

# IPCop: маршрутизатор на основе Linux

(скачать IPCop <http://www.ipcop.org/>)

[Андрей Пировских](#)

## Введение



Решение же на базе Linux позволит не задумываться о покупке лицензионного ПО.

Сегодня существует множество различных маршрутизаторов/брандмауэров, основанных на Linux. Кстати, некоторые из них мы уже рассматривали, например [m0n0wall](#), [Smoothwall Express](#) и [ClarkConnect](#).

## Аппаратные требования

В сопутствующей документации указано, что минимальные требования для IPCop - материнская плата с процессором 386, 32 Мбайт ОЗУ и жёсткий диск ёмкостью 300 Мбайт. Однако мы рекомендуем использовать более быстрое оборудование, если вам нужны скорости до 6 Мбит/с. Процессор класса Pentium и 256 Мбайт ОЗУ справятся с такой задачей без проблем, а жёсткий диск на 20-40 Гбайт станет прекрасным кэшем для прокси-сервера.

Напротив, использование современного "железа" может вызвать ряд проблем. Например, поддержка PCI Express в IPCop находится на начальной стадии, поэтому с некоторыми интегрированными контроллерами LAN могут возникнуть проблемы. Что касается сетевых адаптеров, использующих стандартную шину PCI, например Intel PRO-1000, то здесь всё будет работать сразу же.

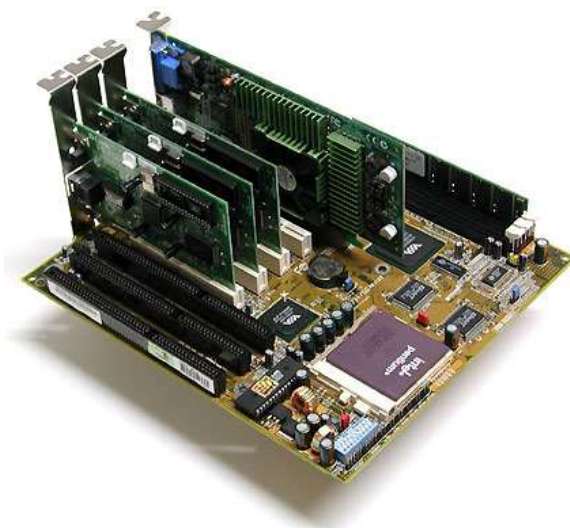


Рис. 1. Система на базе Pentium Socket 7.

В стандартной конфигурации IPCor требует наличия, как минимум, одного сетевого адаптера. Отметим, что даже с дешёвыми адаптерами Fast Ethernet, стоимостью около 150 рублей, проблем не возникает. Так, адаптеры, выполненные на базе чипа Realtek 8139, прекрасно подходят. Если вы хотите наверняка убедиться в поддержке ваших сетевых адаптеров, то рекомендуем ознакомиться со [списком поддерживаемого оборудования](#) (IPCops Hardware Compatibility List - HCL).

Из-за практически полного отсутствия драйверов использование IPCor в качестве беспроводной точки доступа пока достаточно затруднительно и требует серьёзной ручной работы. Поэтому, если вы хотите использовать IPCor в беспроводной сети, рекомендуем установить обычную сетевую карту и подключить к ней точку доступа WLAN. Информацию о том, как настроить такую систему, можно найти на сайте [Host AP-Project](#).

Сколько нужно сетевых карт?

Вообще говоря, количество сетевых карт на маршрутизаторе зависит от задач, которые он будет выполнять. Так или иначе, как минимум, потребуется одна карта. В нашем примере мы будем использовать две, то есть получим классический пример кабельного или DSL-маршрутизатора (см. рис. 2). В такой конфигурации один адаптер подключается к домашней сети ("Green интерфейс"), второй — к сети провайдера или кабельному/DSL-модему ("Red интерфейс").

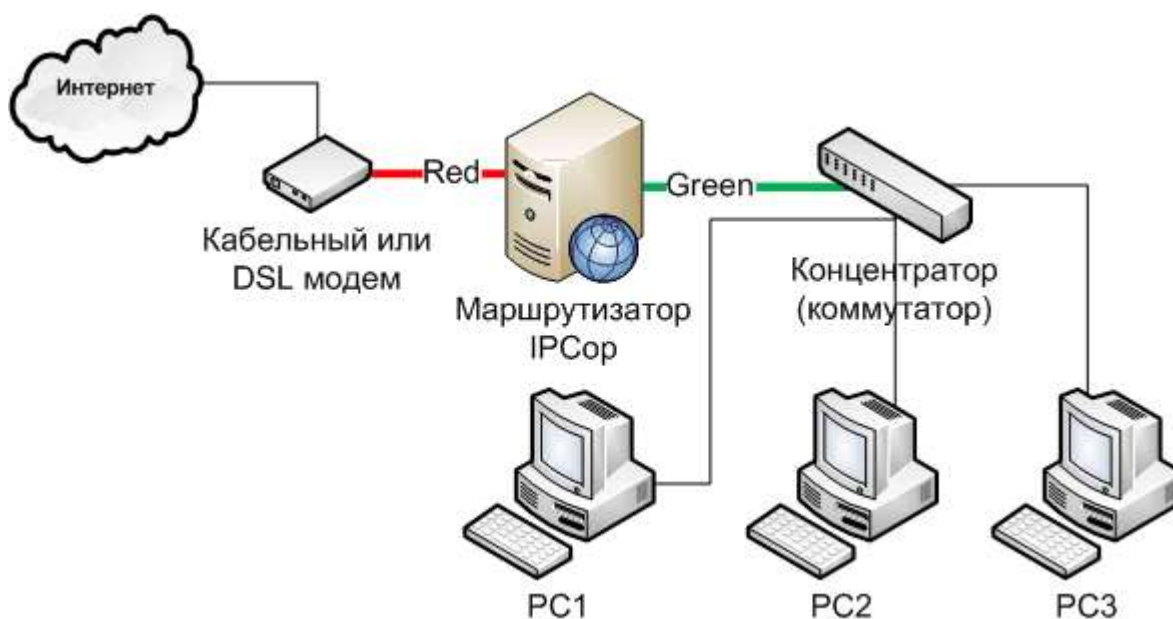


Рис. 2. Схема сети.

Вместо второй карты можно использовать аналоговый модем или ISDN-карту, всё зависит от вашего подключения. Кроме того, можно добавить "Blue интерфейс" для WLAN, и "оранжевый" - для DMZ. На рис. 3 показана максимальная конфигурация с четырьмя картами.

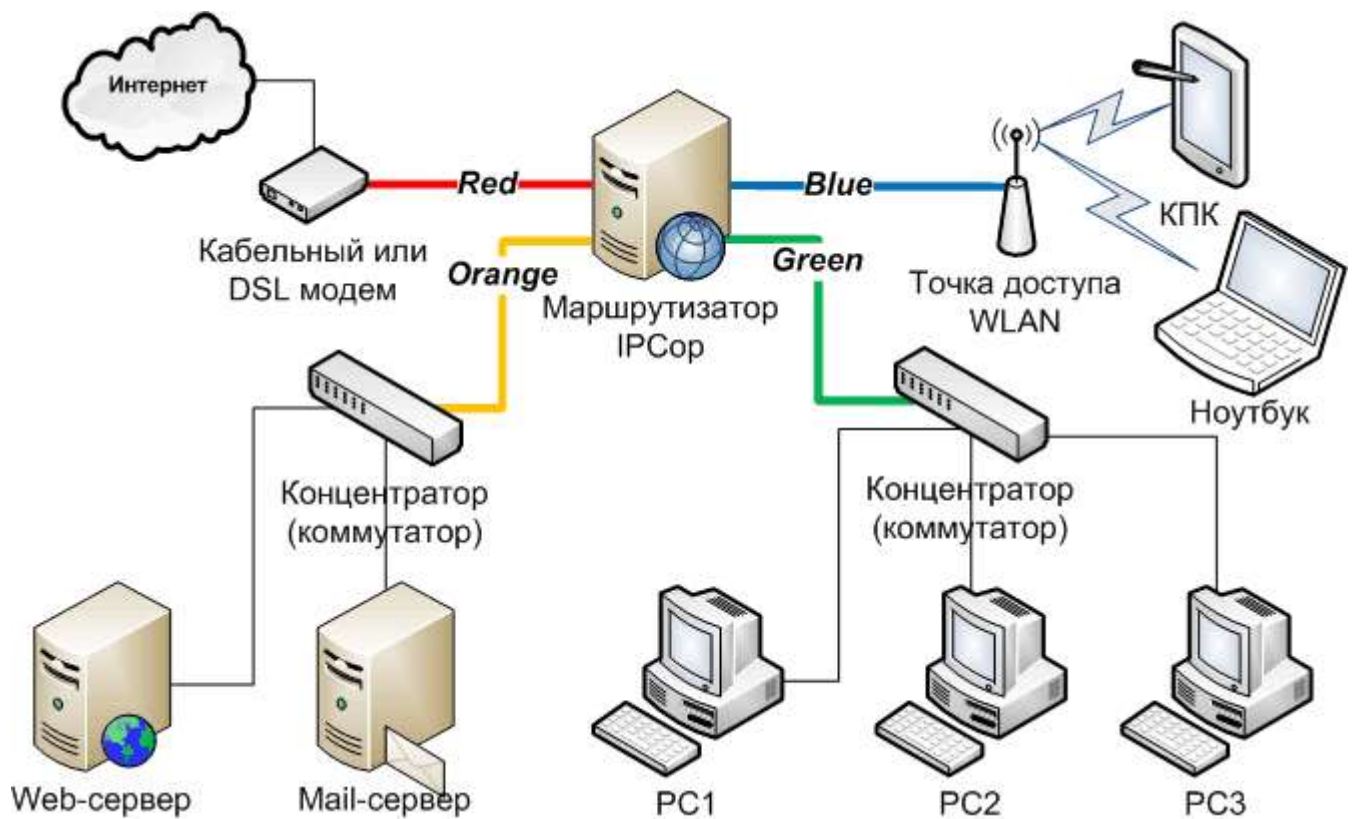


Рис. 3. Топология сложной сети с четырьмя интерфейсами на маршрутизаторе.

### Рекомендуемое аппаратное обеспечение

Процессор - Intel или AMD, например Pentium или выше, 100 МГц или выше.

ОЗУ - 256 Мбайт SDRAM или DDR-SDRAM.

Жёсткий диск - 20-40 Гбайт для кэширования (прокси-сервер).

Сеть - два сетевых адаптера 10/100 Мбит/с.

Видеокарта - любая с памятью от 2 Мбайт, 3D не требуется.

CD/DVD необходим только для установки, после установки можно отключить.

Также для установки может быть использован USB.

FDD не требуется.

Клавиатура необходима только для установки, после установки можно отключить.

### Установка

Как упоминалось ранее, в качестве операционной системы маршрутизатора мы выбрали IPCor. Эта ОС основана на Linux, её исходный код и она сама доступны для свободного скачивания на условиях лицензирования GPL. [Образ ISO CD, объёмом ~ 41 Мбайт](#), можно скачать с сайта IPCor. Также можно воспользоваться образами загрузочных дисков, но в этом случае после загрузки установка пойдёт из сети.

Остановимся на наиболее простом и быстром способе установки, то есть с CD или DVD. Естественно, сначала нужно установить загрузку с привода CD/DVD в BIOS. Напомним, что в большинстве версий BIOS это делается в разделе "Advanced Setup Options" или "Advanced BIOS Setup".

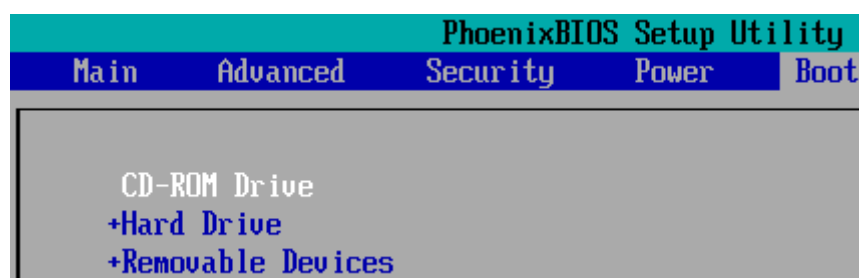


Рис. 4. Настройка загрузки с компакт диска.

Выходим из BIOS, предварительно сохранив настройки (F10) или выбрав в меню пункт "Exit&Saving Changes". На более современных ПК после включения можно нажать F8 (F12 или F2 в зависимости от версии BIOS).

Теперь система будет загружаться с CD/DVD, в результате чего вы увидите загрузчик Isolinux. К сообщению о том, что все данные на жёстком диске будут уничтожены, следует отнестись серьёзно! После этого начнётся разбиение диска на разделы. Так что если на диске осталось что-то важное, сначала сохраните данные в безопасное место!

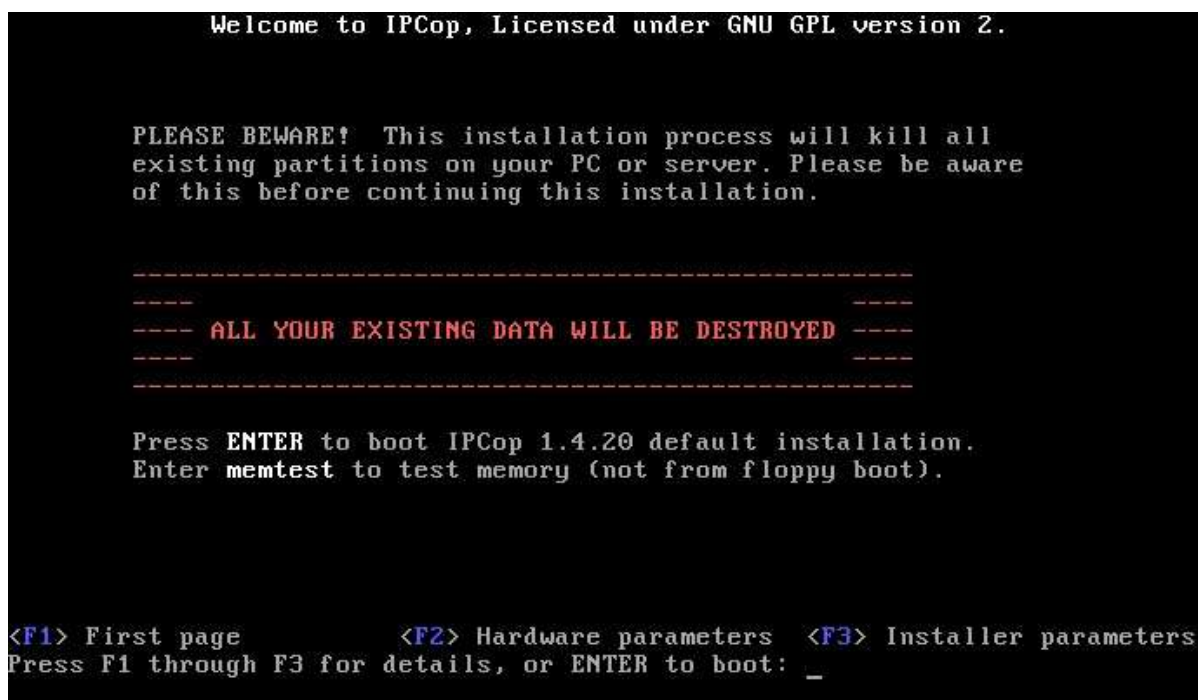


Рис. 5. Старт IPCop с компакт диска.

Нажав клавишу Enter, загружаем ядро Linux. Если на этой стадии возникнут какие-то ошибки, то можно попробовать опции `pousb` и `porcscia` для отключения этих интерфейсов. Поскольку чаще всего маршрутизаторам эти интерфейсы не требуются, то проблем возникнуть не должно.

После загрузки автоматически запускается установка, которая предложит выбрать язык интерфейса. Доступно несколько вариантов, но не все переводы полные. Лучше выбрать английский (см.рис. 6).



Рис. 6. Выбор языка.

Далее появляется предупреждение: выбрав "Cancel" на любом из последующих экранов, вы прекратите установку и перезагрузите систему.



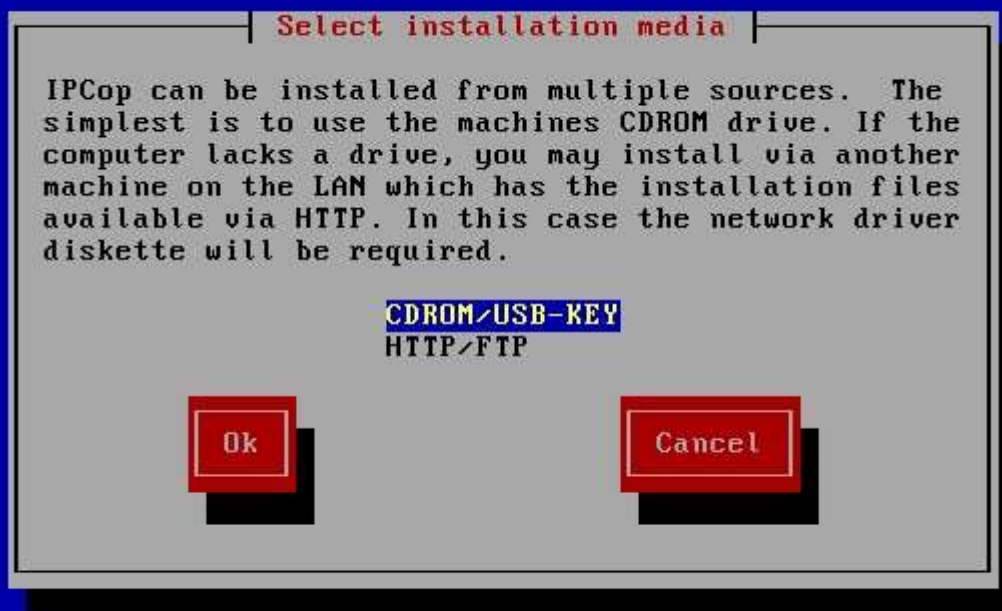
## IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

Затем нужно выбрать, откуда устанавливать систему: с диска или по HTTP/FTP. Если вы загрузились с дискеты, то выбираете HTTP/FTP (при этом надо быть готовым указать IP-адрес сервера!). Конечно, можно выбрать и CD, если, например, диск есть, а возможности загрузиться с него нет. Такое бывает на некоторых старых материнских платах. В нашем случае выбираем CD-ROM.

## IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

Сначала установщик создаёт разделы на жёстком диске и форматирует их. Отметим, что при этом вмешательство пользователя не требуется; система сама исследует диск, создаёт разделы и форматирует их в соответствующей файловой системе. То есть пользователь полностью свободен от вопросов о размерах разделов и вовсе не должен знать, какая файловая система должна использоваться на разделе данных: ReiserFS или ext3.

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

Рис. 6. Просто нажмите ОК.

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

Если вдруг потребуется переустановка маршрутизатора после какого-либо сбоя, то можно воспользоваться сохранением конфигурации на дискету. Если у вас уже есть готовая конфигурация на дискете, то можно указать её и пропустить все экраны установки. Для этого нужно выбрать "Restore/Восстановить" и немного подождать. Но мы устанавливаем всё "с нуля", поэтому выбираем "Skip/Пропустить".

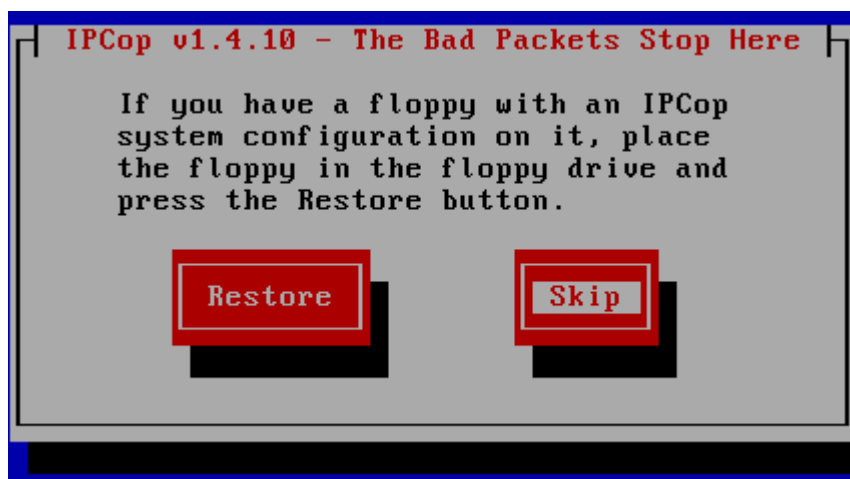
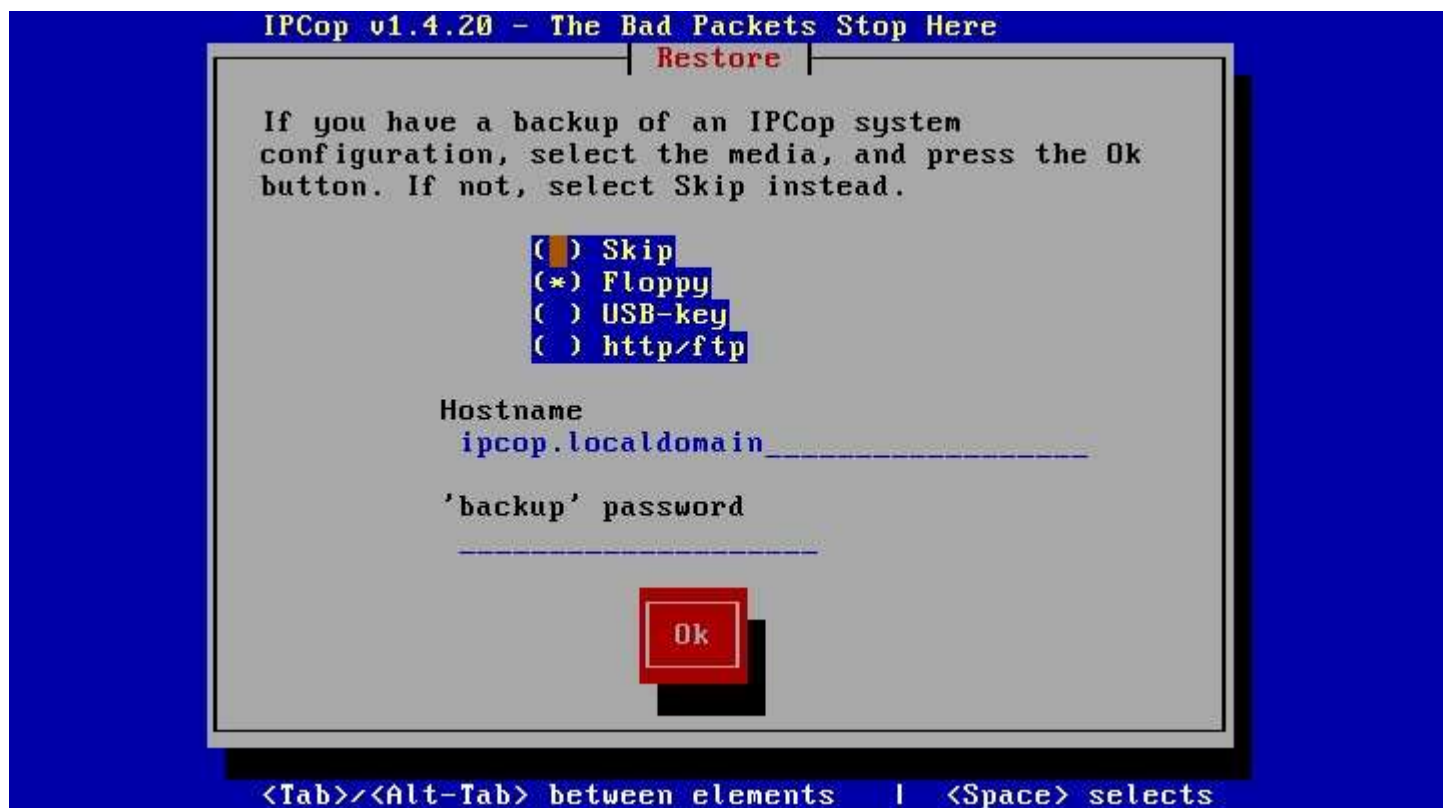


Рис. 7. Запрос на восстановление конфигурации.

#### Настройка интерфейса LAN

IPCop может работать с несколькими интерфейсами в зависимости от сценария использования. "Зелёный" интерфейс присутствует во всех конфигурациях: к нему подключается локальный сегмент сети. Во время установки будет предложено выбрать подходящий драйвер для сетевой карты. В большинстве случаев достаточно указать "Probe/Определить самостоятельно", после чего запустится система автоматического определения, которая обычно хорошо справляется с заданием (Рис. 9).





Рис. 8. Настройка сетевого адаптера.



Рис. 9. Удачная попытка определения.

Если всё же карта не определилась автоматически, придётся установить драйвер вручную, указав для этого "Select/Выбрать".

Если имя, которое выдаст IPCop, не совпадает с названием карточки, не стоит беспокоиться: ядро Linux определяет карточки по чипу, а не по номеру модели. Именно поэтому карточки D-Link могут определиться как Realtek 8139.

После определения сетевого адаптера нужно назначить интерфейсу IP-адрес. Так как мы настраиваем интерфейс LAN, который подключается к домашней сети, то рекомендуем выбрать адрес из одного из зарезервированных диапазонов.

10.0.0.0 - 10.255.255.255 (10/8 prefix)

172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Подробнее о распределении диапазонов адресов можно узнать в [RFC1918](https://www.rfc-editor.org/rfc/rfc1918).

Мы остановились на наиболее часто используемом диапазоне 192.168.0.1 - 192.168.0.254, присвоив нашему маршрутизатору последний адрес диапазона (Рис. 10), при этом маска сети составила 255.255.255.0. Этой настройки достаточно для подключения к сети до 253 сетевых устройств.



Рис. 10. Установка IP-адреса IPCop.

На этом первая часть установки завершена (Рис. 11). Все дополнительные параметры можно подкорректировать позже. Сейчас система уже готова к загрузке.

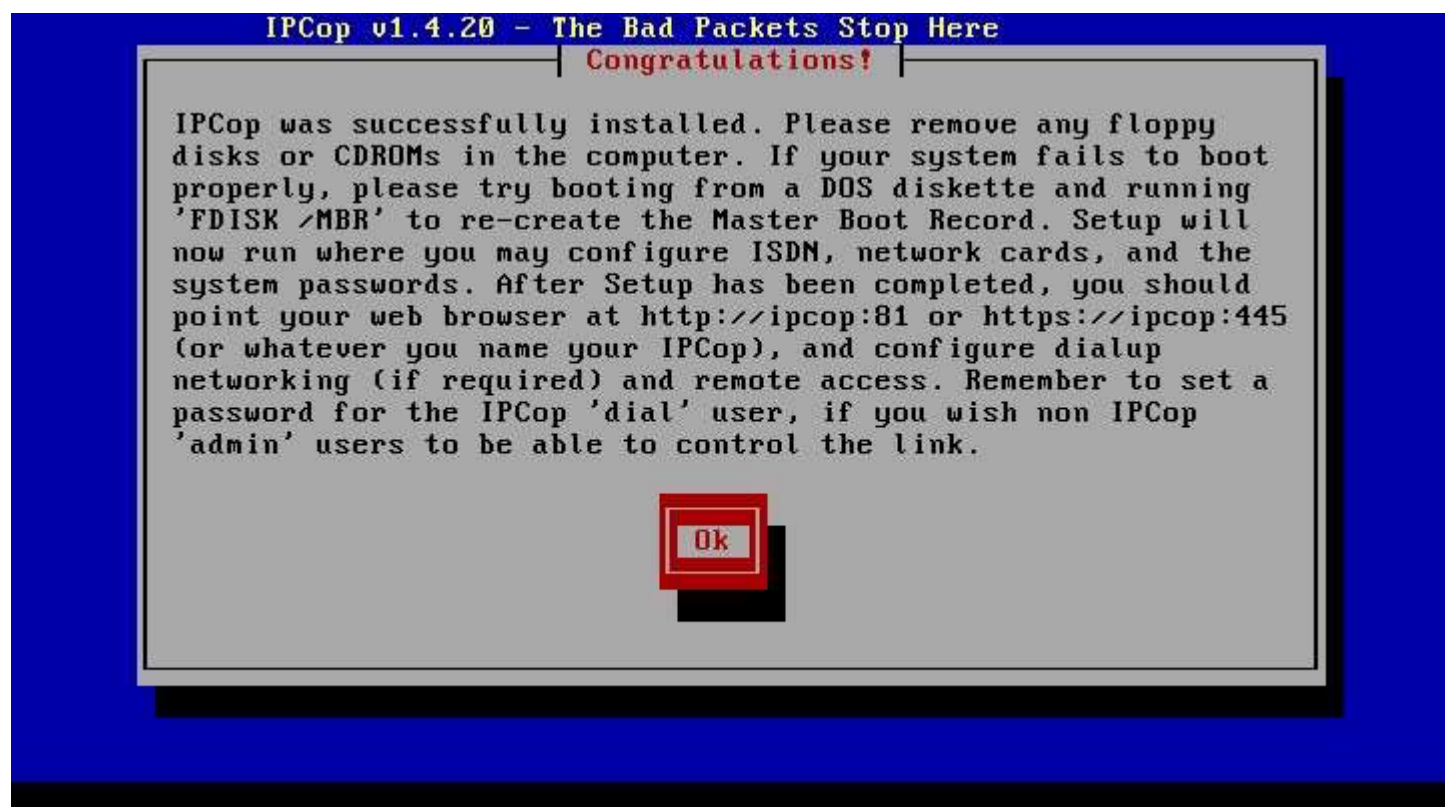


Рис. 11. Установка завершена.

Достаточно часто случается так, что после установки забываются параметры устройства. Поэтому рекомендуем записать наиболее важную информацию, то есть IP-адрес и имя устройства. Это

займёт не больше минуты, но в дальнейшем позволит сэкономить не только драгоценное время, но и нервы.

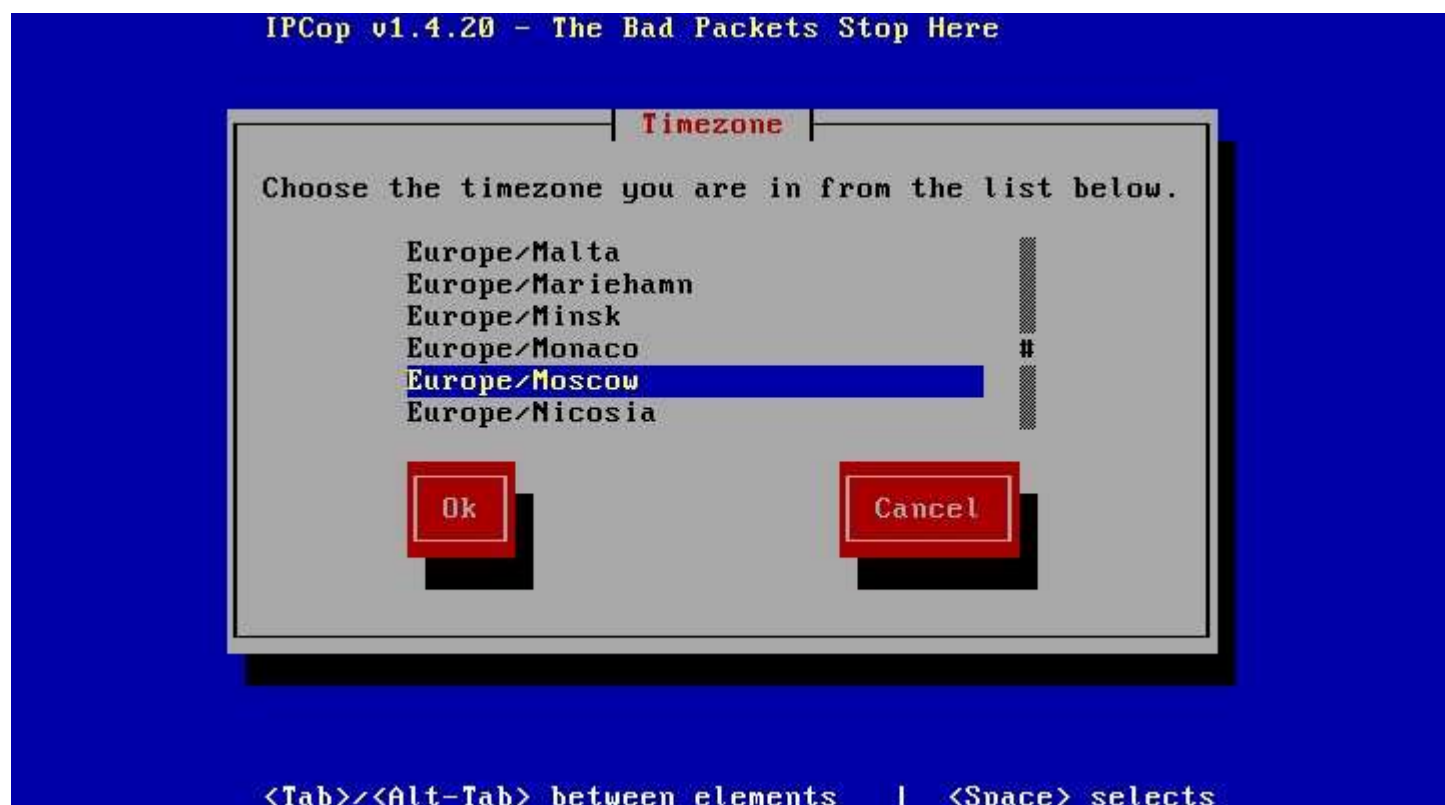
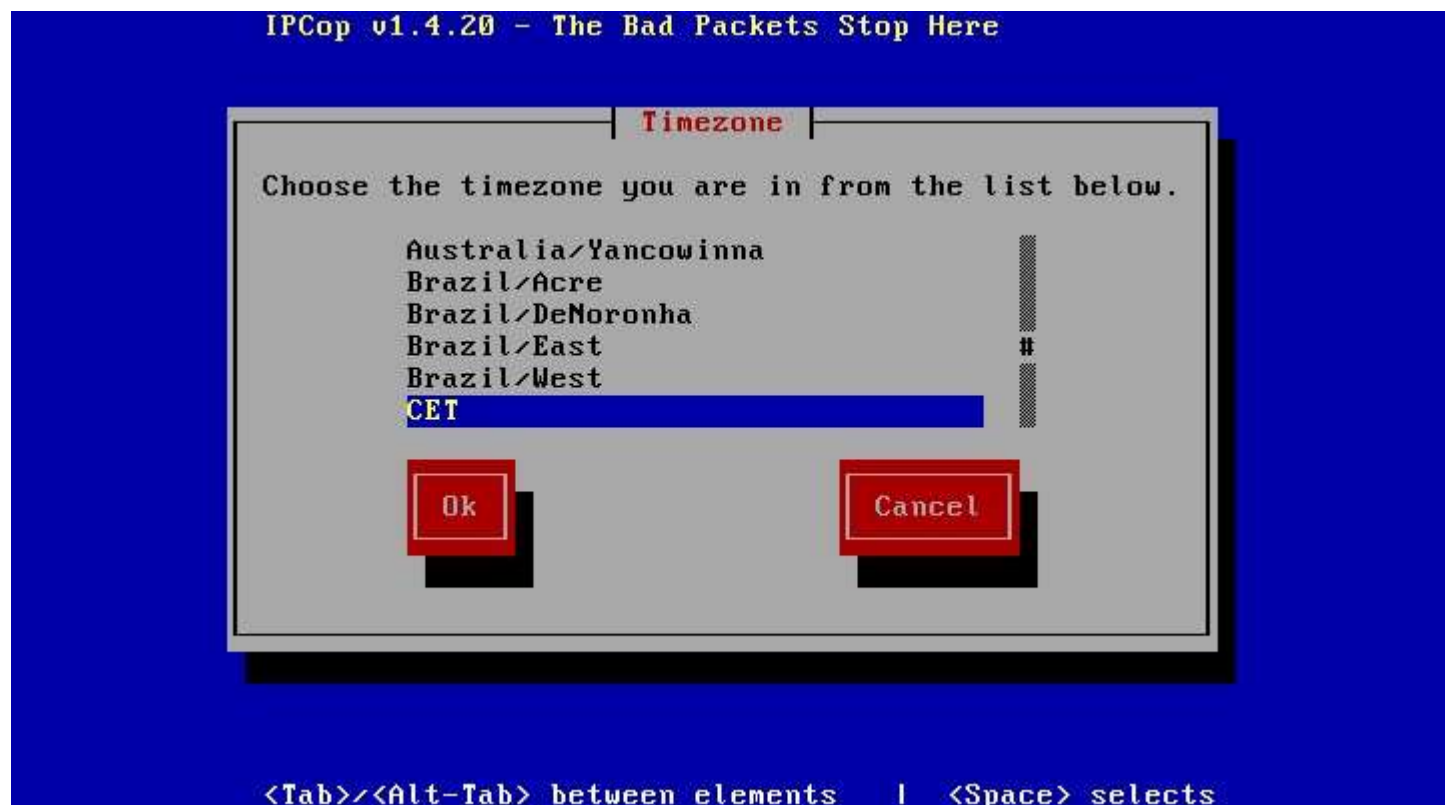
<http://ipcop:81>

<https://ipcop:445>

<https://ipcop:8443> (для версии 2.0.3 IPCop)

Отметим, что номера портов также очень важны, поскольку они не являются стандартными (81 и 445), хотя и не далеки от таковых HTTP (80) и HTTPS (443). Вместо имени можно использовать IP-адрес, в нашем случае 192.168.0.254.

