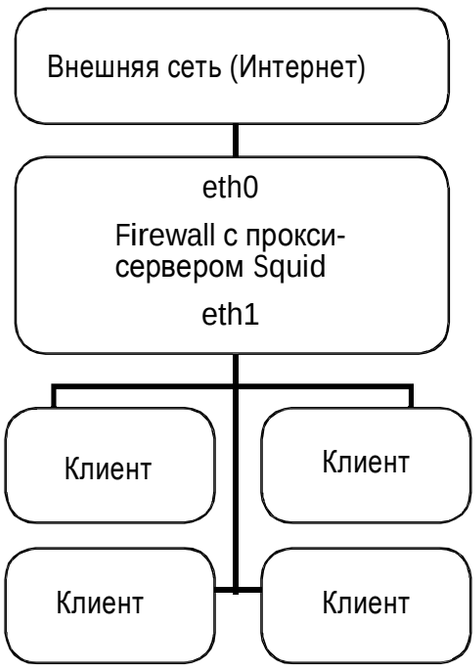
Простое руководство по созданию брандмауэра и прокси-сервера squid

Peter K. Lillian - RHCE
RedHat, Inc.

Введение



WHP154774US 12/05

В этом документе мы рассмотрим конфигурацию и настройку брандмауэра и прокси-сервера squid. Здесь вы найдете исчерпывающие ответы на вопрос "с чего начать".

Предполагаемая инфраструктура сети будет выглядеть как изображено на схеме 1. Сервер, работающий в качестве брандмауэра и прокси-сервера squid, находится между внутренней и внешней сетями. Клиенты сконфигурированы на использование IP адреса брандмауэра, как шлюза по умолчанию и прокси-сервера для доступа к веб-страницам.

Наличие брандмауэра очень важно для среды, в которой системы будут соединяться с незащищенными сетями, подобными Интернет. Также его можно использовать для предотвращения прохождения определенных типов трафика из сети компании. Red Hat Enterprise Linux использует систему Iptables , которая является инструментом фильтрации пакетов на уровне ядра. Iptables использует перечень правил, в которых прописано, что делать с данным пакетом из сети. Этот документ показывает, как настроить простую пересылку пакетов и правила фильтрации при использовании брандмауэра.

Squid является высокопроизводительным кэширующим прокси-сервером для веб-клиентов. Он поддерживает FTP, gopher и HTTP объекты. В отличие от традиционного кеширующего программного обеспечения, Squid рассматривает все запросы в одном, не блокирующем, управляемом процессе ввода-вывода (I/O). Squid хранит метаданные и особенно "горячие объекты" из кеша в оперативной памяти (RAM), хранит DNS-запросы, поддерживает неблокирующие DNS-запросы и осуществляет обратное кэширование неудавшихся запросов.

Squid поддерживает SSL, обширный контроль доступа и полные запросы на регистрацию. Используя Internet Cache Protocol (ICP), кеши Squid можно организовать по иерархической схеме или в виде сети для сохранения дополнительной информации. Squid состоит из главной серверной программы (squid), программы для запросов с использованием Domain Name System (DNS) (dnsserver), дополнительных программ для записи запросов и выполнения аутентификации, инструментов управления и клиентов. Когда происходит запуск Squid, то он создает конфигурируемое количество процессов dnsserver, каждый из которых способен осуществить блокирующие DNS-запросы. Происходит экономия времени, когда кеш ожидает ответ на DNS-запрос.

Кэширование интернет объектов - это способ хранения запрашиваемых интернет объектов (например, данные доступные через HTTP, FTP и протокол gopher) в системе, расположенной ближе к запрашивающему клиенту, чем к источнику. Затем веб-браузеры могут использовать локальный кэш Squid в качестве HTTP прокси-сервера, тем самым, уменьшая как время доступа, так и полосу пропускания. (1)

УСТАНОВКА И КОНФИГУРАЦИЯ БРАНДМАУЭРА

ЧАСТЬ 1: УСТАНОВКА

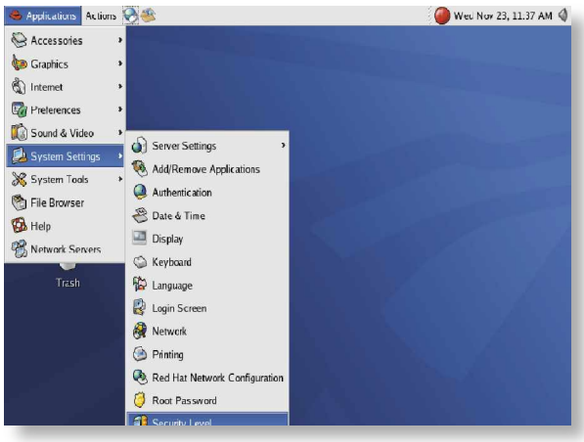
1. Войдите в систему как “root”.

