Пример конфигурации PIX/ASA в качестве сервера и клиента DHCP

Содержание

Введение

Устройство обеспечения безопасности PIX серии 500 и адаптивное устройство обеспечения безопасности Cisco (ASA) поддерживают работу серверов и клиентов протокола динамической конфигурации хоста (DHCP). DHCP – это протокол, который предоставляет параметры автоматической конфигурации, например IP-адрес с маской подсети, шлюз по умолчанию, сервер DNS и IP-адрес сервера WINS для хостов.

Устройство обеспечения безопасности может служить сервером или клиентом DHCP. В качестве сервера устройство обеспечения безопасности предоставляет параметры конфигурации сети непосредственно для клиентов DHCP. В качестве клиента DHCP устройство обеспечения безопасности запрашивает данные параметры конфигурации у сервера DHCP.

В данном документе описана конфигурация сервера и клиента DHCP с помощью диспетчера адаптивных устройств обеспечения безопасности Cisco (ASDM) на устройстве обеспечения безопасности.

Предварительные условия

Требования

В данном документе предполагается, что устройство обеспечения безопасности PIX или ASA находится в рабочем состоянии и настроено, чтобы разрешить Cisco ASDM выполнить изменения конфигурации.

Примечание: См. документ Разрешение HTTPS-доступа для ASDM, чтобы позволить устройству, которое будет настроено ASDM.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Устройство обеспечения безопасности PIX серии 500 версии 7.x**Примечание:** Настройка PIX с помощью CLI, используемая в версии 7.x, также применима к PIX 6. x. Разница состоит в том, что в версии более ранней, чем PIX 6.3, сервер DHCP можно было включать только на внутреннем интерфейсе. В PIX 6.3 и более поздних версиях сервер DHCP можно включать на любых доступных интерфейсах. В следующей конфигурации внешний интерфейс используется для функции сервера DHCP.
- ASDM 5.x**Примечание:** ASDM только поддерживает PIX 7.0 и позже. Диспетчер устройств PIX (PDM) доступен для конфигурации PIX версии 6.x . Дополнительные сведения см. в разделе Совместимость аппаратного и программного обеспечения Cisco ASA серии 5500 и устройства обеспечения безопасности PIX серии 500.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Родственные продукты

Данную конфигурацию также можно использовать с Cisco ASA 7.x.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В следующей конфигурации существует два устройства обеспечения безопасности PIX с версией 7.x. Одно устройство функционирует в качестве сервера DHCP и предоставляет параметры конфигурации другому устройству обеспечения безопасности PIX 7.x, которое функционирует в качестве клиента DHCP. В качестве сервера DHCP PIX назначает IP-адреса клиентам DHCP в пуле назначенных IP-адресов.

Можно настраивать сервер DHCP на каждом интерфейсе устройства обеспечения безопасности. В каждом интерфейсе есть собственный пул адресов для извлечения. Однако другие параметры DHCP, например серверы DNS, имя домена, параметры, время

ожидания ICMP-эхо и серверы WINS, настроены глобально и используются сервером DHCP на всех интерфейсах.

Невозможно настроить клиента DHCP или службы ретрансляции DHCP на интерфейсе, на котором подключен сервер. Кроме того, клиенты DHCP должны быть напрямую подключены к интерфейсу, на котором включен сервер.

Наконец, пока сервер подключен на интерфейсе DHCP, невозможно изменить IP-адрес данного интерфейса.

Примечание: В основном нет никаких параметров конфигурации для установки адреса шлюза по умолчанию в ответе DHCP, передаваемом от сервера DHCP (PIX/ASA). Сервер DHCP всегда передает свой собственный адрес как шлюз для клиента DHCP. Однако определение маршрута по умолчанию, который указывает к Интернет-маршрутизатору, позволяет пользователю достигать Интернета.

Примечание: Количество адресов пула DHCP, которые могут быть назначены, зависит от лицензии, используемой в Устройстве безопасности (PIX/ASA). При использовании Ядра/Безопасности Плюс лицензия тогда, эти пределы применяются к пулу DHCP. Если предел Хоста является 10 хостами, вы ограничиваете пул DHCP 32 адресами. Если предел Хоста является 50 хостами, вы ограничиваете пул DHCP 128 адресами. Если предел Хоста неограничен, вы ограничиваете пул DHCP 256 адресами. Таким образом пул адресов ограничен на основе количества Хостов.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

