2010

Шлюз в Интернет

или маршрутизатор своими руками

Методика создания шлюза в Интернет для локальной сети на основе старого компьютера и файервола Linux IPCop 1.4.21 для слабых машин. Конфигурация маршрутизатора также включает простейшую биллинговую систему с отключением пользователей по превышению лимита трафика и файл-сервер.

Новиков Максим Глебович

Версия 1.0 от 01.12.2010

Оглавление

Последняя версия статьи находится по адресу:
http://novikovmaxim.narod.ru/linux/IPCop/index.htm

Шлюз в Интернет
или маршрутизатор своими руками

на базе ОС Linux IPCop 1.4.21 (ядро 2.4.36)
(межсетевой экран для слабых машин)

Минимальная аппаратная конфигурация:	80386, RAM 12 Мб, HDD 250 Мб
Минимально рекомендуемая конфигурация:	Pentium II, RAM 256 Мб, HDD 4 Гб
Рекомендуемая конфигурация (для 100 Мбит):	Pentium III, RAM 512 Мб, HDD 13 Гб

Часть 1. Выбор «железа» и ПО.

Сегодня и дома, и во многих организациях всё чаще возникает необходимость подключить к Интернету несколько компьютеров, но так, чтобы не тратиться на дополнительное оборудование. Проще всего это можно сделать, объединив несколько рабочих станций в одноранговую локальную сеть и использовав одну из этих станций в качестве шлюза в Интернет. Затрат немного — провода да дешёвый коммутатор (свитч) или вообще концентратор (хаб), хотя последние уже не выпускаются. Минусов у такой схемы несколько:

1. Без покупки дополнительных программных продуктов, невозможно организовать какой бы то ни было контроль трафика и управление им.
2. При выключении рабочей станции, непосредственно подключённой к Интернету (являющейся шлюзом), остальные рабочие станции остаются без Интернета.
3. Защита компьютеров от проникновения из Интернета ложится на брандмауэр каждого отдельного компьютера сети, которым, как правило, пользователь управляет самостоятельно. А управлять он им может по-разному...

Часть этих проблем может снять маршрутизатор (роутер) — устройство, внешним портом подключённое к Интернету, а несколькими внутренними — к компьютерам локальной сети. Обычные маршрутизаторы на небольшое количество портов (4-8) стоят довольно дёшево (от 500 рублей) плюс коммутатор (5-8 портов) для увеличения количества портов маршрутизатора (от 300 рублей). Конечно, самые дешёвые варианты этих устройств любительского сегмента приобретать не стоит, потому что они имеют слабый функционал, а так же заведомо недостаточную пропускную способность, особенно при работе в паре с коммутатором.

Существуют также устройства, имеющие в своём составе жёсткий диск (от 6500 рублей) или USB-разъём для внешнего жёсткого диска (от 2500 рублей) плюс внешний жёсткий диск (от 1500 рублей). Такие устройства помимо маршрутизации могут выполнять функции файл-сервера. Однако под вопросом остаётся биллинг, отключение по превышению трафика и некоторые другие функции его контроля.

В этой статье я предлагаю вам собрать маршрутизатор с функцией файл-сервера своими руками, используя старые компьютерные комплектующие. Такой маршрутизатор имеет как минусы, так и плюсы.

Минусы:

1. Выше потребление электроэнергии.
2. Выше уровень шума от вентиляторов (хотя всё зависит от конкретных моделей обоих устройств).
3. Занимает больше места (даже несмотря на отсутствие монитора и клавиатуры).
4. Требует дополнительных знаний и времени для установки ПО.

Плюсы:

1. Большая пропускная способность по сравнению с любительскими роутерами за счёт мощного центрального процессора и отдельных процессоров на сетевых картах.
2. Дополнительный функционал. Например, биллинговая система и отключение пользователей по перерасходу трафика.
3. Бесплатность, что особенно чувствуется в случае необходимости создания файл-сервера.
4. Гибкость в использовании ПО. Существует много различных бесплатных дистрибутивов Linux, организующих на компьютере программный файервол «из коробки», который, собственно, и превращает компьютер в маршрутизатор. Если не понравилось одно программное решение, можно всегда воспользоваться другим, оставаясь на том же железе.

Так что, взвесив все «за» и «против», принимаем решение в пользу старого компьютера. В этом случае полезно дать несколько рекомендаций по его «железу»:

1. Для работы в составе маршрутизатора рекомендуется применять отдельные (неинтегрированные в материнскую плату) сетевые карты, как обладающие собственными процессорами, а потому меньше загружающие центральный процессор системы.
2. После установки и настройки маршрутизатора следует предпринять меры по снижению электропотребления — отключить CD-привод, дисковод, клавиатуру и другие неиспользуемые компоненты.
3. Как и любой другой компьютер локальной сети, маршрутизатор желательно защитить блоком бесперебойного питания.
4. В BIOS в разделе Power Management Setup следует включить опцию AC PWR Loss Restart (включить компьютер после пропадания питания), отключить останов компьютера во время загрузки при возникновении ошибок клавиатуры, поставить минимальные настройки для видеосистемы, а также по необходимости установить другие настройки управления энергопотреблением.
   Инструкцию по BIOS можно посмотреть тут: http://www.pc-bios.net/bios.html.

После того, как процессорный блок маршрутизатора собран, можно приступить к выбору ПО, исходя из сложившейся конфигурации. Если конфигурация базируется на Pentium 4 и выше, то у вас имеется приличный выбор программных файерволов для превращения системы в маршрутизатор. Если же машина получилось более слабой, то могу порекомендовать файервол IPCop версии 1.4.21, установку и настройку которого я опишу ниже.

