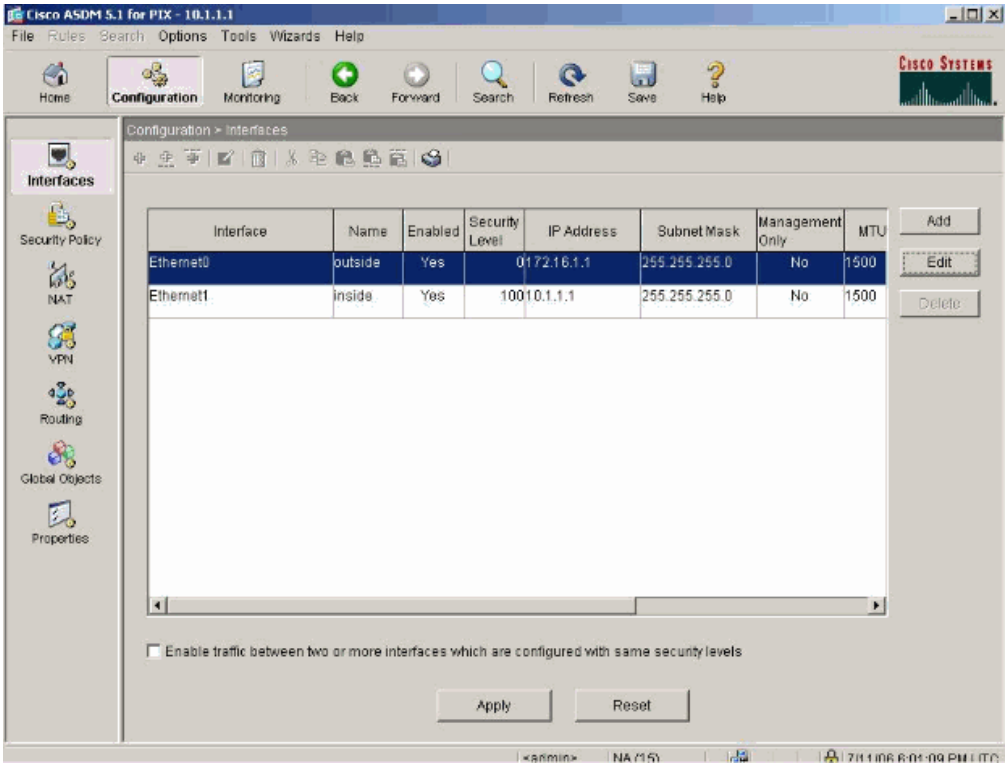
7. Введите все данные интерфейса и после завершения нажмите кнопку **OK**.



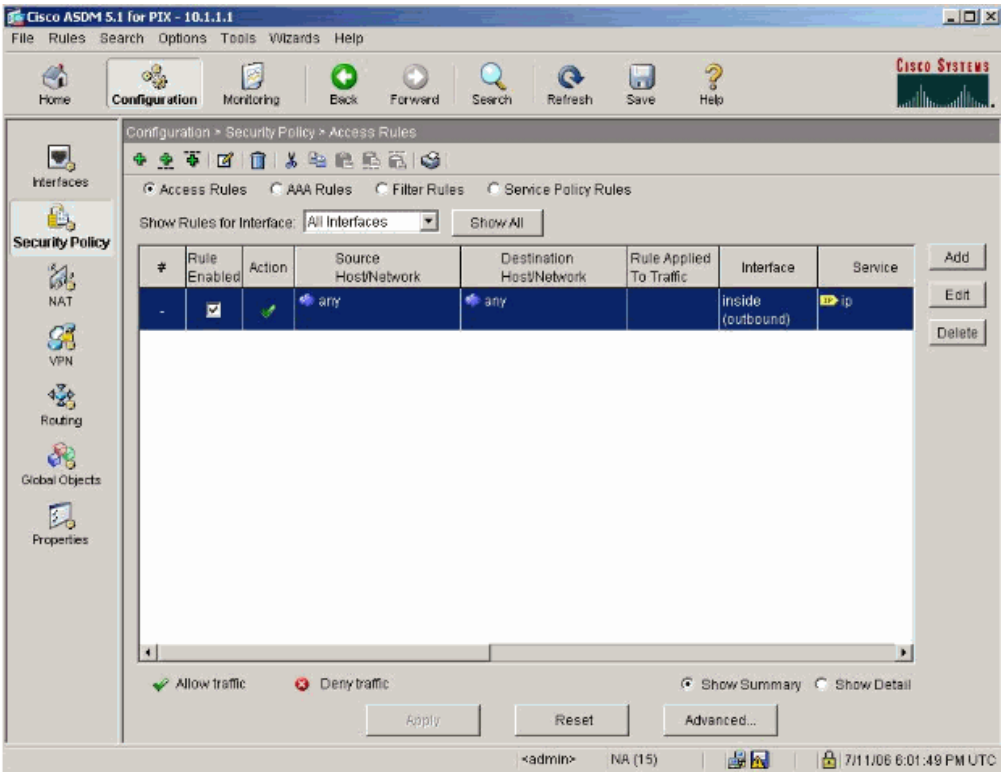
8. В диалоговом окне Security Level Change нажмите кнопку **OK**.



