

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Методические рекомендации по настройке контент-фильтрации на прокси-сервере для различных операционных систем, основанных на ядре Linux (ALT Linux, Ubuntu, OpenSuse)

Коновалов Д.В.
Булгаков Е.В.

2011 г.

Перечень модулей

Введение	4
1. Способы организации контент-фильтрации .	5
1.1. Настройка контент-фильтрации локально на каждом персональном компьютере.	5
1.2. Организация контент-фильтрации в сети с контролируемым доступом в сеть Интернет.	9
2. Организация локальной сети школы.	12
2.1. Организация локальной сети с контролируемым доступом в сеть интернет, на основе ALT Linux.	12
2.1.1. Организация локальной сети с контролируемым доступом в сеть интернет, на основе ALT Linux. Настройки на локальной машине.	15
2.2. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе Ubuntu.	18
2.2.1. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе Ubuntu. Настройки на локальной машине.	25
2.3. Организация локальной сети с контролируемым доступом в сеть интернет, на основе OpenSuse.	28
2.3.1. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе OpenSuse. Настройки на локальной машине.	35
3. Установка и настройка программного обеспечения для организации контент-фильтрации.	38
3.1.1. Установка и настройка прокси-сервера squid в ALT Linux Школьный сервер 5.0	38
3.1.2. Установка и настройка прокси-сервера squid в Ubuntu.	41
3.1.3. Установка и настройка прокси-сервера squid OpenSuse.	44
3.1.4. Настройки на локальной машине на примере браузера Mozilla Firefox.	49
3.2. Установка и настройка контент-фильтра на основе NetPolice в ALT Linux Школьный сервер 5.0	50
3.3. Установка и настройка контент-фильтра на основе DansGuardian.	54
3.3.1. Установка и настройка контент-фильтра на основе DansGuardian в ALT Linux Школьный сервер 5.0	54
3.3.2. Установка и настройка контент-фильтра на основе DansGuardian в Ubuntu.	56
3.4. Установка и настройка контент-фильтра на основе Redirector (Rejik).	59
3.4.1. Установка и настройка контент-фильтра на основе Redirector (Rejik) в ALT Linux Школьный сервер 5.0	59
3.4.2. Установка и настройка контент-фильтра на основе Redirector (Rejik) в OpenSuse.	61
4. Организация электронного журнала работы пользователей в сети Интернет на основе SARG и Light Squid.	63

4.1.	Организация электронного журнала работы пользователей в сети Интернет на основе SARG в ALT Linux.	63
4.2.	Организация электронного журнала работы пользователей в сети Интернет на основе SARG в Ubuntu.	66
4.3.	Организация электронного журнала работы пользователей в сети Интернет на основе Light Squid в OpenSuse.	68
	Заключение.	72
	Литература.	73

Введение.

В свете предоставления образовательным учреждениям высокоскоростного доступа к сети Интернет и участившихся проверок надзорных органов актуальным является организация контролируемого доступа учащихся и сотрудников школы к ресурсам всемирной паутины, а также фильтрации нежелательного контента.

С одной стороны - необходимо предоставить учащимся и сотрудникам школы доступ к ресурсам всемирной паутины, с другой стороны нам нужны только те ресурсы, которые отвечают образовательным задачам учебного заведения. Решений данной проблемы может быть несколько:

1. Заключение договора с провайдером на предоставление услуги контентной фильтрации - такой вариант не всегда доступен, так как не все провайдеры предоставляют такую услугу, да и где гарантии того, что фильтрация будет отвечать требованиям школы. В большинстве случаев образовательные учреждения не могут влиять на списки по которым ведется фильтрация, что не совсем удобно для работы.
2. Самостоятельно организовать контент-фильтрацию В этом случае ответственность целиком ложится на плечи образовательного учреждения, но появляется возможность самостоятельно контролировать списки разрешенных и запрещенных ресурсов.

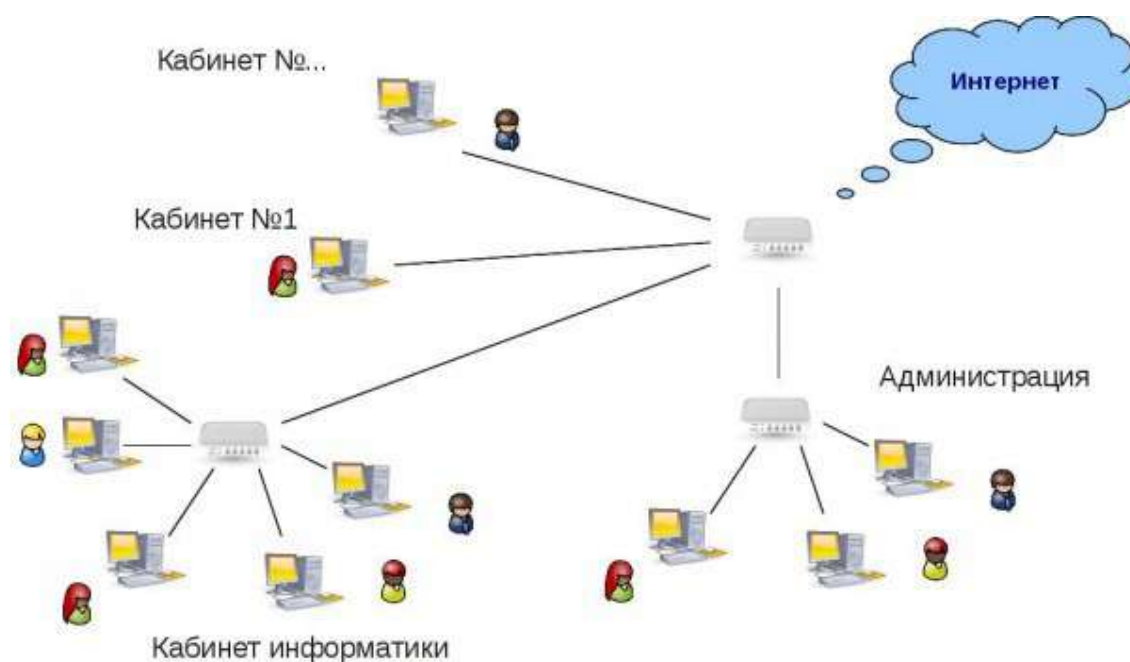
Рассмотрим способы организации контент-фильтрации более подробно на примере трех наиболее популярных в образовательных учреждениях Алтайского края дистрибутивах, основанных на ядре Linux: ALT Linux, Ubuntu, OpenSuse.

1. Способы организации контент-фильтрации.

Рассмотрим какие же способы организации контент-фильтрации доступны образовательным учреждениям:

1. Локально на каждом персональном компьютере.
2. Программа-фильтр устанавливается на компьютере, контролирующему доступ в сеть Интернет всех персональных компьютеров школы, входящих в локальную сеть образовательного учреждения.

Первый способ, несомненно, очень трудоемок и усложняет процесс администрирования программы контент-фильтрации, так как контролировать список доступа к ресурсам необходимо на каждом ПК. В большинстве случаев такую фильтрацию может отключить пользователь самостоятельно, владеющий минимальными навыками работы с ПК.

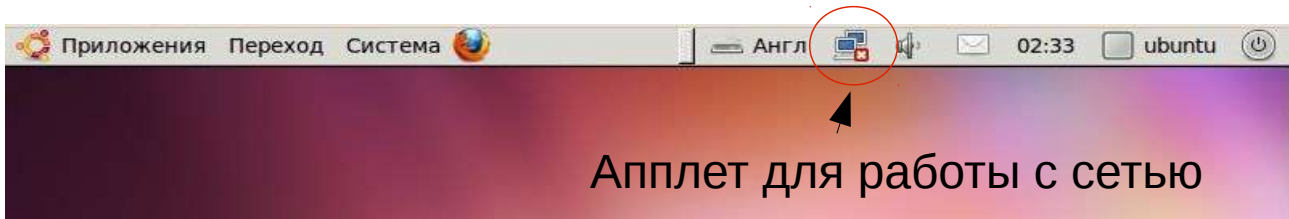


(Рис.1. Схема локальной сети образовательного учреждения без использования контролируемого доступа в сеть Интернет)

1.1. Настройка контент-фильтрации локально на каждом персональном компьютере

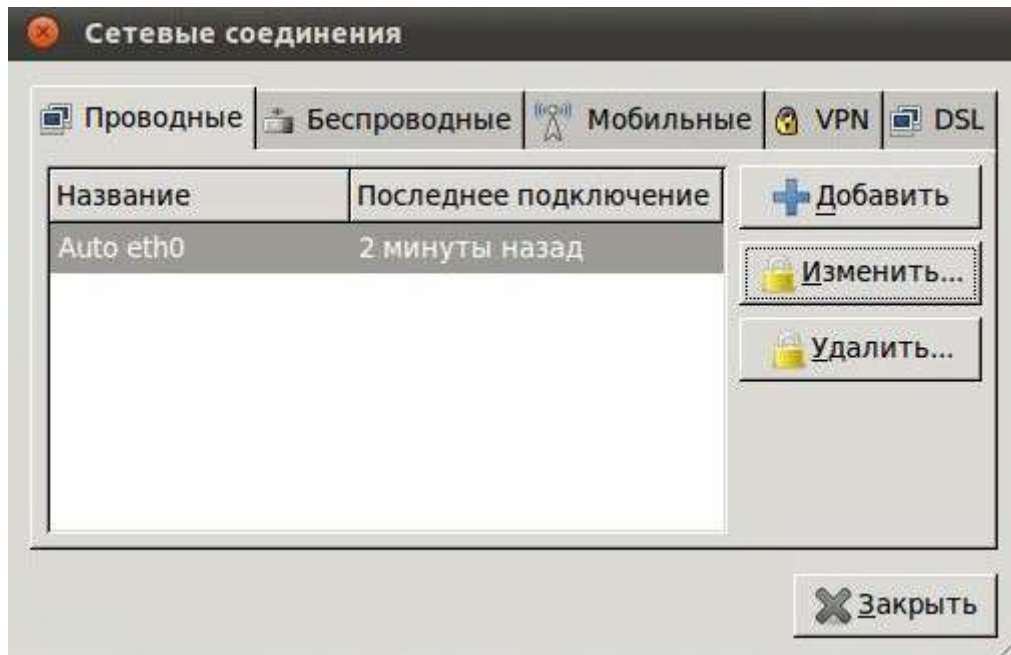
Рассмотрим более подробно настройку контент-фильтрации на локальном компьютере школьной сети. В качестве фильтра остановимся на NetPolice DNS, как наиболее доступном и простом в установке. В данном случае важно, чтобы настройки сети компьютер получал автоматически (DHCP).

1. Настройка в Ubuntu:
 - Воспользуемся апплетом, расположенном на верхней панели рабочего стола. (Или Система — Параметры — Сетевые соединения). Щелчком правой кнопки мыши вызываем меню. Выбираем пункт «Изменить»:



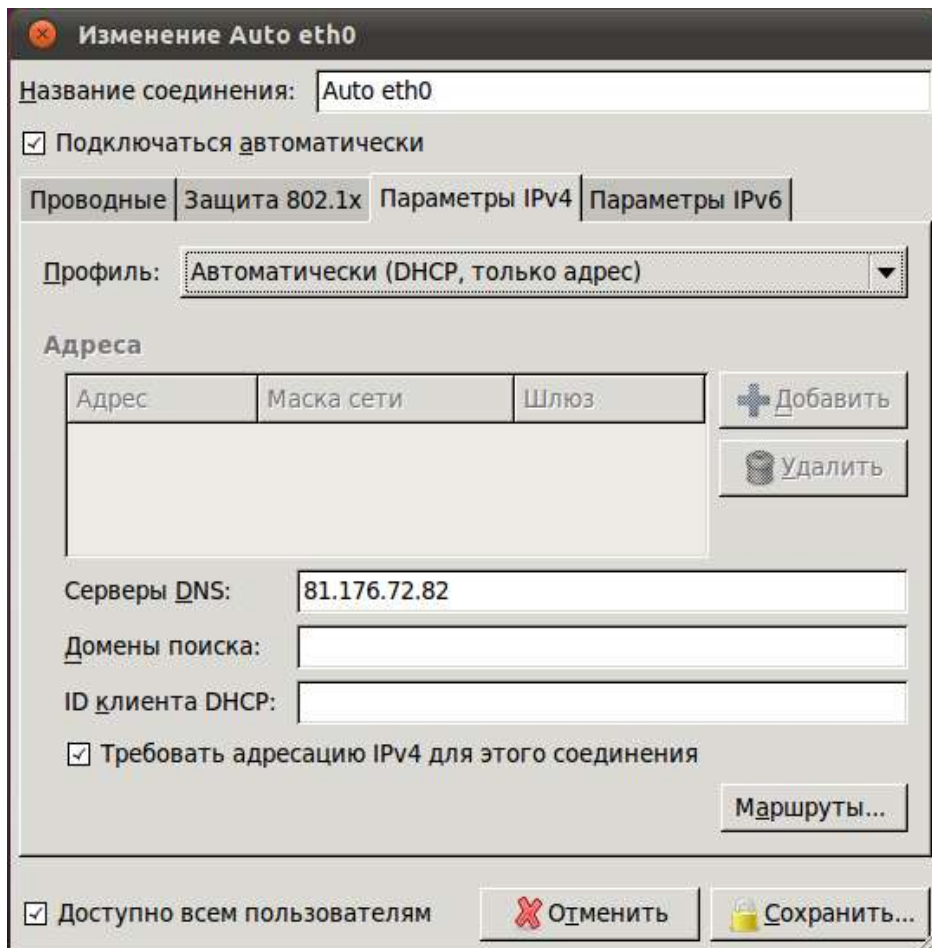
(Рис.2. Апплет для настройки сети в Ubuntu)

- Выбираем сетевой интерфейс и нажимаем кнопку «Изменить»:



(Рис.3. Изменение настроек сети в Ubuntu)

- Выбираем вкладку «Параметры IPv4» и в разделе «Профиль» - «Автоматически (DHCP, только адрес)» и указываем в строке «Серверы DNS» - 81.176.72.82:



(Рис.4. Подключение контент-фильтра NetPolice DNS на локальной машине в Ubuntu)

- Сохраняем настройки и перезагружаем персональный компьютер, чтобы изменения вступили в силу.
- Поверяем работу фильтрации при помощи браузера:

Страница заблокирована фильтром NetPolice!

[Сообщить о неверной категоризации ресурса](#)



Безопасное использование Интернета дома
О безопасном Интернете для преподавателей
О безопасном Интернете для учащихся

Новости:

- [Польский рейд](#)
- [Нет зла страшнее, чем Facebook](#)
- [Интернет-запугивание - прямая дорога к депрессии](#)
- [Индонезийцам будут платить за доносы](#)

(Рис.5. Проверка работы контент-фильтра NetPolice DNS в Ubuntu)

2. Настройка подключения контент-фильтра NetPolice DNS выглядит аналогично:

Подключаться автоматически

Беспроводные | Защита беспроводной сети | **Параметры IPv4** | Параметры IPv6

Профиль: Автоматически (DHCP, только адрес)

Addresses

Адрес	Маска сети	Шлюз
-------	------------	------

+ Добавить

x Удалить

Серверы DNS: 81.176.72.82

Домены поиска:

ID клиента DHCP:

Требовать адресацию IPv4 для этого соединения

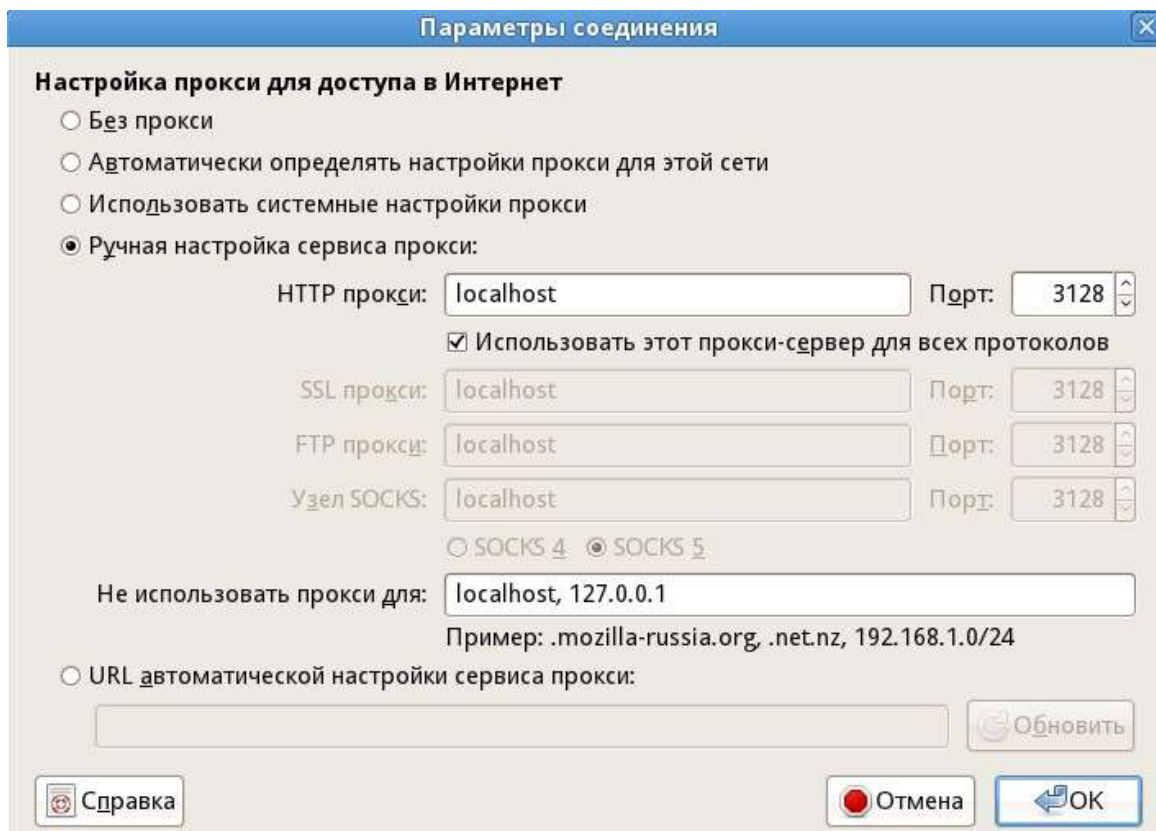
Routes...

Доступно всем пользователям

Отменить Save

(Рис.6. Подключение контент-фильтра NetPolice DNS на локальной машине в ALT Linux)

Отличительной особенностью дистрибутивов Linux является то, что из любого дистрибутива можно сделать серверный и наоборот. Поэтому все настройки контент-фильтрации для серверного дистрибутива применимы и к локальным компьютерам школьной сети. Единственным отличием версии для Desktop в нашем случае — это наличие одного сетевого интерфейса и в настройках браузера, вместо ip-адреса сервера, нужно будет указать 127.0.0.1 или localhost:



(Рис.7. Пример настройки браузера Mozilla Firefox на локальном компьютере)

Надстройку контент-фильтрации на сервере мы рассмотрим ниже.

1.2. Организация контент-фильтрации в сети с контролируемым доступом в сеть Интернет

Второй способ требует от системного администратора более высокого уровня квалификации, так как он подразумевает администрирование школьного сервера. Но при таком способе организации контроля доступа к ресурсам сети Интернет ни одна машина не может миновать программу-фильтр, установленную на сервере. Также контролировать список доступных или запрещенных ресурсов нужно в единственном числе.



(Рис.8. Схема локальной сети образовательного учреждения с использованием контролируемого доступа в сеть Интернет)

Рассмотрим второй способ более подробно. Такой способ позволяет обеспечить доступ в сеть Интернет всех сотрудников и учащихся образовательного учреждения через один общий канал.

В соответствии с требованиями надзорных органов руководители многих образовательных учреждений пришли к выводу о том, что необходима:

1. организация разграничения прав доступа к ресурсам сети Интернет для различных групп пользователей локальной сети образовательного учреждения;
2. фильтрация трафика на основе «черных» и «белых» списков;
3. ведение электронного журнала работы пользователей в сети Интернет, доступного через веб-интерфейс, создаваемого автоматически на основе отчета о работе прокси-сервера.

"Белые списки" - подразумевают перечень ресурсов, доступ к которым разрешен. Несомненно, что "Белые списки" для образовательного учреждения должны содержать только те ресурсы, которые отвечают образовательным задачам школы.

"Черные списки" - подразумевают перечень ресурсов доступ к которым запрещен. Какое-же программное обеспечение выбрать для организации контролируемого доступа в сеть интернет? Интернет изобилует предложениями о программах, для фильтрации трафика, но в большинстве своем это коммерческие решения, требующие покупки дорогостоящих лицензий. Также такое ПО предполагает установку на ОС Windows, что в свете перехода образовательных учреждений на СПО не совсем актуально.

Но зачем же покупать то, что и так уже есть у школы? А именно:

1. Дистрибутивы Linux — распространяются свободно и их можно скачать с сайта производителя.
2. Прокси-сервер squid (предустановлен в большинстве серверных дистрибутивов).

3. Программы для фильтрации трафика: NetPolice, Redirector, DansGuardian. Эти программы способны обеспечить различный уровень доступа пользователей, фильтрацию контента, а также позволяют организовать фильтрацию на основе "черных" и "белых списков".
4. Генератор отчетов работы прокси-сервера SARG (Squid Analysis Report Generator) - позволяют создавать электронный журнал работы пользователей в сети Интернет автоматически.

Таким образом образовательные учреждения имеют полный набор средств и инструментов, для организации контент-фильтрации на основе свободно распространяемого программного обеспечения.