Мой выбор в пользу IPCop основывается не только на низких требованиях этого файервола к железу, но и на том, что к нему существует довольно много дополнений, расширяющих его функционал. Одним из таких дополнений является Traffic Control and Report (TCAR). Это дополнение осуществляет подсчёт трафика для каждого пользователя и его блокировку при достижении определённого лимита. В других дистрибутивах я, как ни странно, не нашёл ничего подобного.

Описанная в этой статье установка и настройка IPCop будет немного отличаться от стандартной, поскольку мы включим в состав IPCop файловый сервер — полезную вещь для общей работы с документами в сети предприятия, и нам придётся увязать его с другими важными дополнениями, а также выделить для его нужд отдельный раздел на диске, что при его обычной установке не предлагается.

Для использования нижеследующего материала вам потребуются начальные знания об операционной системе Linux. В статье будет описана установка таких дополнений, как TCAR (позволяет отключать пользователей от Интернета при превышении лимита трафика), BOT (допускает к Интернету или к машине с IPCop только определённые компьютеры локальной сети по определённым портам) и SAMBA (помогает организовать на машине с IPCop файловое хранилище путём открытия общего доступа к определённым папкам).

Часть 2. Установка IPCop версии 1.4.21

Домашняя страница IPCop: http://sourceforge.net/apps/trac/ipcop/wiki
Характеристики IPCop 1.4.21: http://sourceforge.net/apps/trac/ipcop/wiki/IPCop14xFeatures

Ссылки на дополнения:
BOT: http://www.blockouttraffic.de/download_de.php
TCAR: http://www.onmind.ru/tcar/tcarru.htm
Для установки TCAR также требуется дополнение Addon Server (установщик дополнений через веб-интерфейс), даже если установка производится вручную (таково условие скрипта установки TCAR несмотря на заверения разработчика на домашней странице).
Addon Server: http://firewalladdons.sourceforge.net/install-2.3.b2.html
SAMBA: http://narod.ru/disk/11455902000/samba-0.2.1.tar.gz.html
Для установки SAMBA также требуется дополнение GUIPorts.
GUIPorts: http://www.ipcop.h-loit.de/
или http://unix.opp.homeunix.net/ipcop/addons/guiports-1.7.0.tar.gz

Набор ссылок на различные другие дополнения, которые вы можете установить впоследствии самостоятельно: http://sourceforge.net/apps/trac/ipcop/wiki/Addons

Глава 1. Установка IPCop

Можно выбрать любой вариант установки — обычный или расширенный. Если вы планируете организовать на машине с IPCop файловое хранилище, а у вас на ней только один жёсткий диск, рекомендуется выбрать расширенный вариант, который позволит во время установки добавить на диск дополнительный раздел, а заодно и увеличить размер файла подкачки.

1. Обычная установка

Загружаемся с CD и производим стандартную установку IPCop 1.4.20, например, так, как это описано по ссылке http://www.thg.ru/network/ipcop/ipcop-01.html. До версии 1.4.21 система обновляется позже, в процессе отдельного апгрейда (см. главу 2 «Установка апдейтов IPCop»). Установка IPCop 1.4.20 проста, и, как правило, не должна вызывать вопросов. Но если мы хотим создать на машине с IPCop файловое хранилище, то имеет смысл выделить для него отдельный раздел. В этом нам поможет расширенный вариант установки, описанный ниже.

Замечу, что для создания отдельного раздела после обычной установки, существует дополнение AddPartition (http://www.sischmitz.de/en/addpart.php). Но у меня оно сглючило при установке, и внесло ошибку в таблицу разделов, в результате чего для её исправления пришлось переформатировать раздел с логами. Поэтому я не советую его использовать до выяснения причин глюка, да и разбить диск как надо **до** установки IPCop является более правильным подходом.

2. Расширенная установка

Расширенная установка позволяет более гибко сконфигурировать систему. Этот вариант для нас предпочтительнее, поскольку мы хотим использовать дополнения (а значит, желательно увеличить размер файла подкачки с 32 мегабайт по умолчанию до объёма установленной памяти) а также разместить на машине с IPCop файловое хранилище (а значит, необходимо выделить для него отдельный раздел на диске). Итак, начнём:

1. После загрузки с CD в первом же экране нажимаем F3 для отображения подсказки расширенного режима установки и в нижней строке вводим:

```
vmlinuz lang=en swapfilesize=512 fdisk
```

что означает загрузку ядра vmlinuz со следующими значениями параметров: 1) выбор английского языка и отмены его запроса в дальнейшем (русского языка в описываемой версии нет), 2) установка 512 Мб для файла подкачки, 3) возможность самостоятельно разбить диск на разделы утилитой sfdisk.
Нажимаем Enter и начинаем отвечать на обычные задаваемые инсталлятором вопросы.

2. Когда установка дойдёт до разбиения диска на разделы, инсталлятор выдаст сообщение «NOW FDISK». Переключаемся на третью консоль клавишами Alt+F3 и выполняем команду:

   ```
   sfdisk -l
   ```

   На экран выведется информация обо всех физических дисках, присутствующих в системе, и их разделах. Диски могут называться либо hd(a,b,c,d и т.п.) в случае интерфейса IDE либо sd(a,b,c,d и т.п.) в случае интерфейса SCSI/SATA/SAS, либо ещё как-то в иных случаях. Ниже во всех примерах будут фигурировать диски IDE. У вас же может быть другой вариант, но в контексте настоящей статьи это не имеет значения.