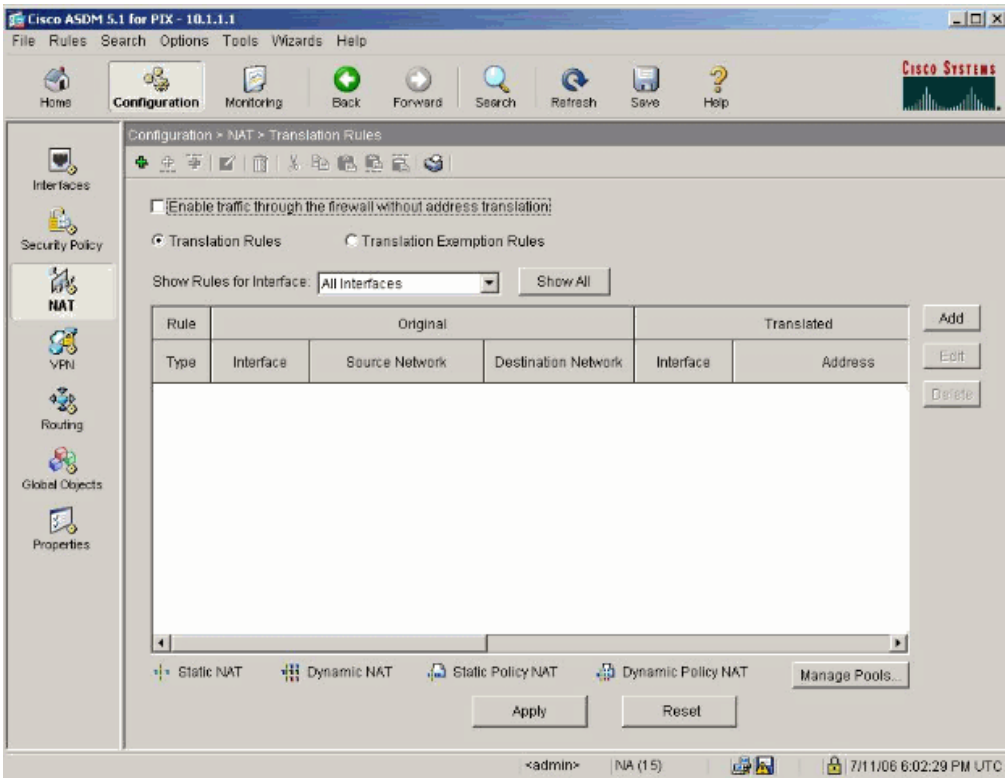
9. Чтобы сохранить конфигурацию интерфейса, нажмите кнопку **Apply**. При этом конфигурация загружается в PIX.



10. Во вкладке Features выберите **Security Policy**, чтобы просмотреть используемое правило политики безопасности. В данном примере используется внутреннее правило по умолчанию.

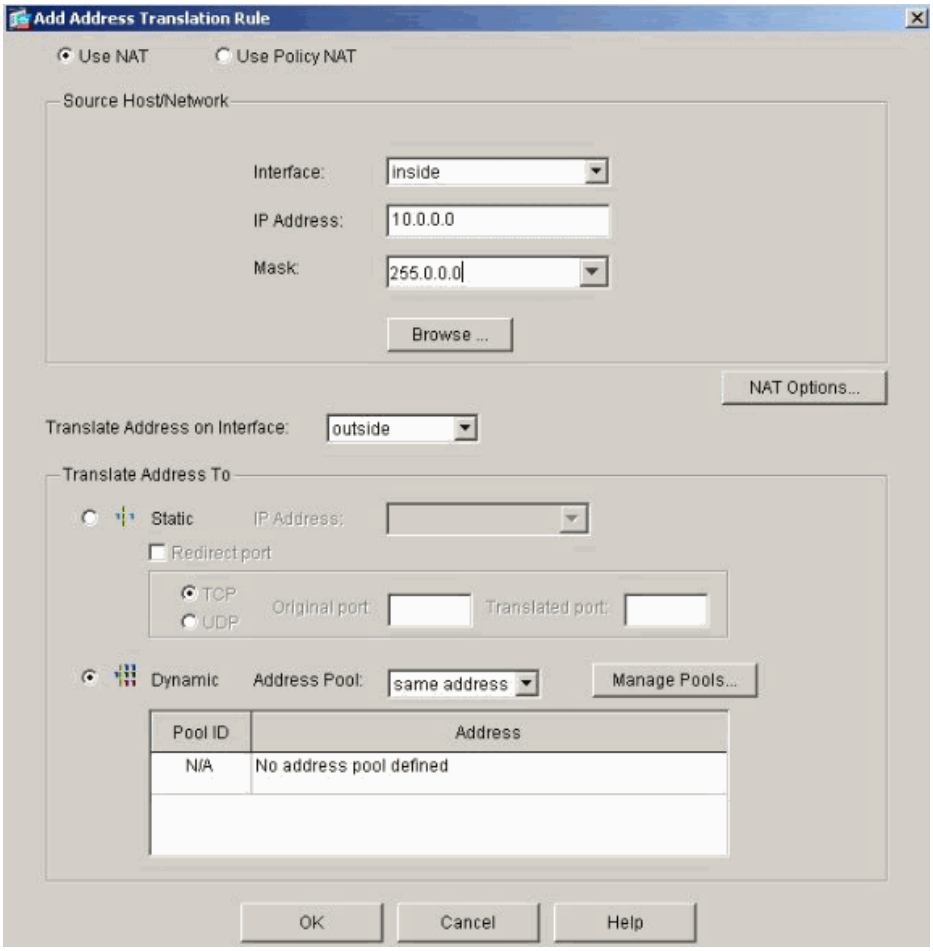


11. В данном примере используется NAT. Чтобы настроить правило NAT, снимите флажок **Enable traffic through the firewall without address translation (включить трафик через брандмауэр без преобразования адреса)** и нажмите кнопку **Add**.