Настройка основных параметров завершена, однако, нужно задать ещё ряд дополнительных: раскладку клавиатуры, если вы пользуетесь отличной от "QWERTY", а также выбрать часовой пояс.



Далее будет предложено задать имя машины IPCop, по которому, как и по IP-адресу, можно будет обратиться к системе из Windows. Под этим именем маршрутизатор будет виден в сети. По умолчанию используется имя ipcop, оставим его.

IPCop v1.4.20 - The Bad Packets Stop Here

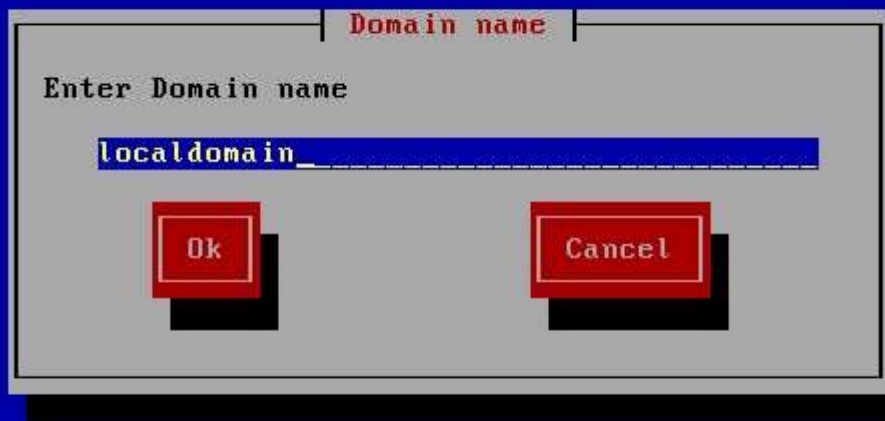


A screenshot of a Windows-style dialog box titled "Hostname" in red text. The dialog has a grey background and a black border. Inside, the text "Enter the machine's hostname." is displayed. Below this, a text input field contains the text "ipcop\_". At the bottom of the dialog, there are two red buttons with black outlines: "Ok" on the left and "Cancel" on the right. The entire dialog is centered on a solid blue background.

<Tab>/<Alt-Tab> between elements | <Space> selects

Домен можно также оставить по умолчанию - localdomain, если, конечно, ваша сеть не использует домены.

IPCop v1.4.20 - The Bad Packets Stop Here



A screenshot of a Windows-style dialog box titled "Domain name" in red text. The dialog has a grey background and a black border. Inside, the text "Enter Domain name" is displayed. Below this, a text input field contains the text "localdomain\_". At the bottom of the dialog, there are two red buttons with black outlines: "Ok" on the left and "Cancel" on the right. The entire dialog is centered on a solid blue background.

<Tab>/<Alt-Tab> between elements | <Space> selects

Напомним, что IPCop может работать с адаптерами ISDN. Мы таковой не использовали, поэтому выбрали "Disable ISDN" и продолжили.

ISDN configuration menu

ISDN is currently Disabled.

Protocol: UNSET

Card: UNSET

Local phone number: UNSET

Select the item you wish to reconfigure, or  
choose to use the current settings.

**Protocol/Country**

Set additional module parameters

ISDN card

Local phone number (MSN/EAZ)

Ok

Enable ISDN

Disable ISDN

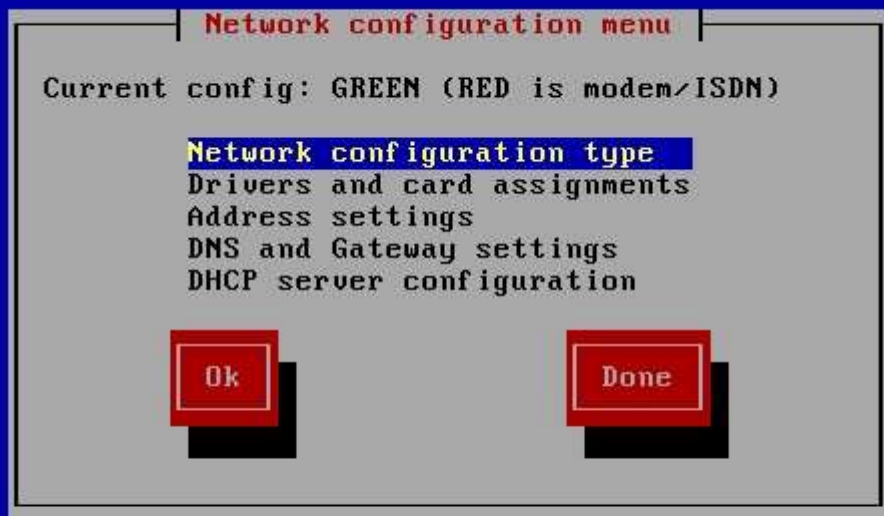
<Tab>/<Alt-Tab> between elements | <Space> selects



## Настройка интерфейса WAN и сервера DHCP

Ранее мы уже определили локальный "зелёный" интерфейс, сейчас нужно выбрать и настроить интерфейс WAN или "красный". На Рис. 12 и 13 показано, как это сделать.

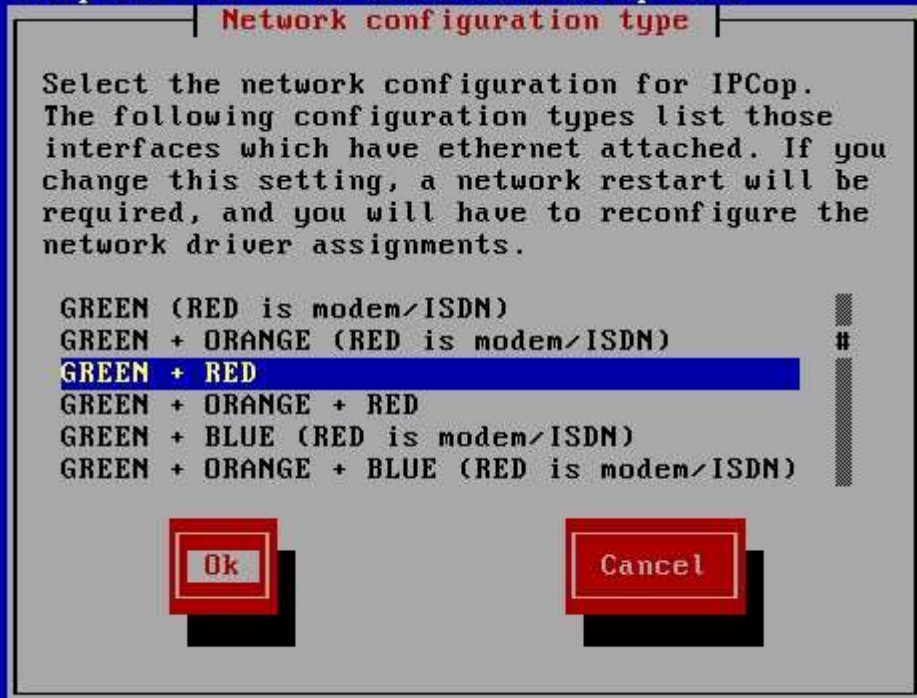
IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

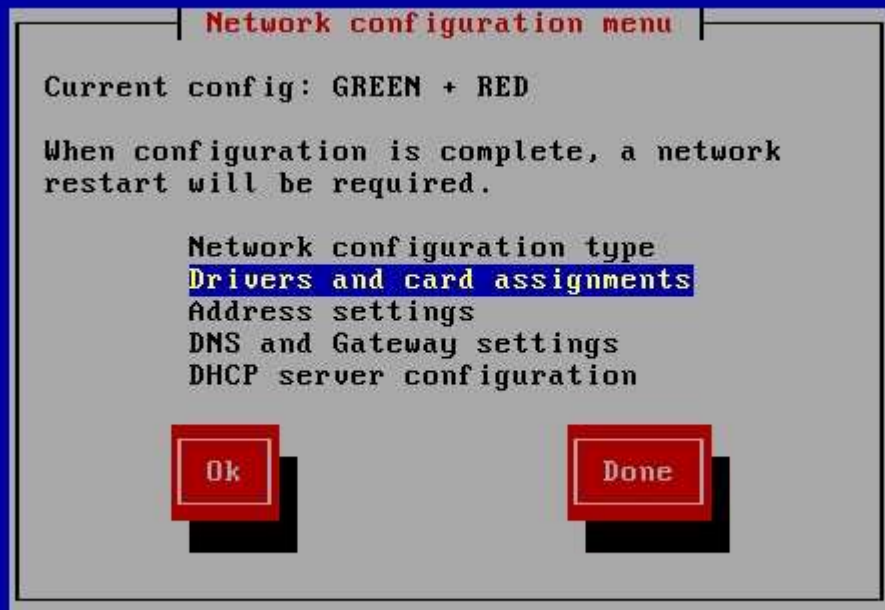
Рис. 12. Настройка сети.

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

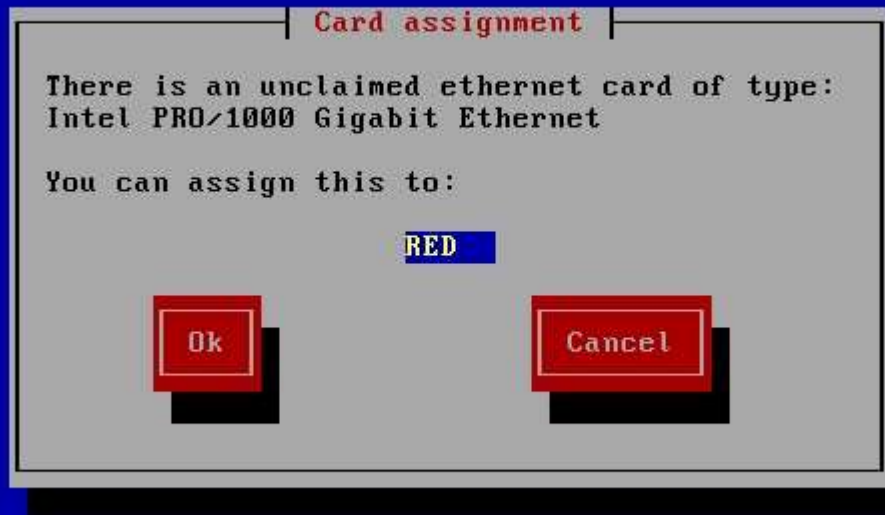
Рис. 13. Наш вариант - "зелёный" и "красный" интерфейсы.



<Tab>/<Alt-Tab> between elements | <Space> selects



<Tab>/<Alt-Tab> between elements | <Space> selects



<Tab>/<Alt-Tab> between elements | <Space> selects



<Tab>/<Alt-Tab> between elements | <Space> selects



<Tab>/<Alt-Tab> between elements | <Space> selects



<Tab>/<Alt-Tab> between elements | <Space> selects

**GREEN interface**

Enter the IP address information for the GREEN interface.

IP address: 192.168.209.238

Network mask: 255.255.255.0

Ok
Cancel

<Tab>/<Alt-Tab> between elements | <Space> selects

**Address settings**

Select the interface you wish to reconfigure.

GREEN

RED

Ok
Done

<Tab>/<Alt-Tab> between elements | <Space> selects

Если потребуется, можно также настроить "синий" и "оранжевый" интерфейсы для беспроводной сети и демилитаризованной зоны, соответственно. Конечно, это не значит, что сервер из локального сегмента нельзя "выставить" наружу без DMZ, однако вариант с DMZ является более безопасным.

После создания нужной конфигурации, вы попадаете обратно в раздел "Настройка сети/Network Configuration Menu", где следует выбрать драйверы для сетевых карт и задать физическое распределение интерфейсов по картам. Внешний, или "красный" интерфейс также нуждается в настройке параметров IP, что и показано на следующем скриншоте (Рис. 14).



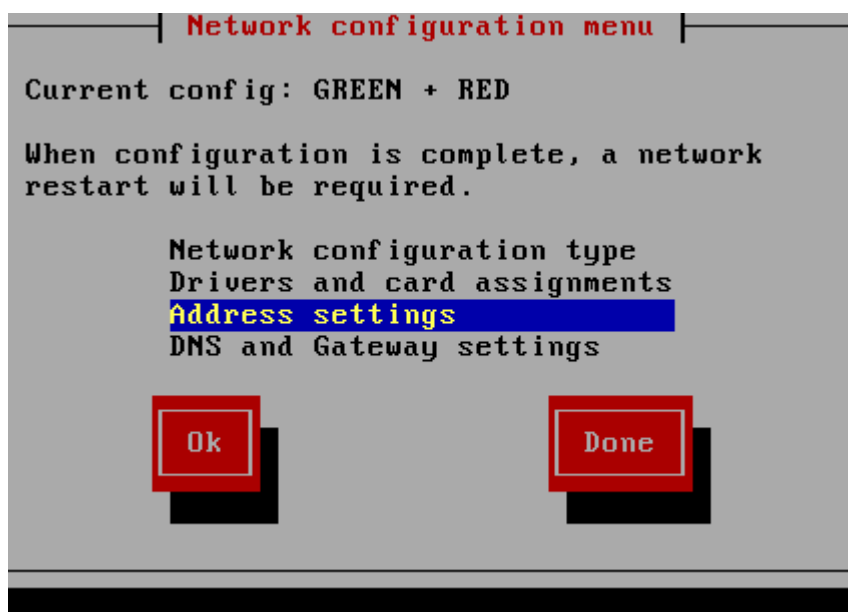


Рис. 14. "Красному" интерфейсу тоже следует задать IP-адрес.

При настройке порта WAN, нам нужно указать, какой тип соединения мы будем использовать.

На Рис. 15 показаны доступные типы подключения WAN.