2. Организация локальной сети школы.

После того как мы определились с программным обеспечением для организации контент-фильтрации и принципом организации локальной сети, перейдем к более детальному рассмотрению организации школьной образовательной сети с контролируемым доступом в сеть Интернет.

Одной из основных проблем на данном этапе является конфигурирование самого сервера, выбор параметров. На самом деле, для обслуживания сравнительно небольшой сети (10-15 компьютеров), вполне подойдет обыкновенный школьный ПК с параметрами: процессор от 233 МГц, от 128 Мб ОЗУ.

Единственное условие для нашей конфигурации - это наличие 2-х сетевых интерфейсов. Первый предназначен для установления соединения с сетью Интернет, второй - для работы с локальной сетью школы.



(Рис. 9. Конфигурирование школьного сервера)

Соответственно первому сетевому интерфейсу присваиваются настройки, полученные образовательным учреждением от провайдера. Второму — параметры локальной сети образовательного учреждения. При такой организации между локальной сетью и сетью Интернет будет стоять система, контролирующая весь входящий и исходящий трафик.

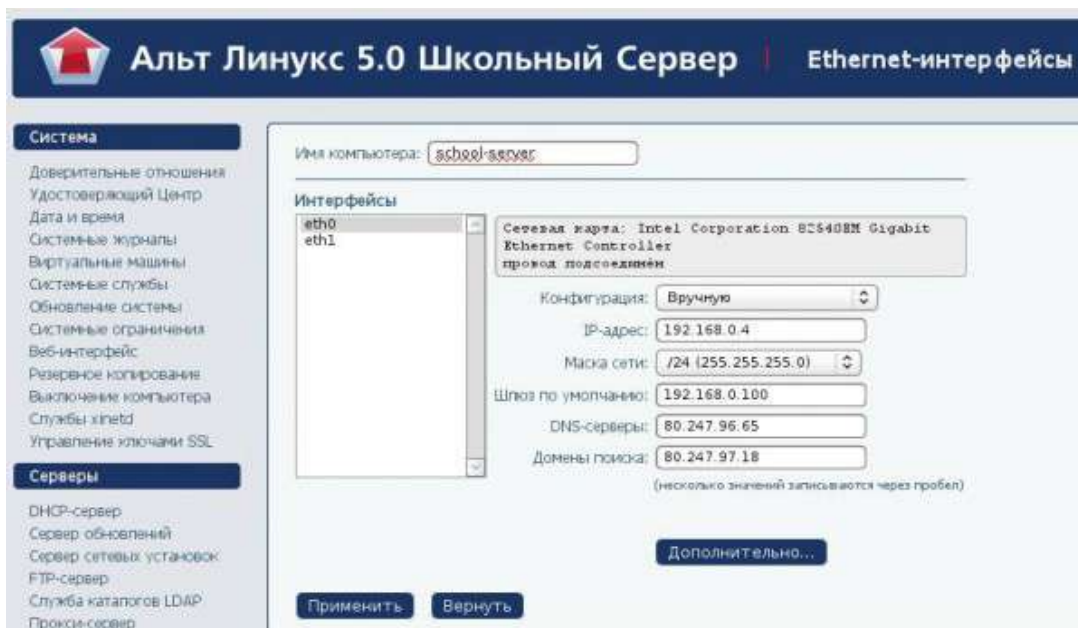
Сетевые интерфейсы настраиваются при установке дистрибутива (рекомендуемый вариант). Либо после установки, что не намного сложнее. Однако для каждого из вышеперечисленных дистрибутивов наблюдается своя специфика.

2.1. Организация локальной сети с контролируемым доступом в сеть интернет, на основе ALT Linux.

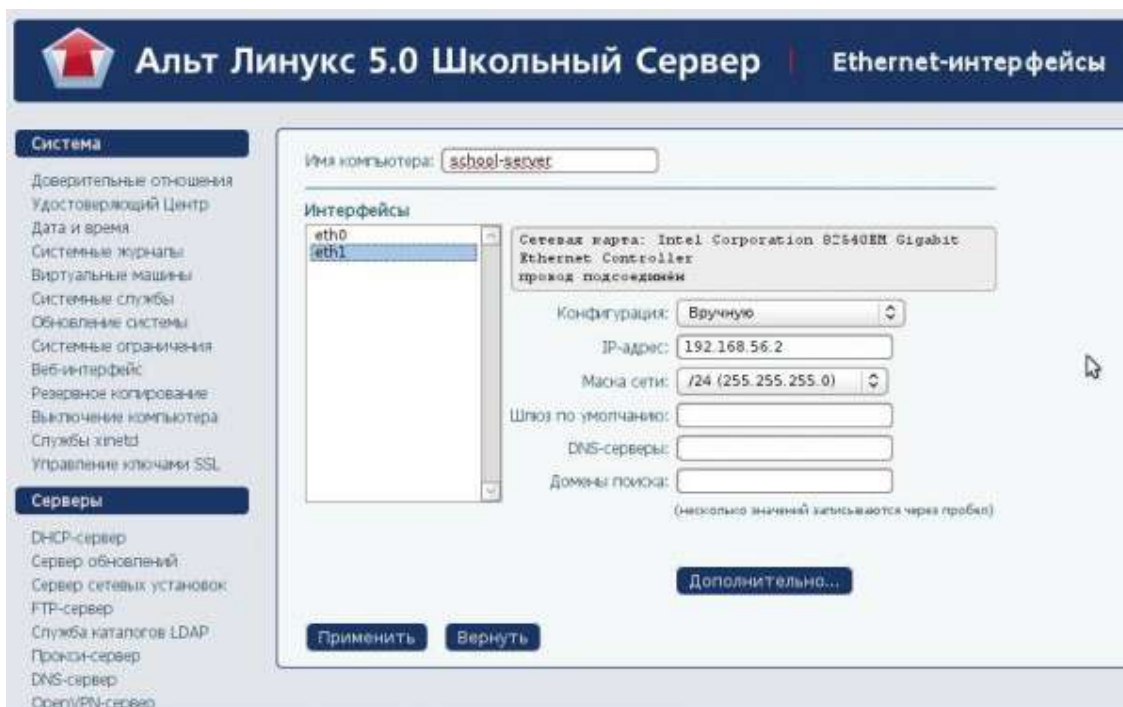
Как уже было отмечено выше сетевые интерфейсы. При работе с ALT Linux Школьный сервер 5.0 настраиваются при установке дистрибутива (рекомендуемый вариант). Либо после установки, например при помощи центра управления системой, доступного через веб-интерфейс (<https://ip сервера:8080>).

Определимся с IP-адресами. В нашем случае настройки для выхода в сеть интернет, полученные от провайдера: IP-адрес для сервера 192.168.0.4, DNS-сервер 80.247.96.65.

Диапазон IP-адресов для компьютеров локальной сети школы 192.168.56.0/24.



(Рис. 10. Настройка внешнего сетевого интерфейса для работы в сети Интернет)



(Рис.11. Настройка внутреннего сетевого интерфейса для работы в локальной сети образовательного учреждения)

После настройки сетевых интересов необходимо проверить имеет ли сервер доступ в сеть Интернет и локальную сеть образовательного учреждения. Для этого воспользуемся командой ping:

```
[root@school-server ~]# ping yandex.ru
PING yandex.ru (87.250.251.11) 56(84) bytes of data.
64 bytes from yandex.ru (87.250.251.11): icmp_seq=1 ttl=55 time=121 ms
64 bytes from yandex.ru (87.250.251.11): icmp_seq=2 ttl=55 time=47.1 ms
64 bytes from yandex.ru (87.250.251.11): icmp_seq=3 ttl=55 time=110 ms
^C
--- yandex.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 47.128/92.931/121.486/32.717 ms
[root@school-server ~]# ping 192.168.56.254
PING 192.168.56.254 (192.168.56.254) 56(84) bytes of data.
64 bytes from 192.168.56.254: icmp_seq=1 ttl=64 time=0.296 ms
64 bytes from 192.168.56.254: icmp_seq=2 ttl=64 time=0.420 ms
64 bytes from 192.168.56.254: icmp_seq=3 ttl=64 time=0.564 ms
^C
--- 192.168.56.254 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 0.296/0.426/0.564/0.112 ms
```

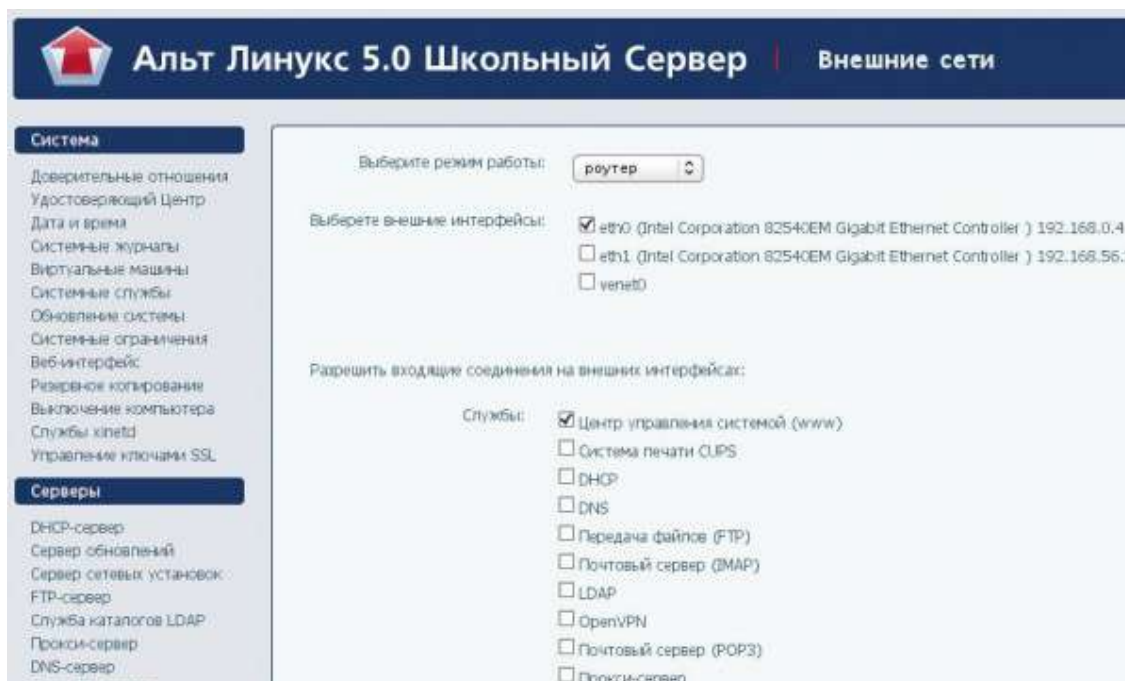
(Рис. 12. Проверка доступа сервера к сети Интернет и локальной сети школы)

Следующая задача - определиться в каком режиме будет работать сервер: роутер или шлюз.

- **Роутер.** В этом режиме перенаправление пакетов между сетевыми интерфейсами происходит без трансляции сетевых адресов.
- **Шлюз.** В этом режиме будет настроена трансляция сетевых адресов (NAT) при перенаправлении пакетов на внешние интерфейсы. Использование этого режима имеет смысл, если у вас настроен по крайней мере один внешний и один внутренний интерфейс.

В режиме шлюза клиенты смогут беспрепятственно выходить в сеть Интернет, достаточно прописать соответствующие сетевые настройки. Поэтому такой вариант нас не устраивает, так как наша задача выпускать только тех пользователей, которым мы разрешим и только по установленным нами правилам.

Поэтому настраиваем работу сервера в режиме роутер (Брандмауэр -> Внешние сети):



(Рис. 13. Настройка работы сервера в режиме «роутер»)

В этом же разделе мы можем указать и внешние сети, и закрыть доступ к тем портам, по которым доступ к нашему серверу нежелателен.

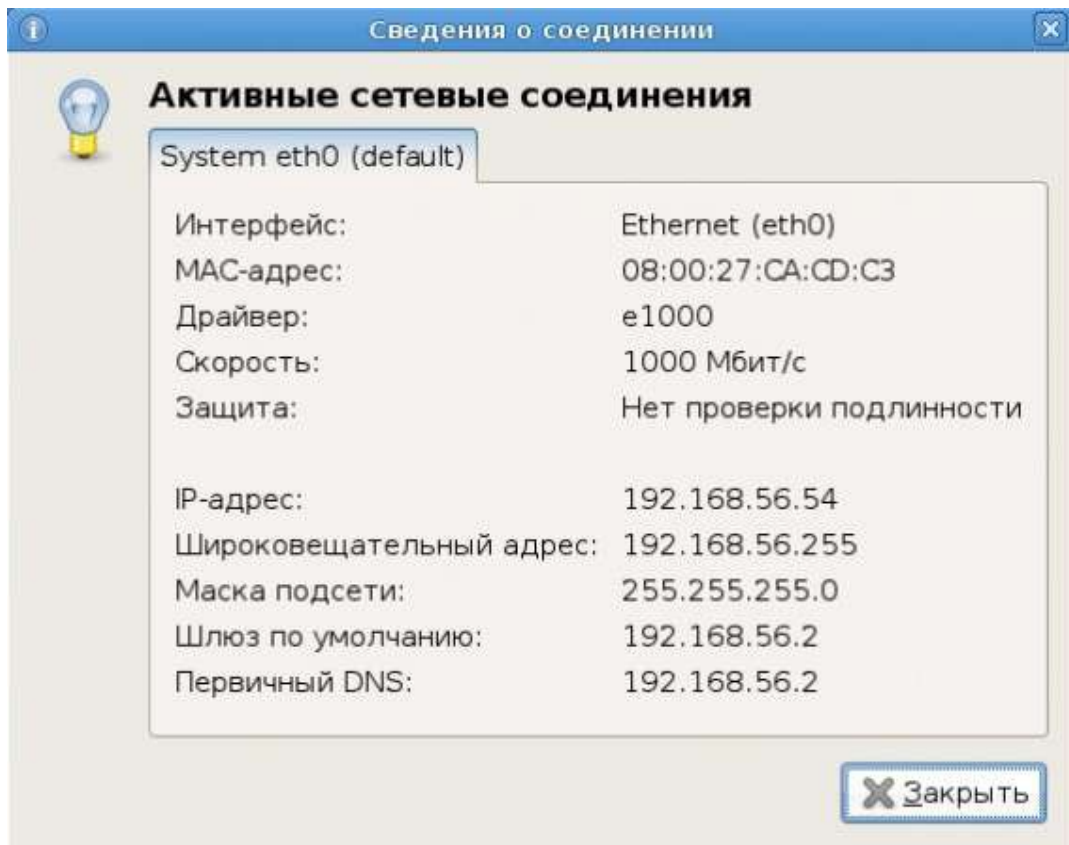
2.1.1. Организация локальной сети с контролируемым доступом в сеть интернет, на основе ALT Linux. Настройки на локальной машине.

Произведя предварительную настройку школьного сервера приступим к настройке локальных машин локальной сети школы.

Первое, что нужно настроить - это сетевой интерфейс ПК. В нашем случае 192.168.0.2 — это внешний адрес для выхода в сеть Интернет, предоставленный провайдером, 192.168.56.2 - это ip-адрес сетевого адаптера школьного сервера для работы в локальной сети школы.

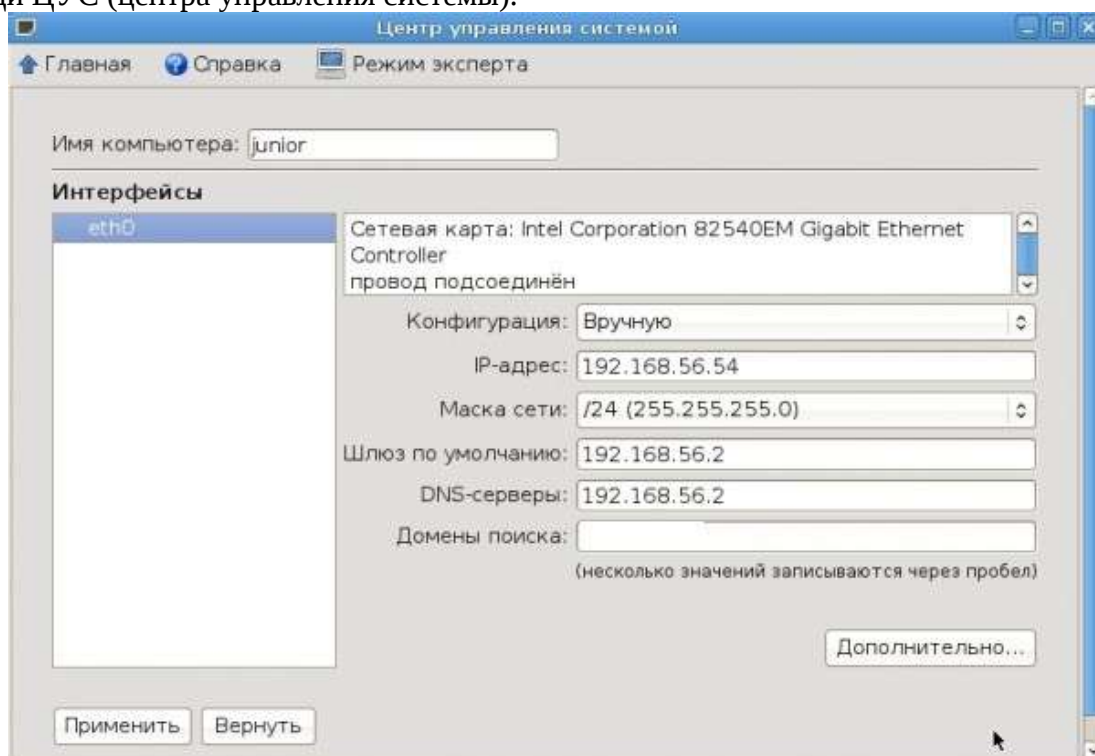
Таким образом ip-адреса на ПК в локальной сети должны быть из диапазона 192.168.56.3 - 192.168.56.254. Но такое количество адресов слишком велико для небольшой школьной сети, поэтому можно ограничиться количеством ПК в сети с учетом перспективы дальнейшего роста.

IP-адрес шлюза, в нашем случае, - ip-адрес школьного сервера (192.168.56.2).



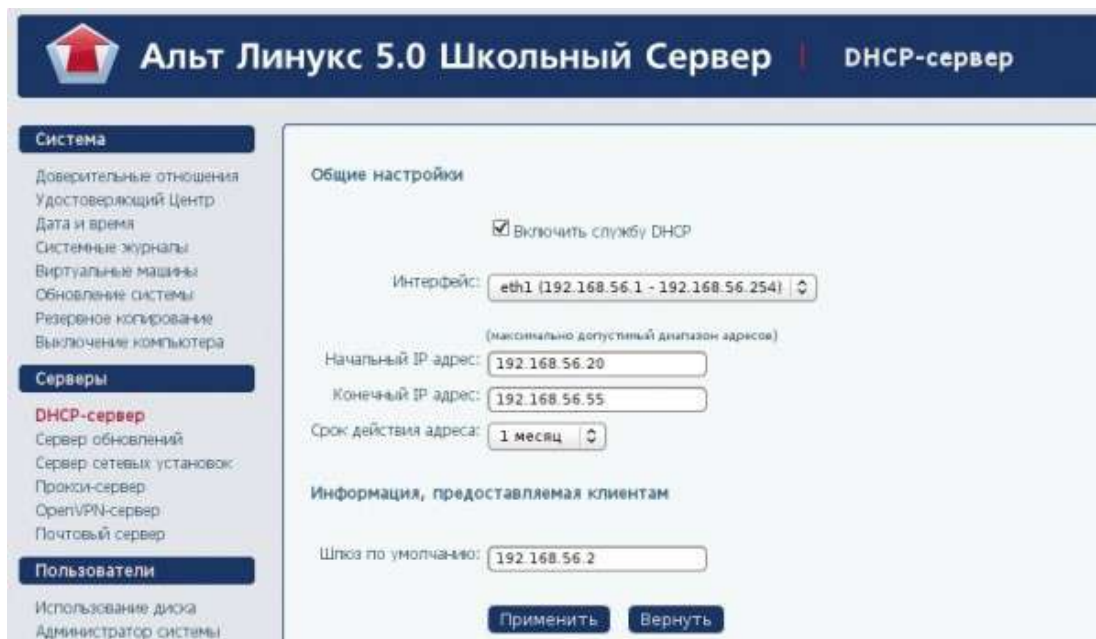
(Рис. 14. Сведения о соединении на персональном компьютере в локальной сети школы)

Произвести настройки сетевого интерфейса на ПК в локальной сети можно также при помощи ЦУС (центра управления системой).



(Рис. 15. Настройка подключения к локальной сети школы на локальном компьютере)

Настройки можно ввести как в ручную, так и получить их при помощи dhcp, при условии, что сервер dhcp настроен и функционирует в школьной сети.