   Определившись с названиями дисков, вводим соответствующую типу диска команду:

   ```
   sfdisk /dev/hda
   ```

   утилита выдаст текущее состояние разделов диска hda и начнёт по порядку запрашивать размеры вновь создаваемых разделов.
3. Размеры разделов запрашиваются не в мегабайтах, а в физических единицах — цилиндрах жёсткого диска. Поскольку вся информация по геометрии жёсткого диска представлена тут же на экране, то перевести одно в другое несложно. Рекомендую посчитать необходимое количество цилиндров для всех разделов заранее, например, подгоняя нужные значения в Excel.

   По своему назначению разделы должны следовать в строго определённой последовательности. Установите приблизительно следующие пропорции разбиения диска на разделы:

   hda1 — 1% но не менее 10 Мб (загрузочный — /boot)
   hda2 — 33% (логи — /var/log)
   hda3 — 50% (общедоступные папки — /mnt/sharedfolders)
   hda4 — 16% (корневой — /)

   Задание размеров разделов в sfdisk производится следующим образом. Сначала пишется номер начального цилиндра первого раздела (0), затем — высчитанное для 10 Мб количество цилиндров (например, 20), затем — тип радела (L — Linux) и в конце — символ загрузочного раздела (*). Все параметры разделяются пробелами:

   ```
   /dev/hda1 :0 20 L *
   ```

   в следующих двух разделах просто набираем первый цилиндр раздела и их количество, например:

   ```
   /dev/hda2 :20 20000
   /dev/hda3 :20020 30000
   ```

   а в последнем разделе просто нажимаем Enter. Под него автоматически распределится всё оставшееся пространство. На запрос о внесении изменений на диск отвечаем «y» и нажимаем Enter.
4. После записи новой таблицы разделов на диск программа завершает работу. Переключаемся снова на первую консоль (Alt+F1), нажимаем кнопку ОК и продолжаем обычную установку.

Замечу, что кроме создания разделов на основном диске, тем же способом вы можете создать разделы и на других подключённых к компьютеру дисках. На каждом физическом диске может быть создано до 4 основных разделов, поэтому утилита sfdisk всегда последовательно предлагает установить размеры всем четырём разделам. Если на каком-либо дополнительном физическом диске вы желаете организовать только один раздел, занимающий весь объём диска, то на запросы о размерах вообще ничего вводить не надо, а на каждое из четырёх приглашений отвечать нажатием на Enter. Утилита автоматически создаст первый раздел величиной во весь диск и 3 раздела нулевого размера, о которых потом можно не вспоминать.

Если необходимо создать на каком-либо физическом диске более четырёх разделов, то один из них следует пометить, как расширенный (E). Тогда, после создания четвёртого раздела, вам будет предложено создать пятый, шестой и т.п. разделы, номера цилиндров которых должны последовательно вписываться друг за другом в диапазон номеров цилиндров расширенного раздела. На диске может быть только один расширенный раздел. В каждом расширенном разделе может быть до 4 разделов, один из которых опять же может быть расширенным, и т.д.

3. Настройка и подключение

В процессе предлагаемой инсталлятором настройки устанавливаем на внутреннем интерфейсе IP-адрес, например, 192.168.0.254 (255-ый адрес занят стандартами под широковещательную рассылку). Можно установить и любой другой свободный адрес локальной сети, но обычно для таких целей используют 254-й адрес, что намного удобнее. Внешний интерфейс настраиваем согласно требованиям провайдера. Замечу, что адресные пространства внешней и внутренней сети не должны пересекаться. Например, если провайдер вам выделил адрес 192.168.4.16, то (учитывая маску 255.255.255.0, характерную для этого диапазона сетей), в вашей локальной сети не должно быть адресов, начинающихся на «192.168.4», однако вы вполне можете использовать адреса, начинающиеся, например, на «192.168.0».

Внимание! Во время установки IPCop отобразит окно «Network configuration menu», в котором необходимо настроить все сетевые параметры, в том числе и DNCP. Если вы пропустите настройку DNCP на этом этапе, то IPCop попросит вас сделать это в конце установки. В этом случае, если просто нажать кнопку отмены, IPCop **пропустит также и установку паролей!** В результате вы не сможете задать пароли для root, admin и backup, а значит, и получить доступ к веб-интерфейсу и командной строке. Поэтому, если вы не используете DNCP, то в окне настройки DNCP необходимо нажать не отмену, а кнопку «OK» при снятой галочке «ENABLED».

После завершения установки машина перезагрузится, и на экране высветится приглашение ввести логин суперпользователя (root) и пароль. Ничего не вводим и оставляем машину в покое. Режим запроса логина-пароля — это обычное рабочее состояние системы IPCop. Можно даже выключить монитор. Соединяем компьютер IPCop с внутренней сетью, и с любого компьютера этой сети пингуем его, набрав в терминале команду ping с сетевым адресом его внутреннего (зелёного) интерфейса, например:

```
ping 192.168.0.254
```

Если пинг не проходит, значит, мы ошиблись сетевой картой — на машине с IPCop перетыкаем шнур в другую сетевую карту и повторяем. Если пинг прошёл, запускаем тут же веб-браузер, и, набрав в адресной строке https://192.168.0.254:445, переходим по этому адресу. На появившееся предупреждение о сертификате безопасности отвечаем положительно. В браузер загрузится интерфейс IPCop.

Можно сразу воспользоваться им, чтобы включить необходимый нам в дальнейшем доступ к IPCop по протоколу ssh: зайти в System -> SSH Access, поставить галочку SSH Access и нажать Save. На появившийся при открытии этой страницы запрос логина и пароля следует ввести логин (admin) и

пароль администратора, который вы задали при установке (операции через веб-интерфейс осуществляются от имени администратора). Доступ по протоколу ssh понадобится нам для дистанционного управления IPCop из его командной строки (от имени суперпользователя (root)) а также для копирования файлов дополнений на машину IPCop, для чего мы будем использовать программы WinSCP и PuTTY.