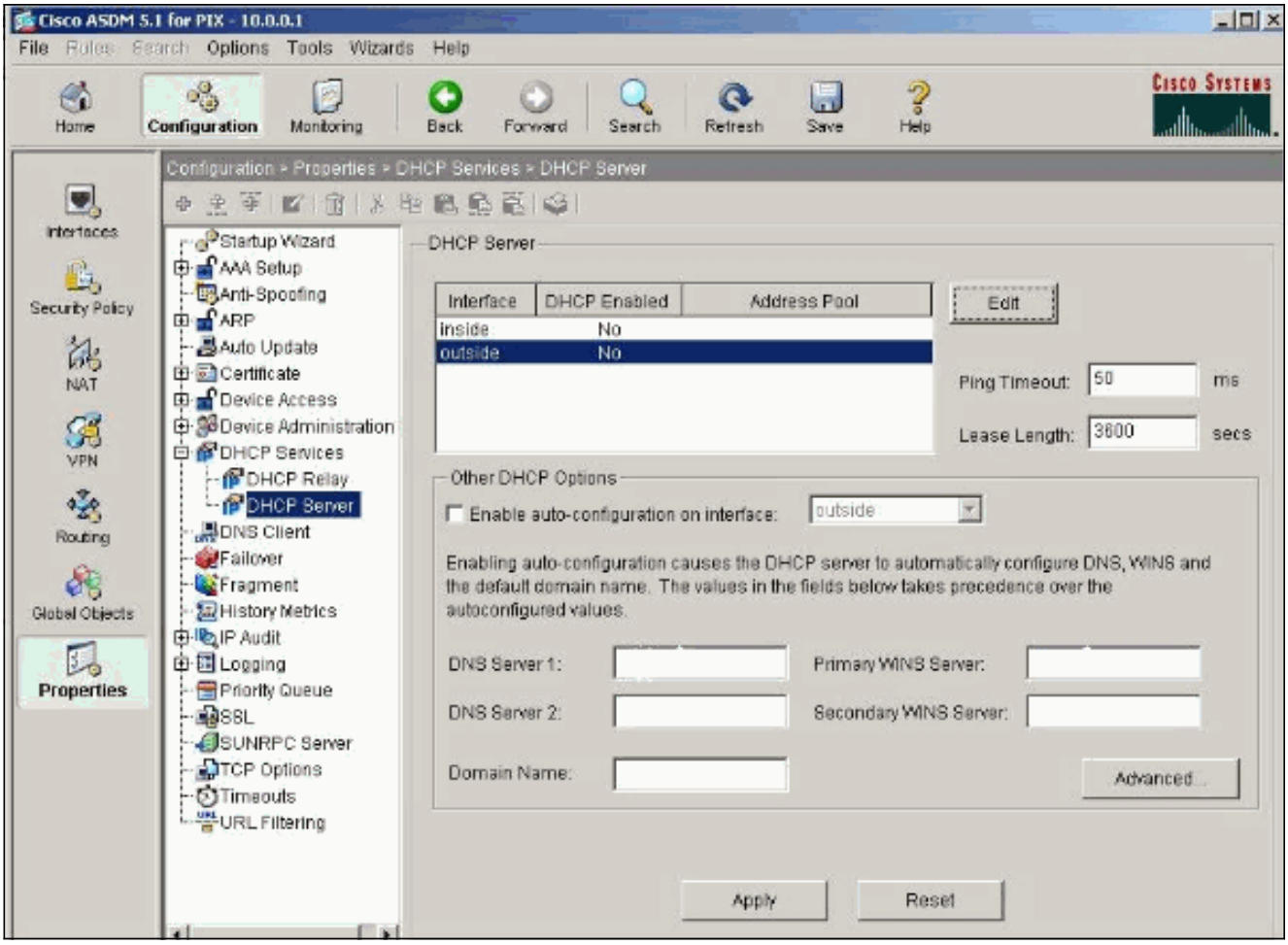
Эти конфигурации используются в данном документе:

- Конфигурация сервера DHCP с помощью ASDM
- Конфигурация клиента DHCP с помощью ASDM
- Конфигурация сервера DHCP
- Конфигурация клиента DHCP

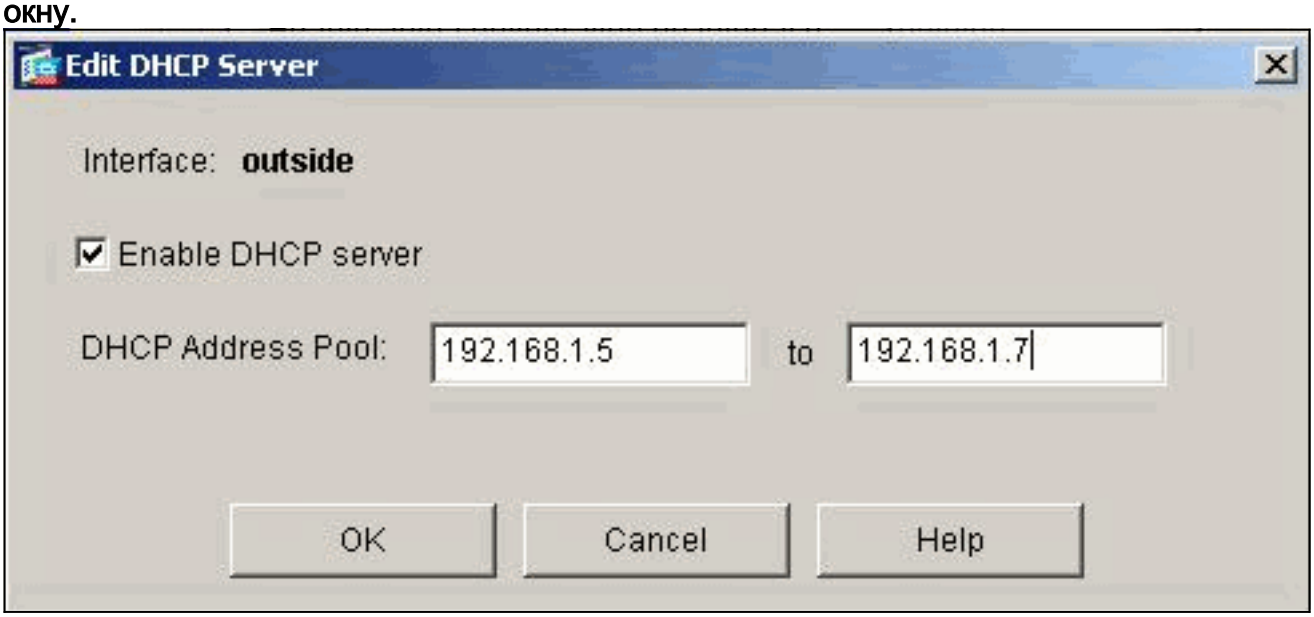
Конфигурация сервера DHCP с помощью ASDM

Чтобы настроить устройство обеспечения безопасности PIX или ASA в качестве сервера DHCP с помощью ASDM, выполните следующие действия.