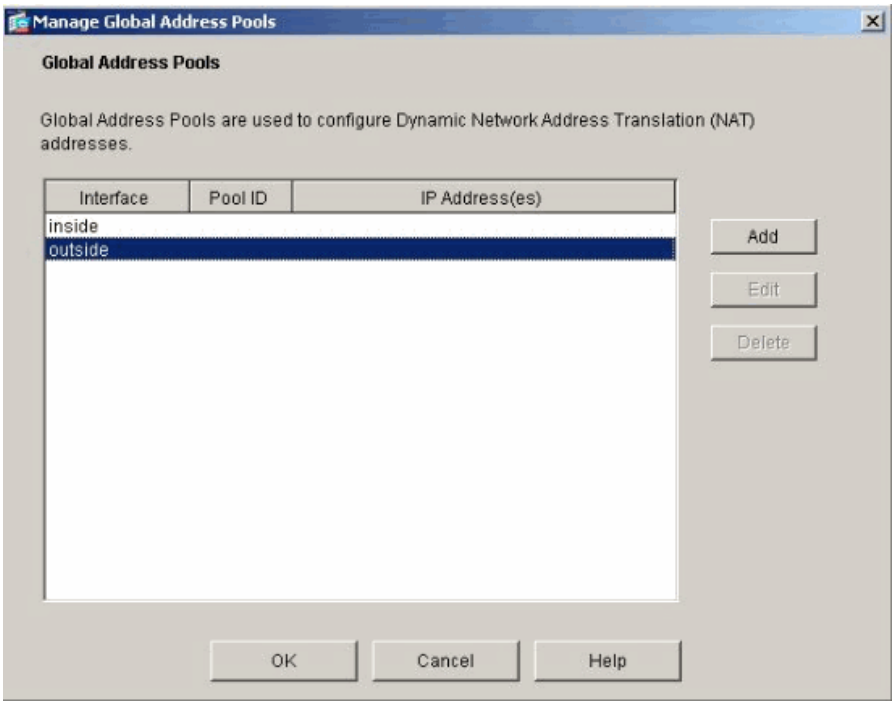


12. Настройте Source Network (сеть-источник). В данном примере в качестве IP-адреса используется 10.0.0.0, а в качестве маски используется 255.0.0.0.

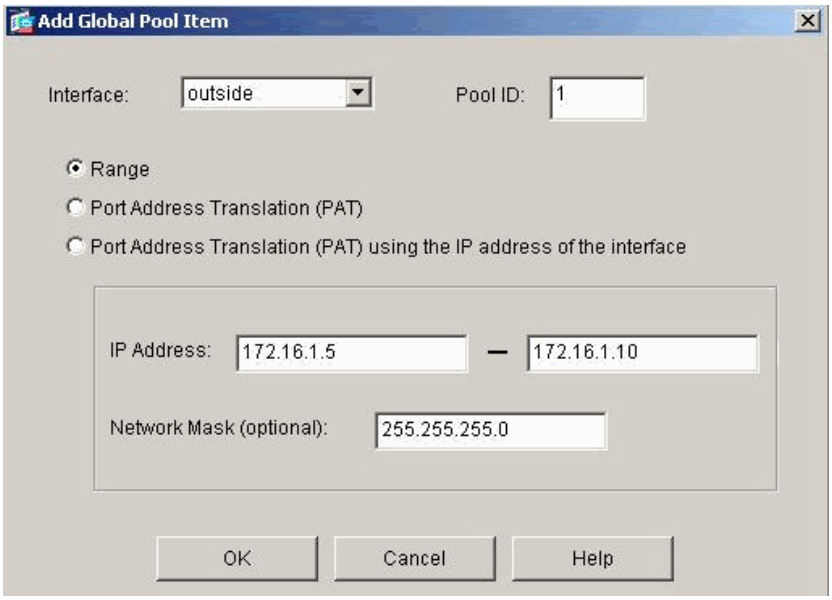
    Чтобы задать пул адресов NAT, нажмите кнопку **Manage Pools**.



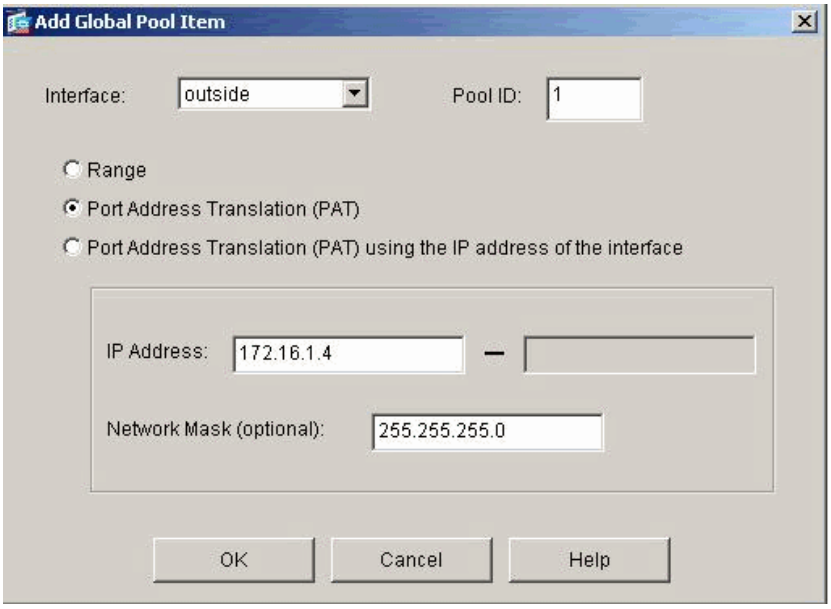
13. Выберите внешний интерфейс и нажмите кнопку **Add**.