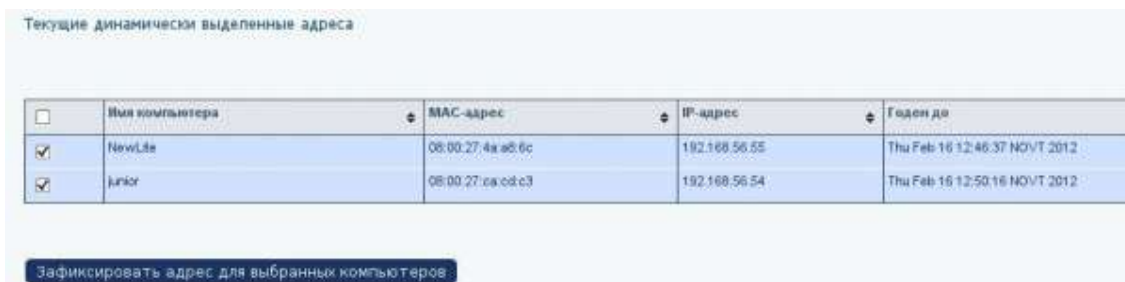
(Рис. 16. Настройка DHCP-сервера при помощи панели управления)

Проверить работоспособность соединения можно при помощи команды ping (ping 192.168.56.2).

```
[root@junior ~]# ping 192.168.56.2
PING 192.168.56.2 (192.168.56.2) 56(84) bytes of data.
64 bytes from 192.168.56.2: icmp_seq=1 ttl=64 time=0.195 ms
64 bytes from 192.168.56.2: icmp_seq=2 ttl=64 time=0.485 ms
^C
--- 192.168.56.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.195/0.340/0.485/0.145 ms
```

(Рис. 17. Проверка соединения в локальной сети школы)

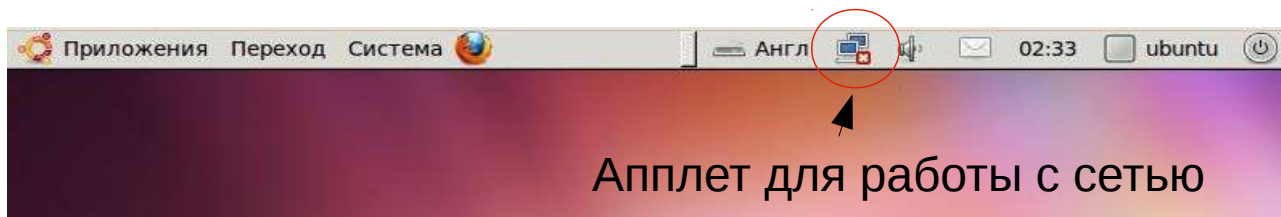
Также имеет смысл закрепить выданные адреса за определенными ПК, на случай, если будут применяться программы, использующие обмен данными по ip (например iTALC).



(Рис. 18. Закрепление IP-адреса за персональным компьютером в локальной сети школы при помощи панели управления сервером)

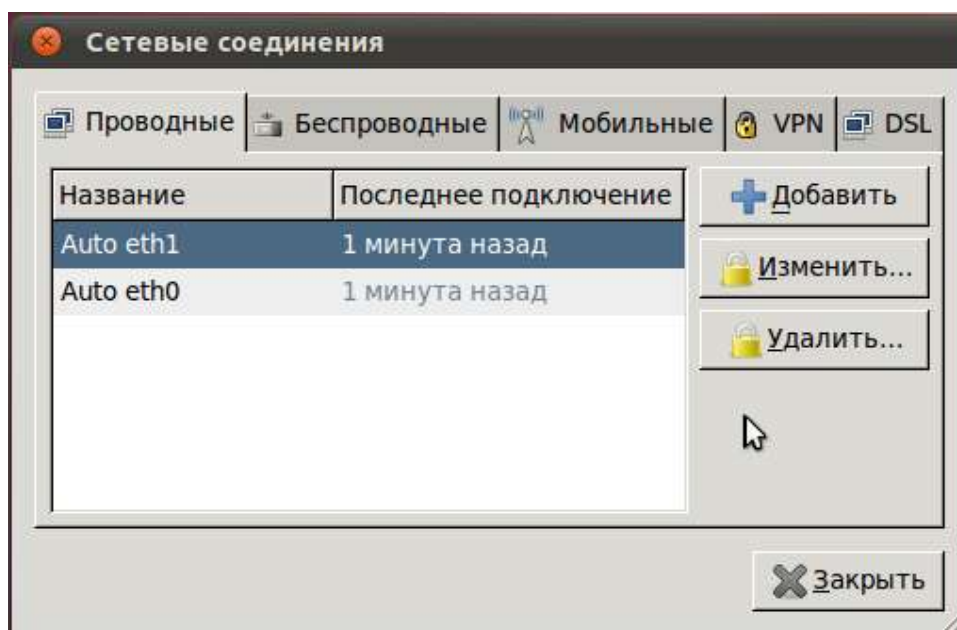
2.2. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе Ubuntu.

В качестве серверного дистрибутива выберем Ubuntu, версию для Desktop, памятуя о том, что любой дистрибутив Linux можно превратить в сервер и наоборот. (на момент написания актуальная версия Ubuntu 11.04). Требования к серверу мы оставляем те же. Основное условие — это наличие 2-х сетевых интерфейсов. В процессе установки система запросит указать основной сетевой интерфейс и задать параметры сети. Указываем параметры, которые предоставил нам провайдер. Второму сетевому интерфейсу задаем параметры локальной сети школы. Если Вы этого не сделали на этапе установки — не беда, настроим их при помощи стандартных инструментов.



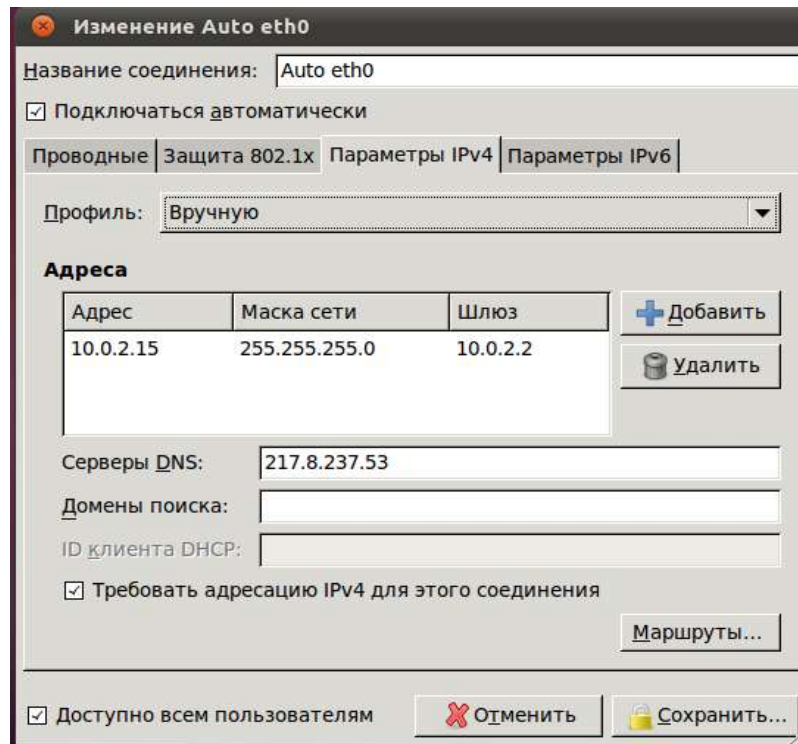
(Рис.19. Апплет для настройки сети в Ubuntu)

Воспользуемся апплетом, расположенном на верхней панели рабочего стола. (Или Система — Параметры — Сетевые соединения). Щелчком правой кнопки мыши вызываем меню. Выбираем пункт «Изменить»:



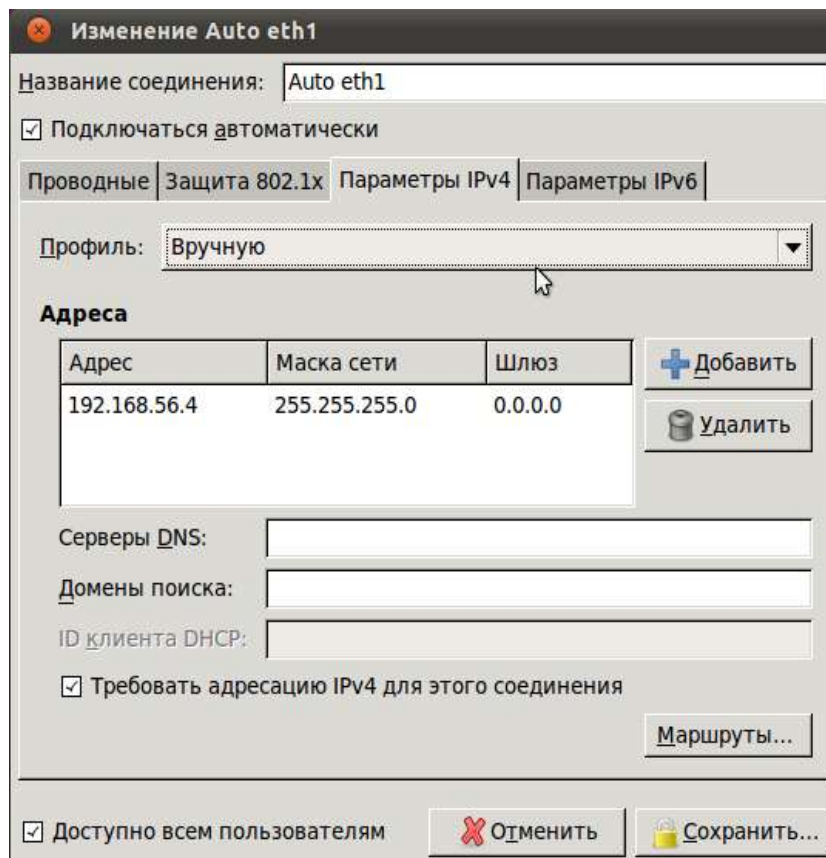
(Рис. 20. Изменение настроек сети в Ubuntu)

Пусть в нашем случае интерфейс eth0 — предназначен для подключения к сети Интернет, eth1 — подключение к локальной сети школы. Выбираем соответствующий сетевой интерфейс и нажимаем кнопку «Изменить». Выбираем вкладку «Параметры IPv4». Профиль — Вручную (если провайдер предоставил нам статичный ip-адрес, иначе можно выбрать «Автоматически (DHCP) и компьютер получит адрес автоматически»). В разделе адреса нажимаем кнопку добавить и вводим параметры подключения к сети Интернет. После проведения манипуляций по вводу параметров сети нажимаем кнопку «Сохранить».



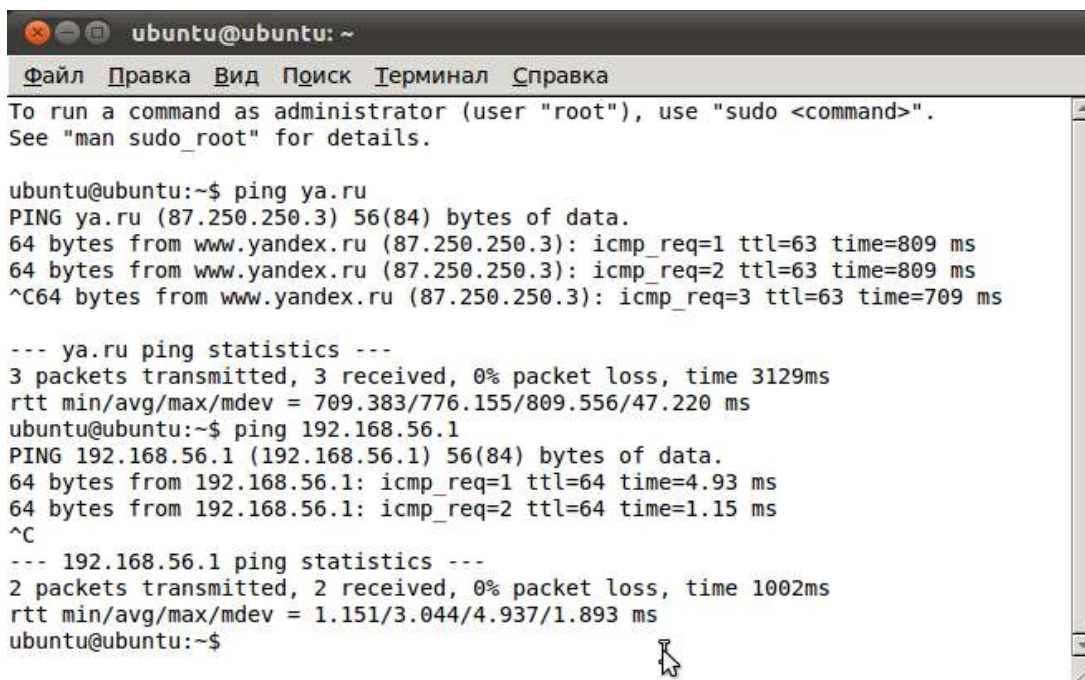
(Рис. 21. Настройка сетевого интерфейса eth0)

Сетевому интерфейсу eth1 присваиваем параметры локальной сети школы:



(Рис. 22. Настройка сетевого интерфейса eth1)

Для проверки доступа к сети Интернет и к локальной сети школы воспользуемся уже знакомой нам командой ping:



```
ubuntu@ubuntu: ~
Файл  Правка  Вид  Поиск  Терминал  Справка
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubuntu:~$ ping ya.ru
PING ya.ru (87.250.250.3) 56(84) bytes of data.
64 bytes from www.yandex.ru (87.250.250.3): icmp_req=1 ttl=63 time=809 ms
64 bytes from www.yandex.ru (87.250.250.3): icmp_req=2 ttl=63 time=809 ms
^C64 bytes from www.yandex.ru (87.250.250.3): icmp_req=3 ttl=63 time=709 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 3129ms
rtt min/avg/max/mdev = 709.383/776.155/809.556/47.220 ms
ubuntu@ubuntu:~$ ping 192.168.56.1
PING 192.168.56.1 (192.168.56.1) 56(84) bytes of data.
64 bytes from 192.168.56.1: icmp_req=1 ttl=64 time=4.93 ms
64 bytes from 192.168.56.1: icmp_req=2 ttl=64 time=1.15 ms
^C
--- 192.168.56.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.151/3.044/4.937/1.893 ms
ubuntu@ubuntu:~$
```

(Рис.23. Проверка настроек сети)

Для того чтобы «раздать Интернет» на компьютеры локальной сети школы произведем следующие действия:

1. Разрешим направление пакетов. Чтобы сделать это, отредактируем `/etc/sysctl.conf`. Откроем файл при помощи текстового редактора `gedit`: **`sudo gedit /etc/sysctl.conf`**
2. Раскомментируем строку `net.ipv4.ip_forward=1` и сохраним изменения.
3. Добавим правило для `firewal`: **`sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE`**
4. Чтобы настройки `iptables` работали после перезагрузки сохраняем настройки в файл: **`iptables-save > /etc/iptables.up.rules`**
5. И добавляем в конец файла `/etc/network/interfaces` строку **`pre-up iptables-restore < /etc/iptables.up.rules`**. Для этого воспользуемся уже знакомой нам командой: **`sudo gedit /etc/network/interfaces`**
6. Также нам понадобится пакет `dnsmasq` для раздачи пакетов по сети: **`sudo apt-get install dnsmasq`**

Теперь наш сервер готов для «раздачи Интернет» на компьютеры локальной сети школы. Однако имеет смысл произвести еще кое-какие настройки, для более удобной и комфортной работы.

К сожалению встроенного веб-интерфейса для управления сервером Ubuntu не имеет, однако есть замечательная разработка для администрирования серверов на базе Linux — `Webmin`.


`Webmin` — это программный комплекс, позволяющий администрировать операционную систему через веб-интерфейс, в большинстве случаев, позволяя обойтись без использования командной строки и запоминания системных команд и их параметров. Используя любой браузер, администратор сервера может создавать новые учётные записи пользователей, почтовые ящики, изменять настройки служб и сервисов, например: веб-

сервера Apache, DNS. Однако, в некоторых случаях необходимо знание операционной системы и редактирование конфигурационных файлов вручную. Кроме того, не все возможности операционной системы и не все программы можно конфигурировать через интерфейс Webmin.

Итак установим Webmin. Запускаем приложение «Терминал» (Приложения — Стандартные — Терминал). Ходим в систему с правами суперпользователя root:

1. Вводим команду **sudo -i**.
2. Вводим пароль суперпользователя root.
3. Получаем ключ для подключения к репозиторию:
 - Переходим в домашнюю директорию суперпользователя root: **cd /root**
 - Скачиваем ключ: **wget <http://www.webmin.com/jcameron-key.asc>**
 - Добавляем скаченный ключ к общему списку ключей системы: **apt-key add jcameron-key.asc**
4. Добавляем источник приложений для установки webmin. Это можно сделать как при помощи менеджера пакетов Synaptic, так и путем редактирования файла /etc/apt/sources.list. Для этого воспользуемся следующей командой:
gedit /etc/apt/sources.list
5. При помощи текстового редактора добавляем строку в конец файла:
deb <http://download.webmin.com/download/repository> sarge contrib
6. Сохраняем изменения и закрываем редактор. Обновляем индексы репозитория и устанавливаем пакет webmin:
 - **apt-get update**
 - **apt-get install webmin**

Порт, на котором работает Webmin — 10000. Запускаем браузер и вводим в адресной строке: <https://ip-адрес сервера:10000> (в нашем случае <https://192.168.56.4:10000> или, если мы работаем на локальной машине — <https://localhost:10000>).



(Рис. 24. Вход в Webmin)

Вводим логин и пароль пользователя системы и нажимаем кнопку «Login» и входим в систему:

Login: ubuntu
 Webmin
 System
 Servers
 Others
 Networking
 Hardware
 Cluster
 Un-used Modules
 Search:

View Module's Logs
 System Information
 Refresh Modules
 Logout

webmin

System hostname	ubuntu.localdomain
Operating system	Ubuntu Linux 11.04
Webmin version	1.570
Time on system	Sat Dec 3 07:19:39 2011
Kernel and CPU	Linux 2.6.38-8-generic on i686
Processor information	Intel(R) Pentium(R) CPU P6100 @ 2.00GHz, 1 cores
System uptime	4 hours, 37 minutes
Running processes	136
CPU load averages	0.00 (1 min) 0.03 (5 mins) 0.07 (15 mins)
CPU usage	0% user, 1% kernel, 0% IO, 99% idle
Real memory	496.09 MB total, 201.75 MB used
Virtual memory	780 MB total, 3.08 MB used
Local disk space	9.09 GB total, 2.90 GB used
Package updates	251 package updates are available

(Рис. 25. Стартовая страница Webmin)

Выбираем язык системы — Russian CP1251(RU_RU) (Webmin - Change Language and Theme) и сохраняем изменения.:

Login: ubuntu
 Webmin
 Backup Configuration Files
 Change Language and Theme
 Webmin Actions Log
 Webmin Configuration
 Webmin Servers Index
 Webmin Users
 System
 Servers
 Others
 Networking
 Hardware
 Cluster
 Un-used Modules
 Search:

View Module's Logs
 System Information
 Refresh Modules
 Logout

Change Language and Theme

This module can be used to change the language that modules are displayed in and the theme that controls Webmin's appearance, for your Webmin account only.

Webmin UI language

Global language (English (US))
 Personal choice .. Russian CP1251 (RU_RU)

Webmin UI theme

Global theme (Blue Framed Theme)
 Personal choice .. Old Webmin Theme

(Рис. 26. Настройка русификации Webmin)

При повторном входе в систему интерфейс будет уже на русском языке:

(Рис. 27. Пример интерфейса Webmin на русском языке)

Для того чтобы обеспечить автоматическую настройку сети запустим сервер DHCP. Для этого перейдем в раздел неиспользуемые модули и выберем **Сервер DHCP**. Так как пакет `dhcp3-server` у нас не установлен установим его при помощи инструментов webmin. Для этого нажмем **Click here** в строке «The ISC DHCPd package can be automatically installed by Webmin. [Click here](#) to have it downloaded and installed using APT.» Система сама установит необходимые пакеты:

(Рис. 28. Установка dhcp3-server средствами Webmin)

Перейдем в раздел «Настройки модуля» и исправим строки:

- в разделе «Исполняемый файл сервера DHCP» с `/usr/sbin/dhcpd3` на `/usr/sbin/dhcpd`

- Команда для запуска сервера DHCP `/etc/init.d/isc-dhcp-server start`
- Команда для применения настроек `/etc/init.d/isc-dhcp-server restart`
- Command to stop DHCP server `/etc/init.d/isc-dhcp-server stop`
- Путь к файлу PID сервера DHCP `/var/run/dhcp-server/dhcpd.pid`
- Файл аренды сервера DHCP `/var/lib/dhcp/dhcpd.leases`

(Рис. 28. Настройка модуля DHCP в Webmin)

и сохраним изменения путем нажатия кнопки «Сохранить».

В разделе «Подсети и разделяемые сети» добавим новую подсеть и указываем её параметры:

Меню модуля

Редактирование подсети

Нажимаем кнопку «Редактировать сетевой интерфейс»

(Рис. 29. Настройка DHCP-сервера в Webmin)

и укажем, на каком сетевом интерфейсе слушать запрос на получение настроек сети:

Сетевой интерфейс

Сервер DHCP может назначать адреса IP только в сетях, подключенных к одному из интерфейсов, выбранных ниже. Сетевой интерфейс для всех определенных подсетей также должен быть сюда включен. Если ничего не выбрано, то сервер DHCP будет пытаться обнаружить их автоматически.

Слушать интерфейсы

eth0 (Ethernet)	▲
eth1 (Ethernet)	■
lo (Loopback)	▼

Сохранить

[← Вернуться к список сети и узлов](#)

(Рис. 30. Выбор сетевого интерфейса, на котором будут приниматься запросы для получения настроек сети автоматически)

Запускаем сервис путем нажатия кнопки «Запуск сервера». Теперь перейдем к настройкам на локальной машине в сети.