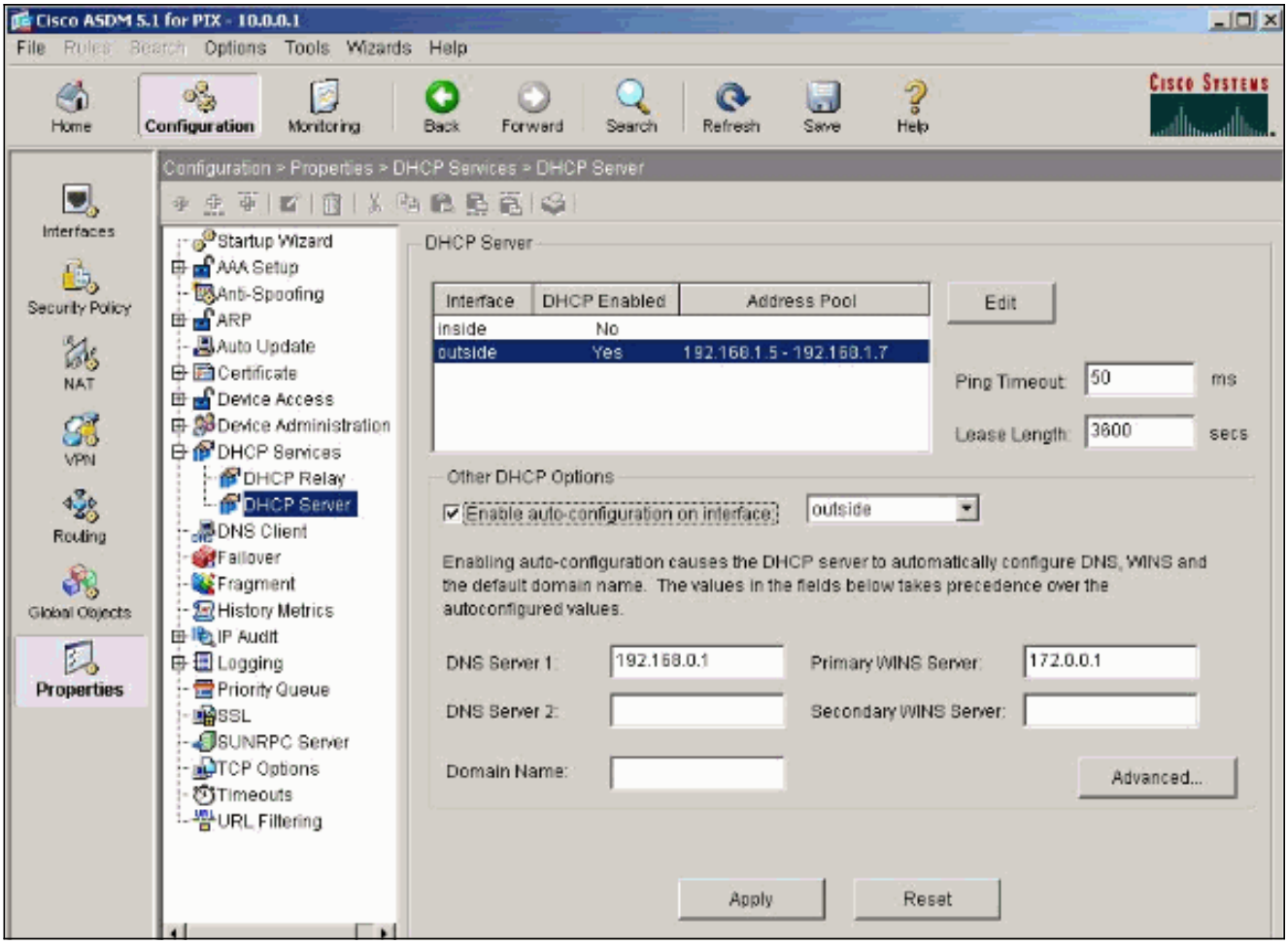
1. **В окне Home выберите Configuration > Properties > DHCP Services > DHCP Server. Выберите интерфейс и нажмите Edit, чтобы включить сервер DHCP и создать пул адресов DHCP.**Пул адресов должен находиться в одной подсети с интерфейсом устройства обеспечения безопасности. В следующем примере сервер DHCP настроен на внешнем интерфейсе устройства обеспечения безопасности PIX.



2. Проверьте, поставлен ли флажок Enable DHCP server на внешнем интерфейсе, чтобы сервер получал запросы клиентов DHCP. Предоставьте пул адресов, который необходимо отправить клиенту DHCP и нажмите OK, чтобы вернуться к главному окну.



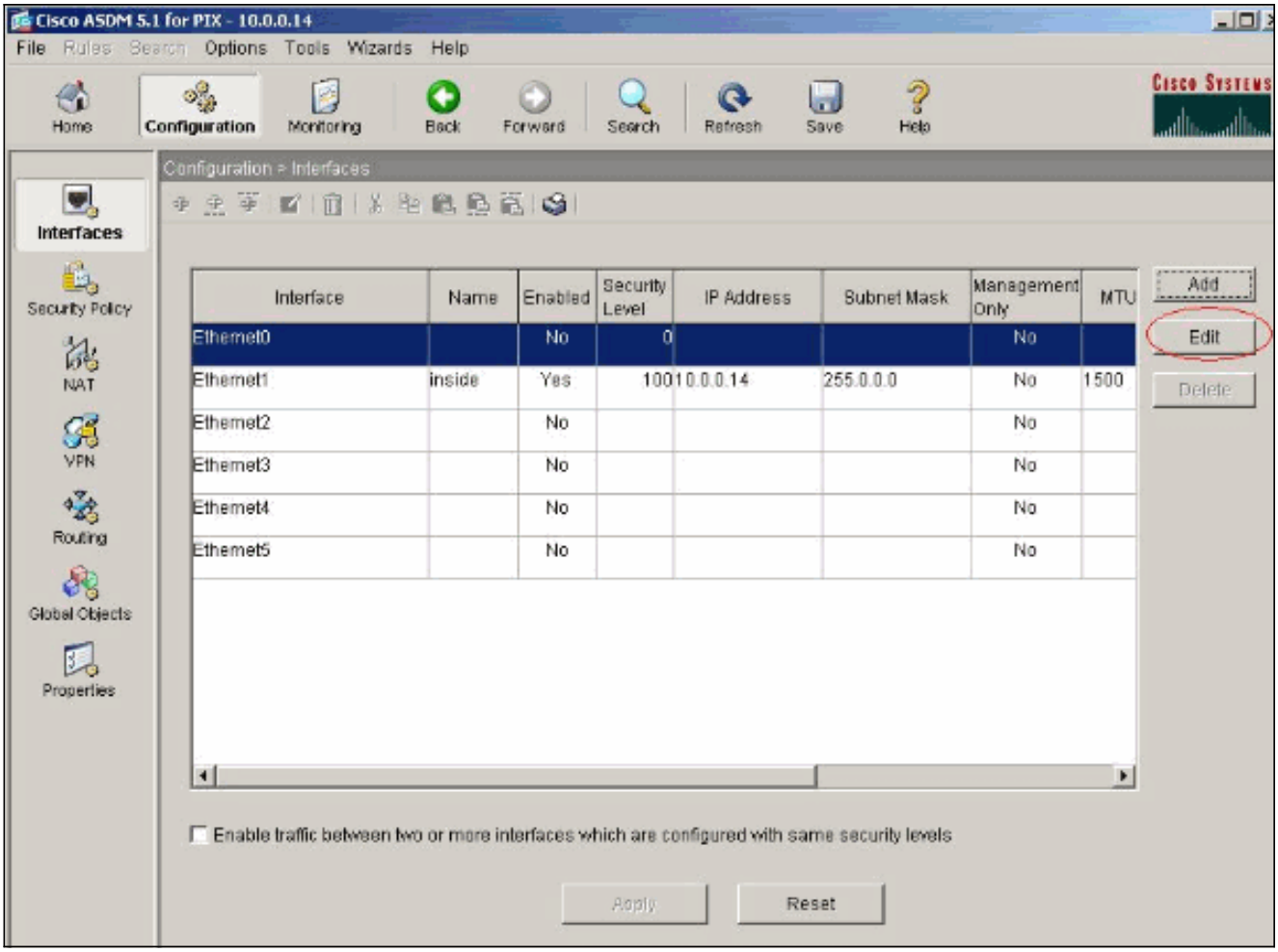
3. Проверьте, поставлен ли флажок Enable auto-configuration, чтобы сервер DHCP автоматически настраивал DNS, WINS и имя домена по умолчанию для клиента DHCP. Нажмите Apply, чтобы обновить текущую конфигурацию устройства обеспечения безопасности.