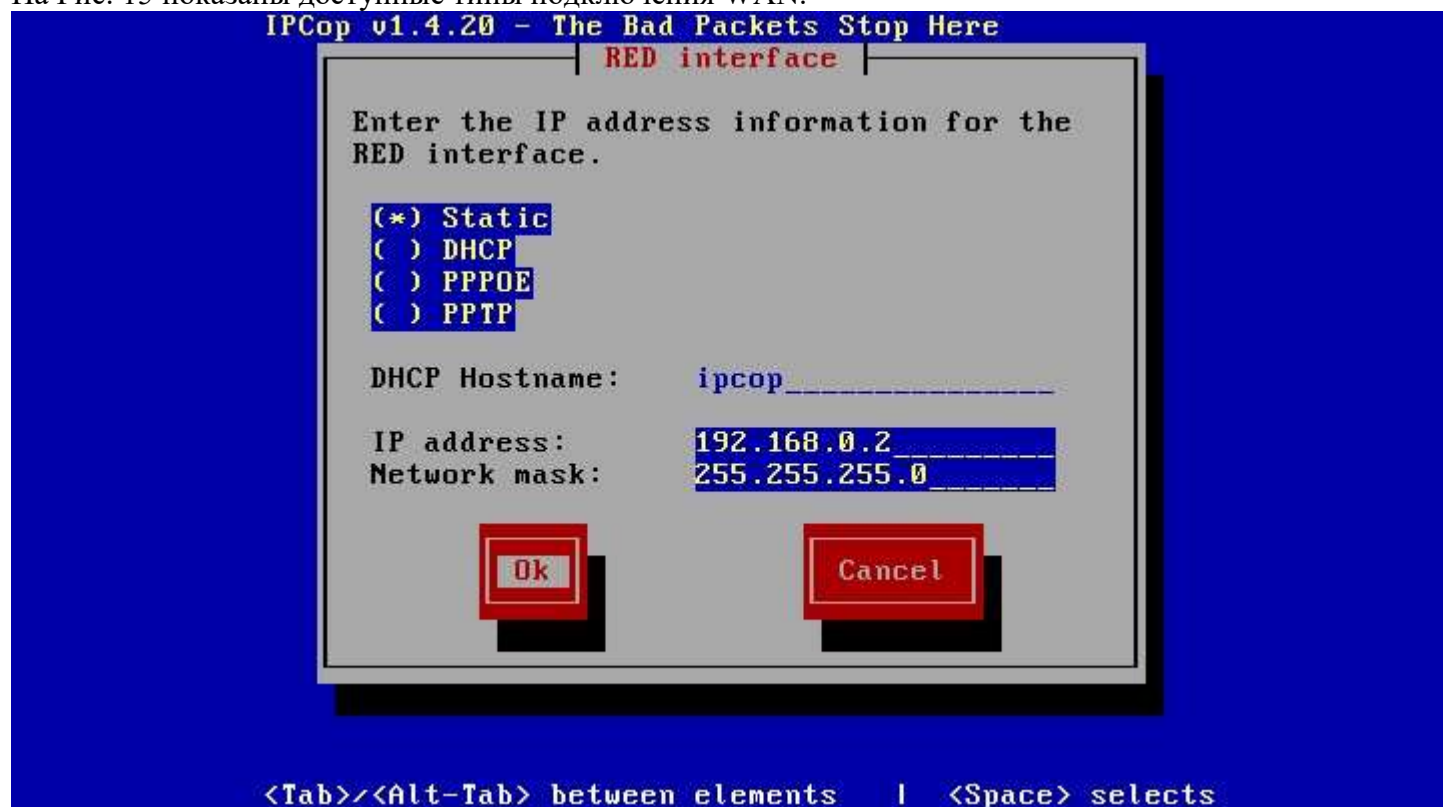


Рис. 15. Варианты подключений "красного" интерфейса (Интернет).

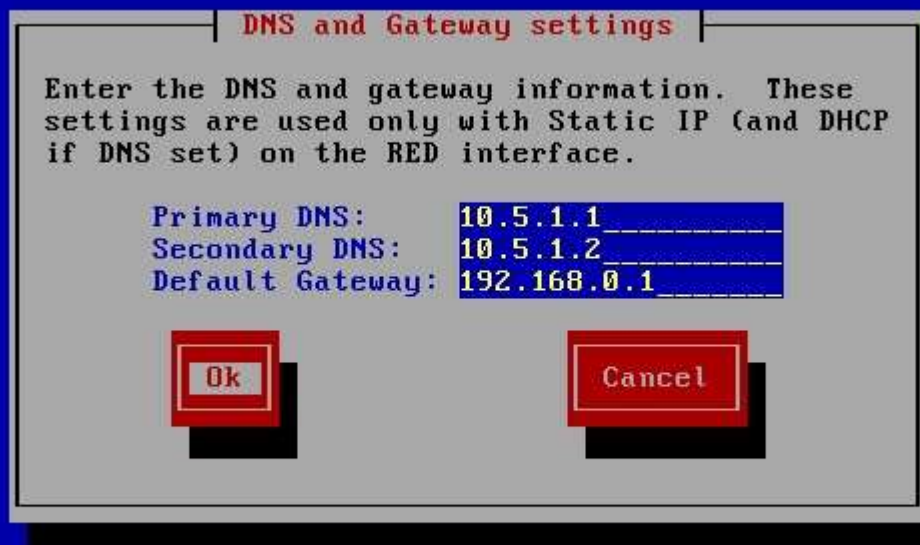
Чаще всего пользователи кабельных модемов выбирают DHCP, пользователи DSL - PPPoE, однако окончательно определить, какой тип соединения вам нужно использовать, подскажет только провайдер.

Пользователи, работающие с подключением со статическим адресом, должны указать адреса DNS-сервера и шлюза (Рис. 16 и 17).



<Tab>/<Alt-Tab> between elements | <Space> selects

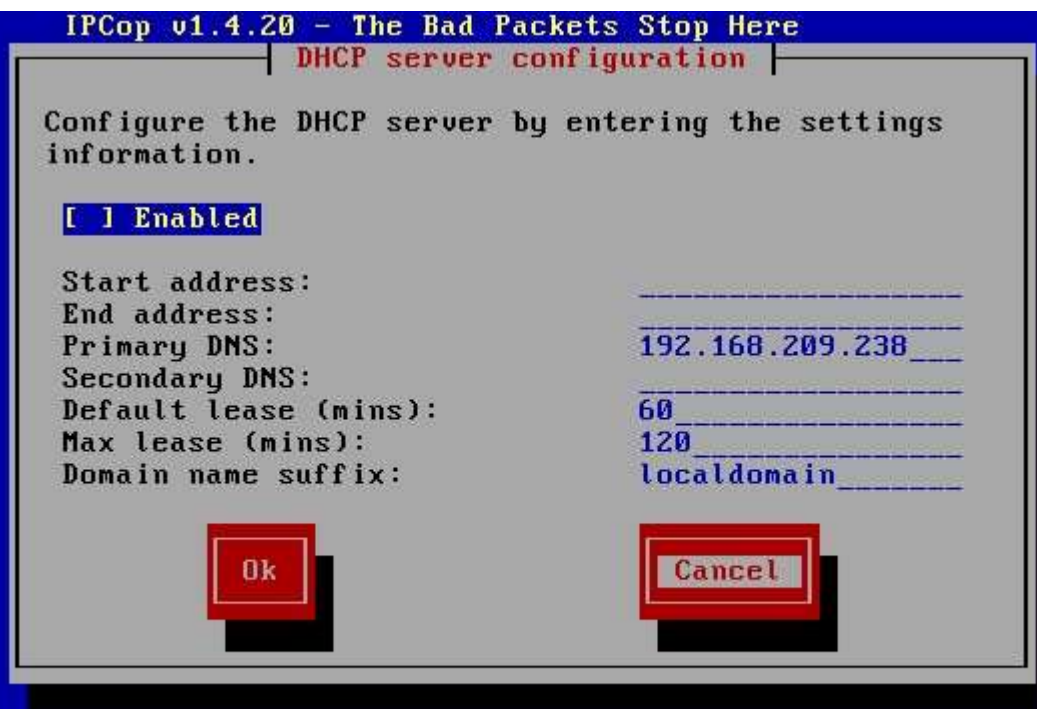
Рис. 16. Настройки DNS и шлюза.



<Tab>/<Alt-Tab> between elements | <Space> selects

Рис. 17. Настройки DNS и шлюза.

IPCop имеет встроенный сервер DHCP, поэтому клиенты LAN могут автоматически получать IP-адреса, а также адреса шлюза и сервера DNS. Как показано на Рис. 18, в настройках DHCP можно задать начальный и конечный адреса диапазона, а также адреса серверов DNS и срок аренды адреса. Через web-интерфейс можно зарезервировать некоторые адреса для определённых ПК. Тогда указанные машины при каждом подключении будут использовать один и тот же адрес.

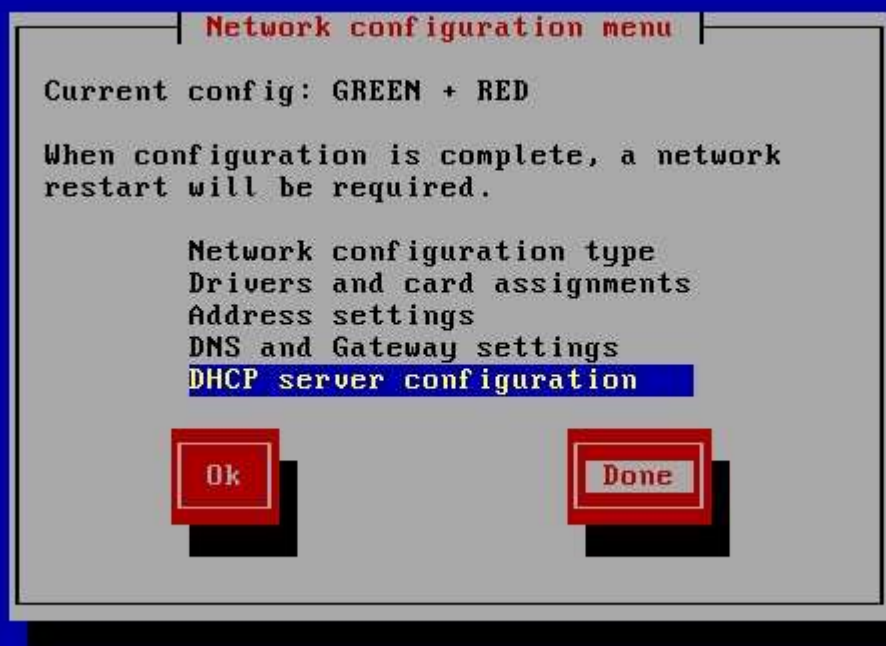


<Tab>/<Alt-Tab> between elements | <Space> selects

Рис. 18. Настройка сервера DHCP.

Завершение установки

IPCop v1.4.20 - The Bad Packets Stop Here



<Tab>/<Alt-Tab> between elements | <Space> selects

На этом этапе мы уже почти закончили с установкой. Необходимо задать пароли для учётных записей "root" и "admin". Учётная запись "root" в системе Linux имеет практически неограниченные привилегии. Это имя вам потребуется для входа в оболочку, например, для установки дополнительного ПО.

## IPCop v1.4.20 - The Bad Packets Stop Here



IPCop v1.4.20 - The Bad Packets Stop Here

Enter the 'root' user password. Login as this user for commandline access.

Password:

Again:

Ok Cancel

No echo from keyboard for password input.

Учётная запись "admin" обладает неограниченным доступом лишь через web-интерфейс. То есть "admin" может менять настройки сервера DHCP, перенаправления портов, подключений, обновлять IPCop, и, конечно, перезагружать его.

## IPCop v1.4.20 - The Bad Packets Stop Here



IPCop v1.4.20 - The Bad Packets Stop Here

Enter IPCop 'admin' user password. This is the user to use for logging into the IPCop web administration pages.

Password:

Again:

Ok Cancel

No echo from keyboard for password input.

## IPCop v1.4.20 - The Bad Packets Stop Here

IPCop v1.4.20 - The Bad Packets Stop Here

Enter the 'backup' password used to safely export the backup key.

Password:

Again:

Ok

Cancel

No echo from keyboard for password input.

Можно поздравить: установка завершена! Теперь можно выключить систему и отсоединить привод CD-ROM, поскольку он больше не потребуется. Кстати, после этого система будет быстрее загружаться и потреблять меньше энергии. Однако не забудьте зайти в BIOS и изменить порядок загрузки, чтобы система загружалась с жёсткого диска.

## IPCop v1.4.20 - The Bad Packets Stop Here

IPCop v1.4.20 - The Bad Packets Stop Here

Setup is complete. Press Ok to reboot.

Ok

<Tab>/<Alt-Tab> between elements | <Space> selects



GNU GRUB version 0.95 (639K lower / 261056K upper memory)

```
IPCop
IPCop SMP
IPCop (ACPI enabled)
IPCop SMP (ACPI enabled)
```

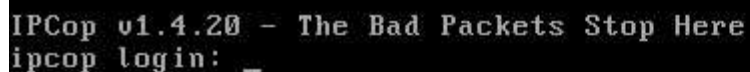
Use the ↑ and ↓ keys to select which entry is highlighted.  
Press enter to boot the selected OS, 'e' to edit the  
commands before booting, 'a' to modify the kernel arguments  
before booting, or 'c' for a command-line.



Рис. 19. Первый экран IP Cop.

При следующей загрузке системы вы увидите появившийся загрузчик Grub (Рис. 19), в котором можно выбрать варианты загрузки. Всего возможны четыре варианта. Обычная загрузка IP Cop, IP Cop SMP - для машин с мультипроцессорностью, в том числе для систем с технологией Hyper-Threading и двухъядерных процессоров. Ещё предлагаются те же два варианта, но с поддержкой ACPI. Отметим, что выбор придётся сделать лишь единожды, в дальнейшем IP Cop запомнит указанный вариант и будет автоматически загружать выбранную систему.

После загрузки появится экран входа (Рис. 20). С этого момента монитор и клавиатура больше не потребуются, и их можно смело отключить.

A screenshot of a terminal window with a black background. The text is white and shows the IPCop version and a login prompt. The first line reads 'IPCop v1.4.20 - The Bad Packets Stop Here'. The second line reads 'ipcop login: \_' where the underscore represents a cursor.

```
IPCop v1.4.20 - The Bad Packets Stop Here
ipcop login: _
```

Рис. 20. Вход в систему.

Если вы решите отключить от компьютера все устройства ввода/вывода, рекомендуем всё же подключить встроенный динамик к материнской плате. Он позволит отслеживать состояние системы. Звуковой сигнал будет информировать о готовности системы к работе и о подключении/отключении Интернета. Ещё маленькое замечание: некоторые системы откажутся загружаться при отключённой клавиатуре. Тогда вам следует войти в BIOS и указать значение опции "Halt on" в "No Error" или "All But Keyboard".

Обзор возможностей IPCop  
Выбор языка

**IP Cop** 1.4.20

**SYSTEM** [HOME](#)

The bad packets stop here.

**SYSTEM** **STATUS** **NETWORK** **SERVICES** **FIREWALL** **VPNs** **LOGS**

**VPNs**

**ipcop.mati**

[Connect](#) [Disconnect](#) [Refresh](#)

**Idle**

1. Your update file is 011 days old. We recommend you update it on the **System > Updates** page.

09:15:14 up 2 min, 0 users, load average: 0.60, 0.22, 0.07



**Idle**

09:15:14 up 2 min, 0 users, load average: 0.60, 0.22, 0.07

[SOURCEFORGE.NET](#)



Начало

Обновления

Пароли

Доступ через SSH

Настройки GUI

Сохранение скрипта

Выключение хоста в названии окна

Создатели

index.cgi page whilst connected

Выберите язык IPCop'a

Russian (Russkij)

### Sound

☒ Сигнал, когда IPCop подключается и отключается

Восстановить начальные установки

Сохранить



Ожидание

09:20:23 up 7 min, 0 users, load average: 0.05, 0.11, 0.07

SOURCEFORGE.NET



## Настройки GUI

### Display

- ☒ Enable Javascript
- ☐ Показать имя хоста в названии окна
- ☐ Refresh index.cgi page whilst connected

Выберите язык IPCop'a

- Russian (Russkij)
- Chinese Traditional (中文-繁)
- Czech (Čeština)
- ☒ Danish (Dansk)
- Dutch (Nederlands)
- English (English)
- Finnish (Suomi)
- French (Français)
- German (Deutsch)
- Greek (Ellinika)
- Gujarati (Gujarātī)
- Hungarian (Magyar)
- Italian (Italiano)
- Japanese (日本語)
- Lithuanian (Lietuvių)
- Norwegian (Norsk)
- Persian (Farsi)
- Polish (Polski)
- Portuguese (Português)
- Romanian (Română)
- Russian (Russkij)

### Sound

- ☒ Enable Sound

Звук

Восстановить начальные установки

Сохранить



### Ожидание

09:20:23 up 7 min, 0 users, load average: 0.05, 0.11, 0.07

SOURCEFORGE.NET

Обновление





## Доступные обновления

Все обновления установлены

To install an update please upload the .tar.gz file below:

Загрузить файл обновления

Файл не выбран

Закачка

## Использование диска:

Устройство	Смонтирован на	Size	Используется	свободно	Проценты
/dev/root	/	8084	261	7742	4%
/dev/harddisk1 /boot		16	4	12	26%
/dev/harddisk2 /var/log		32213	177	30400	1%

Kernel type selection: linux-2.4.36

Kernel type selection

No set was selected

Select a kernel type help with a small main partition.  
Needed on a scsi device when /boot partition is too small

Очистить кеш (squid)

Refresh update list



## Установленные Обновления:

ID	Title	Описание	Освобождён	Установлен
021	1.4.21 update	Fix update download button (after 1.4.21 is installed). Fix vpn-watch for host with aliases. Rework our security perl patches and add CVE-{2005-3962,2007-5116,2008-1927} patches	2008-07-23	2011-04-30



Ожидание

09:20:55 up 7 min, 0 users, load average: 0.03, 0.10, 0.06

SOURCEFORGE.NET

IP  
Cop  
1.4.21

Система

Обновления

Система

Состояние

Сеть

Службы

Файервол

ВЧС

Логи

The bad packets stop here.

Доступные обновления

Все обновления установлены

To install an update please upload the .tgz.gpg file below:

Загрузить файл обновления

Выберите файл

Файл не выбран

Закачка

ID	Title	Описание	Освобождён
021	1.4.21 update	Fix update download button (after 1.4.21 is installed). Fix vpn-watch for host with aliases. Rework our security perl patches and add CVE-{2005-3962,2007-5116,2008-1927} patches	2008-07-23

Удалить

gpg: Signature made Thu Jul 24 01:00:45 2008 MSD using DSA key ID 4A3BFD9E  
gpg: Good signature from "IPCop Development Group (http://www.ipcop.org/) <ipcop-devel@lists.sourceforge.net>"

Использование диска:

Устройство	Смонтирован на	Size	Используется	свободно	Проценты
/dev/root	/	8084	263	7740	4%
/dev/harddisk1 /boot		16	4	12	26%
/dev/harddisk2 /var/log		32213	177	30400	1%

Kernel type selection: linux-2.4.36

Kernel type selection

No set was selected

Select a kernel type help with a small main partition.