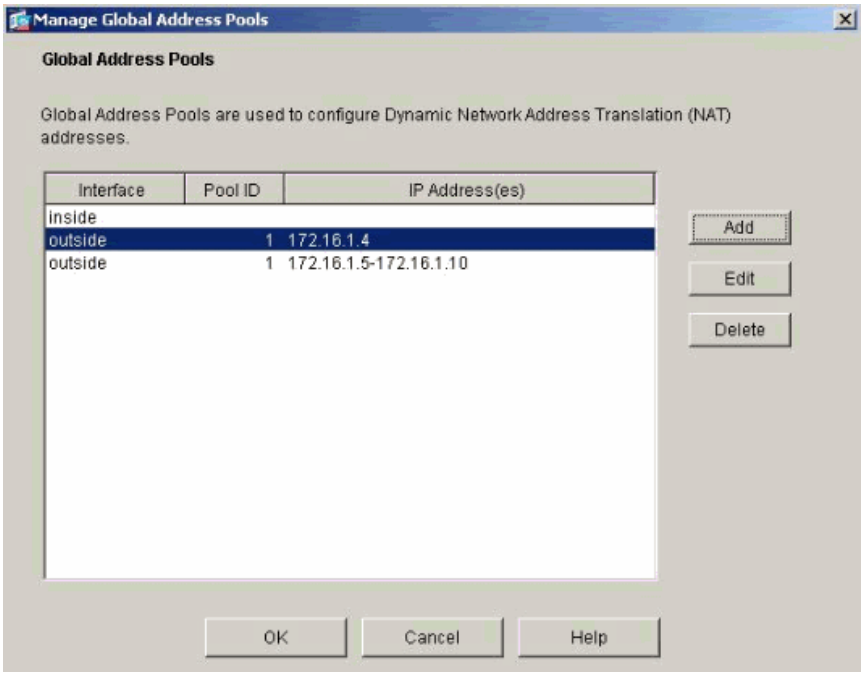
14. В данном примере настраиваются пулы адресов Range и PAT. Настройте диапазон пула адресов NAT и нажмите кнопку **OK**.



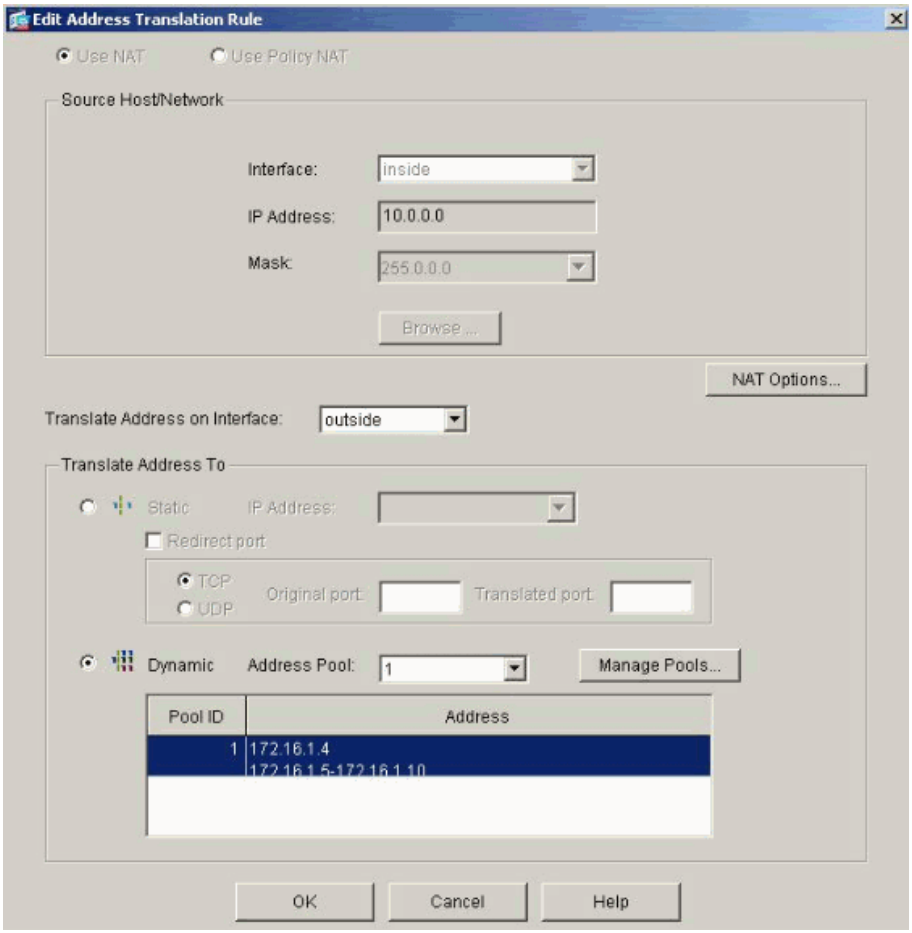
15. Чтобы настроить адрес PAT, выберите внешний интерфейс шага 13. нажмите кнопку **OK**