На этом установка IPCop завершена.

Глава 2. Установка апдейтов IPCop

Для версии 1.4.20, описание установки которой было приведено выше, существует апдейт 1.4.21, который и надлежит установить. Через веб-интерфейс заходим в System -> Updates, выбираем скаченный файл апдейта и нажимаем Upload. Если IPCop уже подключен к Интернету, то проверка на доступные обновления и само скачивание может быть осуществлено непосредственно из веб-интерфейса. После загрузки апдейта устанавливаем его, нажав кнопку «Apply now». Информация об установленном апдейте отобразится в секции Installed Updates IPTABLES.

Часть 3. Установка основных дополнений к IPCop

Глава 1. Общие правила ручной установки дополнений

Для установки дополнений в систему IPCop нам понадобятся две программы дистанционного доступа по протоколу shh для Windows:
WinSCP: http://winscp.net/eng/docs/lang:ru (требуется инсталляция)
PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/ (запускается без инсталляции)

Скачиваем и устанавливаем их, после чего на машине локальной сети:

1. Входим в веб-интерфейс IPCop
   версия 1.4: https:// XXX.XXX.XXX.XXX:**445**
   версия 1.9: https:// XXX.XXX.XXX.XXX:**8443** (информация даётся для справки)
2. Включаем в IPCop доступ по ssh: System -> SSH Access -> Поставить галочку и нажать Save.
3. В WinSCP в разделе Session вводим в поля:
   IP-адрес внутреннего интерфейса машины с ipcop в виде XXX.XXX.XXX.XXX
   Порт: версия 1.4: **222**
   версия 1.9: **8022** (информация даётся для справки)
   Имя: root
   Пароль: тот, что задали для root при установке ipcop
   Private key file: пустое (оставить по умолчанию)
   File protocol: SFTP (оставить по умолчанию)
   Allow SCP fallback: включено (оставить по умолчанию)
4. Нажимаем Save и сохраняем настройки сессии для последующего доступа.
5. Нажимаем Login, в окне предупреждения отвечаем Yes.
6. Копируем архив дополнения, например, в директорию root, в отдельный подкаталог.

На машине IPCop (или на машине локальной сети через PuTTY, настройка которой аналогична WinSCP):

1. Входим как root.
2. Переходим в подкаталог с архивом (cd имя_подкаталога)
3. Набираем для распаковки: tar zxvf, пробел, и нажимаем TAB. Строка допишется единственным именем файла, содержащимся в подкаталоге.
4. Нажимаем Enter. Архив развернётся.

5. Если дополнение было заархивировано вместе с подкаталогом, набираем для входа в развёрнутый каталог: cd имя_подкаталога и нажимаем Enter.
6. Запускаем установку командой ./install -i или ./setup –i (в зависимости от дополнения)

Глава 2. Установка Addon Server

Дополнение, позволяющее выполнять установку некоторых других дополнений (TCAR, Midnight Commander, IPTstat и т.п.) через веб-интерфейс. Очень удобная функция, но для её работы необходимо подключение к Интернету для получения этим дополнением списка доступных дополнений — без этого Addon Server жалуется на устаревший список и отказывается работать, несмотря на то, что нужные дополнения уже скачены. Кроме того, Addon Server нужен даже для ручной установки заточенных под него дополнений — таково требование скрипта установки.

Итак, устанавливаем дополнение согласно общим правилам ручной установки дополнений, описанным выше. Замечу, что дополнение заархивировано вместе с подкаталогом, поэтому после разархивирования не забудьте в него войти (cd addons). Запуск инсталляции осуществляется командой ./addoncfg –i

После перезагрузки веб-интерфейса в конце строки основного меню появится новый пункт — Addons.

Примечание: для удобства инсталляции несовместимых с Addon Server дополнений, а также для упрощения дальнейшего обслуживания системы, вторым же дополнением после Addon Server рекомендую установить командную оболочку, например, Midnight Commander: http://firewalladdons.sourceforge.net/midnight.html.

Глава 3. Установка TCAR

Не могу констатировать, что дополнение TCAR (Traffic Control and Report) выполнено столь же качественно, как, например, BOT, которое мы установим следующим (как в плане скриптов установки, так и в плане гибкости настройки через веб-интерфейс), но это единственное известное мне дополнение, выполняющее отключение отдельных пользователей от Интернета после перерасхода ими установленного трафика за день, неделю или месяц. Из-за наличия этого дополнения, собственно, и был сделан выбор программного файервола в пользу IPCop 1.4.21. Надеюсь, автор этого столь нужного дополнения всё же найдёт в себе силы после длительного перерыва сделать новую версию, совместимую с IPCop 1.9.x (2.0).

Устанавливаем дополнение с помощью Addon Server или вручную, согласно общим правилам ручной установки дополнений. Дополнение заархивировано без подкаталога, поэтому при ручной установке не забудьте создать для него отдельную папку и поместить в неё архив для распаковки. Запуск инсталляции осуществляется командой ./setup

После перезагрузки веб-интерфейса в меню Services появится новый пункт — TrafficControl&Report.

Описываемое дополнение TCAR версии 1.1 b2 от 08.08.2005 разработано для IPCop версии 1.4.4, но работает также и с более новыми версиями этого файервола. Однако при работе с версией IPCop 1.4.21 для корректной отправки почты с отчётами по трафику следует после установки TCAR заменить файл /usr/local/bin/tcar_sendEmail версии 1.5.2, идущий в комплекте с TCAR, на файл последней версии (на текущий момент 1.5.6), который входит в состав пакета SendEmail: http://caspian.dotconf.net/menu/Software/SendEmail/.