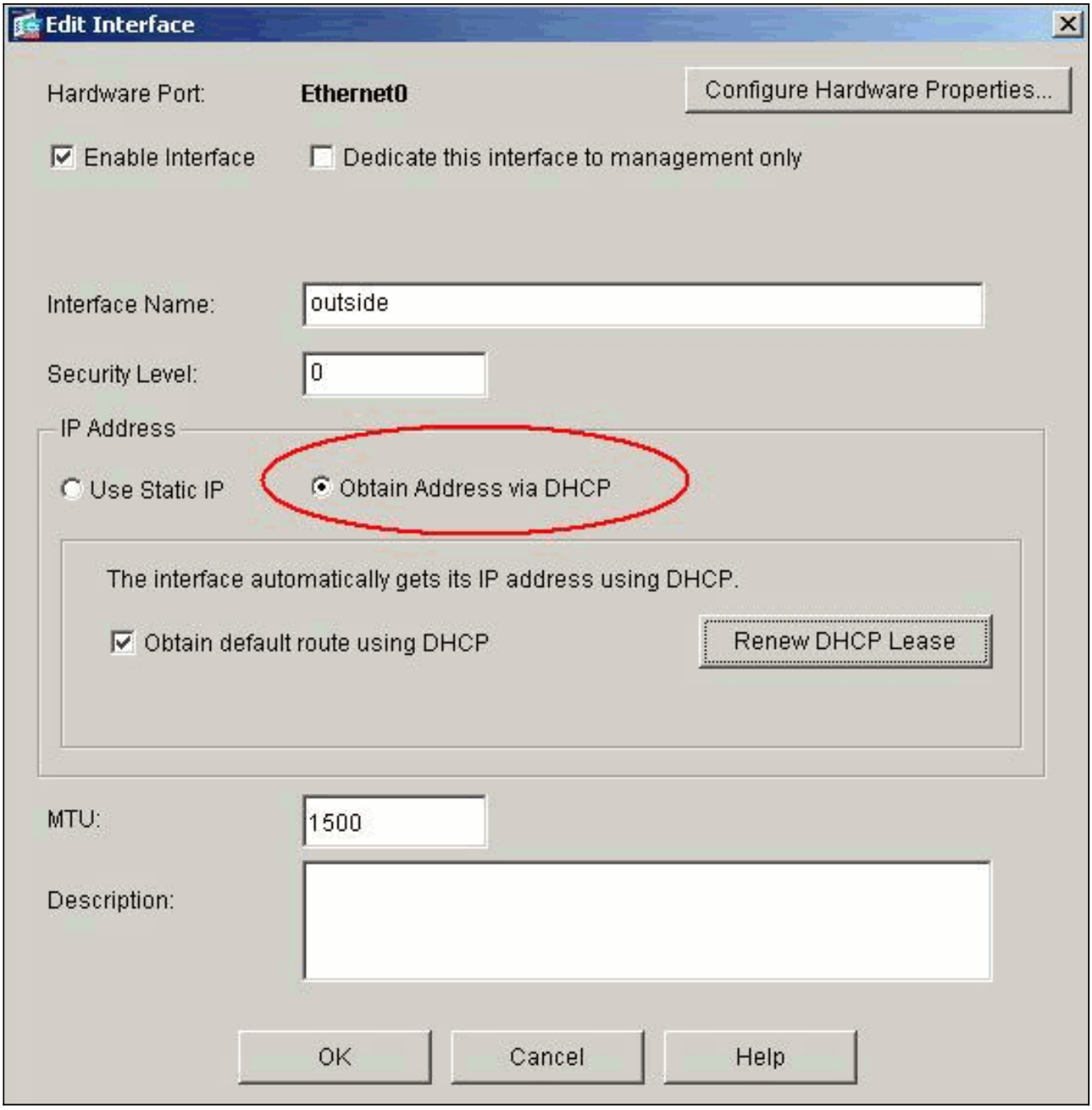
Конфигурация клиента DHCP с помощью ASDM

Чтобы настроить устройство обеспечения безопасности PIX в качестве клиента DHCP с помощью ASDM, выполните следующие действия.