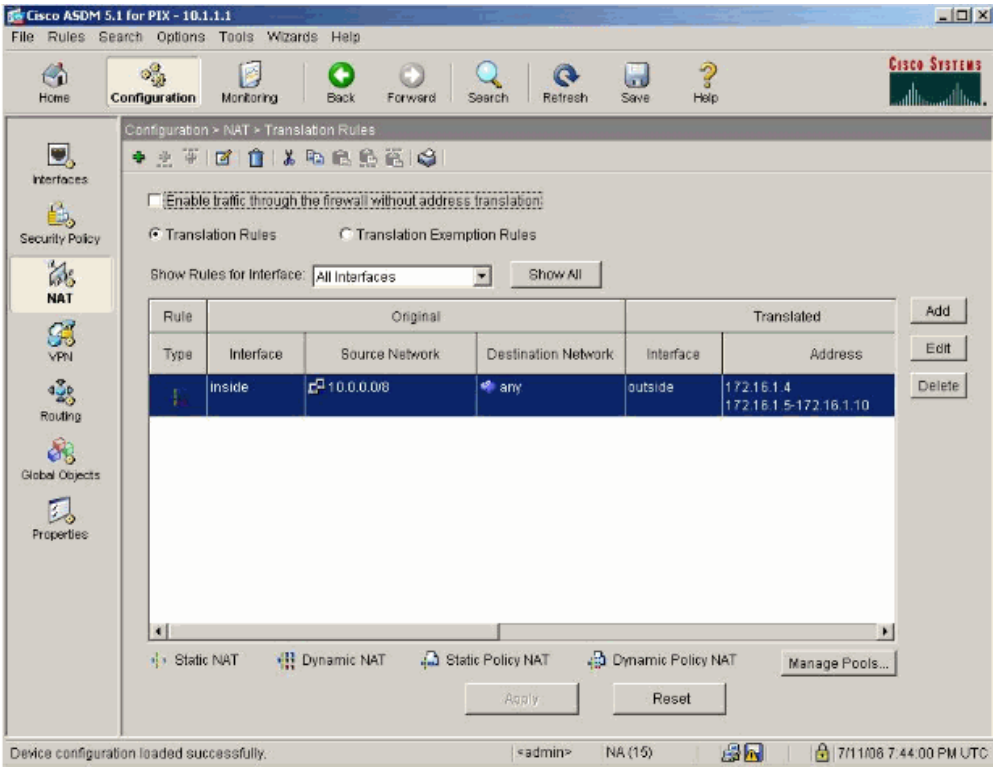
Для продолжения нажмите кнопку **OK**.



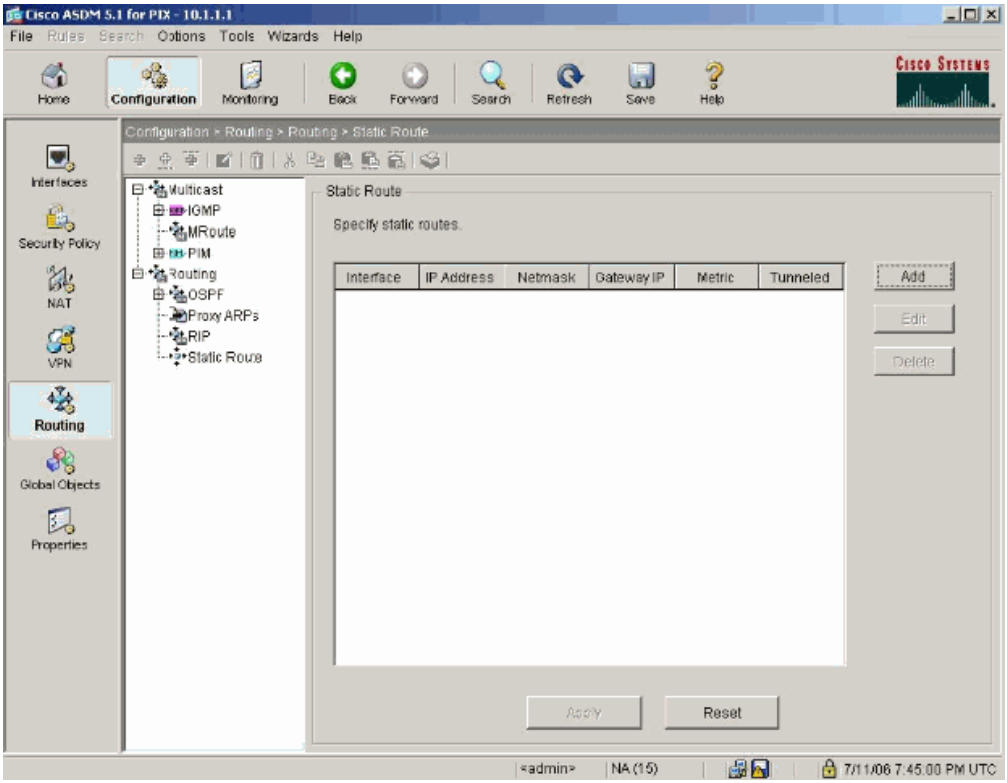
16. В окне Edit Address Translation Rule выберите идентификатор пула Pool ID, который будет использоваться настроенной сетью-источником. нажмите кнопку **OK**.