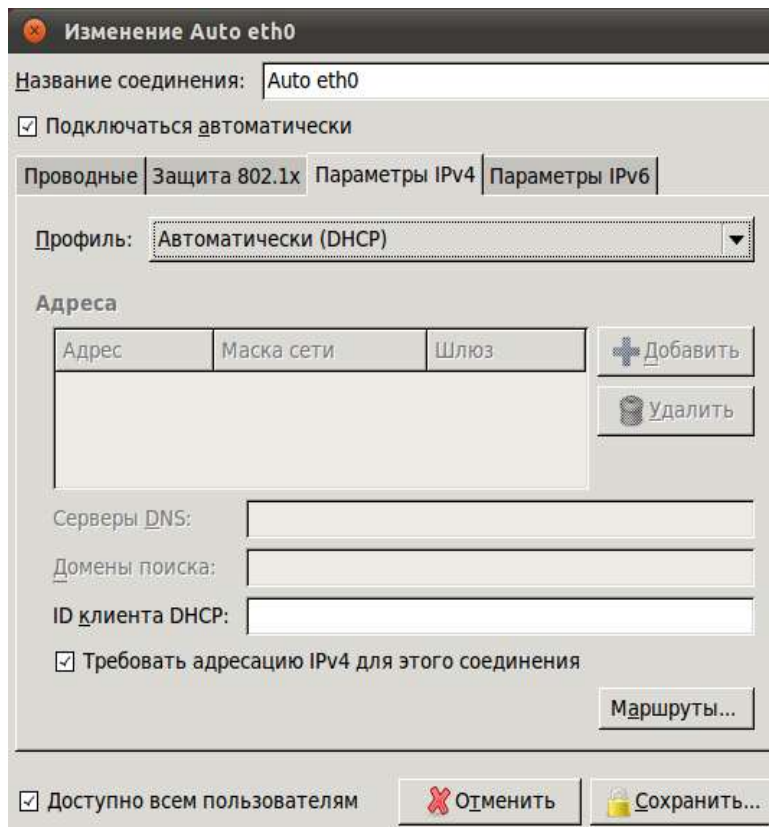
Для более тонкой настройки сервера мы можем воспользоваться прямым редактирование конфигурационного файла. Для этого нажмем кнопку «Manual Edit Configuración» и в открывшемся окне вводим следующее:

```
# shool
subnet 192.168.56.0 netmask 255.255.255.0 {
option routers 192.168.56.4;
option subnet-mask 255.255.255.0;
option domain-name "ubuntu.lan";
option domain-name-servers 192.168.56.4;
range 192.168.56.5 192.168.56.45;
}
```

Сохраняем изменения. И нажимаем кнопку «Применить».

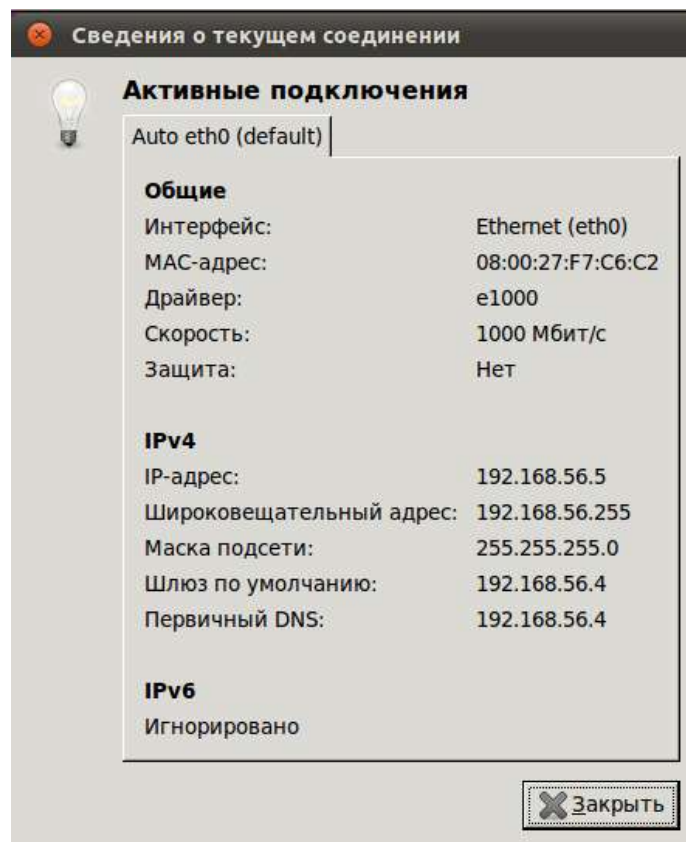
2.2.1. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе Ubuntu. Настройки на локальной машине.

После проведенных настроек на сервере настройка подключения к сети Интернет на компьютерах локальной сети школы сводиться лишь к указанию того, что настройки нужно получать Автоматически (DHCP).



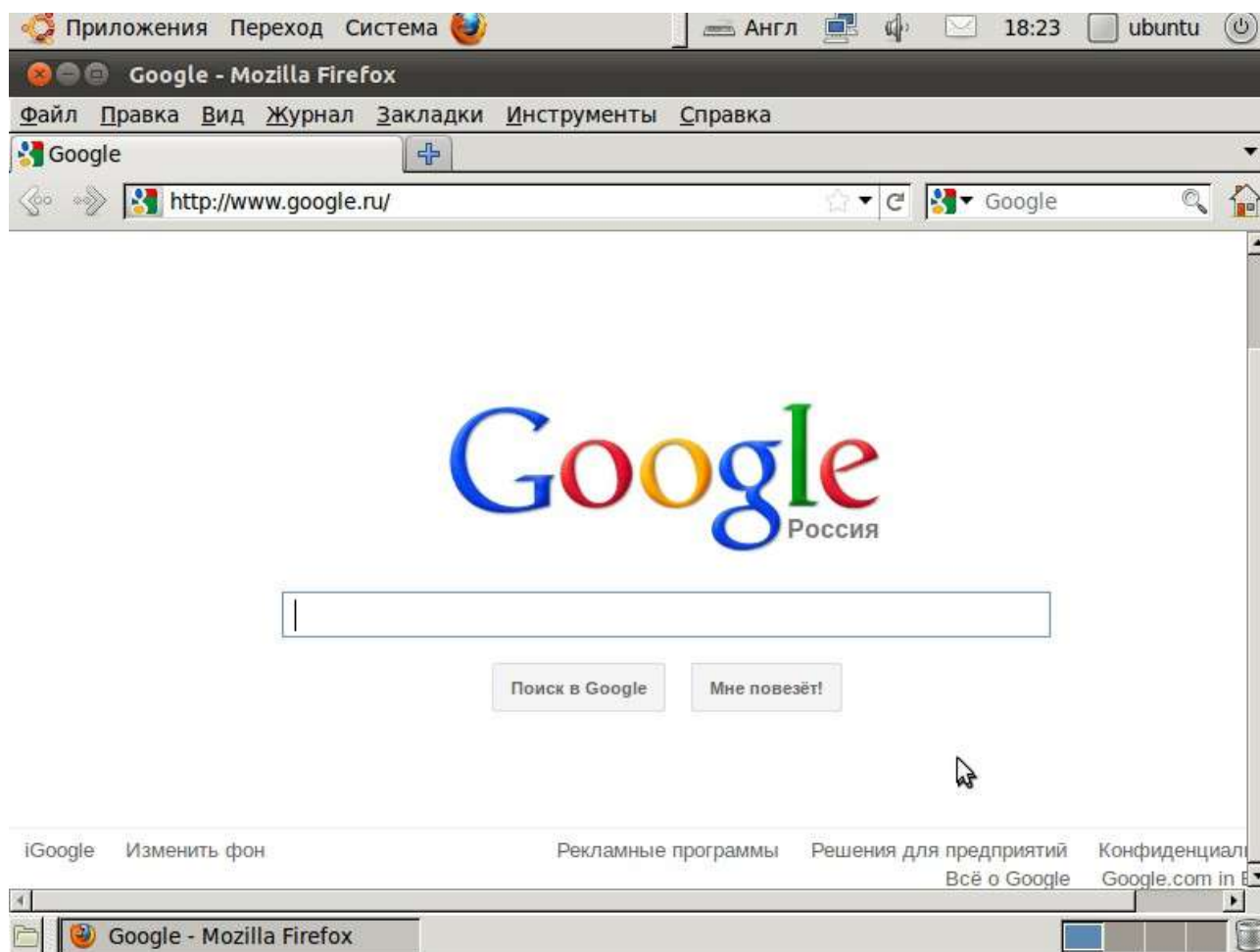
(Рис. 31. Настройка получения настроек сети автоматически)

Посмотрим полученные настройки:



(Рис. 32. Просмотр настроек сети)

Осталось только запустить браузер и проверить доступ в сеть Интернет:



(Рис. 33. Проверка доступа в сеть Интернет при помощи браузера)

2.3 Организация локальной сети с контролируемым доступом в сеть интернет, на основе OpenSuse.

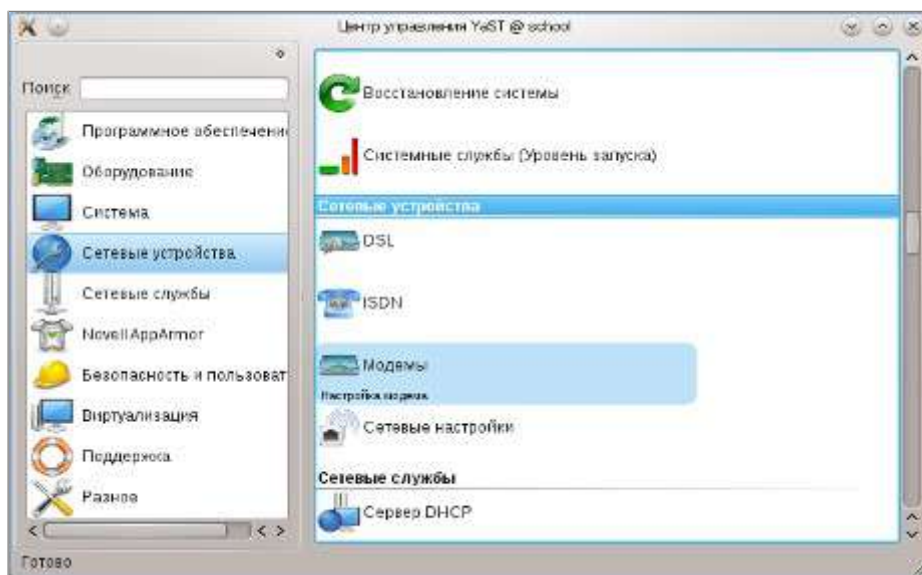
В операционной системе OpenSuse практически все настройки системы осуществляются через YaST (проприетарная утилита конфигурации операционной системы и установки/обновления пакетов с ПО).



(Рис. 34. Запуск YaST)

Настройка сетевых устройств.

Настройка параметров сетевых устройств осуществляется в разделе «Сетевые устройства»

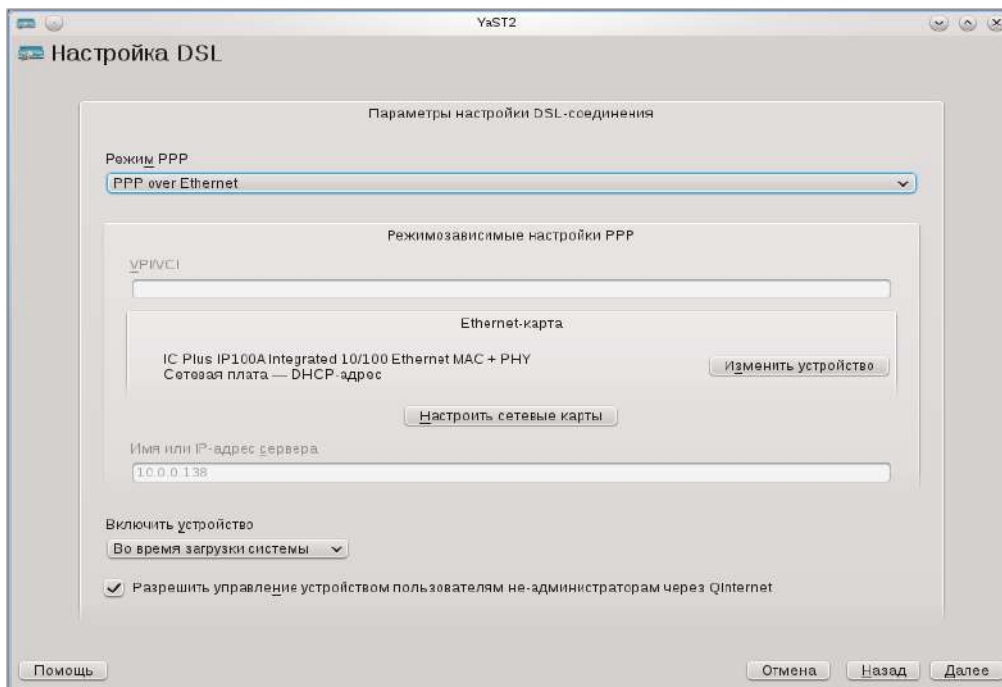


(Рис. 35. YaST)

Для организации шлюза необходимы 2 сетевых интерфейса, первый предназначен для соединения с сетью Интернет, второй - для работы с локальной сетью школы.

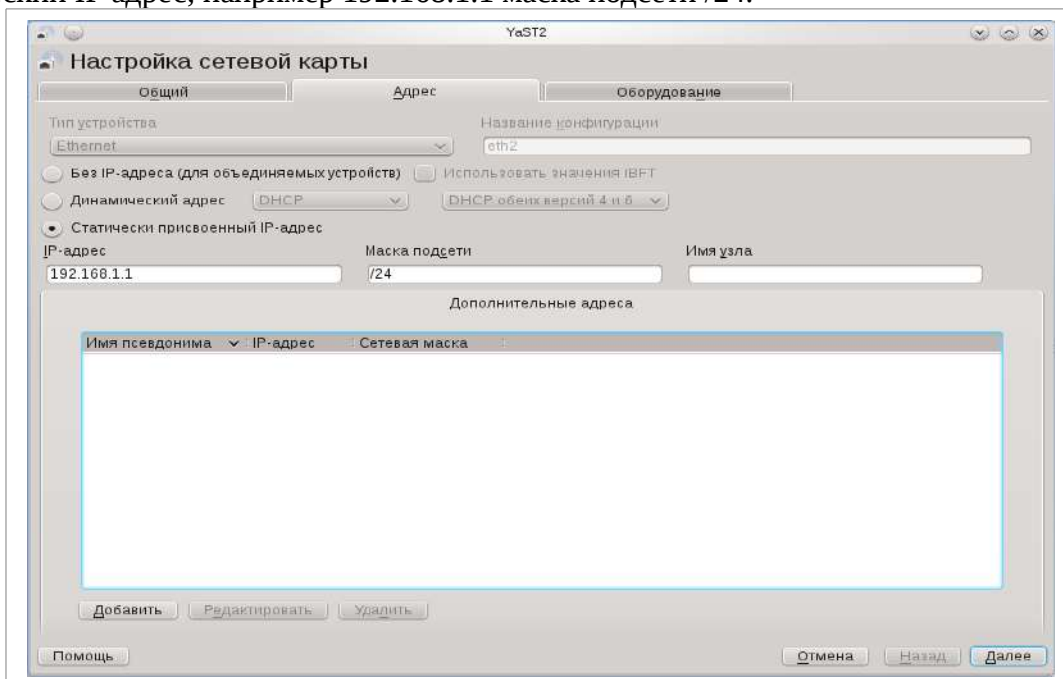
Начнем с подключения к сети интернет через DSL. Выбираем пункт «DSL», в графе «Режим PPP» выбираем «PPP over Ethernet», в графе «Ethernet-карта» выбираем сетевую карту через

которую будет подключен интернет (eth0). В графе «Включить устройство» выбираем «Во время загрузки системы». Для того что бы разрешить управление устройством пользователям не администраторам оставляем включенным данный пункт, при этом будет установлен пакет Qinternet который отображает в системном лотке подключение к интернет.



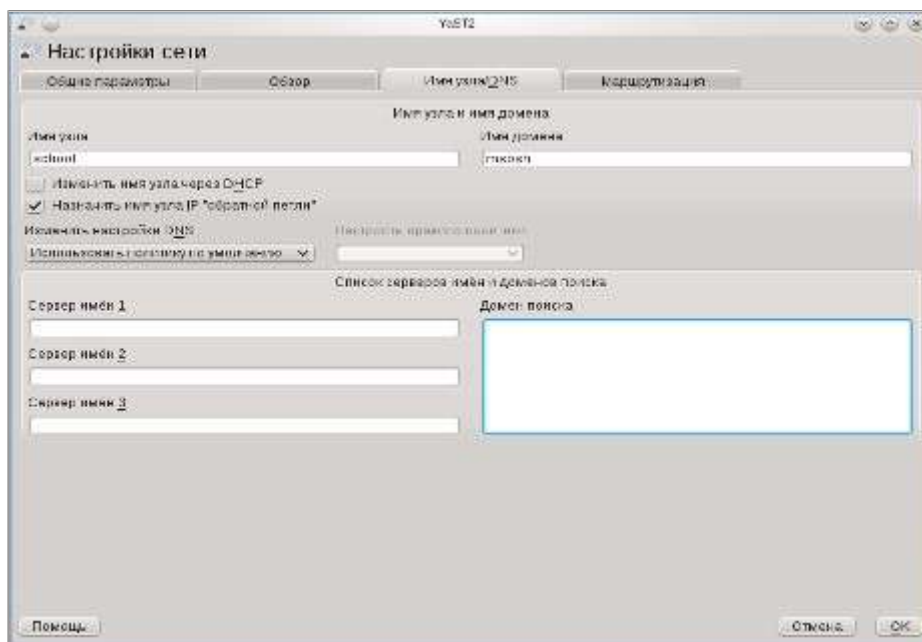
(Рис. 36. Подключение к сети интернет через DSL)

В данном диалоге так же можно настроить сетевые интерфейсы при нажатии на кнопку «Настроить сетевые карты». На вкладке Общие параметры менять ничего не будем, оставим по умолчанию, переходим на вкладку «Обзор», выбираем сетевую карту и нажимаем «Редактировать». Карте eth0 присваиваем динамический адрес (DHCP), eth1 присваиваем статический IP адрес, например 192.168.1.1 маска подсети /24.



(Рис. 37. Настройка сетевого адреса)

На вкладке «Имя узла\DNS» вводим имя сервера (например proxu) и домена (school).



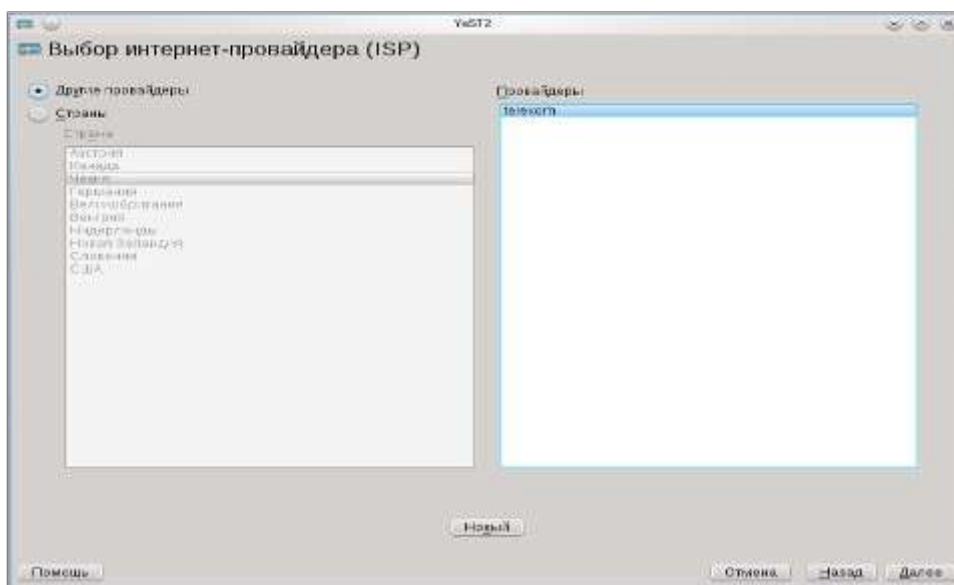
(Рис. 38. Настройка имени узла и DNS)

На вкладке «Маршрутизация» включаем IP-переадресацию для использования системы в качестве роутера.



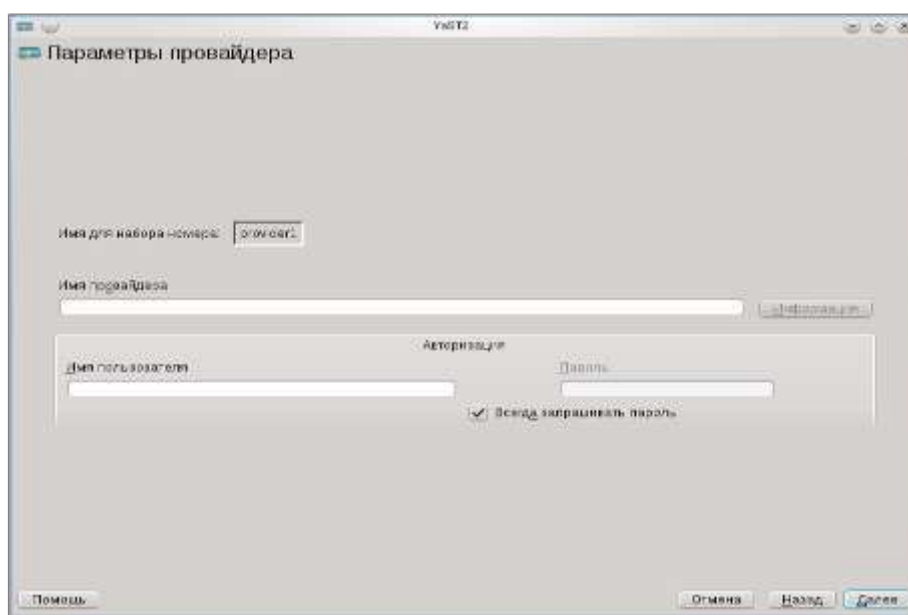
(Рис. 39. Маршрутизация)

Нажимаем «ок» и «далее»



(Рис. 40. Выбор провайдера)

Нажимаем на кнопку «Новый», вводим имя провайдера, логин и пароль для подключения к сети интернет, жмем «далее» «далее».