Needed on a scsi device when /boot partition is too small

Очистить кеш (squid)

Refresh update list

Установленные Обновления:

Пароли  
Система – Пароли



### пароль администратора

Имя  
пользователя: 'admin'

Пароль:

Снова

Сохранить



### Пользовательский пароль соединения:

Имя пользователя: 'dial'

Пароль:

Снова

Сохранить



Ожидание

09:21:40 up 8 min, 0 users, load average: 0.10, 0.11, 0.07

SOURCEFORGE.NET

Система – Доступ через SSH



## SSH:

☐ Доступ через SSH

- ☐ Support SSH protocol version 1 (required only for old clients)
- ☐ Allow TCP Forwarding
- ☒ Пароли ssh
- ☒ Allow public key based authentication

IPCop SSH uses the non-standard Port 222!

Сохранить



## SSH Host Keys

Ключ ssh	Fingerprint	Size (bits)
/etc/ssh/ssh_host_key.pub (RSA1)	0b:0e:4c:4c:ae:f0:42:85:38:17:be:b7:db:76:ac:9b	2048
/etc/ssh/ssh_host_rsa_key.pub (RSA2)	20:76:be:4e:94:89:48:00:5a:bb:c5:19:86:03:c3:6f	2048
/etc/ssh/ssh_host_dsa_key.pub (DSA)	c9:d6:0b:2f:6d:cc:36:1b:ec:69:f5:73:54:e8:8d:a5	1024



Ожидание

09:21:46 up 8 min, 0 users, load average: 0.09, 0.11, 0.07

SOURCEFORCE.NET

Система – сохранение



дискету

Для сохранения конфигурации системы, пожалуйста вставьте диск в дисковод IPCop и нажмите *Сохранение на дискету*. Проверьте аккуратно результаты, чтобы быть уверенным в том, что сохранение прошло успешно.

**Select media  
(only FAT supported for removable media)**☒ **Hard disk**

Plug in a device, refresh, select and mount before usage. Umount before removal.

Обновить

Mount

Umount

**Ключ шифрования резервной копии**

Пароль резервной копии:

Экспорт ключа резервной копии

**Текущий носитель: Hard disk** свободно: 7742 М**Создать новую резервную копию**

Описание:

Создать новую резервную копию

**Импорт файла (.dat) резервной копии:**

Выберите файл

Файл не выбран

Импорт

**Резервные Копии:**

Описание

Действие

Пустой!

Система – выключение



### Выключение:

Перезагрузить

Выключение

### Schedule IPCop reboots

#### Время

03:15

#### День

- ☐ Monday  
☐ Tuesday  
☐ Wednesday  
☐ Thursday  
☐ Friday  
☐ Saturday  
☐ Воскресенье

#### Действие

- ☐ Перезагрузить  
☐ Выключение

Сохранить



### Ожидание

09:22:56 up 9 min, 0 users, load average: 0.19, 0.13, 0.08

SOURCEFORGE.NET

## Состояние – состояние системы



Сервисы: | Память: | Использование диска: | Inodes usage: | Время работы и пользователи | Загруженные модули: | Версия ядра:

#### Сервисы:

CRON сервер	ЗАПУЩЕН	1800 kB
Сервер безопасного соединения	ОСТАНОВЛЕННО	
DNS прокси сервер	ЗАПУЩЕН	1696 kB
Logging Server	ЗАПУЩЕН	1604 kB
NTP Server	ОСТАНОВЛЕННО	
Web сервер	ЗАПУЩЕН	5064 kB
Интернет прокси	ОСТАНОВЛЕННО	
Сервер DHCP	ОСТАНОВЛЕННО	
Сервер регистрирующий события в ядре	ЗАПУЩЕН	2032 kB
Система Обнаружения Атак (GREEN)	ОСТАНОВЛЕННО	
Система Обнаружения Атак (RED)	ОСТАНОВЛЕННО	
ВЧС	ОСТАНОВЛЕННО	

#### Память:

	Size	Используется	свободно	Проценты	Общий	
RAM	256804	23844	232960	9%	буферы	1772
- /+ buffers/cache	8928	247876		3%	кеширован	13144
Подкачка	32764	2180	30584	6%		

#### Использование диска:

Устройство	Смонтирован на	Size	Используется	свободно	Проценты
/dev/root	/	8084M	261M	7742M	4%
/dev/harddisk1 /boot		16M	4M	12M	26%
/dev/harddisk2 /var/log		32213M	177M	30400M	1%





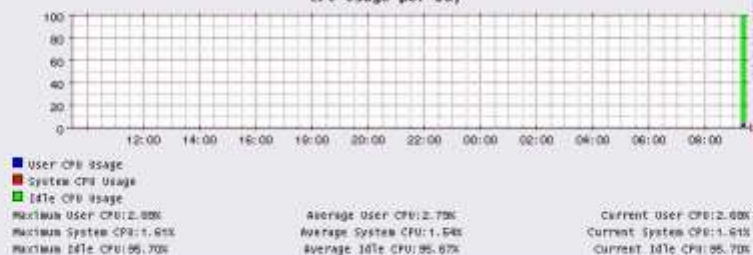


- Система
  - Состояние
  - Сеть
  - Службы
  - Файрвол
  - ВНС
  - Роль
- Состояние Системы
  - Состояние БПЖ
  - График системы
  - Таблицы событий
  - Содержимое

## CPU График

The statistics were last updated at: Sat Apr 30 09:25:09 2011

## CPU Usage per Day



## Memory График

The statistics were last updated at: Sat Apr 30 09:25:09 2011

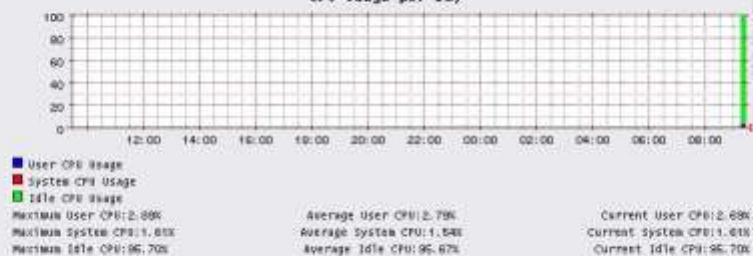
## Memory Usage per Day



## CPU График

The statistics were last updated at: Sat Apr 30 09:25:09 2011

## CPU Usage per Day

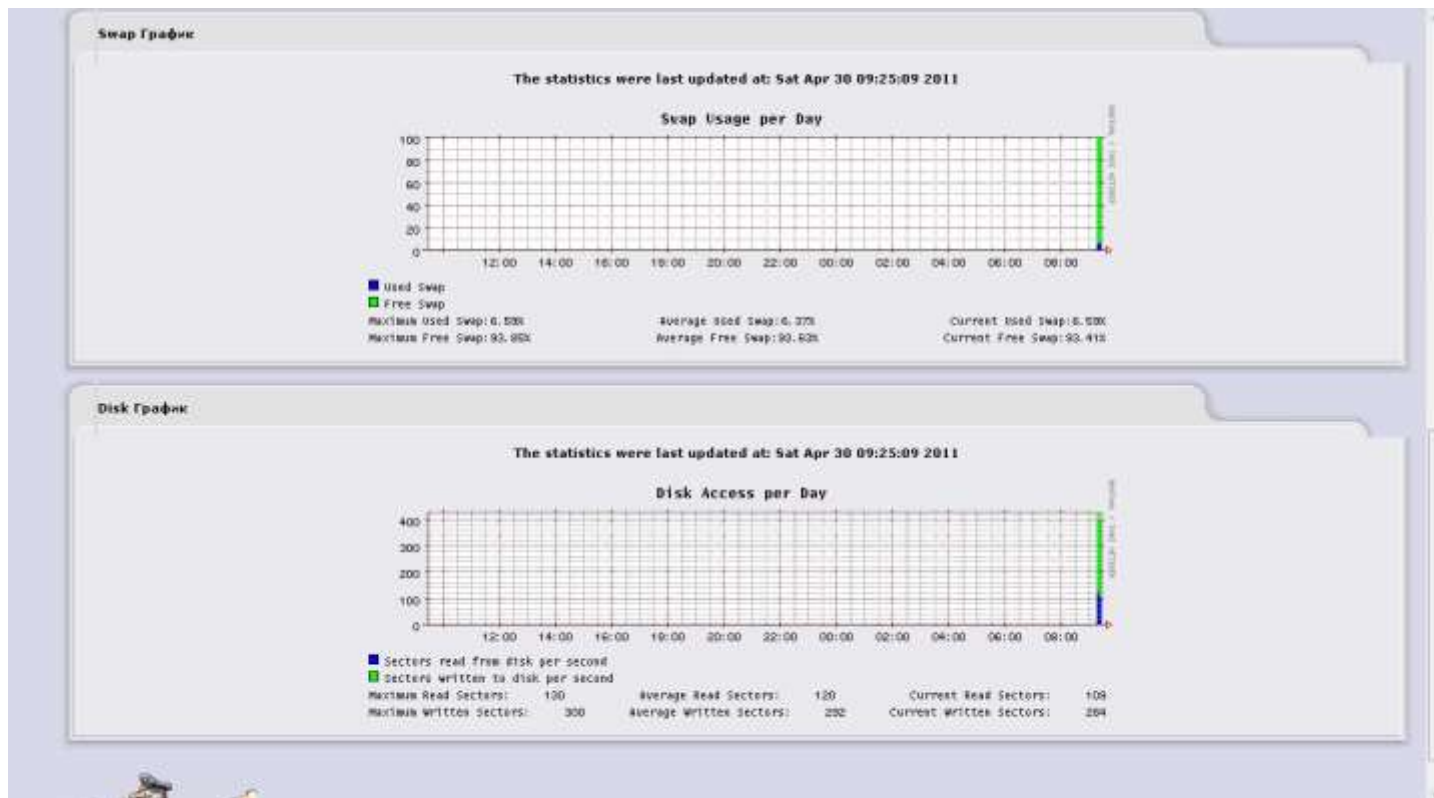


## Memory График

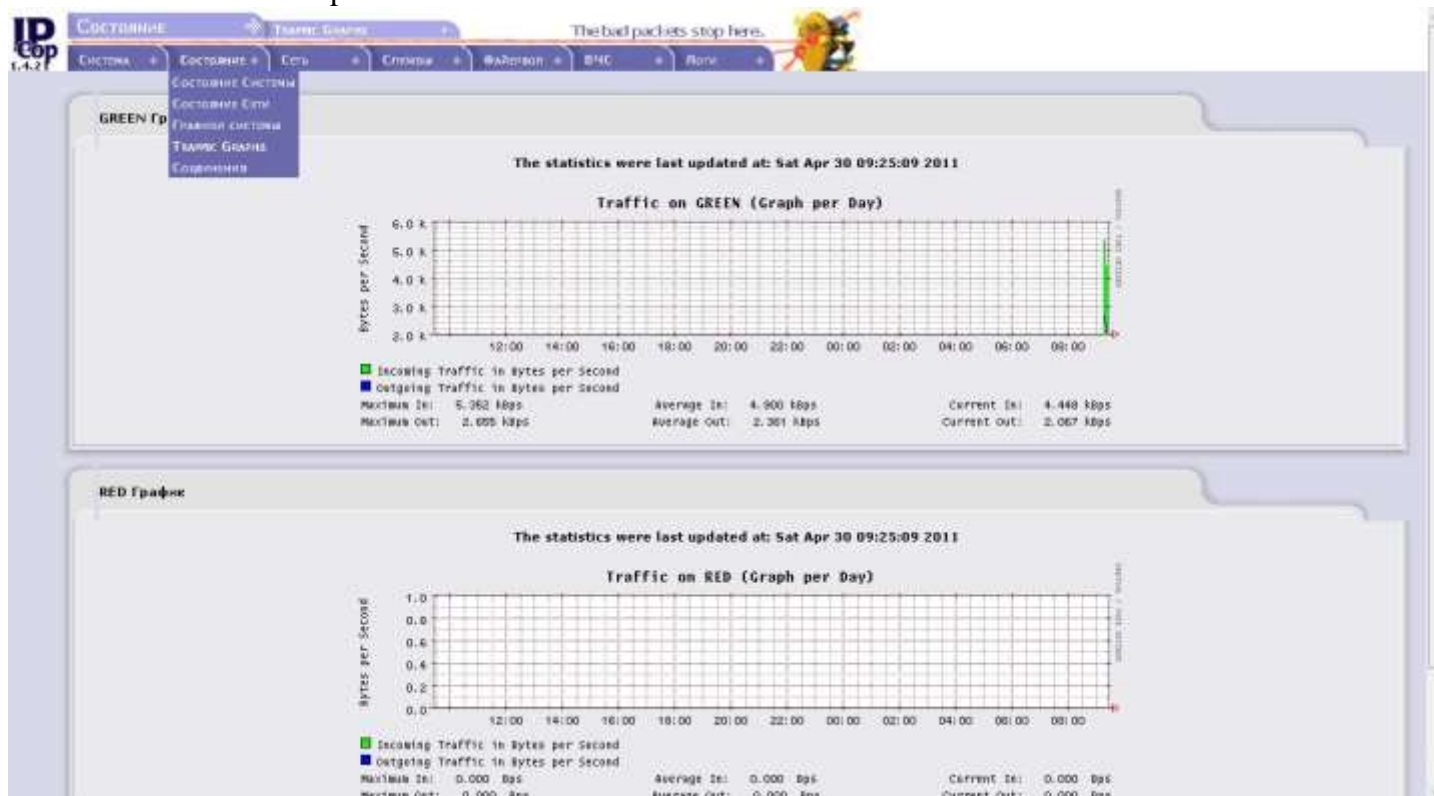
The statistics were last updated at: Sat Apr 30 09:25:09 2011

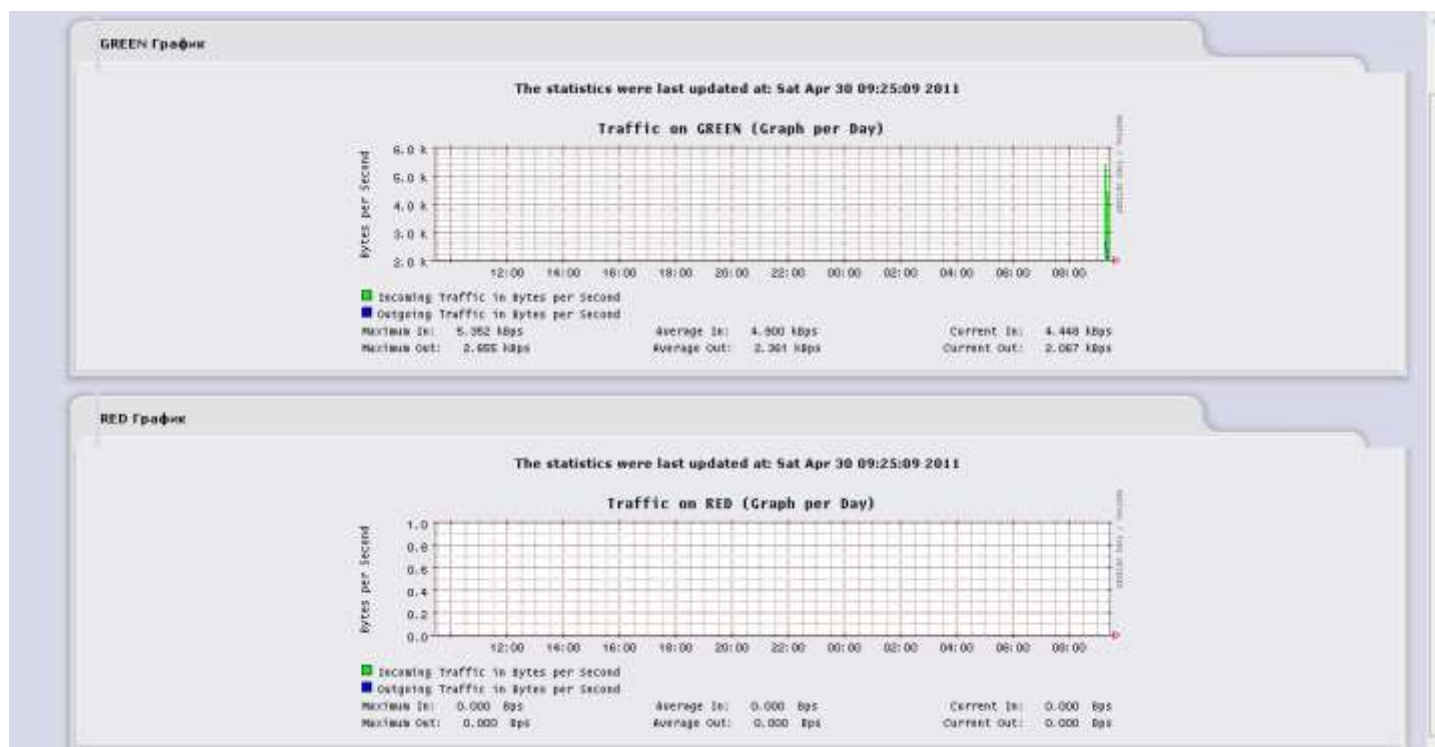
## Memory Usage per Day



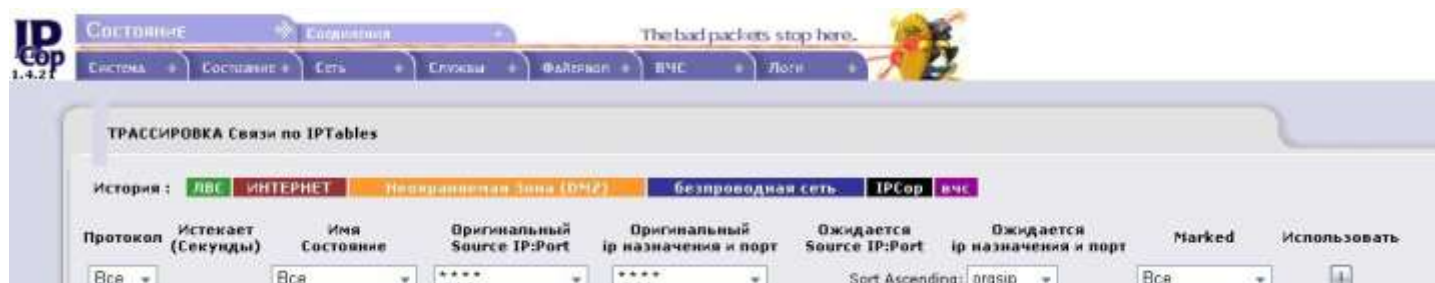
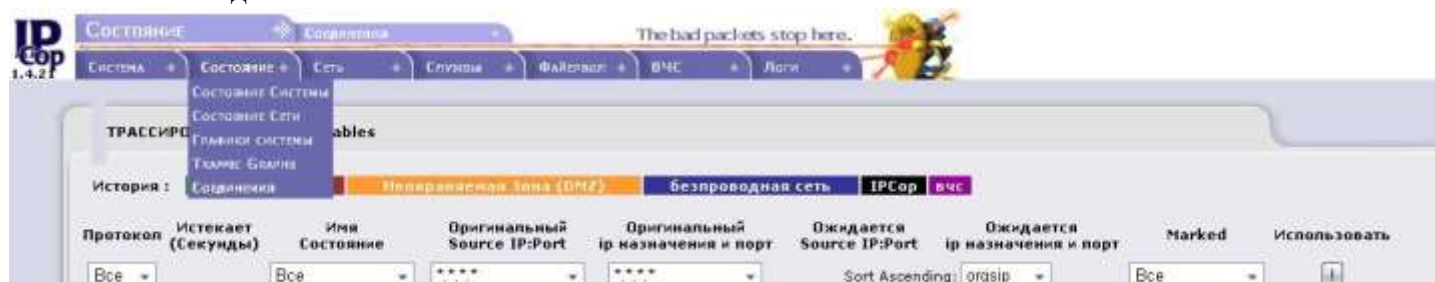