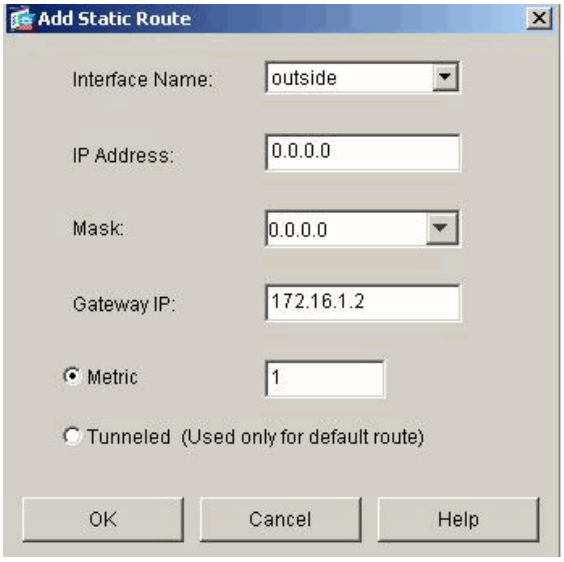
17. Чтобы загрузить настроенное правило NAT в PIX, нажмите кнопку **Apply**.



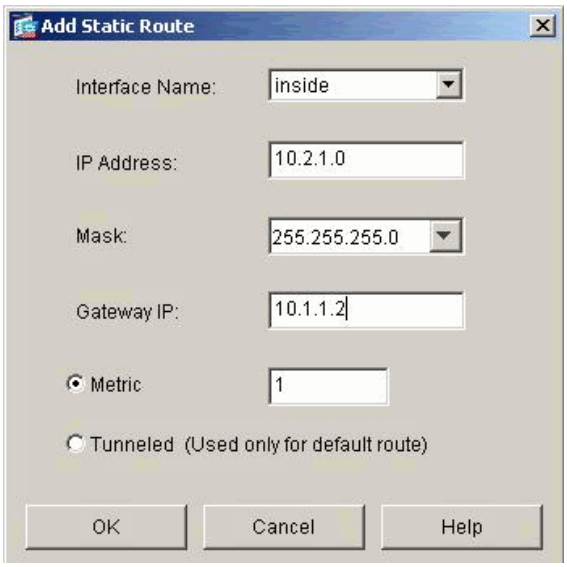
18. В данном примере используются статические маршруты. нажмите кнопку **Routing**, выберите **Static Route** и нажмите кнопку **Add**.



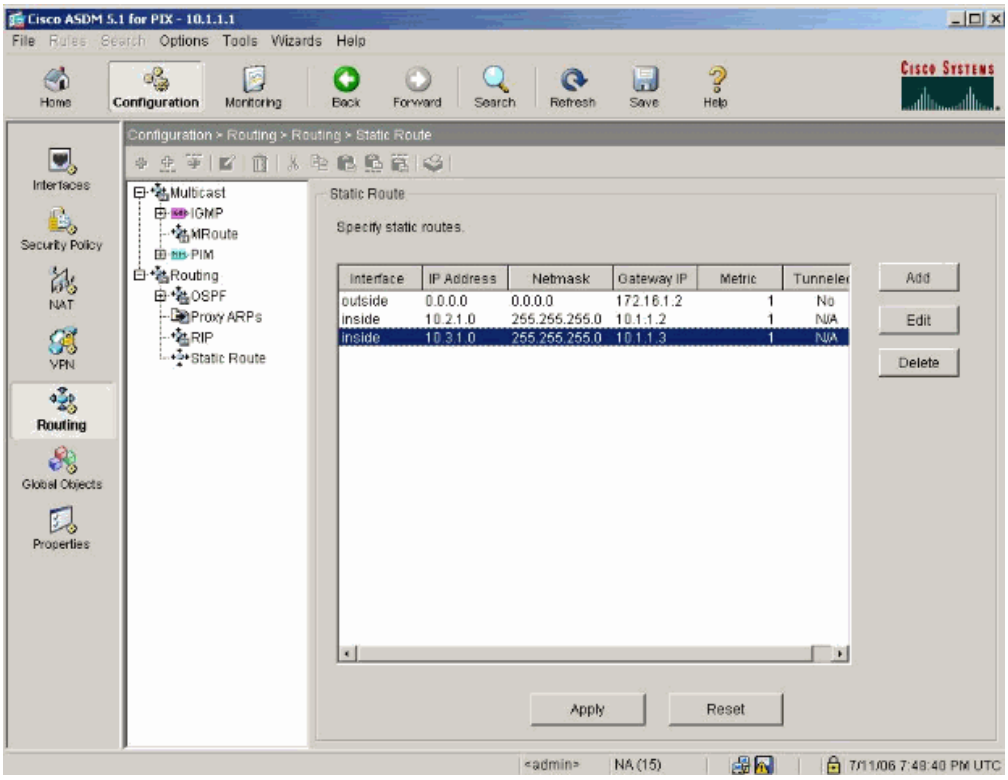
19. Настройте маршрутизатор по умолчанию и нажмите кнопку **OK**.



20. Нажмите кнопку **Add** и добавьте маршруты к внутренним сетям.



21. Подтвердите правильность настройки маршрутов и нажмите кнопку **Apply**.



Настройка при помощи графического интерфейса пользователя ASDM завершена.