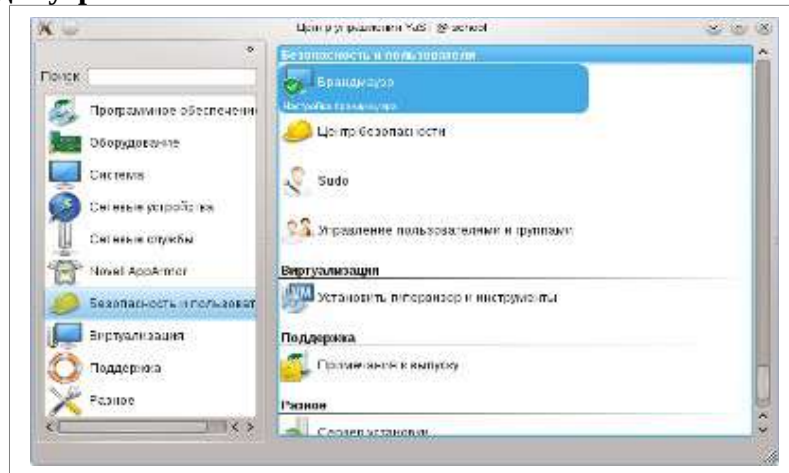


(Рис. 41. Параметры провайдера)

Проверяем подключение к сети интернет открыв браузер интернета. Если через некоторое время подключение **разрывается и не подключается автоматически** необходимо сделать следующее:

1. С помощью диспетчера файлов перейти /var/spool/cron/tabs/
2. Открыть на редактирование файл **root**
3. Добавить следующую строку * * * * * /usr/sbin/smpppd-ifcfg --up --rc -i ifcfg-dsl0

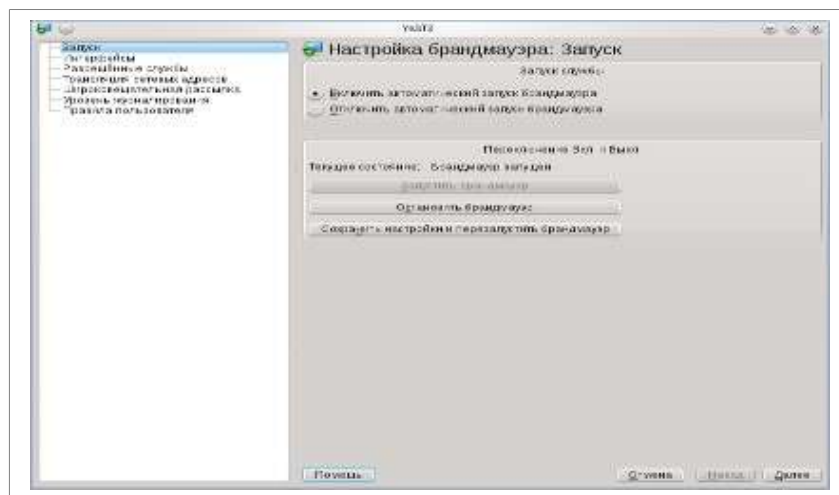
Настройка брандмауэра.



(Рис. 42. Запуск брандмауэра)

Запуск службы.

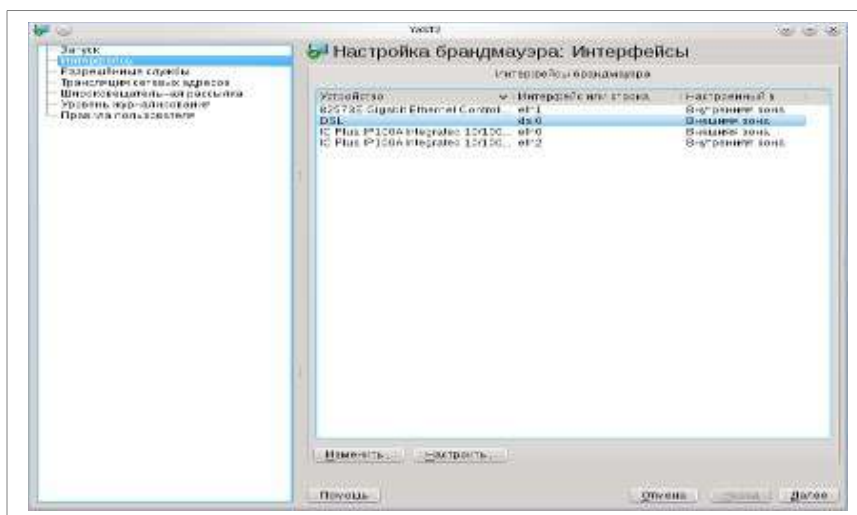
Чтобы служба запускалась каждый раз при загрузке компьютера, установите **Включить автоматический запуск брандмауэра.**



(Рис. 43. Настройка брандмауэра: Запуск)

Интерфейсы

Назначьте сетевому устройству зону брандмауэра, выбрав устройство в таблице, затем нажав Изменить. Сетевой интерфейс eth0 и ds10 будет внешней зоной, eth1 внутренней.



(Рис. 44. Настройка зон брандмауэра)

Разрешённые службы.

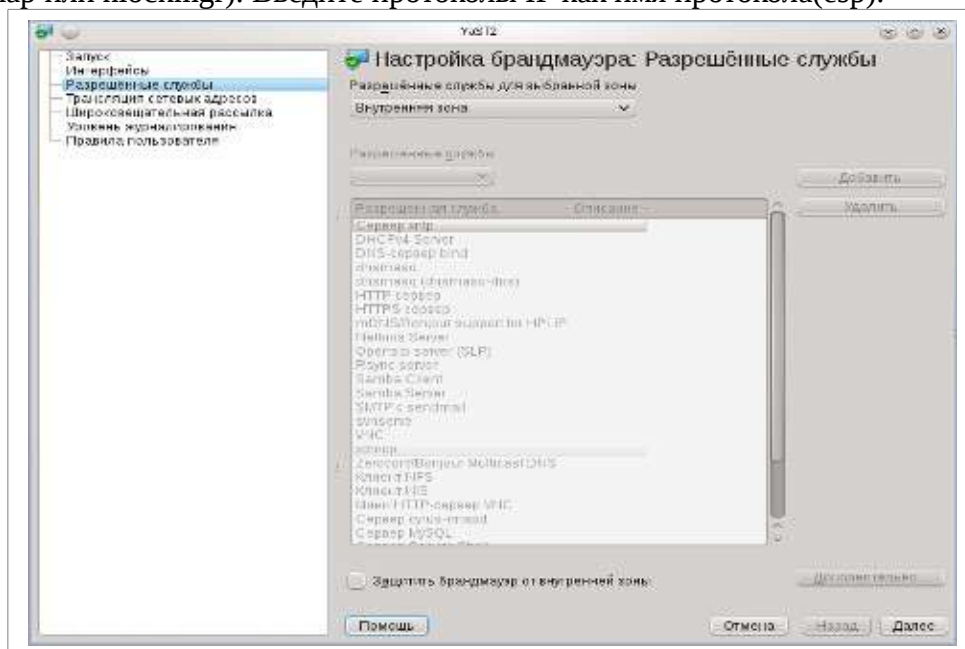
Укажите службы или порты, которые должны быть доступны из сети. Сети поделены на зоны брандмауэра.

Для разрешения службы выберите «Зона» и «Разрешённые службы». Затем нажмите «Добавить». Для удаления службы выберите «Зона», затем «Разрешённые службы» и нажмите Удалить.

Снятием галочки «Защитить от внутренней сети снимите защиту с зоны». Все службы и порты будут не защищены в этой зоне.

Дополнительные параметры могут быть настроены с использованием кнопки «Дополнительно». Значения должны быть разделены пробелами. Здесь вы можете разрешить порты TCP, UDP, RPC и протоколы IP.

Порты TCP и UDP могут быть введены как имена портов (ftp-data), номера портов (3128) и диапазонов портов (8000:8520). RPC-порты должны быть введены в виде служебных имен(portmap или plockmgr). Введите протоколы IP как имя протокола(esp).



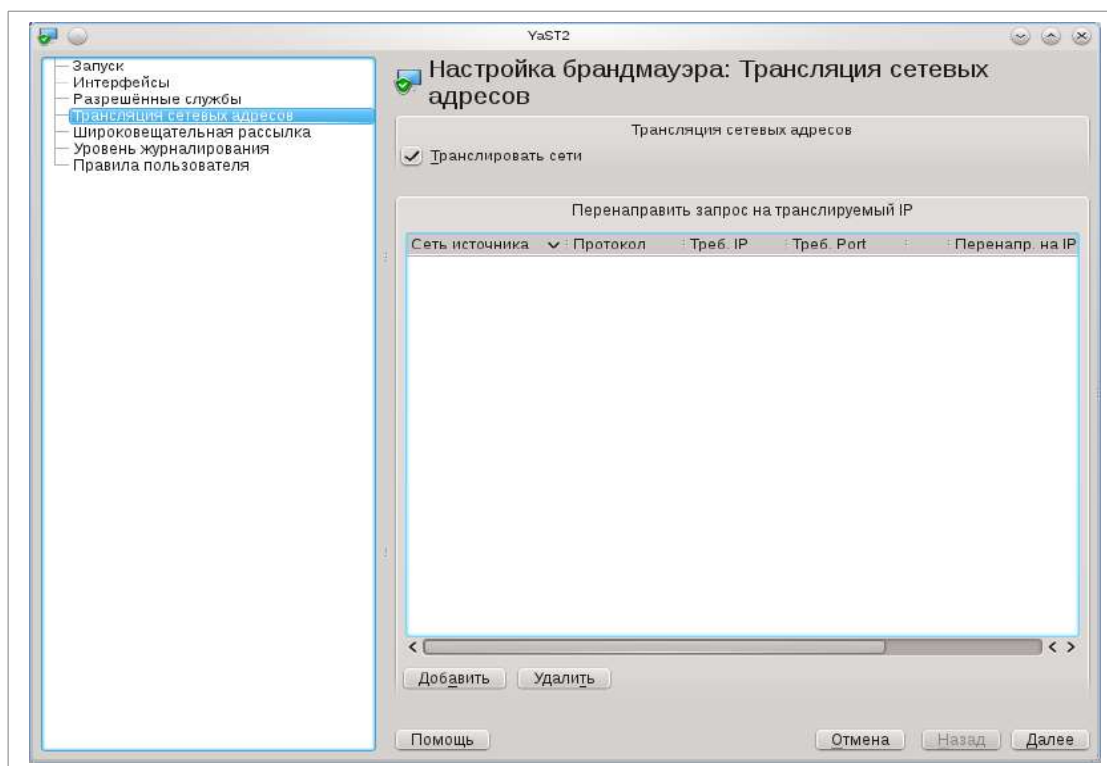
(Рис. 45. Настройка разрешенных служб)

Трансляция.

Трансляция — это функция, которая скрывает вашу внутреннюю сеть за брандмауэром и

позволяет получить прозрачный доступ ко внешней сети, такой как интернет. Запросы из внешней сети во внутреннюю будут заблокированы. Выберите «Транслировать сети», чтобы транслировать ваши сети во внешнюю сеть.

Даже если запросы из внешней сети не могут достичь вашей сети, есть возможность прозрачно перенаправлять любые запрошенные порты на вашем брандмауэре на любой внутренний IP. Для добавления нового правила перенаправления нажмите «Добавить» и заполните необходимые поля.



(Рис. 46. Настройка трансляции сетевых адресов)

Правила пользователя.

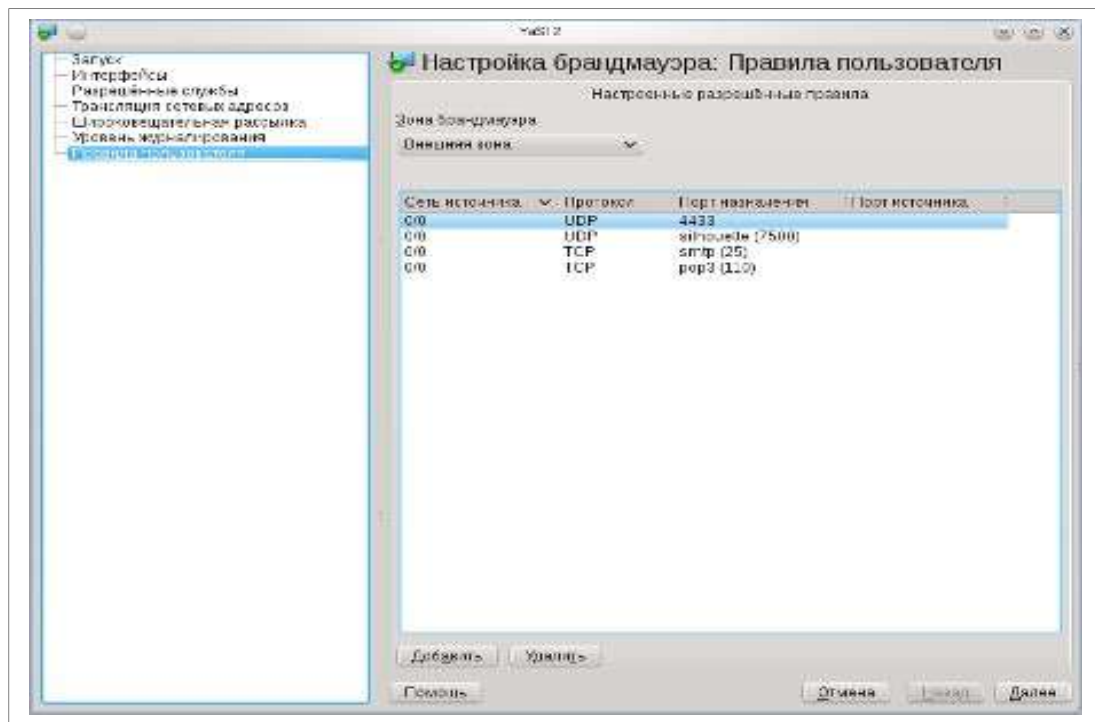
Здесь вы можете установить особые правила брандмауэра, которые разрешат новые соединения, соответствующие этим правилам.

Сеть источника. Сеть или IP, откуда приходит соединение, например, 192.168.0.1 или 192.168.0.0/255.255.255.0 или 192.168.0.0/24 или 0/0 (что означает все).

Протокол. Протокол, используемый пакетом. Особый протокол RPC используется для RPC-служб.

Порт назначения. Имя порта, номер порта или диапазон портов, разрешённых к доступу, например, smtp или 25 или 100:110. В случае протокола RPC используйте имя RPC-службы. Эта запись необязательна.

Порт источника. Имя порта, номер порта или диапазон портов, откуда исходят пакеты. Эта запись необязательна.

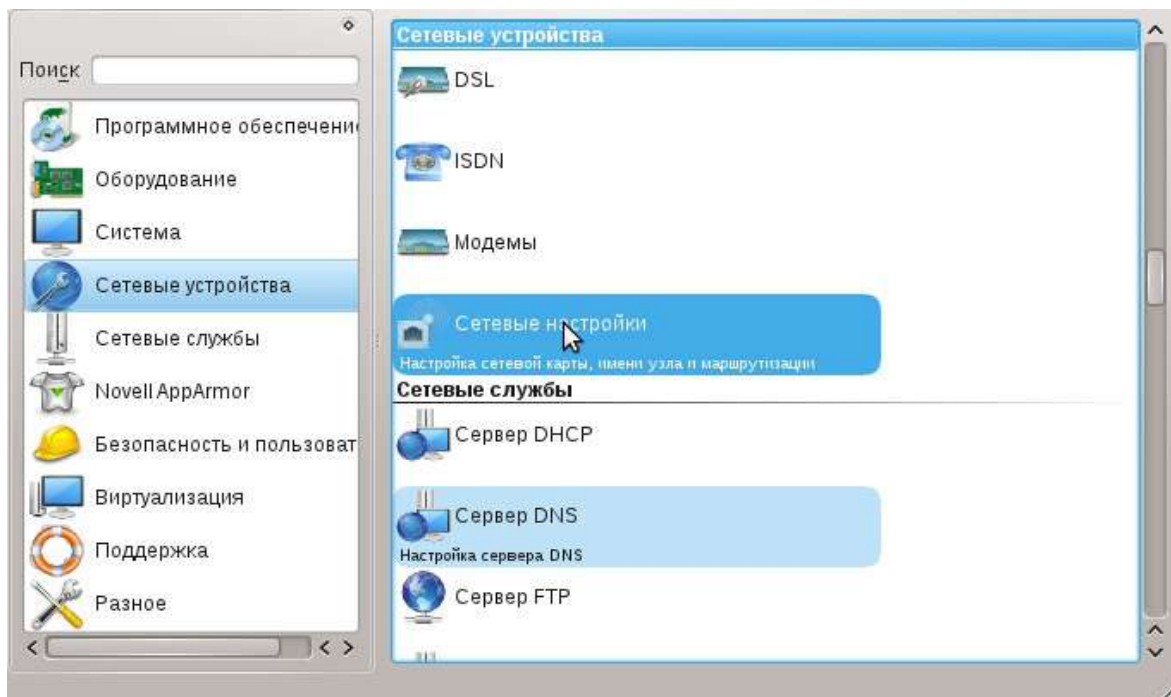


(Рис. 47. Правила пользователя)

Теперь наш сервер готов для «раздачи Интернет» на компьютеры локальной сети школы.

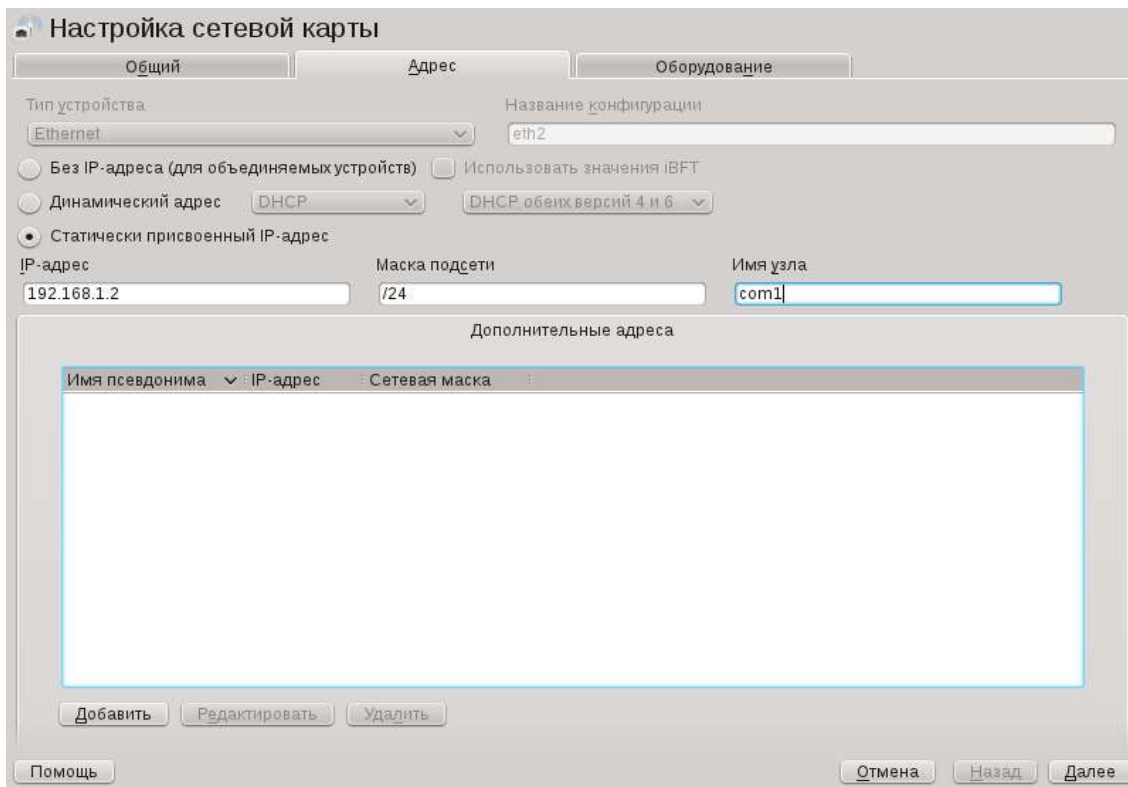
2.3.1. Организация локальной сети с контролируемым доступом в сеть Интернет, на основе OpenSuse. Настройки на локальной машине.

Для настройки будем использовать тот же YaST. Открываем сетевые настройки.