Перед осуществлением замены переименуйте файл tcar_sendEmail в папке /usr/local/bin/ в tcar_sendEmail_old, скопируйте файл sendEmail из скаченного пакета в папку /usr/local/bin/, переименуйте его в tcar_sendEmail и поставьте ему права доступа 755. Теперь отправка почты будет проходить корректно.

Иногда не требуется рассылать отчёты о трафике каждому пользователю. Достаточно одного письма на адрес администратора. В этом случае в файле /usr/local/bin/tcar_sendstat.pl необходимо закомментировать строки с 359 по 364.

Если вы хотите получать в файле /var/log/tcar_email.log не краткий, а развёрнутый лог об отправке почты, то в строке 54 нового файла /usr/local/bin/tcar_sendEmail включите режим debug, изменив в этой опции значение с 0 на 1.

Внимание! Перед повторной установкой дополнения не забудьте деинсталлировать предыдущую версию, поскольку скрипт не проверяет систему на наличие уже установленной версии.

Внимание! Правила TCAR стоят перед правилами BOT в списке правил iptables, и если они что-либо запрещают, то BOT этого уже разрешить не может. Поэтому, если нужен доступ из локальной сети к машине IPCop по определённым портам вне зависимости от срабатывания правил в TCAR, требуется прямое добавление разрешающих правил в скрипт /etc/rc.d/helper/tcar-ac.pl (где уже есть похожие правила для портов ssh и веб-интерфейса, а также служб ICMP и DHCP).

Внимание! Если вы хотите отредактировать несколько уже готовых правил в TCAR, делайте это последовательно, по одному. Не отмечайте для редактирования флажками сразу несколько правил, иначе они сотрутся.

Внимание! Дополнение подсчитывает и отображает трафик с некоторой задержкой, достигающей пяти минут. Учитывайте это при проверке работоспособности дополнения, а также при лимитировании трафика. Целесообразно зажать скорость канала для пользователей, чтобы они не успели закачать за этот период слишком много.

Внимание! Дополнение подсчитывает трафик, дошедший до ip-уровня, то есть, оно не учитывает коллизии, множественные перезапросы, ошибки выравнивания, CRC, заголовки фрагментированных пакетов и т.п. Поэтому расхождение трафика TCAR с трафиком, подсчитанным провайдером на физическом уровне (на уровне пакетов), может достигать 15-20%.

Глава 4. Установка BOT

Достаточно качественно сделанное и удобное дополнение, позволяющее контролировать как доступ отдельных компьютеров сети к Интернету, так и их доступ к компьютеру IPCop (например, к веб-интерфейсу или к расшаренным с помощью дополнения SAMBA папкам).

Устанавливаем дополнение согласно общим правилам ручной установки дополнений. Дополнение заархивировано без подкаталога, поэтому не забудьте создать для него отдельную папку и поместить в неё архив для распаковки. Запуск инсталляции осуществляется командой ./setup

После перезагрузки веб-интерфейса в меню Firewall появится два новых пункта — BLOCK OUTGOING TRAFFIC и Advanced BOT Config.

Замечу, что дополнение разрешает доступ к веб-интерфейсу IPCop по mac-адресу компьютера администратора, прописанному в его настройках, поэтому соответствующее правило в разделе IPCop Access для администратора можно не прописывать. Исключение составляет доступ через порт 222 (WinSCP или PuTTY), для которого необходимо прописать правило, предварительно добавив порт 222 в список сервисов Firewall -> Advanced BOT Config. При добавлении правил не забудьте их включать.

Внимание! Правила BOT стоят после правил TCAR в списке правил iptables, а потому не могут разрешить то, что уже запрещено в TCAR. Кроме того, всё, что явно не разрешено в BOT — запрещено.

Глава 5. Другие полезные дополнения

Кроме вышеописанных дополнений для IPCop 1.4.21 существует множество других, и некоторые из них тоже можно порекомендовать. Например, дополнение IPTstat позволяет просматривать текущие правила iptables, что очень полезно, например, для анализа того, какие изменения в правила внесли те или иные дополнения контроля трафика. Дополнение Net-Traffic позволяет просматривать объёмы входящего и исходящего трафика по разным интерфейсам. Дополнение sysinfo отображает всю информацию о железе, а также о статусах выполняющихся процессов.

Часть 4. Установка дополнения SAMBA

Дополнение SAMBA позволяет делать общедоступными (далее — «расшаривать» от англ. share — владеть совместно) в локальной сети определённые папки, расположенные на компьютере IPCop. Это нужно для создания некой общей среды хранения файлов или обмена документами, которая была бы независима от работы остальных компьютеров сети. Доступ к сервису при желании можно регулировать описанным выше дополнением BOT.

Для успешной работы SAMBA необходимо произвести некоторые подготовительные действия, такие, как смена текущего порта веб-интерфейса 445 (SAMBA использует тот же порт), соответствующая настройка дополнений BOT и TCAR, а также постоянное открытие рабочих портов SAMBA в TCAR.

Для смены текущего порта веб-интерфейса необходимо установить дополнение GUIPorts и с его помощью сменить порт с 445 на 8443, который, кстати, уже используется новой версией IPCop 1.9.x (2.0).

Далее в этой части будут подробно описаны все вышеупомянутые шаги.