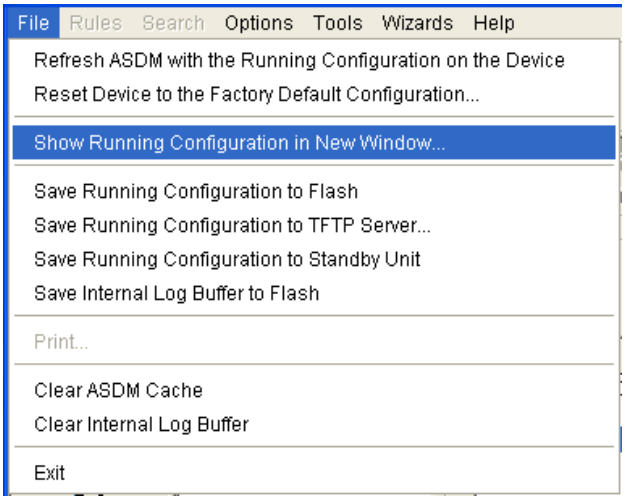
Данную конфигурацию можно просмотреть при помощи интерфейса командной строки:

Интерфейс командной строки PIX Security Appliance

```
pixfirewall(config)#write terminalPIX Version 7.0(0)102
names
!

interface Ethernet0
nameif outside
security-level 0

ip address 172.16.1.1 255.255.255.0
!

interface Ethernet1
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname OZ-PIX
domain-name cisco.com
ftp mode passive
pager lines 24
mtu inside 1500
mtu outside 1500
no failover
monitor-interface inside
monitor-interface outside
asdm image flash:/asdmfile.50073
no asdm history enable
arp timeout 14400

nat-control

global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
global (outside) 1 172.16.1.4 netmask 255.255.255.0
nat (inside) 1 10.0.0.0 255.0.0.0
route inside 10.3.1.0 255.255.255.0 10.1.1.3 1
route inside 10.2.1.0 255.255.255.0 10.1.1.2 1

route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 sunrpc 0:10:00
  h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00
  sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 10.1.1.5 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
telnet timeout 5
ssh timeout 5
console timeout 0
!

class-map inspection_default
match default-inspection-traffic
!
!
policy-map asa_global_fw_policy
class inspection_default
 inspect dns maximum-length 512
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
 inspect sqlnet
 inspect sunrpc
 inspect tftp
 inspect sip
 inspect xdmcp
!
service-policy asa_global_fw_policy global
Cryptochecksum:a0bff9bbaa3d815fc9fd269a3f67fef5
: end
```

Чтобы просмотреть в ASDM конфигурацию интерфейса командной строки, выберите **File > Show Running Configuration in New Window**.



Проверка

Для этой конфигурации отсутствует процедура проверки.

Поиск и устранение неисправностей

Команды поиска и устранения неисправностей

Утилита Output Interpreter (только для зарегистрированных пользователей) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитических данных по выходным данным команды **show**.

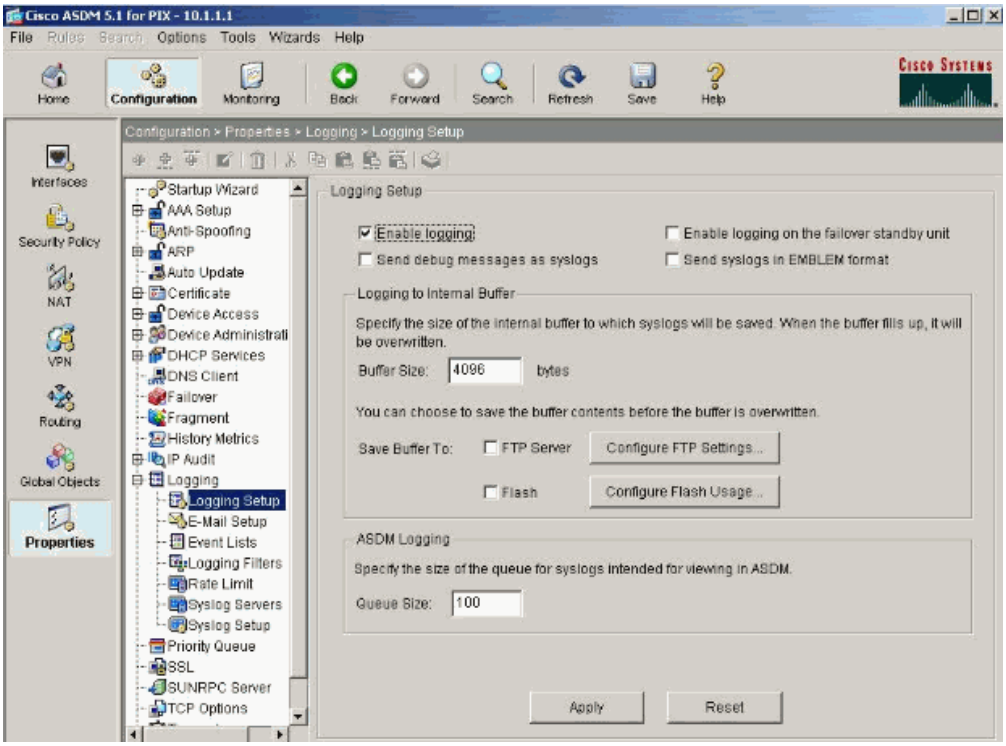
Примечание. Перед использованием команд **debug** ознакомьтесь со статьей Важная информация о командах отладки.

- **debug icmp trace** — показывает, достигают ли PIX ICMP-запросы от узлов. Для выполнения этой отладки добавьте команду **access-list**, чтобы разрешить ICMP в вашей конфигурации.
- **logging buffer debugging** — отображает установленные и запрещенные соединения с узлами, проходящие через PIX. Информация хранится в буфере журнала PIX. Его можно просмотреть при помощи команды **show log**.