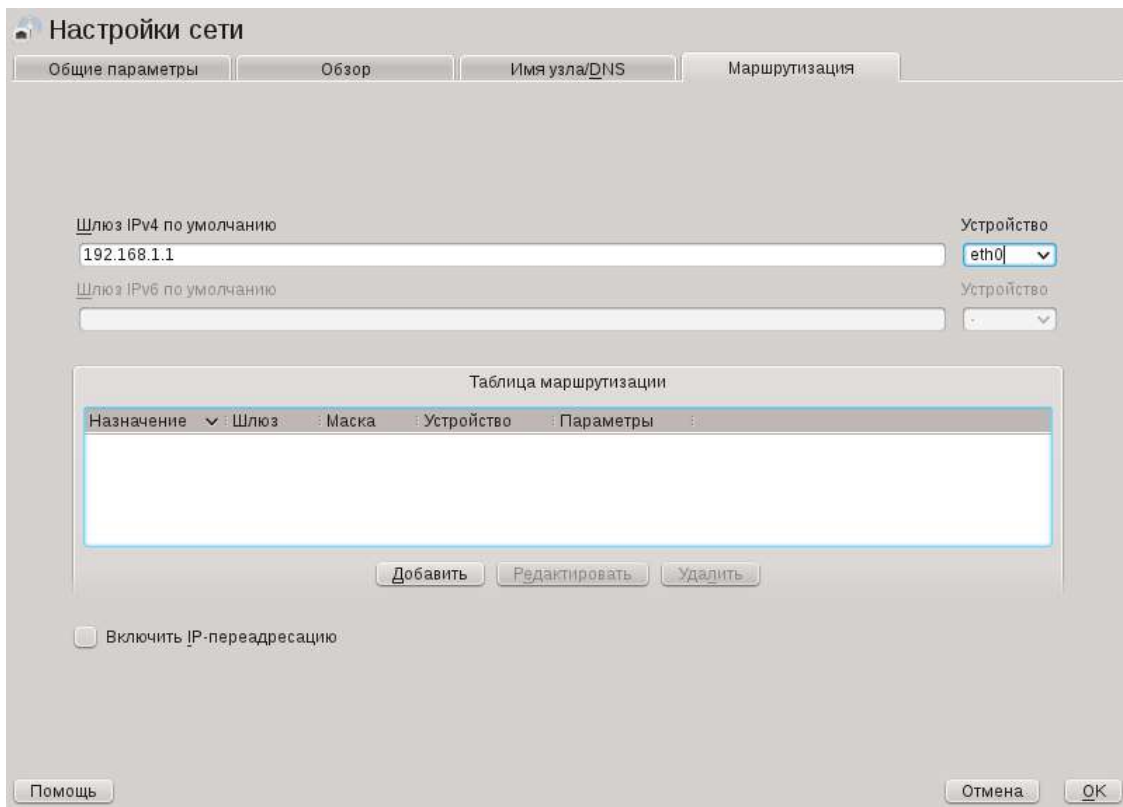
(Рис. 48. YaST)

Переходим на вкладку «Обзор», выбираем из списка сетевую карту и нажимаем кнопку «Редактировать». Вводим IP адрес из диапазона 192.168.1.2-192.168.1.255, маску подсети /24 и имя узла.



(Рис. 49. Настройка сетевой карты: Адрес)

Нажимаем «Далее». Переходим на вкладку «Маршрутизация» и вводим IP адрес нашего сервера в поле «Шлюз IPv4 по умолчанию»



(Рис. 50. Настройка сети: Маршрутизация)

Нажимаем «ок» и проверяем доступ в интернет открыв браузер.

3. Установка и настройка программного обеспечения для организации контент-фильтрации.

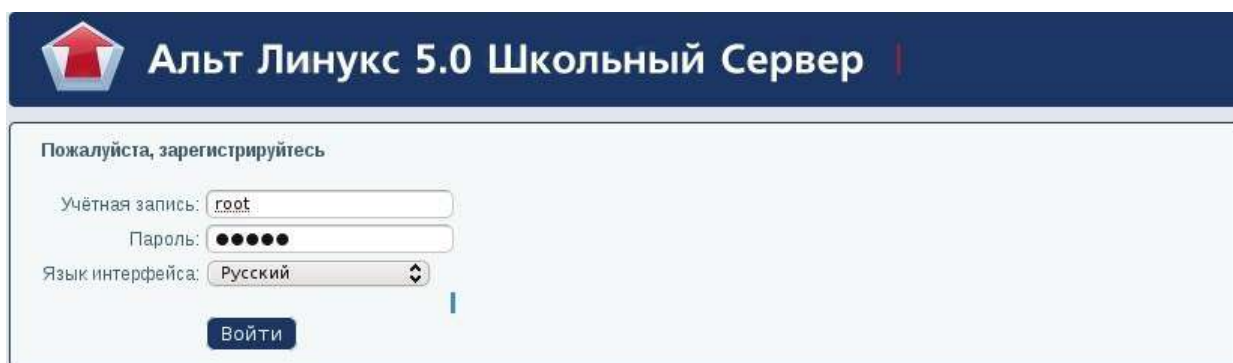
Теперь приступим к настройке программы при помощи которой будем контролировать доступ в сеть Интернет пользователей сети. Это программа squid.

Squid(англ. Squid — «кальмар») — программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS. Разработан сообществом как программа с открытым исходным кодом (распространяется в соответствии с GNU GPL). Все запросы выполняет как один не блокируемый процесс ввода/вывода.

3.1.1. Установка и настройка прокси-сервера squid в ALT Linux Школьный сервер 5.0

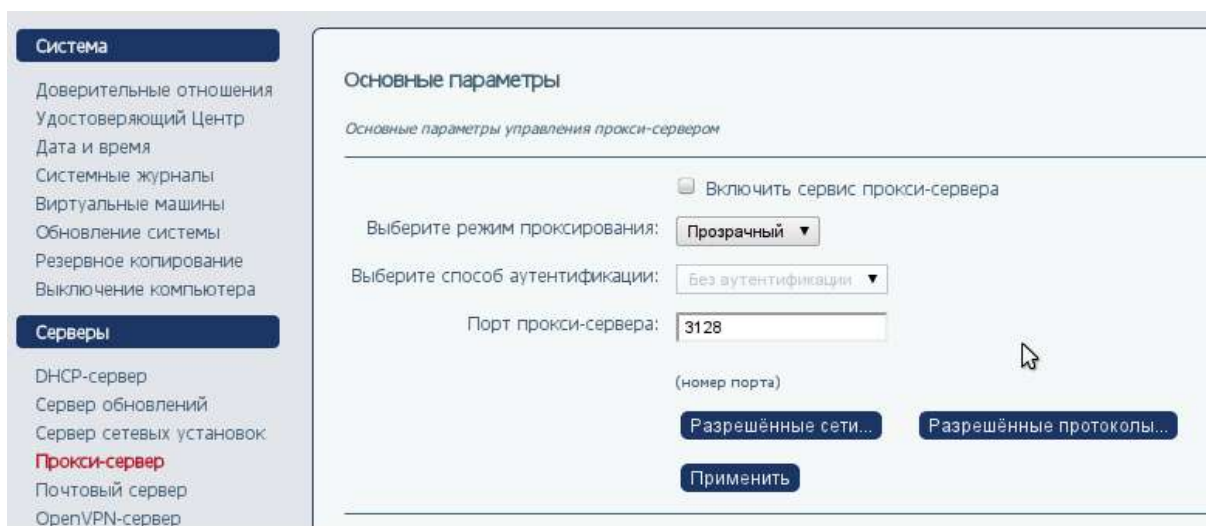
В дистрибутиве ALT Linux Школьный сервер 5 squid предустановлен. Поэтому приступаем к его настройке. Выполнить первоначальную настройку достаточно просто, если воспользоваться центром управления сервера доступного по адресу <https://ip-адрес сервера:8080>.

1. Осуществляем вход в систему используя веб-интерфейс alterator:



(Рис. 51. Окно входа в панель управления школьным сервером)

2. Переходим в раздел «Серверы» - «Прокси-сервер»:
Перед началом работы с прокси-сервером, необходимо ознакомиться с основными положениями в работе прокси. Для этого можно воспользоваться справочной системой alterator: Настройка прокси-сервера . Несколько компьютеров, объединённых в локальную сеть могут быть подключены к глобальной сети (Интернет) через один общий канал. Такое решение имеет ряд преимуществ перед другими. В частности, если разместить в месте соединения двух сетей (шлюзе) прокси-сервер, полученные через него страницы попадут в кеш, и при повторном обращении к ним загрузка из внешней сети уже не потребует. Это может существенно ускорить доступ к популярным сайтам и снизить потребляемый организацией трафик.



(Рис. 52. Настройка прокси-сервера средствами панели управления школьного сервера)

Прокси-сервер принимает запросы из локальной сети и, по мере необходимости, передаёт их во внешнюю сеть. Поступление запроса ожидается на определённом порту, который по умолчанию имеет стандартный номер 3128. Если по каким-то причинам не желательно использовать данный порт, то можно поменять его значение на любое другое.

Перед тем как выполнить перенаправление запроса, прокси-сервер проверяет принадлежность сетевого адрес узла, с которого запрос был отправлен к группе внутренних сетевых адресов. Для того, чтобы запросы, отправленные из локальной сети, обрабатывались прокси-сервером, необходимо добавить соответствующую группу адресов (адрес подсети и адресную маску) в список внутренних сетей в разделе Сети.

Вторым условием передачи запроса является принадлежность целевого порта к разрешённому диапазону. Посмотреть и отредактировать список разрешённых целевых портов можно в разделе Порты.

Прокси-сервер может работать в двух режимах: стандартном и прозрачном. Стандартный режим использования прокси-сервера требует изменения режима работы программ локальной сети, что может потребовать их ручной настройки. По этой причине другим популярным режимом использования прокси-сервера является прозрачный режим. В этом режиме все обращения из внутренней сети по зарегистрированным протоколам (портам) во внешнюю сеть автоматически перехватываются прокси-сервером при прохождении через шлюз. Программы в локальной сети при этом продолжают работать в обычном режиме, не требуя никакой специальной настройки. Недостатком прозрачного режима работы является невозможность идентификации пользователей — все запросы отправляются из локальной сети анонимно. Для указания портов, используемых в режиме прозрачного проксирования, перейдите в раздел «Разрешённые протоколы», выберите из списка протокол и установите для этого протокола флажок «Включить прозрачное перенаправление».

Преимуществом непрозрачного режима работы, требующего перенастройки программ локальной сети, является возможность производить аутентификацию пользователей и контролировать их доступ во внешнюю сеть. Для того, чтобы включить аутентификацию, выберите способ аутентификации, отличный от «Без аутентификации».

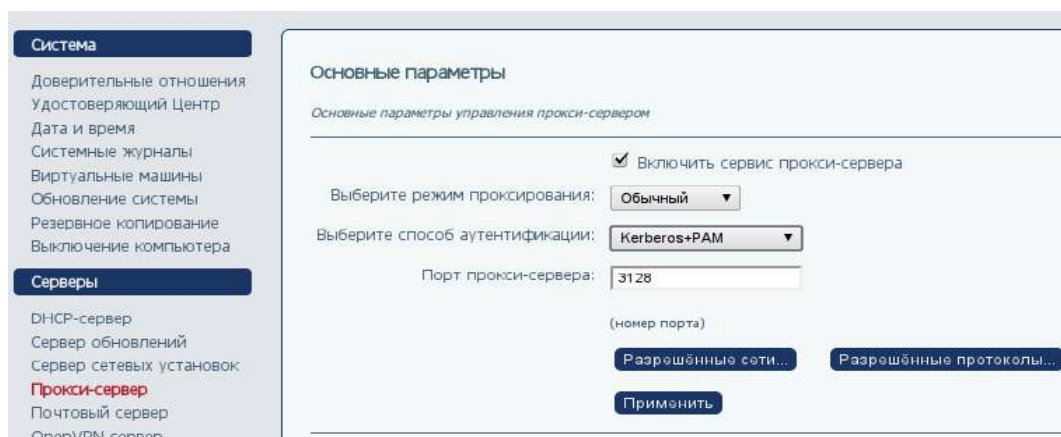
Политика доступа пользователей во внешнюю сеть формируется на основе групп пользователей и сетевых доменов в разделе Группы. Для каждой группы пользователей может быть сформирован список доменов, к которым разрешается (или наоборот, запрещается) обращение. Внесение и исключение пользователей из групп производится с помощью общесистемного модуля "Пользователи/Группы".

3. Перед запуском прокси-сервера добавляем в раздел «Разрешённые сети» адрес нашей локальной сети:



(Рис. 53. Настройка прокси-сервера средствами панели управления школьного сервера)

4. Ставим галочку напротив «Включить прокси-сервер» выставляем нужные нам параметры, с которыми будет работать сервер, руководствуясь справочной системой.

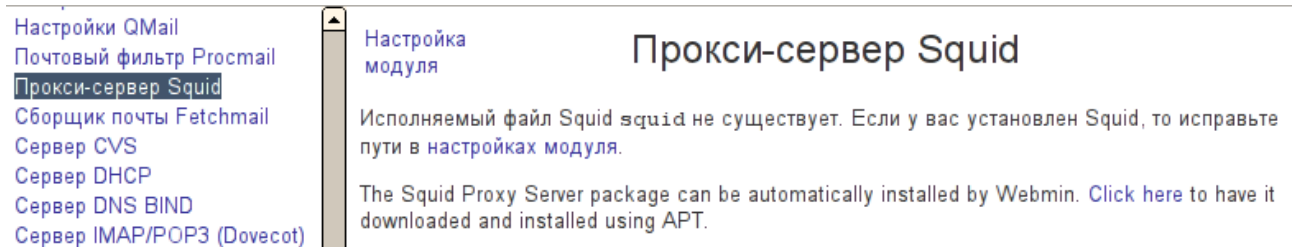


(Рис. 54. Настройка параметров аутентификации прокси-сервера)

5. Нажимаем «Применить» и приступаем к работе.

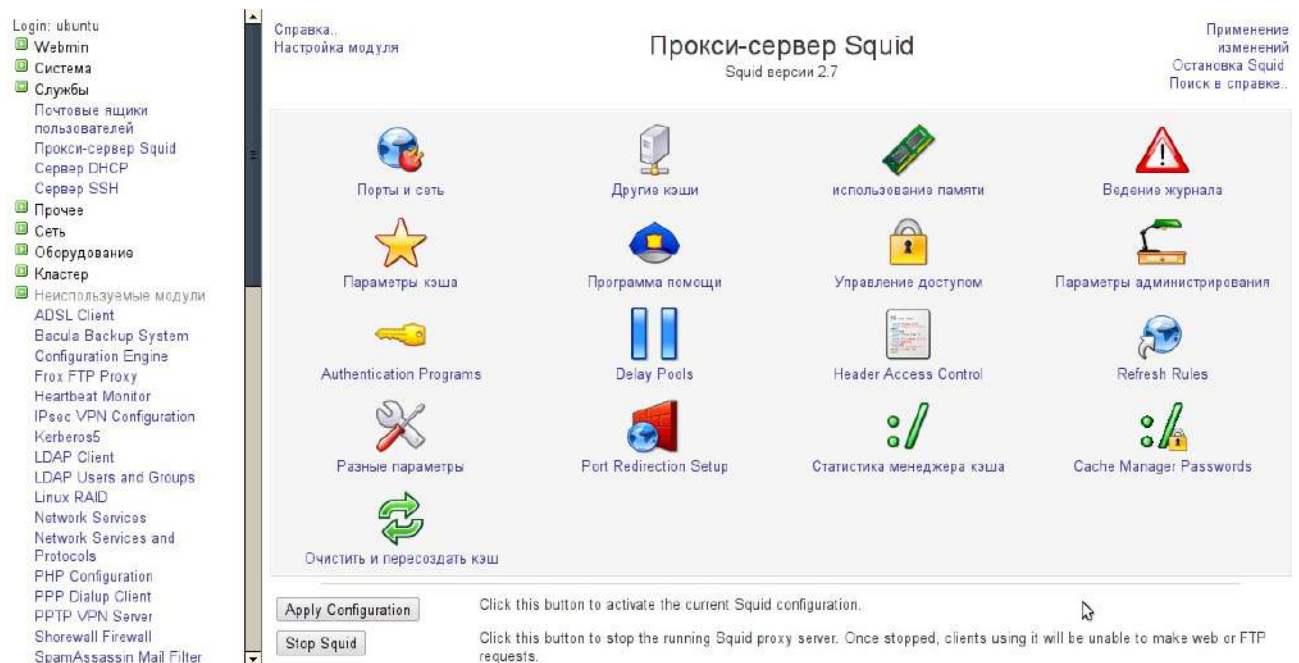
3.1.2. Установка и настройка прокси-сервера squid в Ubuntu.

Для установки и настройки прокси-сервера squid воспользуемся, уже установленной нами, программой Webmin. Для этого в адресной строке браузера укажем <https://192.168.56.4:10000> (или <https://localhost:10000> — если вы работаете на локальной машине). Выполним вход в систему и в разделе «Неиспользуемые модули» выберем «Прокси-сервер Squid»:



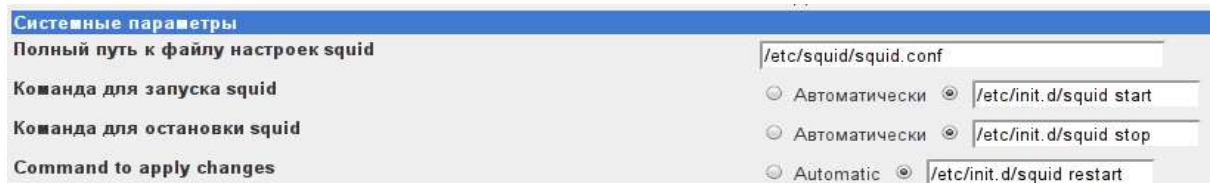
(Рис. 55. Модуль webmin для настройки прокси-сервера squid)

Выполняем установку пакета уже знакомым нам способом — нажимаем здесь: [Click here](#). Дожидаемся окончания установки пакета. Переходим в раздел «Службы» - «Прокси-сервер Squid».



(Рис. 56. Настройка прокси-сервера squid при помощи webmin)

Перейдем в «Настройки модуля» и изменим параметры команд остановки и запуска squid:



(Рис. 57. Изменение параметров запуска/остановки squid)

Далее укажем параметры кэша:

[Меню модуля](#)
[Справка..](#)

Параметры кэша

[Применение изменений](#)
[Остановка Squid](#)

Параметры кэширования и запросов					
Каталоги кэша					
<input type="radio"/> По умолчанию (/var/spool/squid) <input checked="" type="radio"/> Перечисленные..					
Каталог	Тип	Размер (Мб)	каталоги 1го уровня	каталоги 2го уровня	Параметры
/var/spool/squid	UFS	100	16	256	
	UFS				

(Рис. 58. Настройка параметров кэша)

Не забываем сохранять изменения путем нажатия кнопки «Сохранить».

При помощи функции «Очистить и пересоздать кэш» создадим кэш. В разделе «Управление доступом» создадим новый acl — Адрес клиента:

[Меню модуля](#)

Создание ACL

Адрес клиента ACL		
Имя ACL	<input type="text" value="shoolnet"/>	
С IP	На IP	Маска сети
<input type="text" value="192.168.56.0"/>	<input type="text"/>	<input type="text" value="24"/>
URL Отказа	<input type="text"/>	
Store ACL values in file	<input checked="" type="radio"/> Squid configuration <input type="radio"/> Separate file <input type="text"/>	
	<input type="checkbox"/> Just use existing contents of file?	

[← Вернуться к Списку ACL](#) | [Вернуться к меню](#)

(Рис. 59. Создание нового acl)

На вкладке «Ограничения прокси» разрешим новому acl доступ:

Создание ограничений прокси

Ограничения прокси

Действие Разрешить Запретить

<p>Совпадающие ACL</p> <div style="border: 1px solid #ccc; padding: 2px;"> localhost to_localhost localnet SSL_ports Safe_ports purge CONNECT shoutcast apache shoolnet </div>	<p>Не совпадающие ACL</p> <div style="border: 1px solid #ccc; padding: 2px;"> all manager localhost to_localhost localnet SSL_ports Safe_ports purge CONNECT shoutcast </div>
---	--

[← Вернуться к Список ACL](#) | [Вернуться к меню](#)

(Рис. 60. Создание ограничения прокси)

Следующий шаг — поместить список доступа школьной сети (acl) при помощи webmin выше acl all при помощи кнопок в виде стрелок:

Управление доступом

Списки управления доступом
Ограничения прокси
Ограничения ICP
External ACL programs
Reply proxy restrictions

Добавить ограничение прокси

Действие	ACL	Переместить
<input type="checkbox"/>	Разрешить manager localhost	↓
<input type="checkbox"/>	Запретить manager	↓↑
<input type="checkbox"/>	Разрешить purge localhost	↓↑
<input type="checkbox"/>	Запретить purge	↓↑
<input type="checkbox"/>	Запретить !Safe_ports	↓↑
<input type="checkbox"/>	Запретить CONNECT !SSL_ports	↓↑
<input type="checkbox"/>	Разрешить shoolnet	↓↑
<input type="checkbox"/>	Разрешить localhost	↓↑
<input type="checkbox"/>	Запретить all	↑

Добавить ограничение прокси

(Рис. 61. Настройка доступа к сети Интернет)

Применяем изменения при помощи кнопки «Применить изменения» в модуле управления squid в webmin.