Глава 1. Установка GUIPorts

Устанавливаем дополнение согласно общим правилам ручной установки дополнений. Дополнение заархивировано вместе с подкаталогом, поэтому после разархивирования не забудьте в него войти (cd guiports). Запуск инсталляции осуществляется командой ./install -i

После установки обновляем веб-интерфейс и заходим в System -> GUI Settings. В появившейся дополнительной секции «GUI Ports Settings» меняем GUI HTTPS Port на 8443 и нажимаем кнопку «save and change». Секция скроется, и порт будет изменён. Теперь для доступа к веб-интерфейсу в адресной строке браузера следует указывать уже новый порт.

Глава 2. Настройка TCAR для работы с SAMBA

По умолчанию TCAR при перерасходе трафика отрубает пользователя от машины IPCop практически полностью (за исключением трафика ICMP, DHCP и GUI IPCop), в том числе отрубает и от расшаренных дополнением SAMBA папок. Поэтому, чтобы этого не происходило, к упомянутым исключениям добавим порты, по которым работает SAMBA.

Для этого в скрипт TCAR /etc/rc.d/helper/tcar-ac.pl в раздел «PREPEARE EXTENDED FILTER CHAINS» в секцию «make access to remote control ports transparent from ANY GREEN or BLUE user's ip to IPCOP» в каждый из четырёх блоков правил добавим аналогичные правила для портов, используемых SAMBA:

901/tcp — SWAT (веб-интерфейс к SAMBA)
445/tcp — SAMBA (правило уже существует, поскольку этот порт использовался для веб-интерфейса)
139/tcp — SAMBA
137/udp — SAMBA
138/udp — SAMBA

Кроме того, добавим правило для нового порта веб-интерфейса IPCop:

8443/tcp — веб-интерфейс IPCop

По умолчанию TCAR подсчитывает весь трафик, прошедший в локальную сеть через внутренний интерфейс IPCop, в том числе и трафик из внутреннего файл-сервера. Чтобы запретить подсчёт внутреннего трафика между IPCop и локальной сетью, откроем на редактирование файл /etc/rc.d/helper/writeipac.pl и просто закомментируем в нём строку 97.

Если помимо этого мы хотим подсчитывать для пользователей не только входящий, но и исходящий Интернет-трафик, то строку 97 не комментируем, а просто удаляем из неё вертикальную палочку, стоящую перед $userip и ставим её после этого параметра, а вместо ipac~i пишем ipac~fi.

Вообще, в этом скрипте мы можем сформировать разные варианты подсчёта трафика, дополнив его для этого нужными строками. Скрипт формирует правила подсчёта трафика, сохраняя их в конфигурационном файле /etc/ipac-ng/rules.conf, который в дальнейшем используется утилитой подсчёта трафика ipac-ng. Ниже приведён пример пронумерованных строк скрипта writeipac.pl, формирующих некоторые правила (само правило указано в кавычках). При копировании в свой скрипт номера строк удалите:

```
97  print FILE "$username|ipac~fo|$useripinterfacename|all||$userip||\n"; #from Internet to client
98  print FILE "$username|ipac~fi|$useripinterfacename|all|$userip|||\n"; #from client to Internet
99  print FILE "$username|ipac~i|$useripinterfacename|all||$userip||\n";  #from client to ipcop
100 print FILE "$username|ipac~o|$useripinterfacename|all|$userip|||\n";  #from ipcop to client
```

Формат строки правил:

1. Наименование правила по имени пользователя (только латиница, цифры и пробелы). В приведённом выше фрагменте скрипта имя пользователя находится в переменной **$username**.
2. Направление подсчитываемого трафика (указываются названия цепочек соответствующего назначения в iptables, в которые будут вписаны эти правила).
   ipac~fo — трафик из Интернета в локальную сеть (Forwarding Out — форвардинг внешнего)
   ipac~fi — трафик из локальной сети в Интернет (Forwarding In — форвардинг внутреннего)
   ipac~i — трафик только на машину IPCop на указанный интерфейс (Input — входящий в IPCop)
   ipac~o — трафик только с машины IPCop с указанного интерфейса (Output — исходящий с IPCop)
3. Интерфейс, чрез который идёт подсчитываемый трафик (eth0, eth1 и т.п.)
4. Протокол (tcp, udp, icmp, или all), трафик которого подсчитывается
5. IP источника (0/0 - любой IP). Можно включать маску (напр./24) и порт (через пробел)
6. Целевой IP (те же правила записи, что и для источника)
7. Расширения для netfilter

Если TCAR настраивался и включался ранее, то все его цепочки правил в iptables уже существуют, и откорректированное дополнение можно смело перезапустить с новыми настройками запуском файла **/usr/local/bin/tcar-reload**. Если же TCAR ещё не настраивался, перезапуск выдаст ошибки и этого делать не следует. Замечу, что после перезапуска новые настройки вступают в силу не сразу, а через несколько секунд.

Напомню, что TCAR по умолчанию запрещает всем доступ в Интернет, поэтому не забудьте добавить в него разрешающие правила.

Глава 3. Настройка BOT для работы с SAMBA

В дополнении BOT необходимо сменить порт веб-интерфейса, чтобы оно во время перекрытия доступа к Интернету не перекрывало доступ к веб-интерфейсу IPCop. Для этого в веб-интерфейсе открываем Firewall -> Block Outgoing traffic и отключаем дополнение, если оно включено (при включенном BOT поменять порт невозможно). В разделе установок нажимаем кнопку Edit и меняем HTTPS Port на 8443. Нажимаем Save и снова включаем BOT. Замечу, что порт можно также поменять непосредственно в файле настроек /var/ipcop/fwrules/settings.