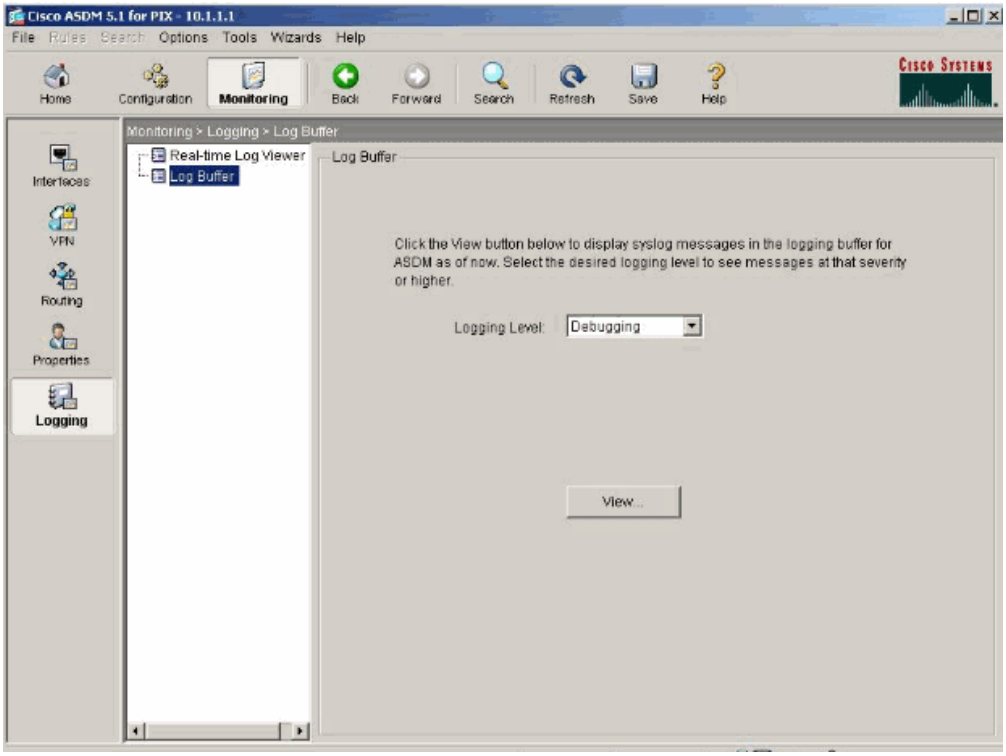
Процедура поиска и устранения неисправностей

ASDM можно использовать для включения регистрации, а также для просмотра журналов.

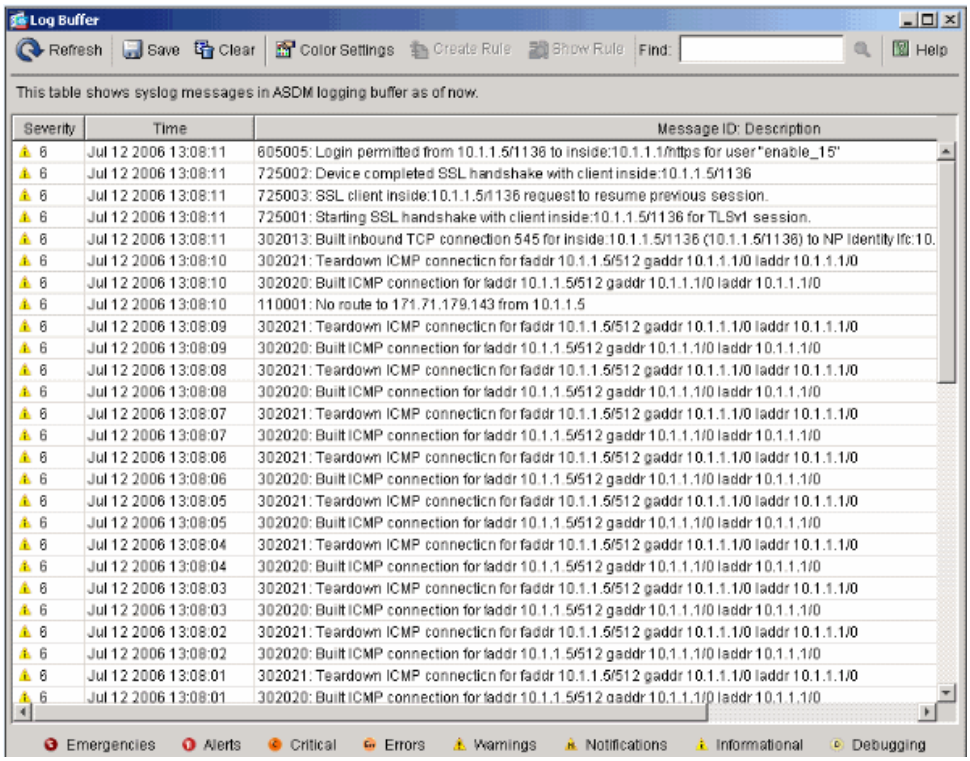
1. Выберите **Configuration > Properties > Logging > Logging Setup**, установите флажок **Enable Logging** и нажмите кнопку **Apply**.



2. Выберите **Monitoring > Logging > Log Buffer > Logging Level**, а затем в выпадающем списке выберите **Logging Buffer**. Нажмите кнопку **View**.



3. Пример буфера журнала:



Дополнительные сведения

- **Устройства защиты PIX серии 500**
- **Документация брандмауэра PIX**
- **Справочник по командам PIX**
- **Поиск и устранение неисправностей и предупреждения Cisco Adaptive Security Device Manager (ASDM)**
- **Документация RFC**
- **Техническая поддержка и документация – Cisco Systems**