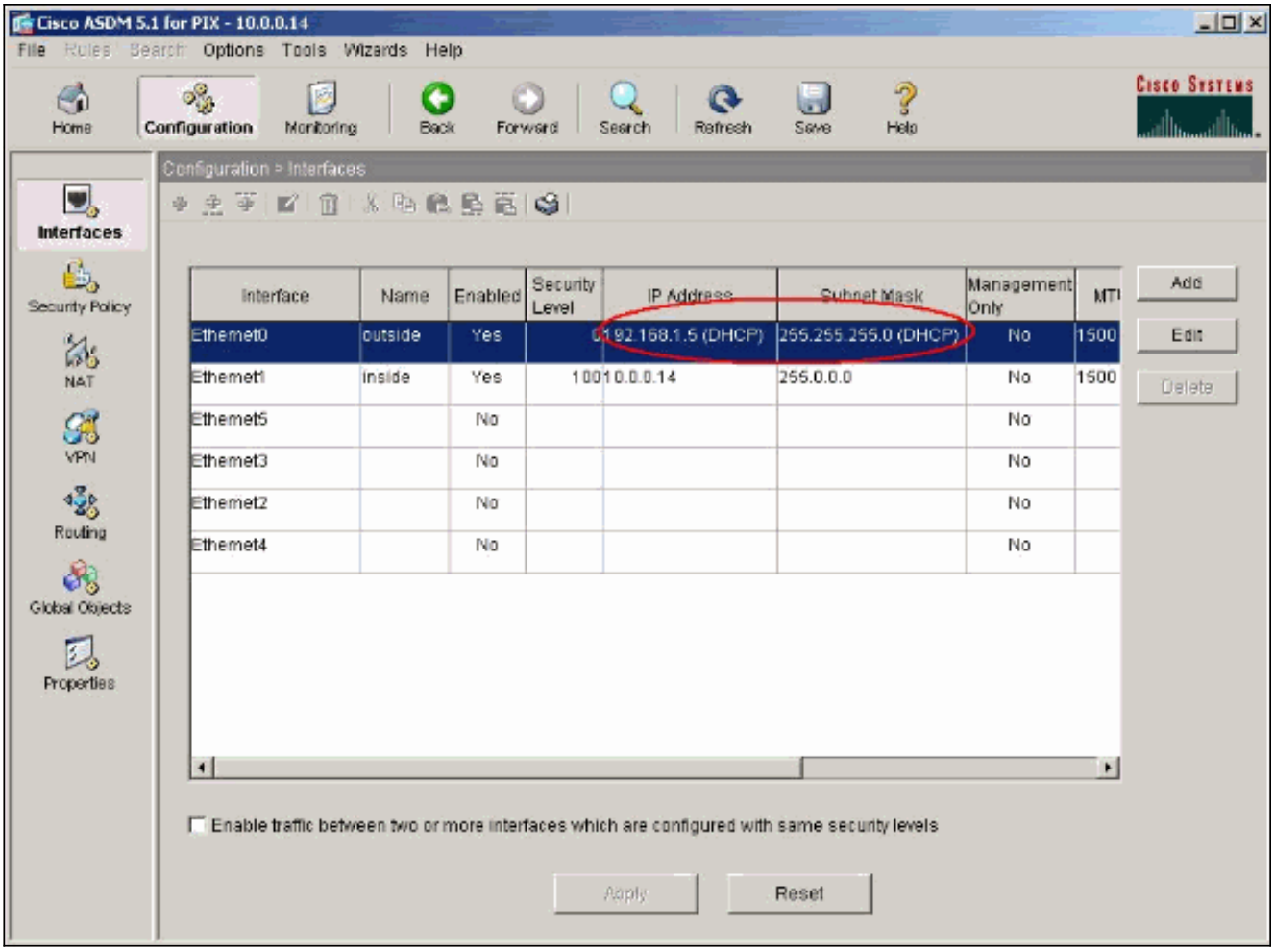
1. **Выберите Configuration > Interfaces и нажмите Edit, чтобы включить интерфейс Ethernet для получения параметров конфигурации, например IP-адрес с маской подсети, шлюз по умолчанию, сервер DNS и IP-адрес сервера WINS, с сервера DHCP.**



2. Выберите Enable Interface и введите имя интерфейса и уровень безопасности для интерфейса. Выберите Obtain address via DHCP для IP-адреса и Obtain default route using DHCP для шлюза по умолчанию, а потом нажмите OK, чтобы перейти к главному окну.



3. **Нажмите Apply, чтобы просмотреть полученный с сервера DHCP IP-адрес для интерфейса.**



Конфигурация сервера DHCP

Следующая конфигурация создана с помощью ASDM:

DHCP Server

```
pixfirewall#show running-config PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 ip
address 192.168.1.1 255.255.255.0 ! interface Ethernet1
nameif inside security-level 100 ip address 10.0.0.1
255.0.0.0 ! !--- Output is suppressed. logging enable
logging asdm informational mtu inside 1500 mtu outside
1500 no failover asdm image flash:/asdm-511.bin http
server enable http 10.0.0.0 255.0.0.0 inside no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart telnet timeout 5 ssh timeout 5 console timeout
0 !--- Specifies a DHCP address pool and the interface
for the client to connect. dhcpd address 192.168.1.5-
192.168.1.7 outside !--- Specifies the IP address(es) of
the DNS and WINS server !--- that the client uses. dhcpd
dns 192.168.0.1 dhcpd wins 172.0.0.1 !--- Specifies the
lease length to be granted to the client. !--- This
lease equals the amount of time (in seconds) the client
!--- can use its allocated IP address before the lease
expires. !--- Enter a value between 0 to 1,048,575. The
default value is 3600 seconds. dhcpd lease 3600 dhcpd
ping_timeout 50 dhcpd auto_config outside !--- Enables
the DHCP daemon within the Security Appliance to listen
```

```
for !--- DHCP client requests on the enabled interface.
dhcpd enable outside dhcprelay timeout 60 ! !--- Output
is suppressed. service-policy global_policy global
Cryptochecksum:7a8cd028ee1c56083b64237c832fb5ab : end
```

Конфигурация клиента DHCP

Следующая конфигурация создана с помощью ASDM:

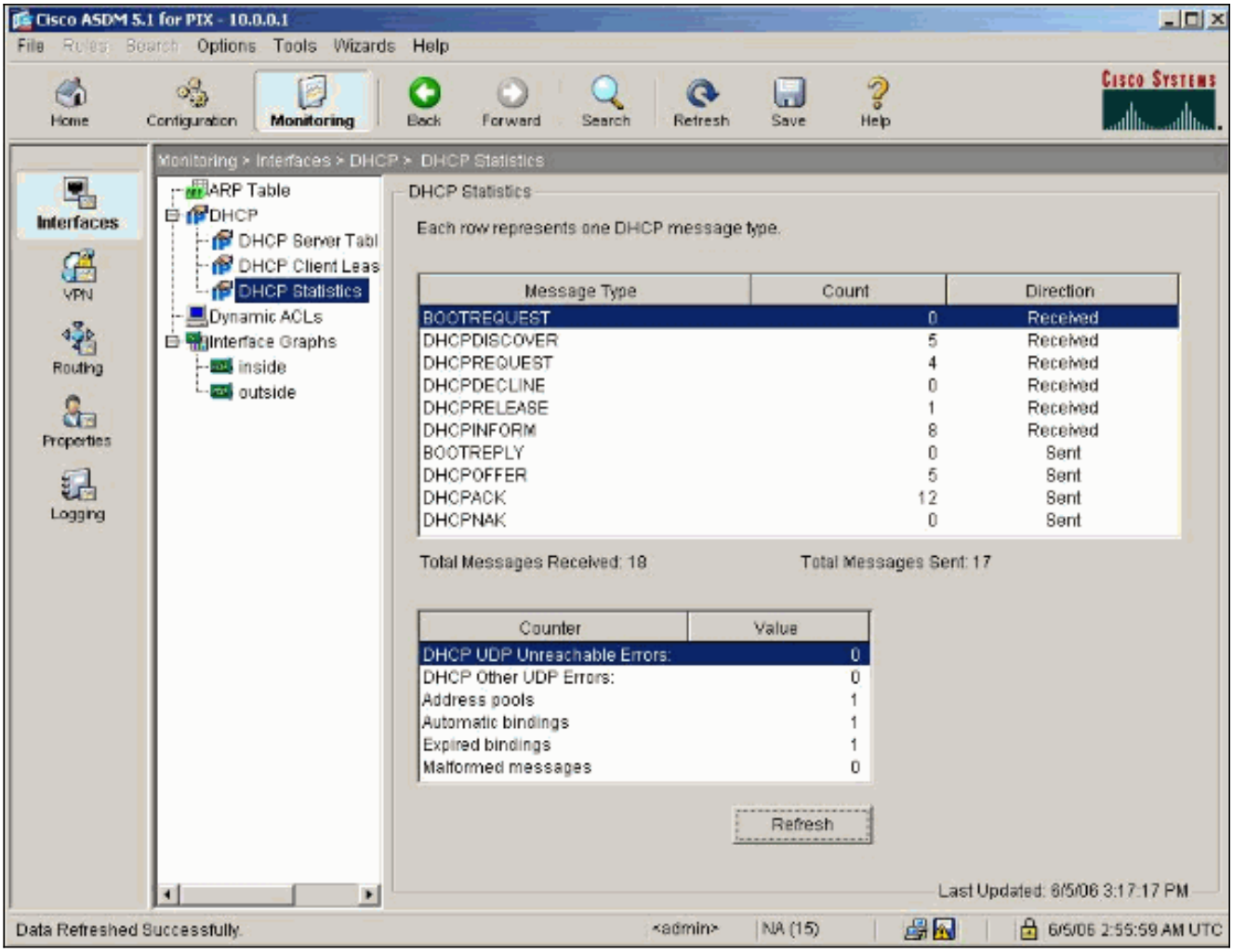
DHCP-клиент

```
pixfirewall#show running-config PIX Version 7.1(1) !
hostname pixfirewall domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface Ethernet0 nameif outside security-level 0 !---
Configures the Security Appliance interface as a DHCP
client. !--- The setroute keyword causes the Security
Appliance to set the default !--- route using the
default gateway the DHCP server returns. ip address dhcp
setroute ! interface Ethernet1 nameif inside security-
level 100 ip address 10.0.0.14 255.0.0.0 !--- Output is
suppressed. ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid pager lines 24 logging enable
logging console debugging logging asdm informational mtu
outside 1500 mtu inside 1500 no failover asdm image
flash:/asdm-511.bin no asdm history enable arp timeout
14400 timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc
0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout
uauth 0:05:00 absolute http server enable http 10.0.0.0
255.0.0.0 inside !--- Output is suppressed. ! service-
policy global_policy global
Cryptochecksum:86dd1153e8f14214524359a5148a4989 : end
```