Теперь в секцию правил IPCop Access необходимо добавить несколько разрешающих правил:

1. Прежде всего, разрешим доступ с компьютера администратора через порт 222/tcp&udp. Это позволит соединяться с IPCop с помощью WinSCP и PuTTY. Порта 222 в списке сервисов нет, поэтому добавим его туда через веб-интерфейс Firewall -> Advanced BOT Config.
2. Для работы веб-интерфейса SAMBA разрешим доступ для компьютера администратора через порт 901 (SWAT). Он есть в списке служб.
3. Для работы собственно SAMBA откроем в локальную сеть ещё 4 порта: 445, 139, 137 и 138. Для удобства на странице Firewall -> Advanced BOT Config создадим группу сервисов, и наберём в неё сервисы, соответствующие вышеперечисленным портам. Теперь, на основой странице BOT добавим правило с этой группой, открывающее доступ по этим портам либо для всей сети сразу, либо для отдельных компьютеров. Можно также сначала открыть доступ для всей сети, а затем создать запрещающие правила для отдельных компьютеров, которые поставить в начало, до разрешающего правила.

Глава 4. Подключение раздела для общедоступных папок

Если в процессе расширенной установки IPCop мы выделили на диске отдельный раздел для общедоступных папок, то теперь нам следует его отформатировать и смонтировать. Запускаем PuTTY (или садимся за машину с IPCop), входим в систему от имени суперпользователя (root), и выполняем команду:

```
mke2fs -m 0 -j /dev/hda3
```

где

-m 0 — отмена пятипроцентного резервирования блоков для суперпользователя
-j — форматирование в файловую систему ext3

После того, как утилита создаст журнал и запишет служебную информацию в раздел, её работа завершится. Теперь в каталоге /mnt создадим каталог для точки монтирования (принадлежащий пользователю samba и группе samba), например, /sharedfolders, и выполним команду:

```
mount /dev/hda3 /mnt/sharedfolders
```

раздел будет смонтирован в подготовленный нами каталог.

Если всё прошло успешно, значит, мы всё сделали правильно, и можно автоматизировать произведённое выше монтирование, чтобы оно всегда происходило при старте системы. Для этого открываем файл /etc/fstab и добавляем в него строку:

```
/dev/harddisk3 /mnt/sharedfolders ext3 nodev,nosuid,noatime 1 2
```

где

harddisk3 — символическая ссылка на устройство hda3 (теоретически можно использовать и hda3, но поскольку есть символическая ссылка, следует использовать именно её).
nodev — на монтируемой системе не будут создаваться файлы устройств.
nosuid — не будет возможности делать общими файлы, созданные пользователями разных групп (все файлы в нашем разделе будут создаваться от имени пользователя samba группы samba, поэтому такая возможность нам точно не нужна)
noatime — Не обновлять время доступа к файлу, чтобы ускорить быстродействие.
1 — включить резервное копирование файловой системы утилитой dump. Поскольку самой утилиты dump в составе IPCop нет, то здесь можно поставить и 0.
2 — при загрузке проверять файловую систему не в первую очередь (первая очередь должна быть для корневого раздела).

Кроме раздела harddisk3 тем же способом можно смонтировать к другим каталогам и разделы других дисков, если таковые существуют. Но поскольку символических ссылок типа «harddisk» для них в системе не существует, обращаться к ним можно по их фактическим именам (hdb1, hdc1 и т.п.)

Глава 5. Собственно установка SAMBA

Устанавливаем дополнение согласно общим правилам ручной установки дополнений. Дополнение заархивировано вместе с подкаталогом, поэтому после разархивирования не забудьте в него войти (cd samba).

Внимание! Перед тем, как запустить инсталляцию дополнения samba v0.2.1, откройте файл install на редактирование и в строке 705 смените номер версии с 2.4.34 на 2.4.36. Запуск инсталляции осуществляется командой ./install -i (для деинсталляции SAMBA необходимо таким же образом исправить файл uninstall в папке дополнения /option, а именно поменять версию в строке 459 с 2.4.34 на 2.4.36).

В процессе инсталляции будет запрошено адресное пространство внутренней сети, из которого будет разрешён доступ к общедоступным папкам. Вводим его в следующем виде: 192.168.0.0/24, где 24 означает маску сети (24 единичных бита, что соответствует маске 255.255.255.0). Будьте внимательны, клавиши «Backspace» и «Delete» во время ввода не работают и у вас есть только одна попытка.

После завершения установки и перезагрузки веб-интерфейса в меню Services появится новый пункт — Samba Server. При выборе в веб-интерфейсе этого пункта, помимо пароля администратора будет запрошен логин и пароль суперпользователя (root) для отображения интерфейса SAMBA (SWAT).

Чтобы сделать папку общедоступной, следует прописать в настройках интерфейса SAMBA (Services -> Samba Server -> SWAT) рабочую группу локальной сети (кнопка GLOBALS) и указать общую папку (кнопка SHARES). Для настройки общей папки выбираем из выпадающего списка пункт files, нажимаем кнопку Choose Share и внизу, в поле path, вбиваем адрес общедоступного каталога (например, /home/sharedfolders). Затем нажимаем кнопку Commit Changes. После этого запускаем сервер кнопкой в верхней секции.

Замечу, что после некоторых некорректных действий по управлению Samba-сервером, не все его службы начинают запускаться. Помогает полная деинсталляция и повторная установка дополнения.

Теперь следует изменить права доступа к папке, а именно включить её в группу samba и владельцем сделать пользователя samba. Это можно осуществить как с помощью операционной оболочки Midnight Commander, так и простыми консольными командами:

```
chgrp samba /home/sharedfolders
chown samba /home/sharedfolders
```

Если для общих папок выделен отдельный раздел, не забудьте смонтировать его в систему, например, в каталог /mnt/sharedfolders, и прописать в поле path доступ уже к этому каталогу.