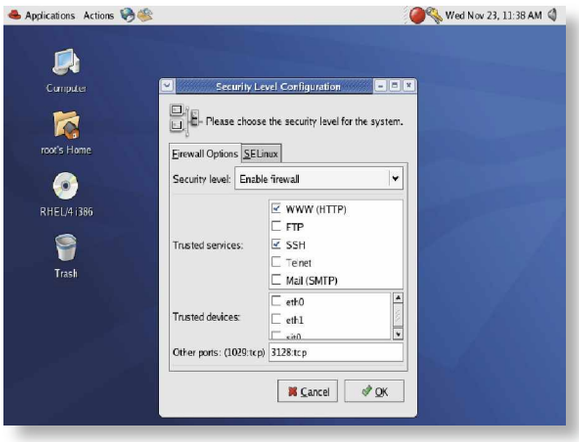
2. Активизируйте брандмауэр в системе. Для этого, щелкните:

• Приложения => Системные параметры =>Настройка уровня безопасности
(Applications => System Settings => Security Level)
• Удостоверьтесь в том, что выбрана вкладка Настройка брандмауэра (“Firewall Options”). Щелкните на выпадающем меню "Уровень безопасности"и выберите "Включить брандмауэр” (“Enable Firewall").

3. В области «Доверенные службы» (“Trusted Services”) , выберете “SSH” и “WWW (HTTP)” , чтобы secure shell и веб-сервер были доступны на машине с брандмауэром.

4. В область «Другие порты» (“Other Ports”) добавьте порт 3128:tcp, чтобы запросы на прокси-сервер погли пройти через брандмауэр.





5. Щелкните “OK”. Появится предупреждение о том, что брандмауэр активизирован. Щелкните “OK” снова. Теперь брандмауэр настроен и запущен.

ЧАСТЬ 2: КОНФИГУРАЦИЯ

Затем, система должна быть установлена как брандмауэр. У нее должны быть две отдельных сетевых карты (NIC - Network Interface Cards). Мы будем исходить из того, что eth0 связан с "внешним миром", а eth1 связан с внутренней сетью.

Первоначально для работы с брандмауэром необходимо сконфигурировать NAT (Преобразование сетевых адресов - Network Address Translation) и пересылку пакетов – форвардинг (IP forwarding). Это позволит переслать любой сетевой запрос из внутренней сети во внешнюю сеть.

1. Откройте терминальное окно и сделайте следующее:

```
cd /etc/
gedit sysctl.conf
```

2. Перейдите к строке “net.ipv4.ip_forward = 0” и измените 0 на 1, чтобы строка стало такой:

```
net.ipv4.ip_forward = 1
```

Этот шаг активизирует форвардинг пакетов IP. Сохраните файл и закройте окно.

3. Произведенные изменения дадут эффект при следующей перезагрузке. Чтобы немедленно активизировать данные изменения наберите в терминальном окне:

```
sysctl -p
```

Этот шаг позволит заново перечитать конфигурационный файл (/etc/sysctl.conf), который вы только что отредактировали, и увидеть результаты проведенных изменений.

4. Далее следует добавить правила NAT к брандмауэру. В терминальном окне наберите следующее:

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Это «правило» говорит о том, что на выходе брандмауэр будет маскироваться под запрашивающий сервер. Это означает, что любые запросы, исходящие из внутренней сети брандмауэра сначала пройдут сам брандмауэр и затем попадут в Интернет. В последствии, любые запросы, возвращаемые из Интернета, будут возвращены брандмауэром в систему, где запрос был порожден.

5. Теперь необходимо настроить iptables так, чтобы передавать пакеты от eth1 к eth0, а брандмауэр будет отправлять их дальше. Напомним, что ключ -I означает “вставить правило”, ключ -i применяется для обозначения “интерфейса принимающего пакеты”, ключ -o для “выходного интерфейса” и -j определяет, что делать, если пакет соответствует правилу (в данном случае - принять).

```
iptables -I FORWARD -i eth1 -o eth0 -j ACCEPT
```

6. Сохраните ваши изменения:

```
service iptables save
```

Теперь firewall сконфигурирован. На клиентских системах, в качестве шлюза по умолчанию в сетевых настойках необходимо указать IP-адрес интерфейса eth1 брандауэра.

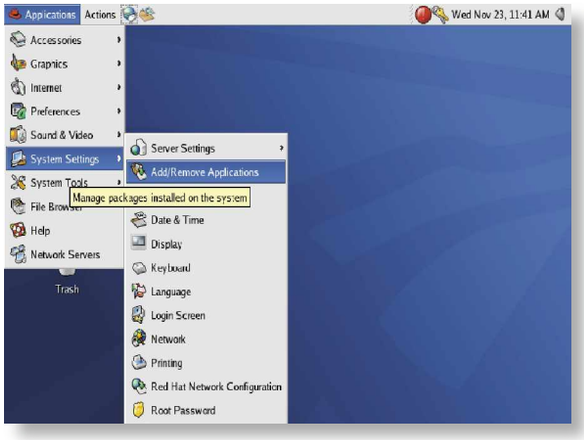
ЧАСТЬ 1: УСТАНОВКА

1. Войдите в систему как “root”.