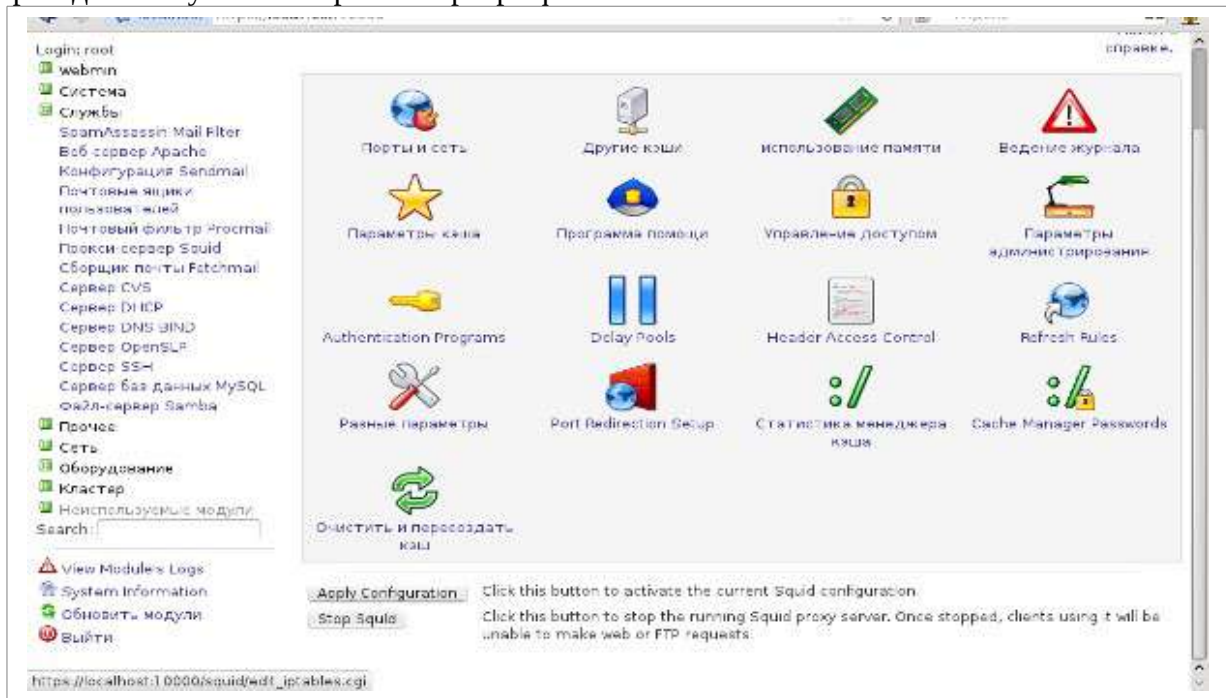
После чего нужно только настроить браузер на работу через прокси-сервер. Об этом подробнее в пункте 3.1.4.

3.1.3. Установка и настройка прокси-сервера squid OpenSuse.

Установить программное обеспечение прокси-сервера squid можно при установке операционной системы выбрав соответствующий пункт в разделе «Функции сервера» или с помощью YaST-> Управление программным обеспечением.

Для настройки прокси сервера squid будем использовать **webmin**. Запускаем браузер, переходим по адресу <http://www.webmin.com>, в разделе downloads ищем rpm пакет для OpenSuse, скачиваем и устанавливаем. После установки набираем в браузере <https://localhost:10000>, заходим под пользователем root.

Переходим «Службы → Прокси-сервер squid»

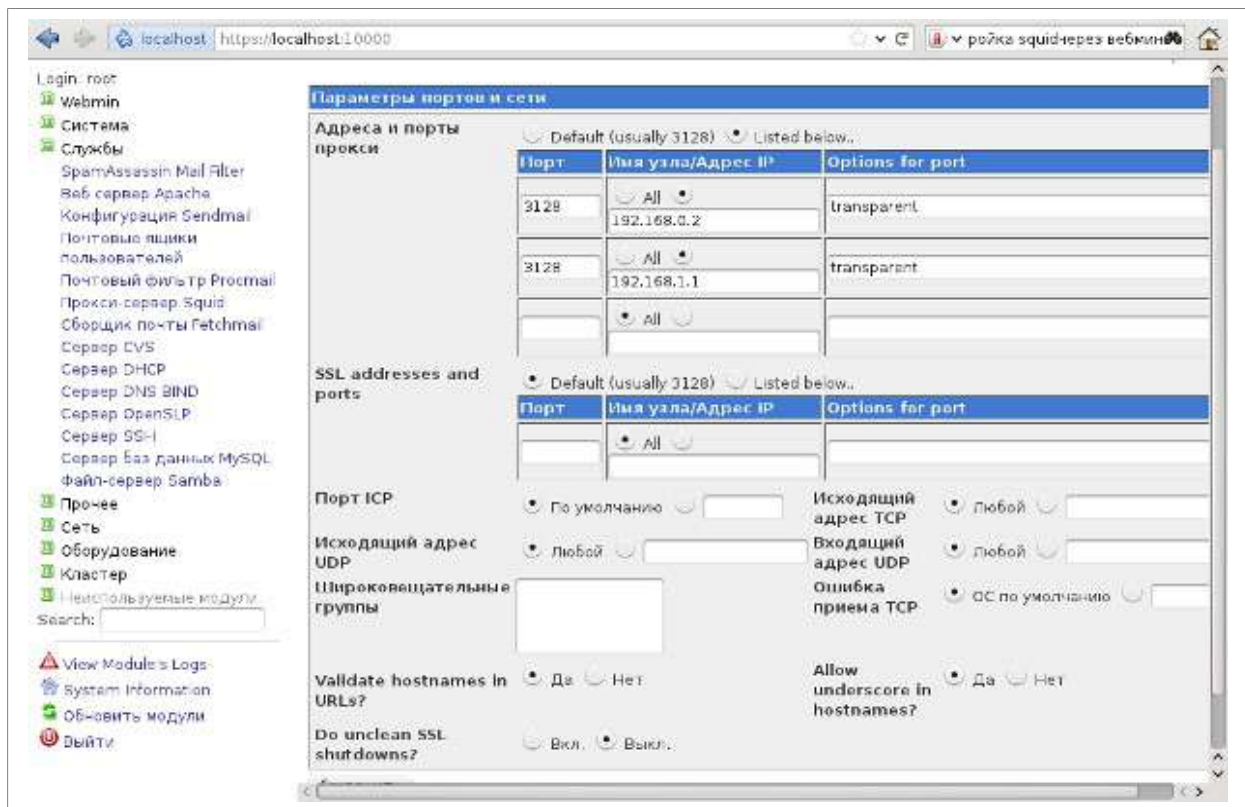


(Рис. 62. Главная страница настроек прокси-сервера squid)

Чтобы указать порты на которых будет слушать Squid, выполните следующие действия:

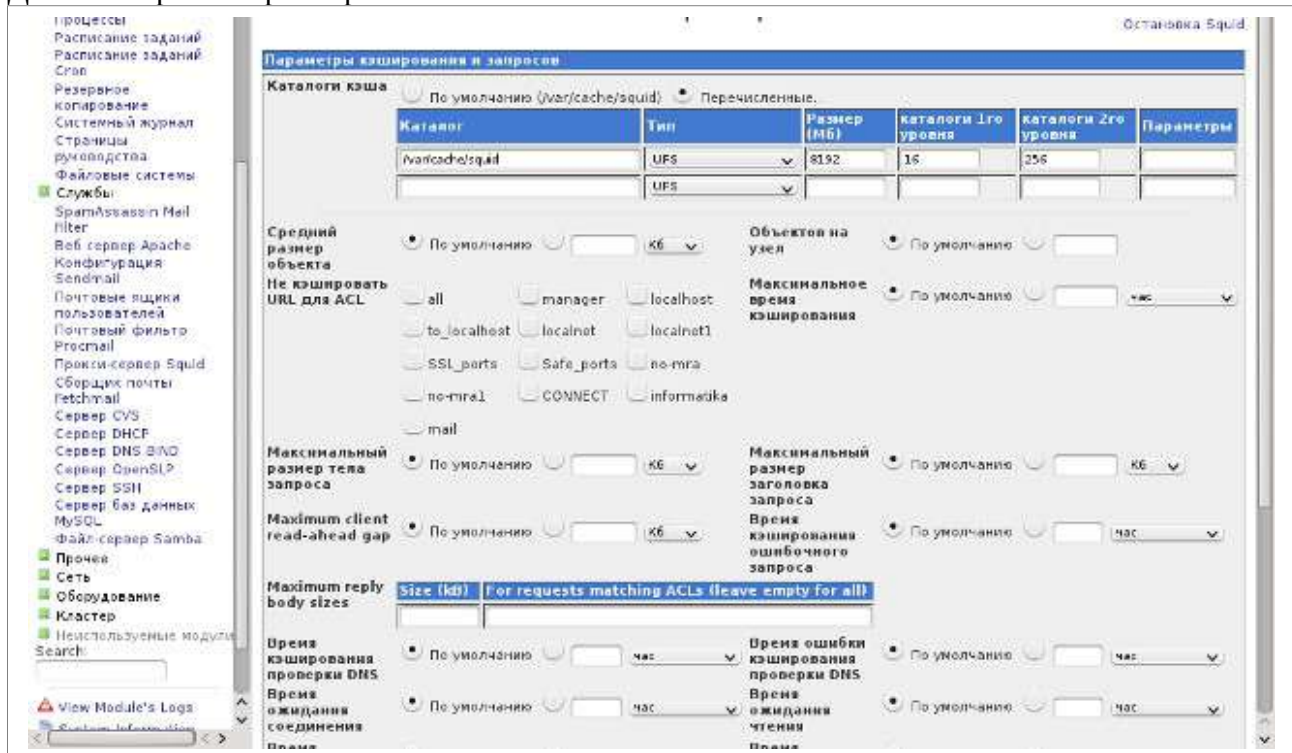
1. На главной странице модуля, нажмите на «Порты и сеть»
2. В таблице **Адреса и порты прокси**, выберите **Listed below (слушать указанные)** опцию. В таблице введите порт для прослушивания и при необходимости IP адрес на котором следует принимать соединения от клиентов. Вводить следует **по одному значению порта (или порта + ip адрес) в строку**.

Если нужно сделать прокси-сервер **прозрачным** указываем в графе «Options for port» параметр **transparent**. Но этого будет недостаточно. Необходимо соответствующим образом настроить **firewal** чтобы все запросы перенаправлялись на адрес и порт прокси. Открываем диспетчер файлов, переходим **/etc/sysconfig/**, ищем файл **SUSEfirewall2** и открываем его на редактирование. Находим в файле параметр **FW_REDIRECT** и меняем его значение например на **"192.168.1.0/24,0/0,tcp,80,3128"**. Таким образом все запросы из сети 192.168.1.0 по 80 порту будут перенаправлены на порт 3128.



(Рис.63. Параметры портов и сети)

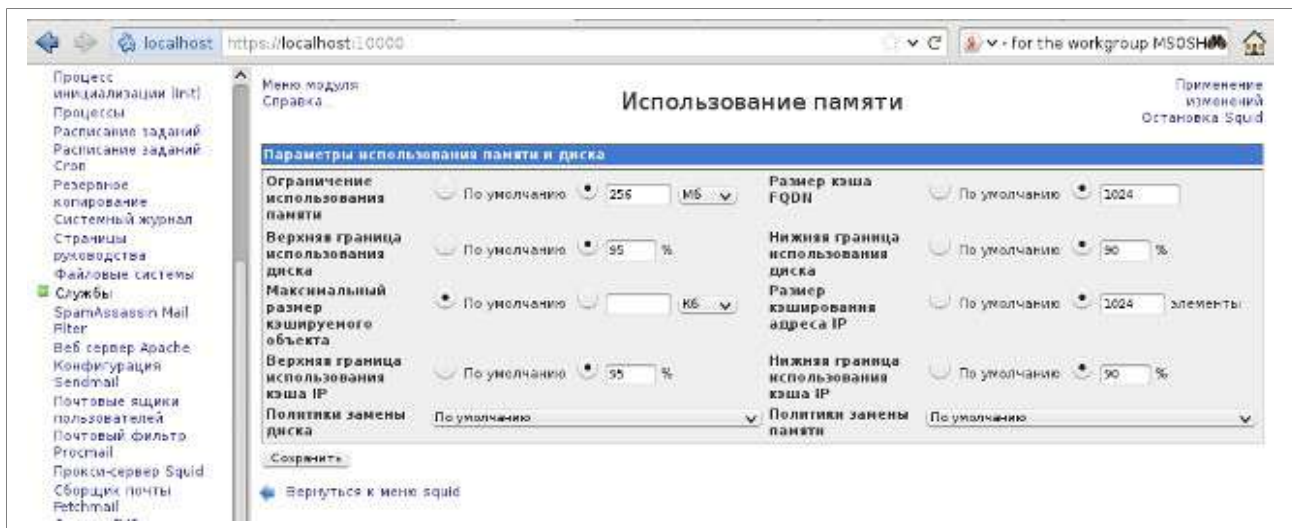
Далее настроим параметры кэша.



(Рис.64. Параметры кэша)

Заполним таблицу согласно рисунку и нажмем сохранить.

Использование памяти.

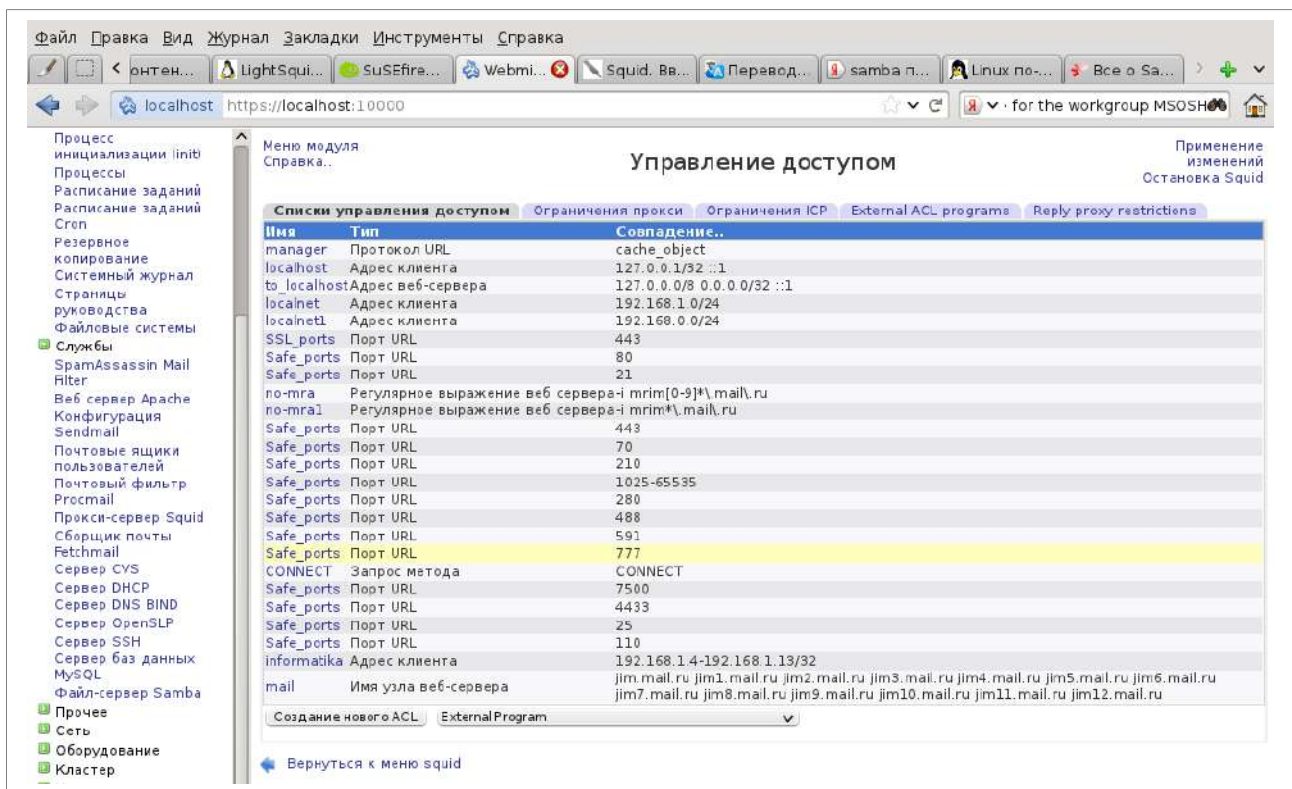


(Рис. 65. Использование памяти)

Управление доступом.

Прежде чем клиенты смогут использовать прокси-сервер, вам придется настроить его, чтобы дать доступ к нему с некоторых IP адресов. Для этого выполните следующие действия:

1. На странице **Списки управления доступом**, выберите Адрес клиента, из списка существующих ACL. При нажатии кнопки **Создать новый ACL**, будет отображена форма для ввода адресов в ACL.



(Рис. 66. Управление доступом)

2. В **Имя ACL** введите короткое имя, например localnet.

Меню модуля

Создание ACL

Адрес клиента ACL

Имя ACL

С IP На IP Маска сети

URL Отказа

Store ACL values in file Squid configuration Separate file

Just use existing contents of file?

[← Вернуться к Список ACL](#) | [Вернуться к меню](#)

(Рис. 67. Создание ACL)

3. В пустом поле с **IP**, введите начальный IP-адрес диапазона, например 192.168.1.0.
4. В поле **до IP**, введите конечный IP-адрес диапазона, например 192.168.1.100. Только клиенты, которые входят в этот диапазон будут проходить по ACL.
5. Вы также можете указать IP сеть, введя начальный IP-адрес в поле с **IP** и маску подсети (например, 255.255.255.0), в поле **Маска сети**.
6. Нажмите на кнопку «Сохранить», чтобы добавить ACL и вернуться на страницу **Списки управления доступом**, на которой ваш новый ACL уже будут отображен.
7. Нажмите кнопку **Добавить ограничение прокси** под таблицей **Ограничения Прокси**.

Списки управления доступом **Ограничения прокси** Ограничения ICP External ACL programs Reply proxy restrictions

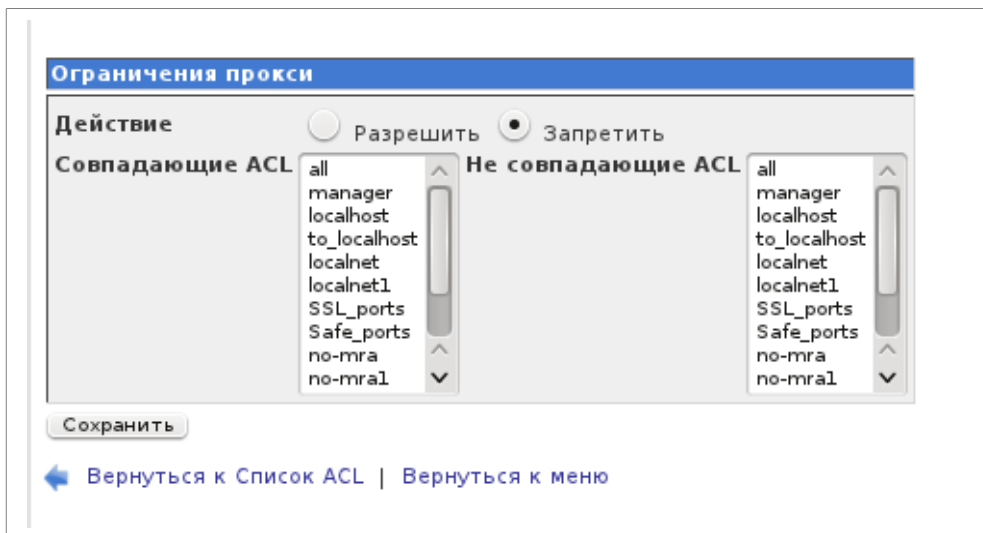
Добавить ограничение прокси

Действие	ACL	Переместить
<input type="checkbox"/> Разрешить	manager localhost	↓
<input type="checkbox"/> Разрешить	manager	↓↑
<input type="checkbox"/> Запретить	!Safe_ports	↓↑
<input type="checkbox"/> Запретить	mail	↓↑
<input type="checkbox"/> Запретить	no-mra	↓↑
<input type="checkbox"/> Запретить	no-mra1	↓↑
<input type="checkbox"/> Запретить	CONNECT !SSL_ports	↓↑
<input type="checkbox"/> Разрешить	localnet	↓↑
<input type="checkbox"/> Разрешить	localnet1	↓↑
<input type="checkbox"/> Разрешить	localhost	↓↑
<input type="checkbox"/> Разрешить	localhost	↓↑
<input type="checkbox"/> Запретить	all	↑

Добавить ограничение прокси

(Рис. 68. Настройка ограничений прокси)

8. На форме, которая появится, выберите **Разрешить** в поле **Действие**.



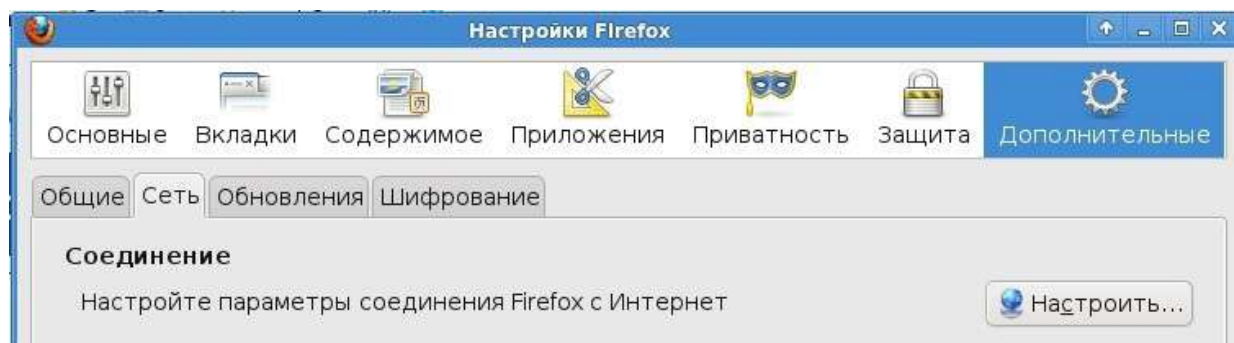
(Рис. 69. Ограничения прокси)

9. В **Совпадающие ACL** выберите ваш новый localnet ACL.
10. Нажмите кнопку «Сохранить» на этой форме, чтобы вернуться к странице **ограничения прокси** снова. Новое ограничение будет отображено в нижней части таблицы, скорее всего, ниже **Запретить all**.
11. Нажмите кнопку «**стрелка вверх**» рядом с вашим новым ограничением, чтобы переместить его выше пункта **Запретить all**. Это означает, что в Squid будут разрешены соединения из вашей сети и запрещены все остальные.
12. Наконец, нажмите кнопку Применить изменения в верхней части страницы. Прокси-сервер теперь будет доступен клиентам во внутренней сети, но никому более.