При подключении к общедоступной папке с компьютеров локальной сети, система запросит логин (samba) и пароль (samba), которые необходимо будет ввести для открытия доступа и сохранить для дальнейшего использования, поставив в окошке ввода пароля соответствующую галочку.

Дополнительную информацию о SAMBA и её настройке можно найти здесь:
http://rus-linux.net/lib.php?name=/MyLDP/server/samba-security/samba-security-1.html
http://www.osp.ru/lan/2000/03/130995/_p1.html
http://samba-doc.ru/samba3example/index.html
http://smb-conf.ru/

Часть 5. Дополнительная информация

Неплохой справочный материал по Linux (30 страниц) можно скачать и распечатать отсюда:
ftp://diyaorg.dp.ua/books/LinuxShortAll.pdf

Глава 1. Полезные файлы и каталоги IPCop

/etc/fstab – файл, содержащий команды автоматического монтирования накопителей при старте системы.
/etc/rc.d/helper/tcar-ac.pl – скрипт дополнения TCAR, в котором можно изменить настройки порта веб-интерфейса а также добавить свои порты, которые не должен блокировать TCAR ни при каких условиях.

/usr/local/bin/tcar_sendstat.pl – скрипт TCAR отправки статистики почтой, в котором можно отключить рассылку, закомментировав определённые строки.
/usr/local/bin/tcar-reload – перезагрузка дополнения TCAR.
/usr/local/bin/restarthttpd – перезапуск веб-сервера.

/usr/sbin/httpd – каталог содержит программы различных сервисов.

/var/ipcop – настройки файервола и дополнений.
/var/ipcop/fwrules – скрипты и настройки дополнения BOT (**/settings** – настройки порта и mac-адреса для работы веб-интерфейса).
/var/ipcop/tcar – настройки и шаблоны отчётов TCAR (**/settings** – здесь можно отключить дополнение, не пользуясь веб-интерфейсом, если вдруг оно заблокировало веб-интерфейс).

/var/log – логи работы IPCop и дополнений. Очень полезно периодически их просматривать, чтобы во-время заметить и исправить ошибку.

Глава 2. Назначение основных каталогов Linux

Более полное описание каталогов:
http://itshaman.ru/articles/10/directory-linux

/bin – системные программы (базовый набор: ls, cp и т.п.).
/boot – ядро Linux, менеджер загрузки GRUB.
/dev – файлы реальных устройств, через которые программы могут обращаться к их драйверам.
/etc – основная часть конфигурационных файлов операционной системы и различных программ.
/etc/rc.d – файлы инициализации системы.
/home – личная информация пользователей системы.
/lib – системные библиотеки, необходимые для работы программ, компоненты ядра и программ
/mnt – файлы смонтированных носителей информации.
/proc – файлы выполняющихся процессов, через которые они сообщают пользователю различную информацию.
/root – домашний каталог суперпользователя.
/sbin – системные программы (дополнительный набор)
/tmp – временнные файлы
/usr – все установленные пакеты программ, библиотеки к ним, ресурсы и исходные коды приложений.
/usr/local/bin – программы, предназначенные для работы только на локальной машине (не общие для нескольких компьютеров) или программы, не входящие в комплект конкретного дистрибутива.
/usr/sbin – дополнительные системные программы.
/var – log-файлы, cache-файлы и другие часто меняющиеся данные.

Глава 3. Некоторые полезные команды Linux:

uname –a — вывести системную информацию
uname –r — вывести только версию ядра Linux.
cd XXX — вход в подкаталог XXX.
ls — просмотр содержимого текущего каталога (ls -l — полная информация)
less XXX — просмотр текстовых файлов
mkdir XXX — создание каталога XXX
rm XXX — удаление файла (опции -r -f — удаление каталога)
cp XX1 XX2 — копирование файлов и каталогов
mv XX1 XX2 — перемещение файлов и каталогов
chgrp — изменение группы файла (см. chgrp --help)
chown — изменение владельца файла (см. chown --help)
chmod — изменение прав доступа файла (см. chmod --help)
tar zxvf XXX — разархивирование файла XXX
vim — запуск текстового редактора
Управление редактором:
i — вход в режим редактирования, ESC — выход из режима;
:w ИмяФайла — запись файла на диск;
:q! — выход из редактора без сохранения файла
sfdisk –l — вывести информацию о всех дисках и разделах системы
sfdisk /dev/hdb — разбиение диска hdb на разделы (hdb1 — hdb4)
mke2fs –m 0 –j /dev/harddisk3 — создание файловой системы ext3 (-j) без резервирования блоков для суперпользователя (-m 0).
mount -t ext3 /dev/hda3 /mnt/shareffolders — монтирование раздела hda3 с файловой системой ext3 к точке /mnt/shareffolders
umount /dev/hda3 — размонтирование раздела hda3

Глава 4. Устранение некоторых неисправностей IPCop

1. Полностью потеряна информация из раздела /dev/harddisk2, который смонтирован в /var/log. В результате не запускается веб-сервер httpd, а следовательно, невозможно подключиться к веб-интерфейсу.
   Решение: httpd не запускается, поскольку не может записать лог в отсутствующую папку. Создайте папку /var/log/httpd и перезапустите веб-сервер, запустив файл /usr/local/bin/restarthttpd (напрямую запустить сервер можно файлом /usr/sbin/httpd).
   Заодно восстановите папку /var/log/ip-acct.