## Состояние – Traffic Graphs





## Состояние – соединения



## Сеть – DialUp



IP Cop 1.4.2

Сеть

Система + Системы + Сеть + Службы + Фаервол + ВНС + Язык

Профиль: 1. Пустой

Выбрать Удалить Восстановить

Имя:

Интерфейс: Модем Обновить

USB:

Время ожидания (в минутах; 0 чтобы отключить): 15

Подключится после перезагрузки IPCop: ☐

Отладка соединения: ☐

Пересоединение:

☒ Ручной

☐ Persistent

☐ Набирать по запросу

Если не удастся пересоединиться, переключиться на профиль: 1. Пустой

Dial on Demand for DNS: ☐

Время задержки (в секундах): 30

Максимальное число попыток: 5

Ввод

Имя пользователя:

Пароль:

Метод: PAP or CHAP

Имя сценария:

DNS:

☒ Автоматический

☐ Ручной

Первичный DNS:

Вторичный DNS:

## Сеть – загрузка

IP Cop 1.4.2

Сеть

Система + Системы + Сеть + Службы + Фаервол + ВНС + Язык

Загрузка firmware для Speedtouch USB

Чтобы использовать Speedtouch USB модем, вам нужно загрузить программное обеспечение (firmware) на IPCop. Пожалуйста скачайте пакет **Embedded Firmware** со speedtouch.com, распакуйте и загрузите файлы соответствующие вашему модему: KQD6\_3.xxx для Rev<4, ZZL\_3.xxx для Rev=4 используя страницу внизу.

URL: <http://www.speedtouch.com/support.htm>

Модем: Rev USB not running

Загрузить файл:  Файл не выбран

не доступен

Upload ECI ADSL Synch.bin File

Чтобы использовать ECI ADSL модем, загрузите файл synch.bin на IPCop. Пожалуйста скачайте его с ECIADSL сайта и загрузите файл **synch.bin** используя страницу внизу.

URL: <http://eciadsl.flashbus.org/>

Загрузить файл:  Файл не выбран

не доступен

Upload FritzDSL Driver

To utilise one of FritzDSL fcdsl / fcdsl1 / fcdsl2 / fcdslusb / fcdslusb modem, you must upload a package to your IPCop box. Please download the tarball corresponding to your version from the IPCop Website and then upload the entire **fcdsl-(your\_version).tgz** using the form below.

URL: <http://www.ipcop.org/>

Загрузить файл:  Файл не выбран

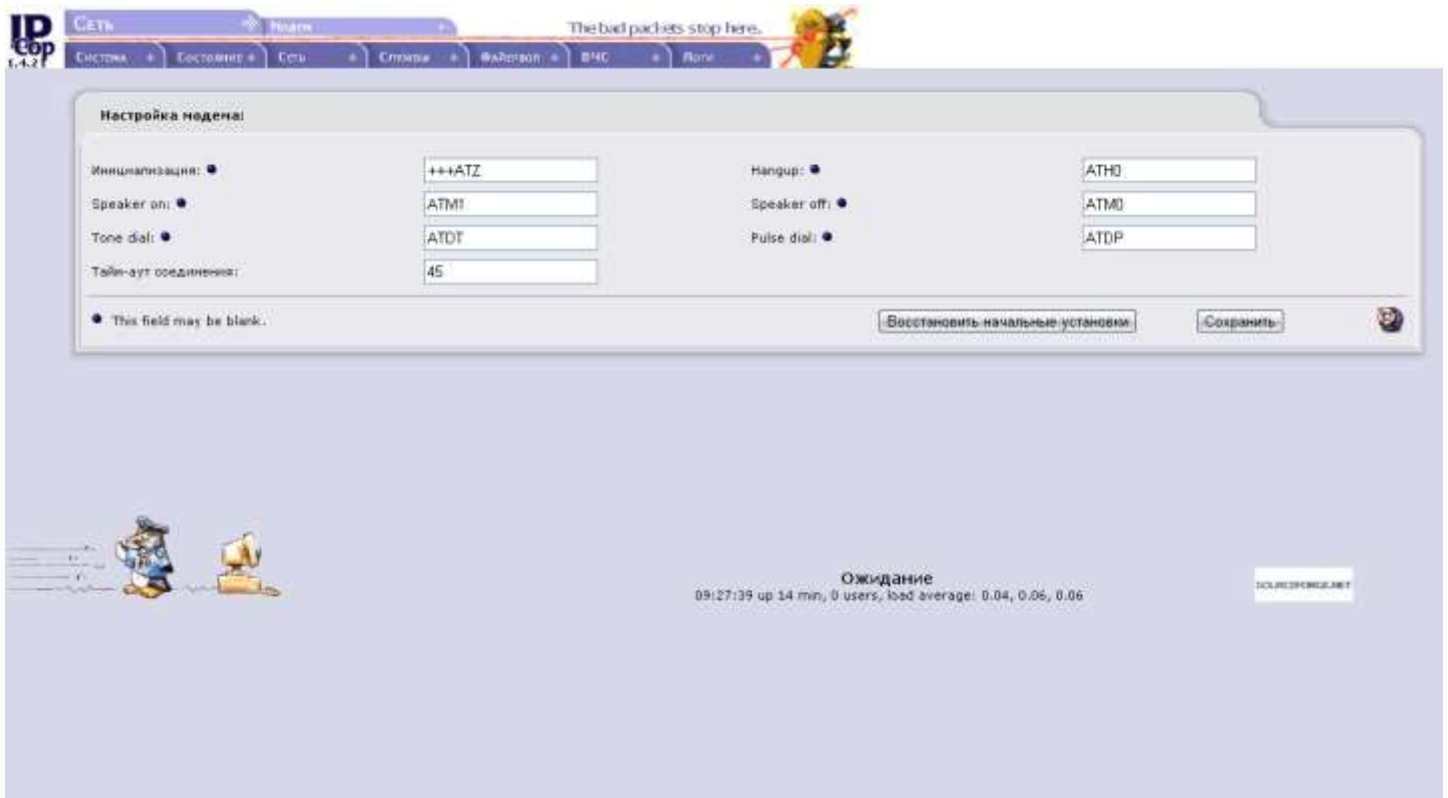
не доступен

Ожидание

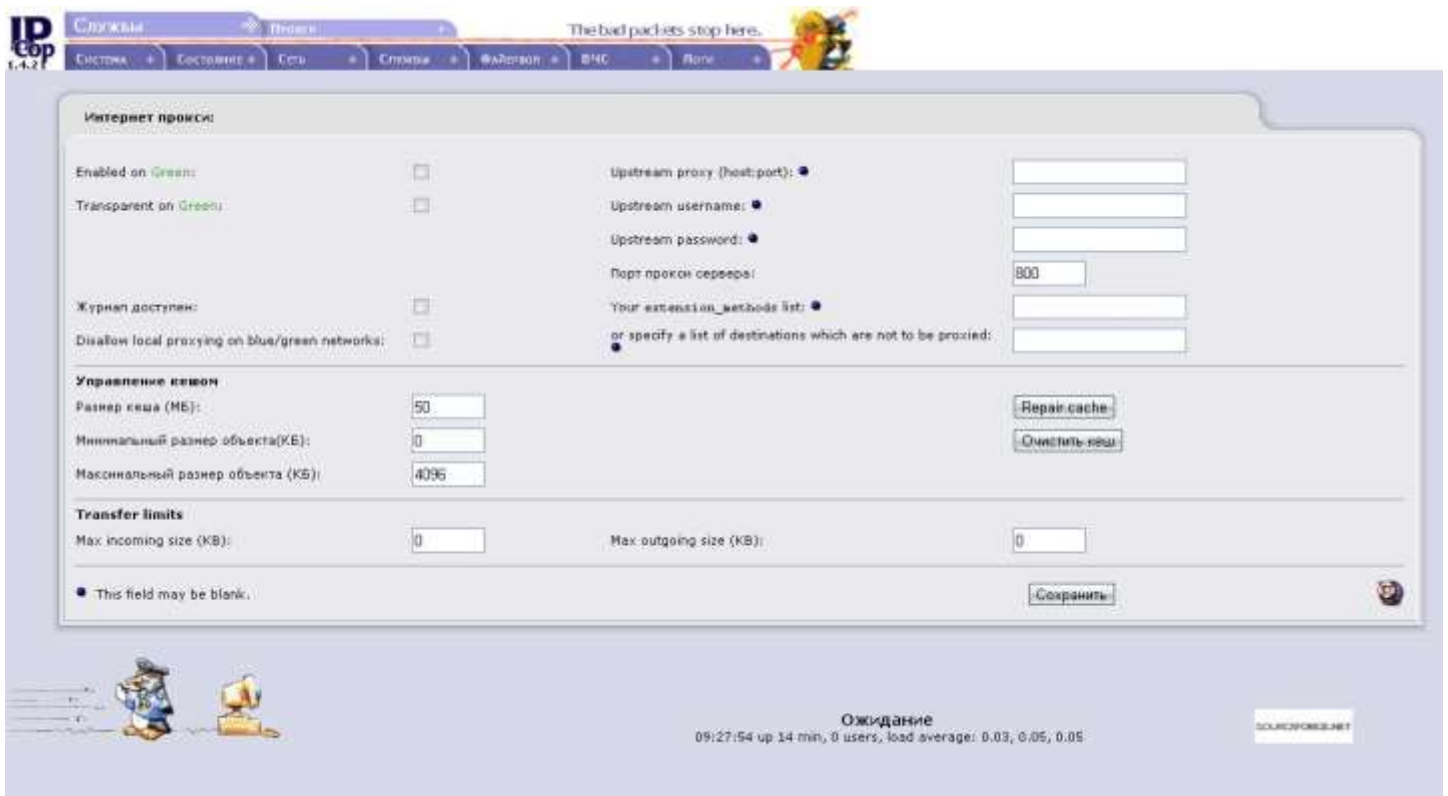
09:27:03 up 13 min, 0 users, load average: 0.08, 0.07, 0.06

SOURCEFIRE.COM

## Сеть – модем



## Службы – прокси



## Службы – сервер DHCP





**DHCP**

**Зелёный Интерфейс:**

Start address:

Время аренды по умолчанию (мин):

Base IP for fixed lease creation:

Domain name suffix:

Первичный DNS:

Первичный Сервер Времени (NTP):

Primary WINS Server address:

IP адрес/Маска сети: **192.168.209.228/255.255.255.0**

Конечный адрес:

Max lease time (mins):

Allow bootp clients: ☐

Вторичный DNS:

Вторичный Сервер Времени (NTP):

Secondary WINS Server address:

☐ This field may be blank.

**Additional DHCP Options**

Добавить параметр DHCP

Option name:  or Выбрать

Option value:

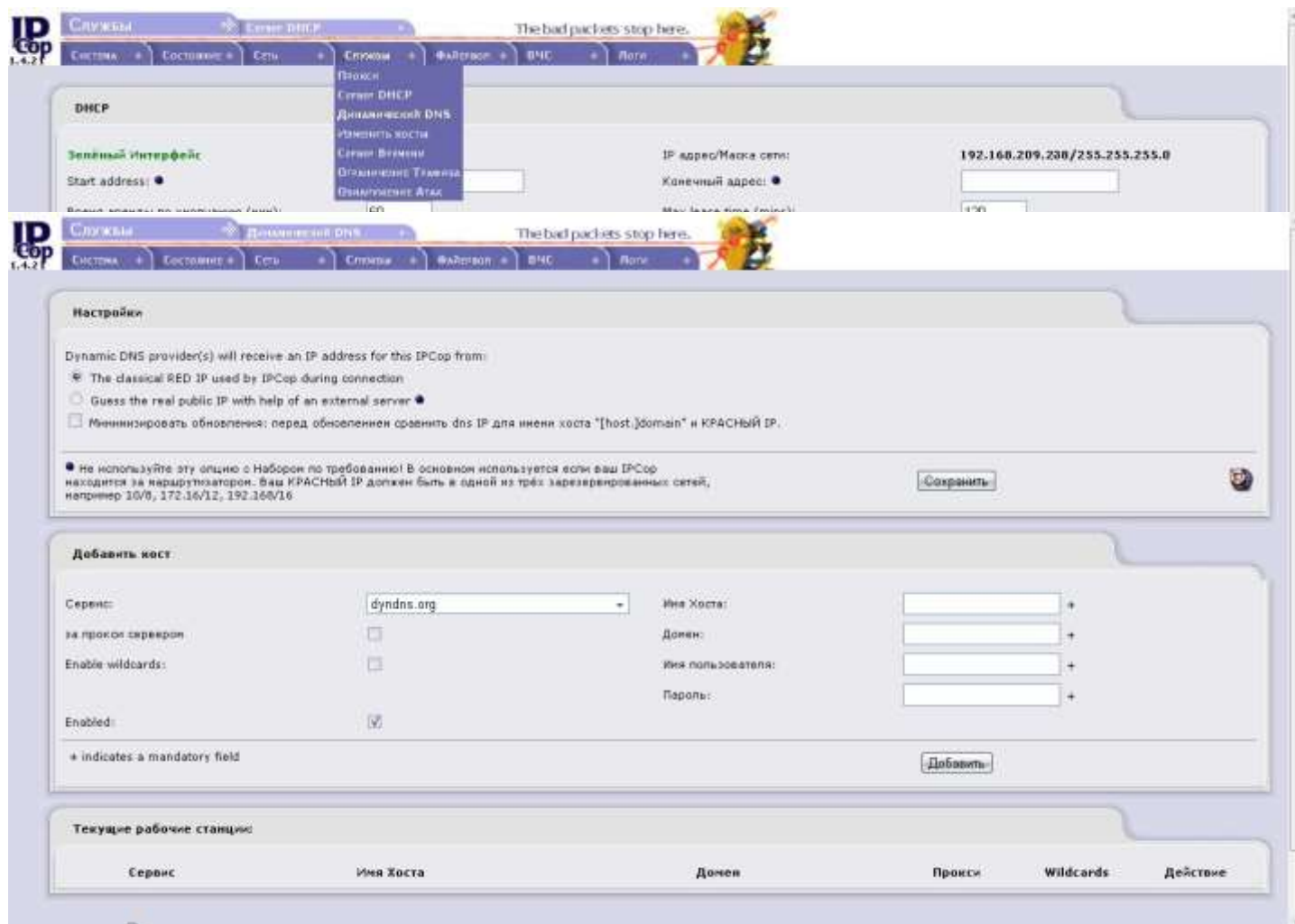
Enabled: ☐

Option scope: ☒ ЗЕЛЁНЫЙ ☐ Голубой ☐

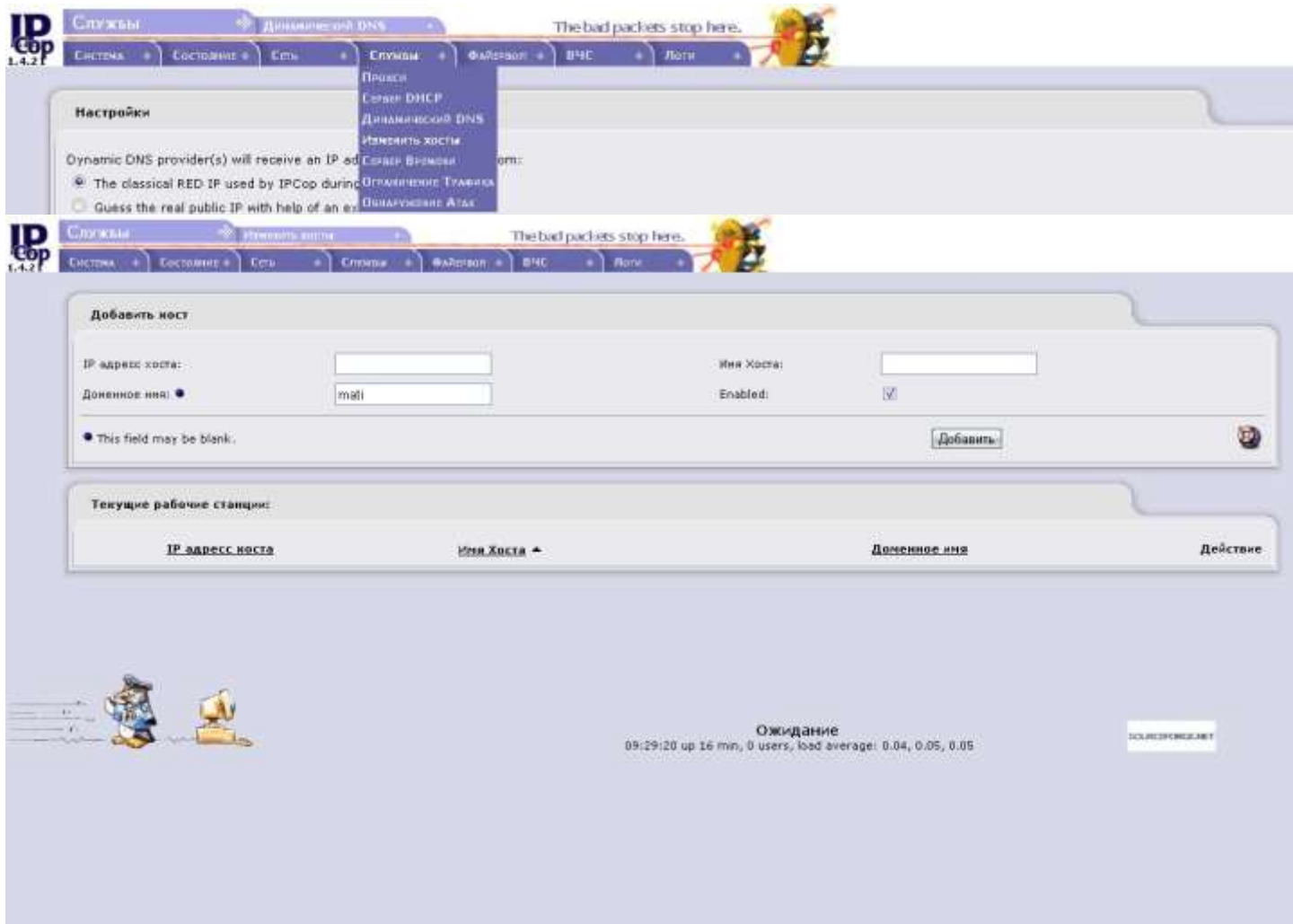
☒ Global scope or limit scope to checked interfaces.

Option name	Option value	Option scope	Действие
<b>Текущие фиксированные аренды</b>			
Добавить новую фиксированную аренду	Enabled: <input checked="" type="checkbox"/>		

Службы – Динамический DNS



Службы – Изменить хосты



Службы – сервер времени

IP Cop 1.4.2

Службы

Имя хоста

The bad packets stop here.

Система + Системные + Сеть + Службы + Фаервол + ВНС + Логг +

Добавить хост

IP адрес хоста:

Дочерняя имя:

Имя Хоста:

Enabled: ☒

Получить  
Сервер DHCP  
Динамический DNS  
Имя хоста  
Сервер времени  
Ограничение трафика  
Обнаружение атак

Use a Network Time Server:

☐ Obtain time from a Network Time Server

Часы не синхронизированы

Первичный Сервер Времени (NTP):

Вторичный Сервер Времени (NTP):

☐ Клиенты разрешены

Время обновления

To queue a synchronization event at any time (even while using a repeating schedule), press the Set Time Now button.

☐ Каждый:  дней

☒ Вручную

Время обновления

Год:  Месяц:  День:  Часов:  Минуты:

Ожидание

09:29:46 up 16 min, 0 users, load average: 0.03, 0.05, 0.05

СЛУЖБЫ

## Службы – ограничение трафика

IP Cop 1.4.2

Службы

Ограничение трафика

The bad packets stop here.

Система + Системные + Сеть + Службы + Фаервол + ВНС + Логг +

Настройки:

☐ Ограничение Трафика

Downlink speed (kbit/sec):

Скорость загрузки (кбайт/сек):

Добавить службу

Приоритет:

Порт:

Протокол:

Enabled: ☒

Сервис ограничения трафика

Приоритет	Порт	Протокол	Действие
-----------	------	----------	----------

Ожидание

09:29:55 up 16 min, 0 users, load average: 0.02, 0.05, 0.05

СЛУЖБЫ

## Службы – Обнаружение атак

**IP Cop 1.4.21** | Службы | Ограничение Трафика | The bad packets stop here.

Система | Состояние | Сеть | Службы | **Файрвол** | ВНС | Лог

**Настройка:**

☐ Ограничение Трафика  
Downlink speed (kbit/sec):

Поиск  
Сервер DNS  
Динамический DNS  
Изменить хосты  
Сервер Виртуал  
Ограничение Трафика  
Обнаружение Атак

**Службы** | Динамический Атак | The bad packets stop here.

Система | Состояние | Сеть | Службы | **Файрвол** | ВНС | Лог

**Система Обнаружения Атак:**

Интерфейсы:  
☐ GREEN Smart eth0  
☐ RED Smart eth1

Состояние:  
**ОСТАНОВЛЕННО**  
**ОСТАНОВЛЕННО**

Память:

To utilize Sourcefire VRT Certified Rules, you need to register on <http://www.snort.org>. Acknowledge the license, receive your password by email, and connect to the site. Go to [USER PREFERENCES](#), press the 'Get Code' button at the bottom and copy the 40 character Cink Code into the field below.

Cink Code:

**Snort rules update:**

☒ No  
☐ Sourcefire VRT rules for registered users  
☐ Sourcefire VRT rules with subscription

File download is limited to once every 15 minutes.

Ожидание  
09:30:16 up 17 min, 0 users, load average: 0.02, 0.04, 0.05

SOURCEFIRE.COM

## Файрвол – перенаправление портов

**IP Cop 1.4.21** | Файрвол | Перенаправление портов | The bad packets stop here.

Система | Состояние | Сеть | Службы | **Файрвол** | ВНС | Лог

Добавить новое правило:

Протокол: TCP | IP адрес: DEFAULT IP | Source port:   
IP назначения:  | Порт Назначения:   
Заголовок замечания:  | Enabled: ☒  
Source IP, or network (blank for "ALL"):   
This field may be blank.

**Текущие правила:**

Proto	Source	Порты назначения	Замечание	Действие
-------	--------	------------------	-----------	----------

Ожидание  
09:30:17 up 17 min, 0 users, load average: 0.01, 0.04, 0.04

SOURCEFIRE.COM

## Файрвол – Внешний доступ

IP Cop 1.4.2

ФАЙЕРВОЛ

Внешний доступ

The bad packets stop here.

Система + Системы + Сети + Службы + Файервол + ВМС + Язык +

Перенаправление портов

Внешний доступ

FIREWALL OPTIONS

Добавить новое правило:

TCP + Source IP, or network (blank for "ALL"): Порт Назначения:

Enabled: ☒ IP назначения: DEFAULT IP +

Замечание: \*

This field may be blank.

Добавить

Текущие правила:

Proto	Source IP	IP назначения	Порт Назначения	Замечание	Действие
TCP	ВСЕ	DEFAULT IP	113		<input checked="" type="checkbox"/>

История: ☒ Активировано (нажмите для деактивации) ☐ Деактивировано (нажмите для активации) Изменить Удалить

Ожидание

09:30:44 up 17 min, 0 users, load average: 0.01, 0.04, 0.04

SOURCEFIRE.COM

## Файервол – Firewall options

IP Cop 1.4.2

ФАЙЕРВОЛ

Firewall options

The bad packets stop here.

Система + Системы + Сети + Службы + Файервол + ВМС + Язык +

Перенаправление портов

Внешний доступ

FIREWALL OPTIONS

Disable ping response

☒ No

☐ Only RED

☐ Все интерфейсы

Сохранить

Ожидание

09:30:54 up 17 min, 0 users, load average: 0.01, 0.03, 0.04

SOURCEFIRE.COM

## Виртуальные частные сети



**IPsec** v.4.2.7 **ВЧС** The bad packets stop here.

Система + Состояние + Сети + Службы + Фаервол + ВЧС + Лог + 

### Глобальные настройки

Public IP or FQDN for RED interface or <%defaultroute>:  Enabled: ☐

Override default MTU:

Delay before launching VPN (seconds):

Restart net-to-net vpn when remote peer IP changes (dyndns), it helps DPD: ☐

PLUTO DEBUG = crypt: ☐, parsing: ☐, emitting: ☐, control: ☐, klips: ☐, dns: ☐, nat: ☐

• This field may be blank.  
 • If required, this delay can be used to allow Dynamic DNS updates to propagate properly. 60 is a common value when RED is a dynamic IP.

[Сохранить](#)

---

### Статус и управление соединением

Имя	Тип	Общее Имя	Замечание	Состояние	Действие
<a href="#">Добавить</a>					

---

### Администрация сертификатов:

Имя	Subject	Действие
Корневой сертификат:	не доступен	
Сертификат Хоста:	не доступен	


CA имя:  [Выберите файл](#) Файл не выбран

Resetting the VPN configuration will remove the root CA, the host certificate and all certificate based connections:

[Сгенерировать корневые/хоста сертификаты](#)  
[Загрузить CA сертификат](#)  
[Remove all CA and certs](#)

## Логи – Настройки журнала

**IPsec** v.4.2.7 **Логи** The bad packets stop here.

Система + Состояние + Сети + Службы + Фаервол + ВЧС + Лог + 

Настройка Журнала

Log viewing options

Sort in reverse chronological order: ☐ Lines per page:


Итоги Журнала

Keep summaries for:  дней Уровень детализации:

Запись удалённых событий

Enabled: ☐ Syslog server:

[Сохранить](#)



**Ожидание**

09:33:10 up 19 min, 0 users, load average: 0.01, 0.03, 0.03

SOURCEFIRE.NET

## Логи – Сводка журнала



## Логи – Журналы Файрвола



## Логи – Системный протокол



### Настройка учётной записи DSL

С этого момента административный интерфейс маршрутизатора доступен через любой браузер по IP-адресу (или имени), заданному вами ранее. Не забывайте, что нужно указывать и порт (через двоеточие).

Первое, что нужно сделать пользователям DSL, - ответить на сообщение, которое появится сразу же после входа на интерфейс IPCop (Рис. 21).

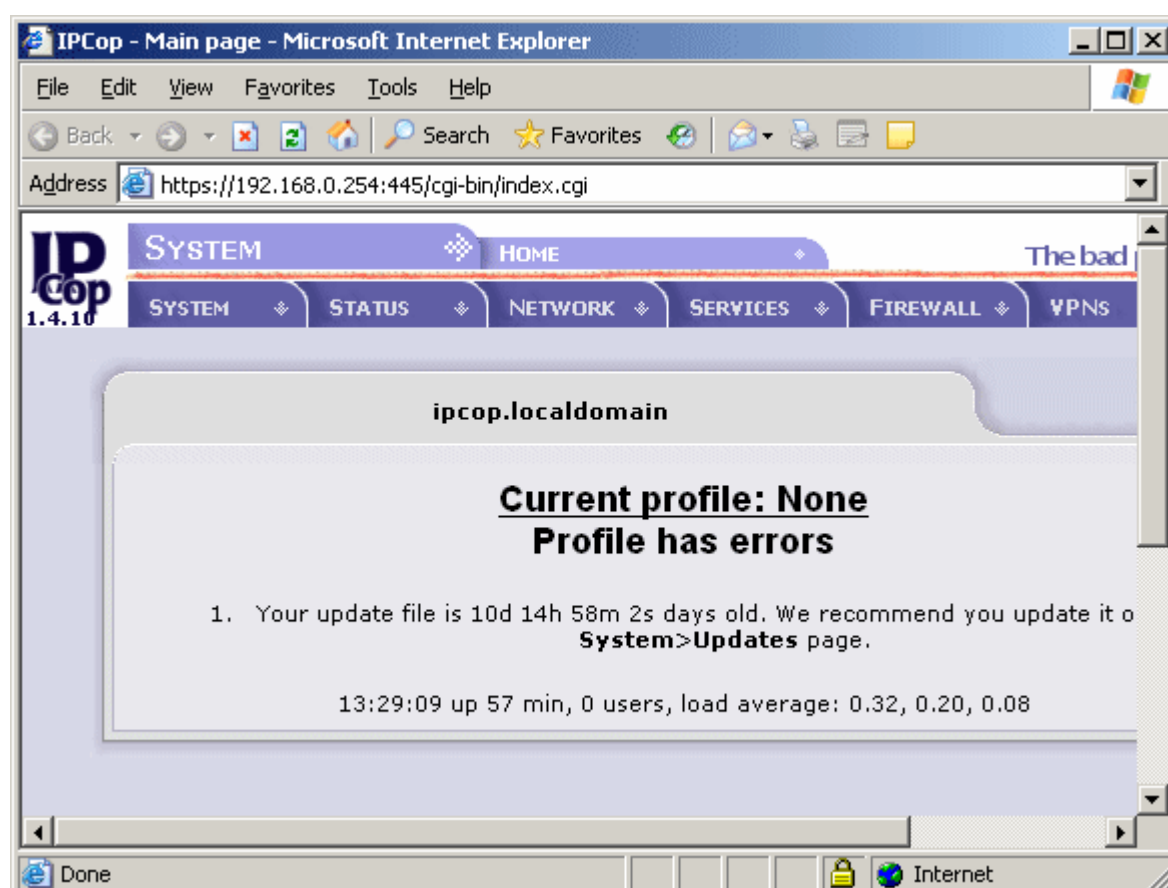


Рис. 21. Ошибка из-за отсутствия учётных данных DSL.

Ошибка связана с отсутствием учётных данных DSL, которые указываются в разделе "Сеть/Network", пункт "Dialup". Учётные данные можно задать, если войти с правами admin или root. На Рис. 22 показаны все доступные параметры подключения PPPoE/DSL.

**Connection:**

Interface:

USB: usb-uhci

Idle timeout (mins; 0 to disable):

Connect on IPCop restart: ☒

Connection debugging: ☐

**Reconnection:**

☐ Manual

☒ Persistent

☐ Dial on Demand

Holdoff time (in seconds):

In case reconnection fails, switch to profile:

Dial on Demand for DNS: ☐

Maximum retries:

**Additional PPPoE settings:**

☒ PPPoE plugin

☐ PPPoE

Service name:

Concentrator name:

**Authentication:**

User Name:

Method:

Password:

Script name:

**DNS:**

☒ Automatic

☐ Manual

Primary DNS:

Secondary DNS:

Profile name:

Legend: ☒ This field may be blank.

Рис. 22. Параметры DSL.  
Сервер DHCP

Как упоминалось ранее, сервер DHCP позволяет назначить некоторым клиентам сети статические IP-адреса. Однако прежде чем это делать, рекомендуем ознакомиться с Рис. 23 и 24, на которых показаны левая и правая части окна web-интерфейса (мы специально разделили скриншот).

**DHCP**

**Green Interface** Enabled: ☒

Start address:

Default lease time (mins):

Domain name suffix:

Primary DNS:

Primary NTP Server:

Primary WINS Server address:

☐ This field may be blank.

Рис. 23. Настройки сервера DHCP (левая часть).

IP Address/Netmask: **192.168.0.254/255.255.255.0**

End address:

Max lease time (mins):

Allow bootp clients: ☐

Secondary DNS:

Secondary NTP Server:

Secondary WINS Server address:




Рис. 24. Настройки сервера DHCP (правая часть).

Фиксированные адреса присваиваются на основе MAC-адресов (физический адрес сетевой карты). Пользователи Windows для просмотра MAC-адресов могут воспользоваться командной строкой, выполнив "ipconfig /all", либо посмотреть состояние подключения локальной сети, закладка "Support/Поддержка" (это справедливо для Windows XP).

Зная MAC-адрес, мы можем задать для него постоянный IP-адрес. Это делается в нижней части экрана. В нашем случае назначим адрес 192.168.0.168 (Рис. 25).



**Current fixed leases**

**Add a new fixed lease**

MAC Address:

Next Address:

Enabled: ☒

IP Address:

Filename:

Remark:

Root Path:

☐ This field may be blank.

Рис. 25. Задание статического IP.

Для более простого поиска клиентов в дальнейшем можно занести дополнительную информацию в поле "Remark" (комментарий). Поля "Next Address", "Filename" и "Root Path" необходимы для загрузки клиентов по сети. Новые клиенты добавляются в общий список (Рис. 26).

**Current fixed leases**

MAC Address	IP Address	Action
00:0C:6E:FF:D5:E2	192.168.0.168	<input checked="" type="checkbox"/>

**Legend:**

- ☒ Enabled (click to disable)
- ☐ Disabled (click to enable)
- Edit
- Remove

Рис. 26. Список клиентов с фиксированными IP-адресами.

#### Перенаправление портов и DDNS

Любой NAT-маршрутизатор, в том числе IPCor, отклоняет все запросы, приходящие из Интернета. Такой подход защищает компьютеры сети от атак из Интернета, но, в то же время, блокирует доступ и к внутренним серверам, например, Web или FTP. Естественно, IPCor, как и другие маршрутизаторы, может перенаправлять внешние запросы на машины локальной сети на основе портов (Port Forwarding).