2. Убедитесь в том, что пакеты squid установлены. Щелкните:

Приложения => Системные параметры =>Установка/удаление приложений
(Applications => System Settings => Add/Remove Packages)

Прокрутите вниз до раздела «Серверы» (Server). Проверте, что Веб-сервер (Web Server) помечен. Щелкните на Сведения (“Details”). Прокрутите вниз и проверьте, что squid помечен. Эти пакеты надо установить до начала работы.



Установка: Щелкните по кнопке «Обновить» (“update”) (Это требует наличия инсталляционных дисков, а также система не должна была обновляться после установки) или используйте up2date и Red Hat Network для установки пакетов. Для установки с помощью up2date, наберите следующее в терминальном окне:

up2date squid httpd

После получения подтверждения об установке пакетов следует сконфигурировать прокси-сервер squid.

ЧАСТЬ 2: КОНФИГУРАЦИЯ СЕРВЕРА

1. Откройте терминальное окно и наберите следующее:

cd /etc/squid
gedit squid.conf

(помните, что можно использовать любой текстовой редактор вместо gedit)

Это конфигурационный файл прокси-сервера squid. Он содержит инфорцию по доступным конфигурационным опциям. Выделите немного времени для просмотра некоторых опций. В этом документе процесс конфигурации упрощен ради демонстративных целей.

2. Найдите строку “INSERT YOUR OWN RULE(S) HERE TO ALLOW...”. Проще всего это можно сделать, если щелнуть на «Найти» (“Find”) и поискать вышеупомянутую фразу:

acl <group> src IPADDRESS
http_access allow <group>

<group> - может быть любое произвольное имя для группы (например, my_connection), а IPADDRESS это список или группа IP-адресов, у которых по вашему желанию должен быть доступ к серверу Squid (например, 192.168.0.0/24). На основе этого примера добавленные строки будут выглядеть так:

acl my_connection src 192.168.0.0/24
http access allow my connection

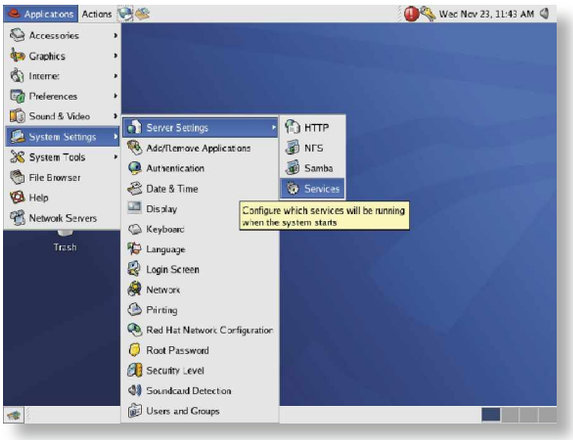
3. Сохраните изменения и закройте редактор.

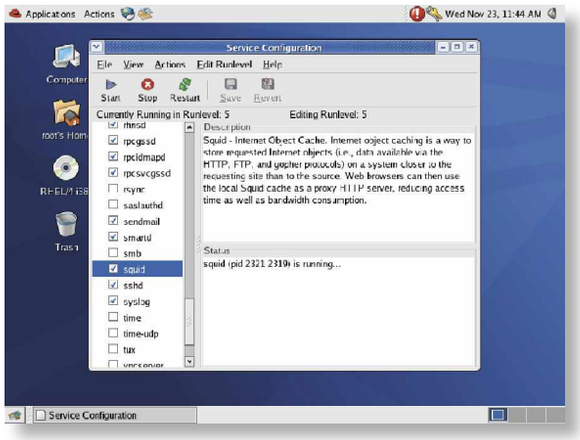
ЧАСТЬ 3: ЗАПУСК

1. После конфигурации прокси-сервера squid, эту службу следует запустить. Щелкните:

Приложения => Системные параметры => Настройка сервера => Службы
(Applications =>System Settings =>Server Settings =>Services)

Прокрутите вниз до “squid”. Пометьте эту службу. Это включит службу при перезагрузке системы.





2. Нажмите «Запустить» (“Start”) для запуска службы. Появится окно с сообщением об успешном запуске службы.

3. Сохраните изменения щелкнув по кнопке «Сохранить» (“Save”) вверху окна и закройте его. Сейчас прокси-сервер squid сконфигурирован и работает.

ЧАСТЬ 4: КОНФИГУРАЦИЯ КЛИЕНТОВ

Последний шаг- это конфигурация клиентских систем, которые используют эту систему в качестве прокси-сервера для веб запросов.

1. Откройте веб-браузер на клиентской машите.

2. Найдите управление настройками прокси-сервера. Это зависит от браузера. Например, в Firefox, выполните:

Правка => Настройки => Основные => Параметры соединения
(Edit=> Preferences =>General => Connection Settings)

3. Введите IP-адрес прокси-сервера squid в строке HTTP-прокси. Используйте порт 3128. Нажмите “OK”, а затем еще раз “OK”.

4. Наберите в адресной строке браузера:

http://www.redhat.com

Откроется домашняя страница Red Hat. Повторите часть 4 на других клиентских машинах.

Ссылки:

(1) http://www.squid-cache.org
(2) http://www.netfilter.org
(3) http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/sysadmin-guide/

redhat