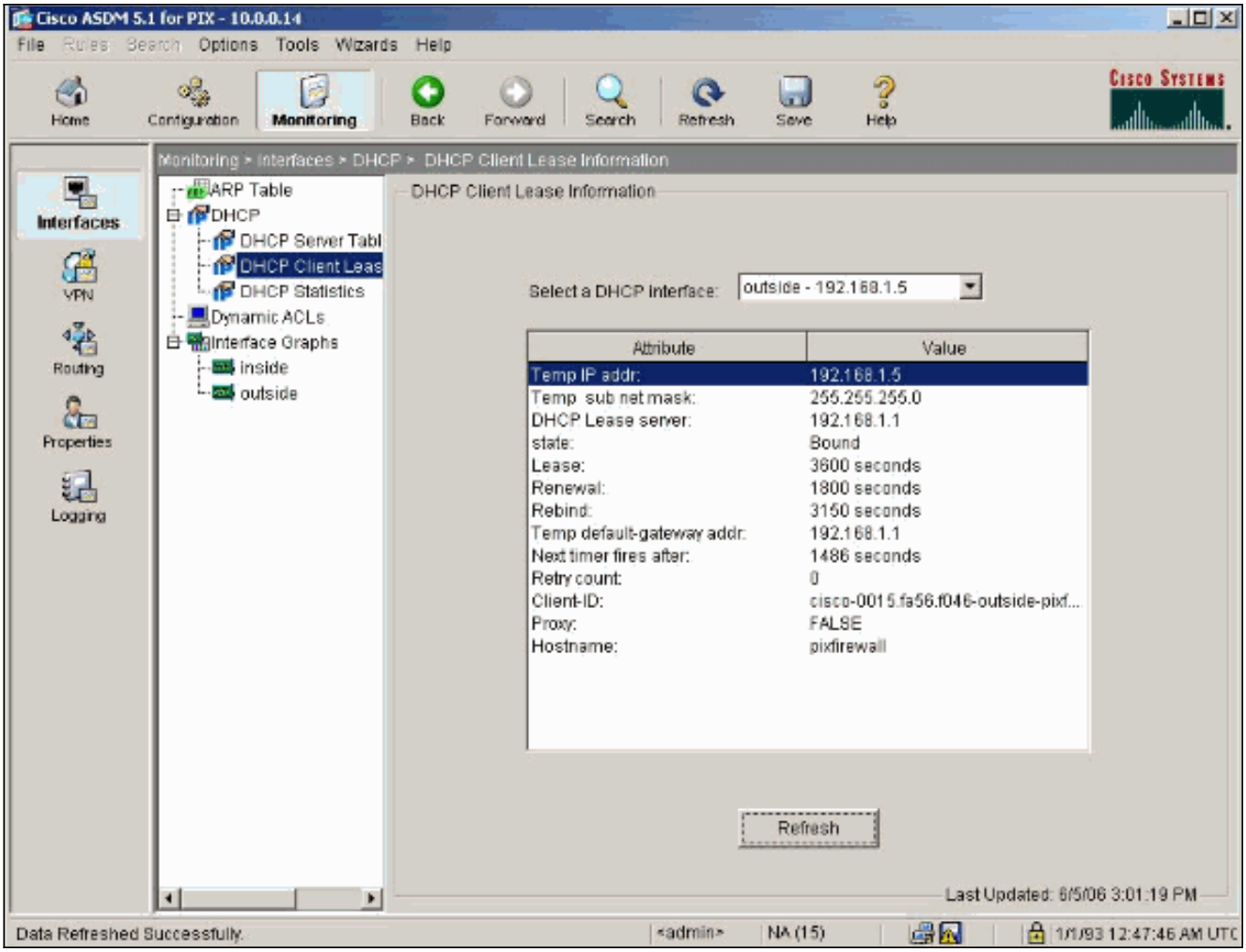
Проверка

Чтобы проверить статистику DHCP и информацию связывания в сервере и клиенте DHCP, выполните следующие действия.

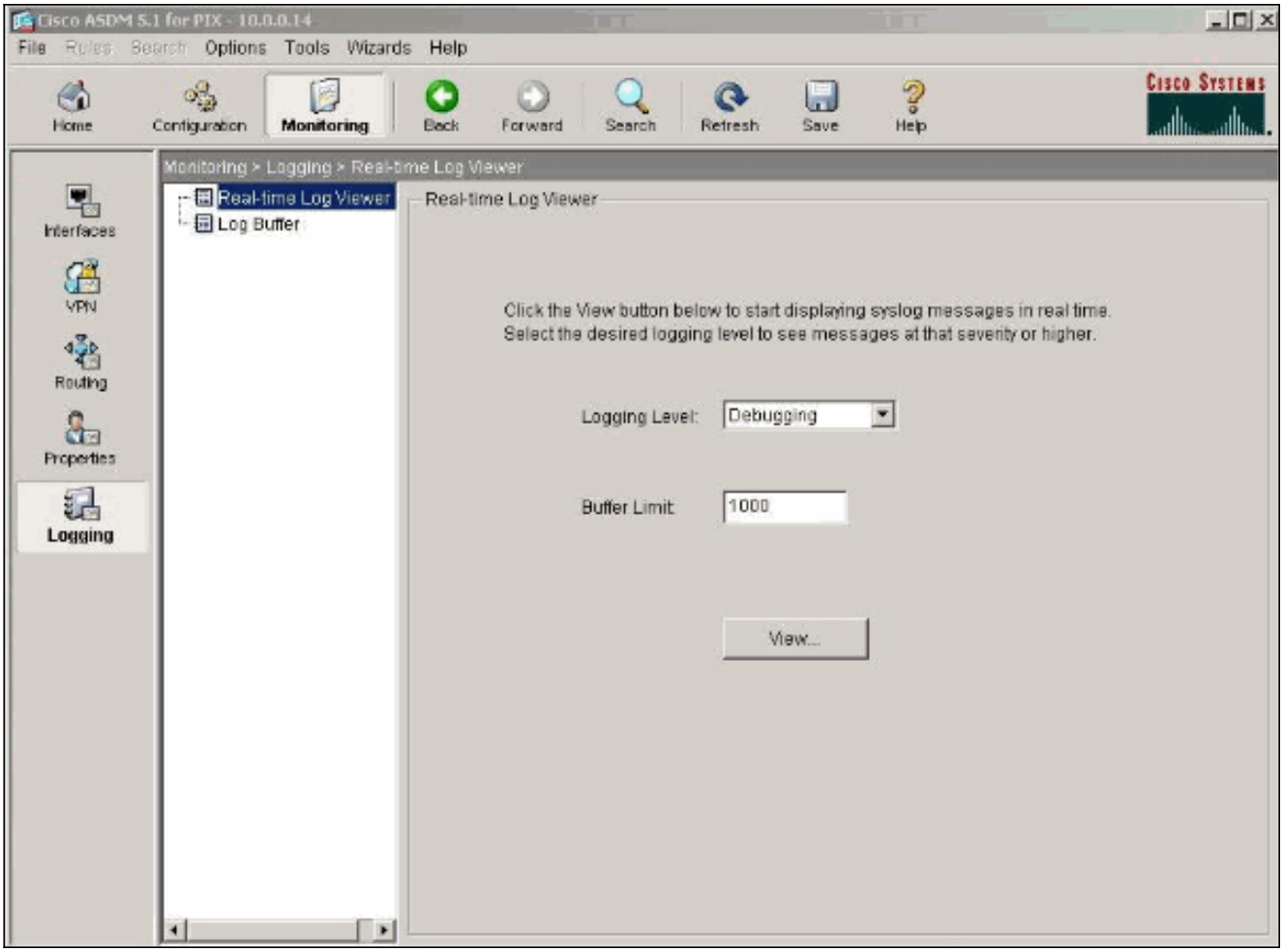
1. **Выберите Monitoring > Interfaces > DHCP > DHCP Statistics в сервере DHCP, чтобы проверить статистику DHCP, например DHCPDISCOVER, DHCPREQUEST, DHCPOFFER и DHCPACK.Введите команду show dhcpd statistics в CLI, чтобы просмотреть статистику**
   DHCP.