Пример перенаправления портов показан на Рис. 27. Запросы, приходящие из Интернета на порт 80 маршрутизатора, будут перенаправлены на порт 80 локального компьютера с адресом 192.168.0.168. Поле "Remark", как и ранее, может использоваться для комментариев. В нашем случае мы указали "Webserver".

**Add a new rule:**

Protocol: TCP

Alias IP: DEFAULT IP

Destination IP: 192.168.0.168

Source port: 80

Destination port: 80

Remark: Webserver

Enabled: ☒

Source IP, or network (blank for "ALL"):

☐ This field may be blank.

Add Reset

Рис. 27. Добавление правила перенаправления портов.

Для добавления правила в список и активации нужно нажать кнопку "Add/Добавить".

Если вам нужно получать доступ к сети снаружи, то вы можете столкнуться ещё с одной проблемой - многие провайдеры назначают IP-адреса динамически, то есть при каждом следующем подключении ваш адрес будет изменяться. К счастью, для обхода этой проблемы можно воспользоваться службой DDNS, которая отслеживает изменение IP-адреса и позволяет по имени DNS всегда найти нужный адрес. Для того чтобы такое было возможным, в сети должен работать клиент, который отслеживает изменение внешнего адреса и сообщает об этом серверам Dynamic DNS. Как и многие другие маршрутизаторы, IPСор содержит встроенный клиент, который, несомненно, упростит работу с DDNS.

Рис. 28. Настройка клиента DDNS.

При настройке, вам будет предложено создать учётную запись DDNS. Отметим, что некоторые серверы предлагают эту услугу бесплатно, например <http://www.dyndns.org/>. После регистрации вы получаете имя и пароль, которые следует указать в соответствующих полях интерфейса IPCop (Рис. 28). Клиент IPCop Может работать через HTTP-прокси (флажок "Behind a Proxy"), как это требуют некоторые провайдеры. А галочка "Enable Wildcards" позволяет создавать суб-домены.

И, наконец, IPCop должен определять свой IP-адрес для DDNS. В большинстве случаев внешним считается адрес "красного" интерфейса, как показано на Рис. 29. Второй параметр интересен лишь при наличии дополнительного маршрутизатора между IPCop и Интернетом.

Рис. 29. Способ определения IP-адреса DDNS.

## Прокси-сервер

Прокси-сервер, в основном, используется для кэширования Web-страниц. При использовании прокси браузер пользователя обращается не напрямую к сайту, а к прокси-серверу. А он уже отвечает за связь с сайтом. Но перед тем как обратиться к сайту, прокси-сервер просматривает свой кэш в поиске запрашиваемой страницы, а также появление новой версии страницы в Интернете. Тогда из Интернета запрашивается лишь обновлённая информация, остальная берётся из кэша. Это позволяет снизить нагрузку на используемый канал, увеличить скорость обработки запросов, и, соответственно, снизить трафик.

Существует два типа прокси. В классическом варианте прокси-сервер отвечает на определённом порту, обычно 8080 или 3128. Пользователи же должны соответствующим образом настроить свои браузеры. Второй вариант - прозрачный прокси, он перехватывает запросы соединений HTTP, не требуя настройки на клиентской стороне. В этом случае обход прокси невозможен, и этот вариант для многих компаний более предпочтителен, поскольку позволяет ограничить доступ на некоторые сайты.

IPСор поддерживает оба типа прокси, хотя по умолчанию прокси-сервер отключён. Для включения нужно перейти в раздел "Services -> Proxy". Прокси-сервер можно включить отдельно для каждого из интерфейсов. На Рис. 30 показано, как можно активировать прокси-сервер для "зелёного" интерфейса ("Enabled on Green"). Если установлен беспроводной адаптер, для него также можно включить прокси ("Enabled on Blue").

**Web proxy:**

Enabled on **Green**: ☒

Transparent on **Green**: ☒

Log Enabled: ☐

Upstream proxy (host:port):

Upstream username:

Upstream password:

Proxy Port:

---

**Cache management**

Cache size (MB):

Min object size (KB):

Max object size (KB):

---

**Transfer limits**

Max incoming size (KB):

Max outgoing size (KB):

---

☒ This field may be blank.

Рис. 30. Настройка прокси-сервера.

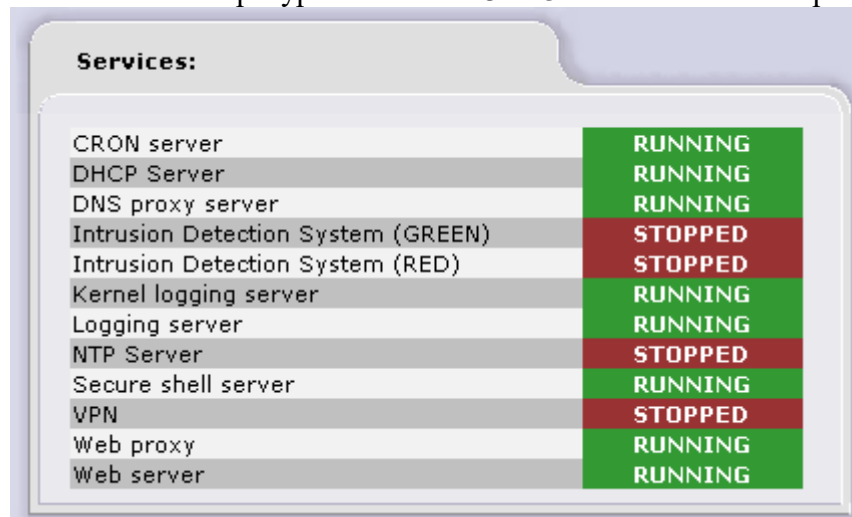
Флажок "Transparent" делает прокси-сервер прозрачным. В этом случае настройка порта в браузерах клиентов не требуется. Размер кэша прокси-сервера настраивается в разделе "Cache Management", сам же кэш физически располагается на жёстком диске маршрутизатора. Мы ограничили размер кэша отметкой 40 Гбайт, максимальный размер кэшируемого файла - 32 Мбайт; минимальный размер не задали.

Совет. При выборе большого размера кэша, после нажатия на кнопку "Save/Сохранить", web-интерфейс какое-то время не будет реагировать на ваши действия. Происходит выделение дискового пространства. Следует немного подождать.

В заключение отметим, что прокси позволяет ограничивать размер передаваемых файлов, что особенно полезно для тех, кто платит за каждый принятый мегабайт.

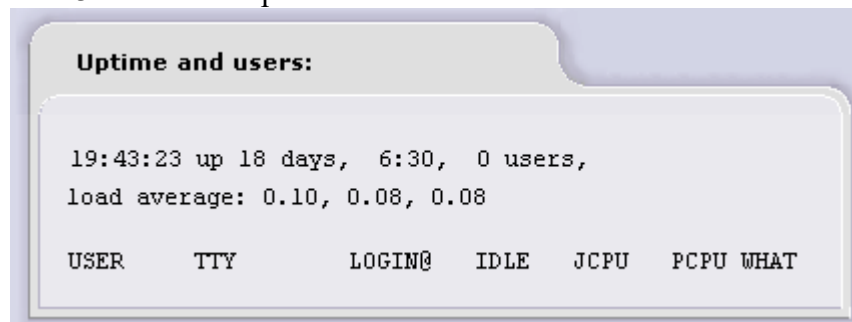
#### Мониторинг

Настроив IPCor, вы можете забыть о его существовании. Но если у вас есть желание, то можете контролировать состояние IPCor, благо, для этого есть множество экранов состояния, а также графиков использования ресурсов. На Рис. 31 - 34 показаны некоторые из них.



Services:	
CRON server	RUNNING
DHCP Server	RUNNING
DNS proxy server	RUNNING
Intrusion Detection System (GREEN)	STOPPED
Intrusion Detection System (RED)	STOPPED
Kernel logging server	RUNNING
Logging server	RUNNING
NTP Server	STOPPED
Secure shell server	RUNNING
VPN	STOPPED
Web proxy	RUNNING
Web server	RUNNING

Рис. 31. Список сервисов.



Uptime and users:						
19:43:23 up 18 days, 6:30, 0 users, load average: 0.10, 0.08, 0.08						
USER	TTY	LOGIN@	IDLE	JCPU	PCPU	WHAT

Рис. 32. Время работы.

## Interfaces:

```
eth0      Link encap:Ethernet  HWaddr 00:E0:4C:21:D8:2C
          inet addr:10.0.0.1  Bcast:10.0.0.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:26554792 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28849032 errors:0 dropped:0 overruns:1 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3185884714 (3038.2 MB)  TX bytes:1116547394 (1064.8 MB)
          Interrupt:9 Base address:0xb000

eth1      Link encap:Ethernet  HWaddr 00:E0:4C:21:D8:34
          inet addr:68.245.238.247 Bcast:68.245.238.249 Mask:255.255.255.248
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:29015232 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26186754 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1110276191 (1058.8 MB)  TX bytes:3153220084 (3007.1 MB)
          Interrupt:9 Base address:0xd000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3398 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3398 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:561478 (548.3 KB)  TX bytes:561478 (548.3 KB)
```

Рис. 33. Статус сети (отображает результаты команды ifconfig).

## GREEN Graph

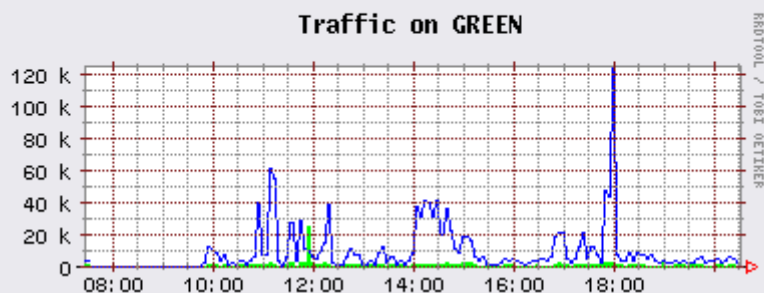


Рис. 34. Трафик "зелёного" интерфейса.



## Журналирование

Хотя просмотр журнала гораздо скучнее диаграмм, он всё же может существенно помочь в деле выявления проблем. Для просмотра журналов нужно перейти по закладке "Logs/Журналы".

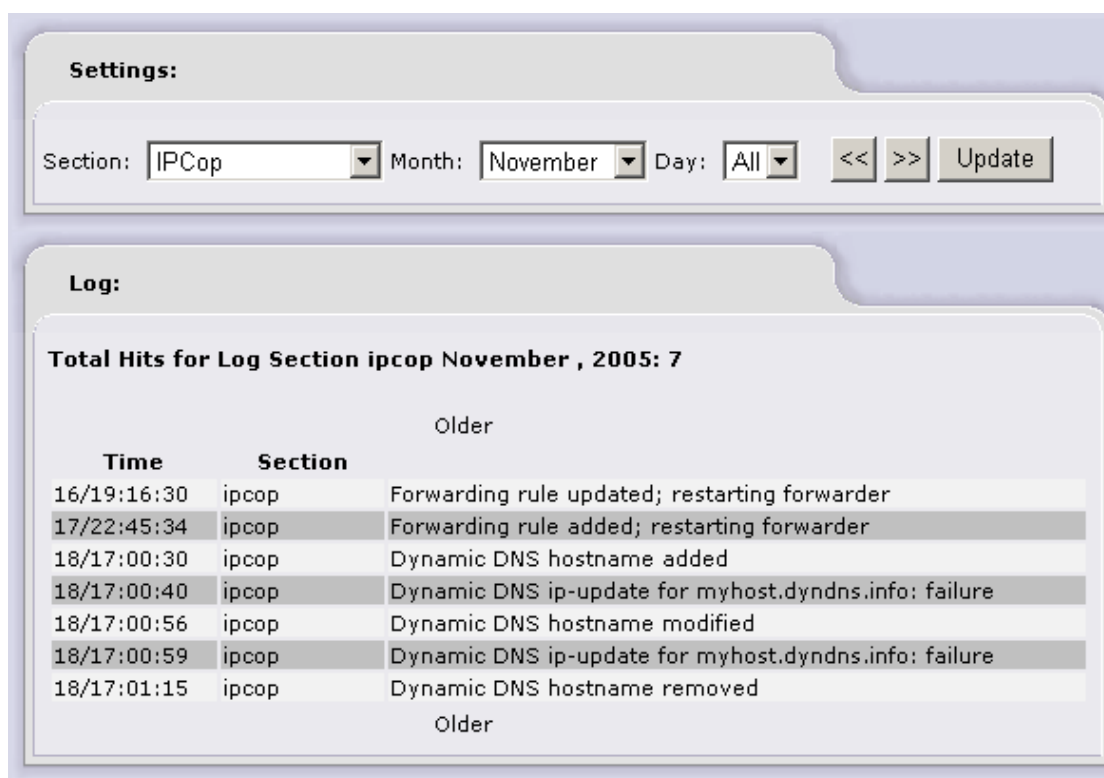


Рис. 35. Запись об ошибке обновления DDNS.

Для любителей интерфейса командной строки IPCop может предоставить доступ непосредственно к оболочке (только под учётной записью "root"). Кроме того, такой доступ окажется полезным и в том случае, если по какой-то причине web-интерфейс станет недоступен. На Рис. 36 показана команда `shutdown now -r`.

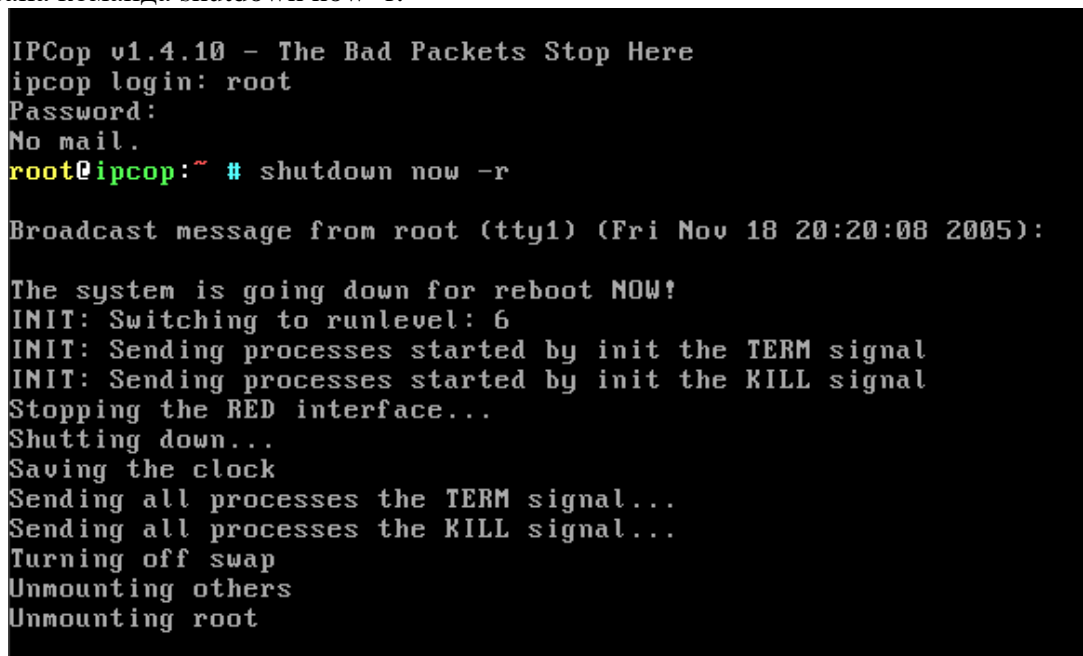


Рис. 36. Завершение работы из командной строки

Конечно, командная строка позволяет и устанавливать дополнительное ПО. Но мы не рекомендуем изменять конфигурацию IPCop, если вы не особенно хорошо разбираетесь в Linux. Кроме того, дополнительное ПО может снизить защищённость маршрутизатора.

## Заключение

Кроме всего перечисленного, маршрутизатор IPCop способен ещё на многое. Например, он содержит встроенную систему [Snort](#) для обнаружения вторжений, которую можно настроить на отслеживание всех интерфейсов. (Наш материал по Snort можете найти [здесь](#)).

Мы не рассмотрели управление полосой пропускания ("Traffic shaping"). Но вы тоже можете включить эту функцию через модуль [WonderShaper](#). Можно задать разные приоритеты (высокий, средний или низкий) для различных сервисов или портов.

Приятно удивило наличие встроенного сервера IPsec VPN, который позволяет объединить две сети через Интернет, (как между двумя IPSec, так и между IPSec и другим IPsec-маршрутизатором). Технология VPN позволяет также подключить удалённый узел к вашей сети (любой клиент IPsec подключается к IPSec). Сервер IPsec может работать с общим ключом/паролем или с сертификатом X.509. К сожалению, [документация IPSec](#) по VPN недостаточно подробна. Поэтому можно рекомендовать ознакомиться с другими ресурсами, указанными на [странице поддержки](#) сайта IPSec.

Если ваше желание создать маршрутизатор собственными руками ещё не исчезло, вы можете использовать большое количество дистрибутивов. Вариант IPSec содержит ряд несомненных преимуществ: простота установки, широкие возможности, прекрасный дизайн пользовательского интерфейса.

Ссылки на другие обзоры Linux-маршрутизаторов/брандмауэров на сайте THG.ru.

["Брандмауэр m0n0wall: надёжное программное решение";](#)

["SmoothWall Express Firewall 2.0: межсетевой экран на базе Linux";](#)

["Сервер ClarkConnect: надёжность Linux плюс дружественный интерфейс".](#)