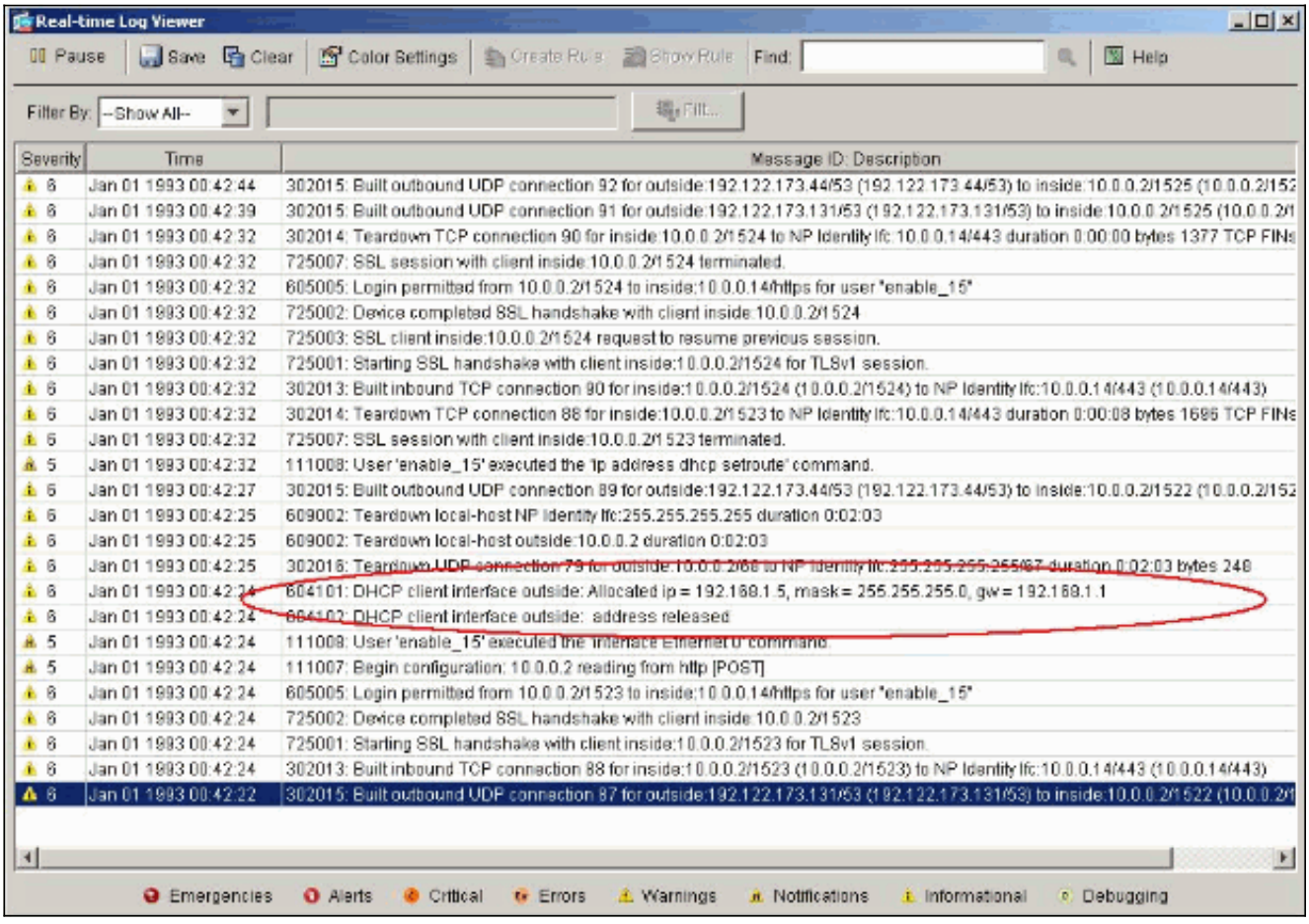
2. Выберите Monitoring > Interfaces > DHCP > DHCP Client Lease Information в клиенте DHCP, чтобы просмотреть информацию связывания DHCP.Введите команду show dhcpd binding, чтобы просмотреть информацию связывания DHCP в CLI.



3. Выберите Monitoring > Logging > Real-time Log Viewer, чтобы выбрать уровень регистрации, и ограничение буфера, чтобы просмотреть сообщения журнала реального
времени.



4. Просмотрите события журнала реального времени в клиенте DHCP. Данный IP-адрес выделен для внешнего интерфейса клиента DHCP.



Устранение неполадок

Команды для устранения неполадок

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- **debug dhcpd event – отображает сведения о событиях, связанных с сервером DHCP.**
- **debug dhcpd packet – отображает сведения о пакетах, связанных с сервером DHCP.**

Сообщения об ошибках

`CiscoASA(config)#`**`dhcpd address 10.1.1.10-10.3.1.150 inside Warning, DHCP pool range is limited to 256 addresses, set address range as: 10.1.1.10-10.3.1.150`**

Пояснение: размер пула адресов ограничен 256 адресами на пул на устройстве безопасности. Это не может быть изменено и является программным ограничением. Общее количество может только быть 256. Если диапазон пула адресов больше, чем 253 адреса (например, 254, 255, 256), маска подсети интерфейса устройства защиты не может быть адресом Класса C (например, 255.255.255.0). Это должно быть что-то большее, например, 255.255.254.0.

См. Руководство по конфигурации Командной строки Cisco Security Appliance для получения информации о том, как внедрить характеристику сервера DHCP в устройство безопасности.

Часто задаваемые вопросы: Присвоение адреса

Вопрос — действительно ли возможно назначить статический/постоянный IP-адрес на компьютер, который использует ASA в качестве сервера DHCP?

Ответ — Это не возможный PIX/ASA использования.

Вопрос — действительно ли возможно связать адреса DHCP с определенными MAC-адресами на ASA?

Ответ — нет, это не возможно.

Дополнительные сведения

- Страница поддержки устройства безопасности PIX Security Appliance
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Cisco Systems – техническая поддержка и документация