3.1.4. Настройки на локальной машине на примере браузера Mozilla Firefox.

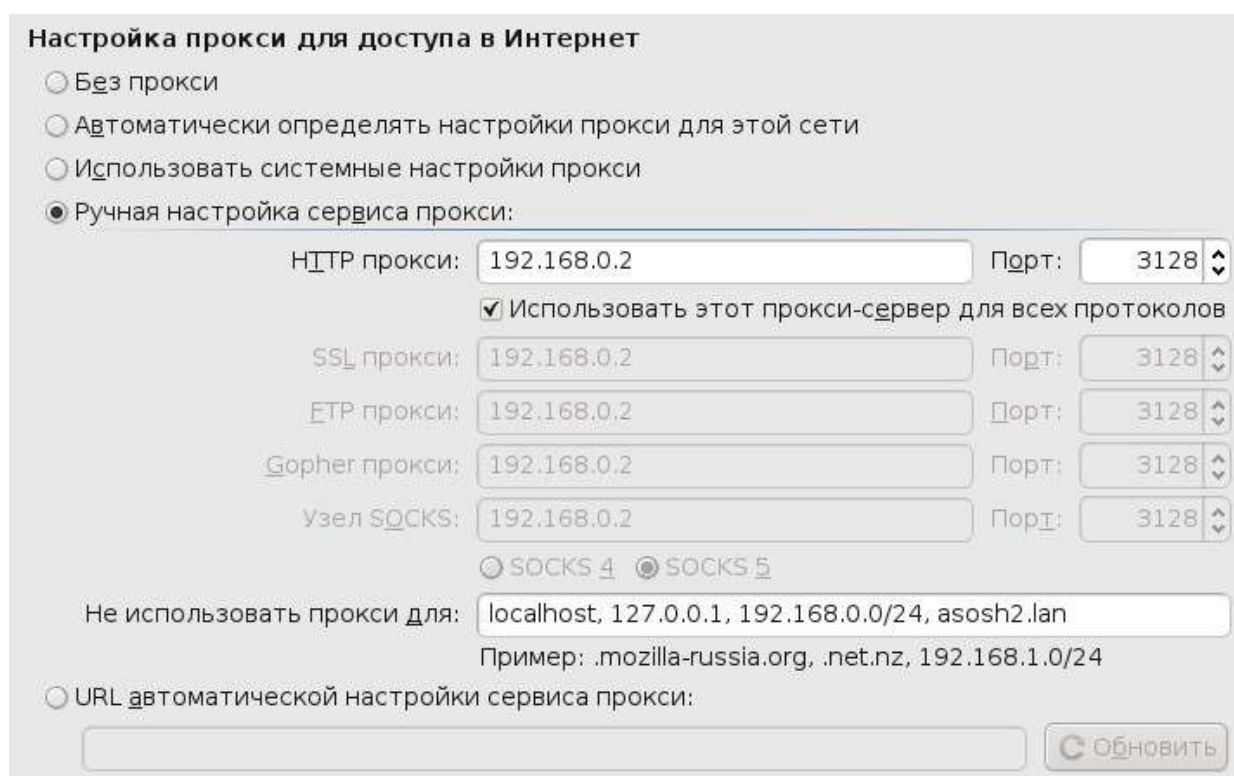
Для того, чтобы пользователи локальной сети получили доступ к сети Интернет используя наш сервер, необходимо произвести настройку браузера на локальных машинах:

1. Запускаем браузер (будем по умолчанию использовать Firefox, во всех остальных настройках производятся аналогично).
2. В главном меню «Правка» - «Настройка» - «Дополнительные» - вкладка «Сеть» -



(Рис. 70. Настройка браузера Firefox)

«Настроить» - вносим параметры нашего прокси-сервера (ip-адрес сервер или его доменное имя и порт):



(Рис. 71. Указываем настройки прокси-сервера для браузера Firefox)

3. После всех манипуляций пользователь получит доступ в сеть Интернет.

Настроить фильтрацию контента можно и средствами прокси-сервера squid, но так как для этого существуют специализированные программы мы рассмотрим настройку контент-фильтрации именно при помощи таких программ.

3.2. Установка и настройка контент-фильтра на основе NetPolice в ALT Linux Школьный сервер 5.0

NetPolice ALT Linux – версия программы NetPolice для операционной системы ALT Linux, предназначена для использования на домашнем ПК, а также может быть установлена в качестве выделенного сервиса фильтрации сети протокола http, так как построена на основе технологий прокси-сервера.

1. Проверяем, подключены-ли репозитории:
Вводим команду: `cat /etc/apt/sources.list`, команда покажет нам содержимое файла `/etc/apt/sources.list`.

```
rpm [p5] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p5/branch i586 classic
rpm [p5] ftp://ftp.altlinux.org/pub/distributions/ALTLinux/p5/branch noarch classic
```

Если репозитории не подключены. Подключаем их. Для редактирования файла `/etc/apt/sources.list` воспользуйтесь командой `mcedit /etc/apt/sources.list`. Клавиша F2 — сохранить изменения. F10 — выход из режима редактирования.

2. Подключаем репозиторий NetPolice. Для этого вводим строку

```
rpm http://update.netpolice.ru/altlinux/p5/branch/netpolice/ i586 netpolice
```

3. Устанавливаем необходимые пакеты:

```
apt-get update
apt-get install netpolice-main
```

4. Для обеспечения работоспособности системы NetPolice ее необходимо настроить на категоризирующий DNS сервер. Для этого редактируем файл `/etc/sysconfig/host2cat` и прописываем в поле `DNS_LIST` один из серверов NetPolice. Рекомендуемым вариантом является сервер `dnsc1.netpolice.ru` (для редактирования файла используем команду `mcedit /etc/sysconfig/host2cat`. Сохраняем изменения клавишей F2, выход F10)

```
MEMCACHED_LIST=127.0.0.1:11211
UDP_PORT=6666
# DNS LIST SERVER IP
#for example DNS_LIST=127.0.0.1
DNS_LIST=dnsc1.netpolice.ru
TTL=3600
HOST2CAT_OPTIONS="-m $MEMCACHED_LIST -u $UDP_PORT -s $DNS_LIST -t $TTL"
```

(Рис. 72. Настройка системы на категоризирующий DNS сервер)

5. Запускаем службы под правами суперпользователя root:

```
service memcached start
service host2cat start
service c-icap start
service squid restart
```

6. При помощи браузера заходим в панель администрирования фильтрации NetPolice по адресу `http://ip-адрес сервера/cgi-bin/login.cgi`
Имя пользователя: root

Пароль: root

Вход в систему

Админ

Пароль

(Рис. 73. Вход в панель управления NetPolice)

7. Заводим пользователя в группе student (Создать нового юзера). Пример:
Имя юзера: user
IP адрес: (реальный IP пользователя или 0.0.0.0 если он не известен)
Маска подсети/суффикс: < пусто >
Роль: my_student

Список администраторов

Имя	Действие
admin	Изменить пароль

Список ролей

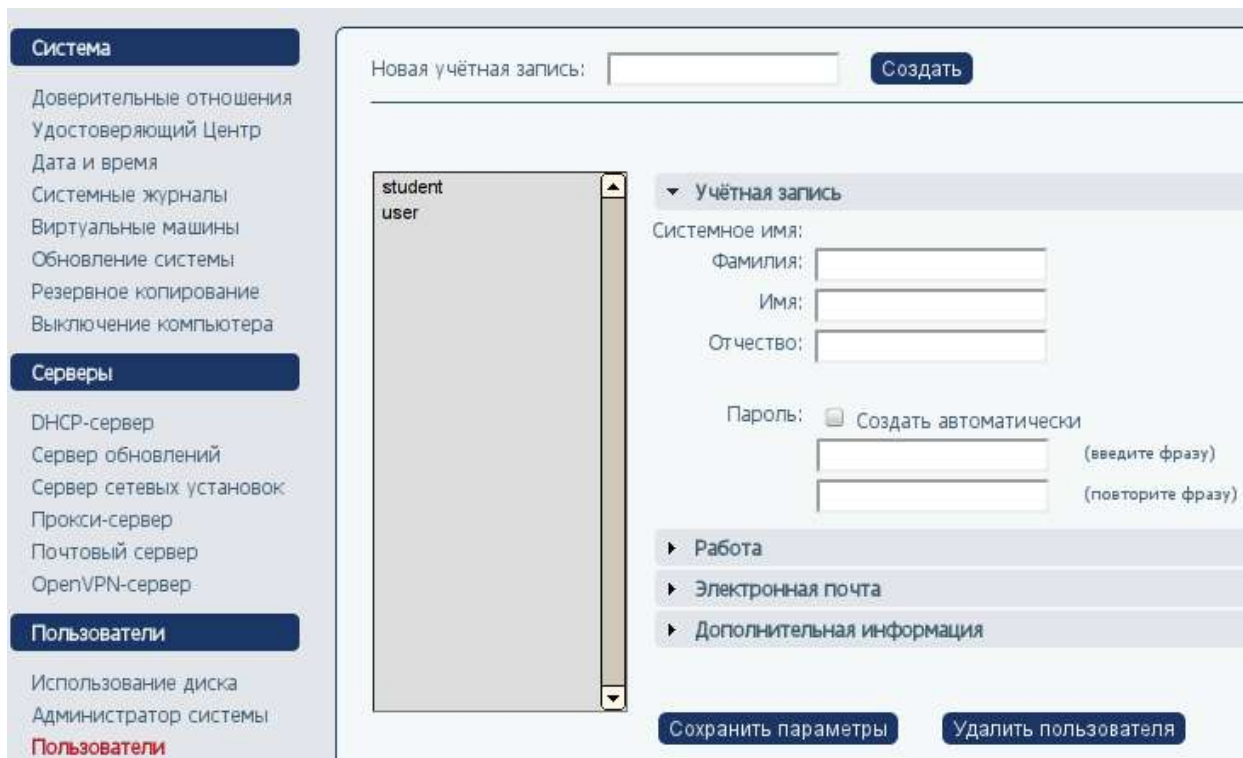
Тип	Название	Родители	Действие
General	admin		Подробнее
General	teacher		Подробнее
General	student	user	Подробнее
Custom	my_student	student	Подробнее Редактировать Удалить
Custom	my_teacher	admin teacher	Подробнее Редактировать Удалить
General	user	student	Подробнее
Создать новую роль			

Пользователи и роли

Пользователь	Сеть	Роль	Действие
netpolice	*	student	Редактировать Удалить
user	*	my_student	Редактировать Удалить
*	*	student	Редактировать Удалить
Создать нового юзера			

(Рис. 74. Панель управления NetPolice на школьном сервере)

8. Заводим пользователя с таким-же логином в панели управления сервером:



(Рис. 75. Добавление пользователя при помощи панели управления школьным сервером)

9. Редактирование политики доступа осуществляется под администратором. Выберите роль с типом Custom и нажмите "Редактировать".
 - "Черный список" и "Белый список" - списки URL запрещенных и разрешенных URL адресов соответственно.
 - "Список редиректов" - это список категорий (идентификаторов) интернет-ресурсов, определенных как перенаправляемые (по умолчанию перенаправление происходит на www.google.com).
 - "Список реджектов" - это список запрещенных категорий интернет-ресурсов.
10. После завершения редактирования политик доступа необходимо перезагрузить службы, необходимые для работы NetPolice:


```
service memcached restart
service host2cat restart
service c-icap restart
service squid restart
```
11. После этого при попытке зайти на веб-страницу запрашивается имя пользователя (в нашем примере — user) и пароль. При доступе на запрещенный ресурс (например, rotpo.ru). Страница заблокирована фильтром NetPolice! (при условии, что браузер настроен на работу с прокси-сервером)

Страница заблокирована фильтром NetPolice!

[Сообщить о неверной категоризации ресурса](#)



(Рис. 76. Проверка работоспособности контент-фильтра NetPolice)

Список категорий и их идентификаторов для домашнего категоризирующего DNS сервера.

105 алкоголь	34 фото
101 эротика, порнография	35 афиша
3 реклама, баннерные сервера	36 недвижимость
4 власти, правительство	37 религия
5 авто	38 школа
6 кино	39 наука
7 строительство и ремонт	40 спорт
8 предметы потребления	41 театры
9 кулинария	42 транспорт
10 дача	43 туризм
11 курсы, обучение	44 университеты
12 электроника и электротехника	111 работа и вакансии
13 оборудование	46 создание сайтов
14 семья	112 чаты
15 мода и стиль	48 сайты знакомств
16 финансы	49 войска и вооружение
17 изобразительное искусство	50 форумы и блоги
18 компьютеры, аппаратное обеспечение	51 сервера бесплатной электронной почты
19 здоровье	52 бесплатные хостинги
20 хобби	107 нелегальная помощь школьникам и студентам
21 юмор	54 убийства, насилие, трупы
22 интерьер	110 онлайн-казино
23 доступ в интернет	102 социальные сети
24 юридические услуги	57 терроризм
25 литература	58 торговля
26 СМИ	108 нижнее белье, купальники
27 машиностроение	109 обеспечение анонимности, обход контентных фильтров
28 металлургия	103 службы обмена сообщениями
29 мобильная связь	104 файлообменные сети и сайты
30 музыка	106 табак
31 общественные организации	
113 компьютерные игры	
33 домашние животные	

3.3. Установка и настройка контент-фильтра на основе DansGuardian.

DansGuardian – это программное обеспечение, которое создано компанией SmoothWall и предназначено для управления доступом пользователей к тем или иным веб-сайтам. Оно включает функции проверки контента на вирусы и предоставления детальной статистики о своей работе.

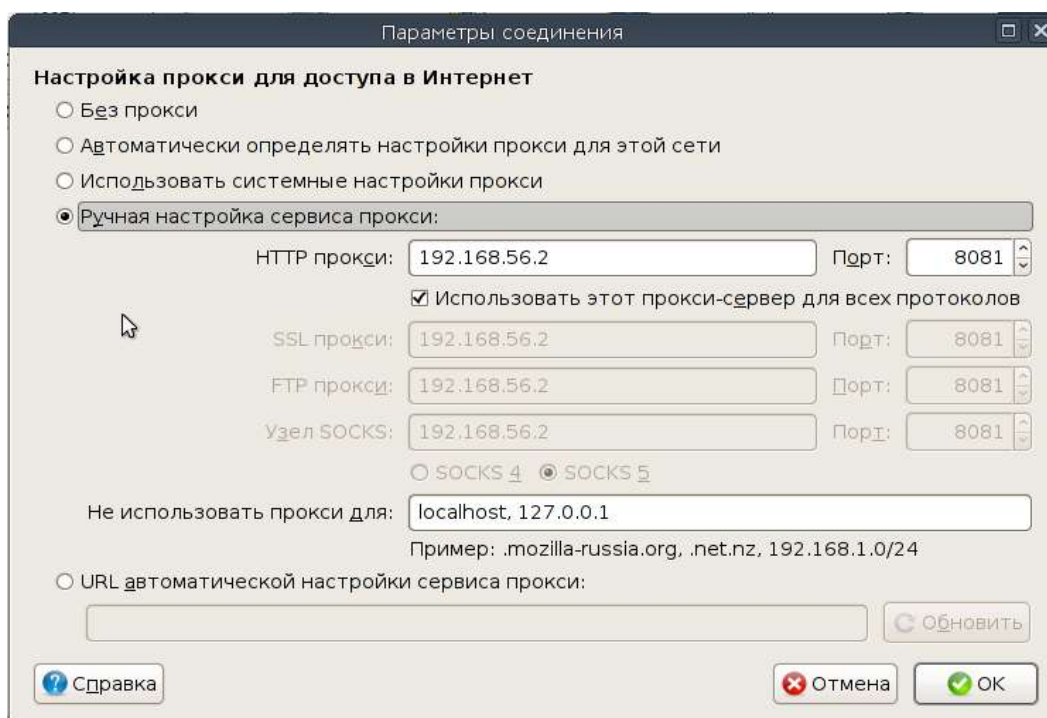
3.3.1. Установка и настройка контент-фильтра на основе DansGuardian в ALT Linux Школьный сервер 5.0

Для настройки контент-фильтрации при помощи DansGuardian нам потребуются две программы:

- squid
- dansguardian

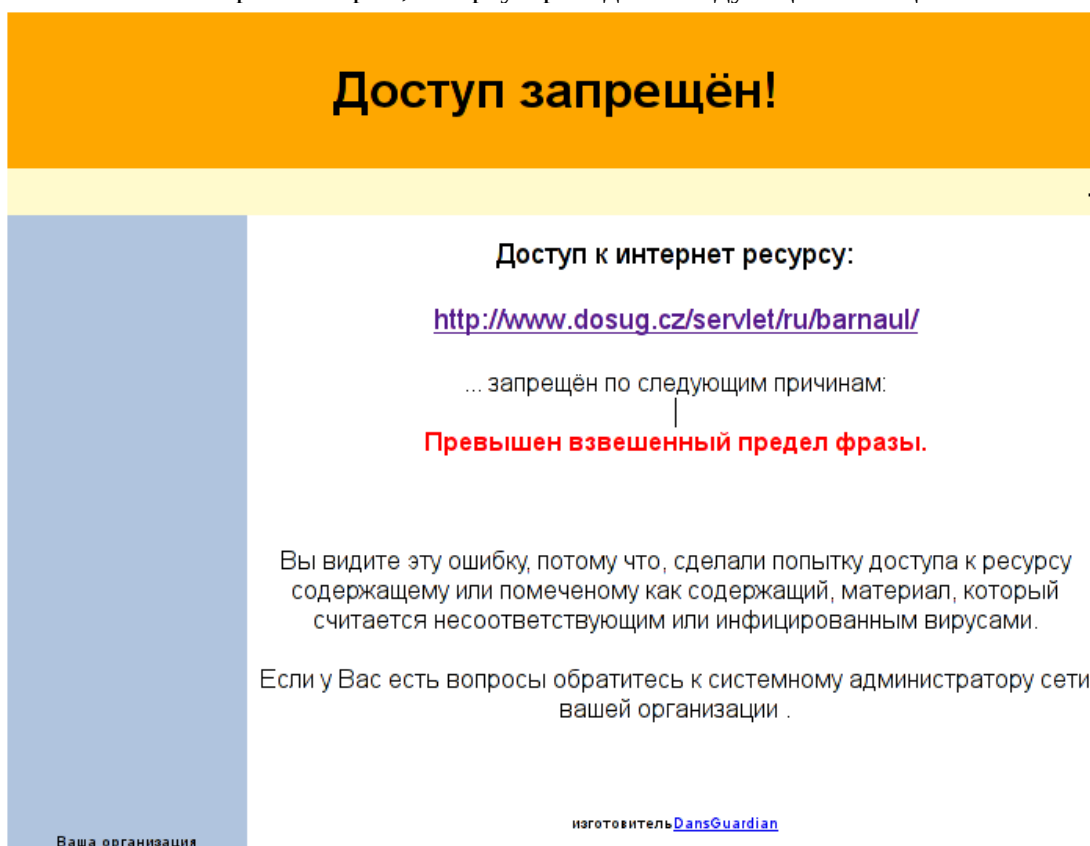
Прокси-сервер squid у нас уже настроен и запущен. Осталось установить и настроить программу-фильтр DansGuardian:

1. Устанавливаем пакет: **apt-get install dansguardian**
2. Настройка DansGuardian, как и практически любой программы в Linux, сводится к редактированию конфигурационного файла **dansguardian.conf**. Для этого открываем файл для редактирования (будем использовать встроенный редактор файлового менеджера Midnight Commander): **mcedit /etc/dansguardian/dansguardian.conf**
3. Изменяем следующие параметры:
 - 1) Параметру language присваиваем значение «russian-1251»(**language = 'russian-1251'**)
 - 2) Порт на котором работает контент-фильтр: **filterport = 8081** (по умолчанию установлен 8080 — но этот порт занят системой управления школьным сервером).
 - 3) Указываем порт, на котором работает прокси-сервер squid: **proxyport = 3128**
 - 4) Запускаем DansGuardian:
service dansguardian start
 - 5) В настройках браузера на локальной машине в сети указываем следующие параметры прокси-сервера:



(Рис. 77. Настройка браузера Mozilla Firefox на локально компьютере)

- б) Проверяем работу контент-фильтра. Для этого введем в адресной строке браузера ресурс, не соответствующий задачам образования, например <http://www.dosug.cz> . Если все настроено верно, то браузер выдаст следующее сообщение:



(Рис. 78. Проверка работы контент-фильтра DansGuardian)

- 7) Для более детальной настройки необходимо заглянуть в файл `dansguardianf1.conf`. В нем перечислены файлы, в которых указаны запрещенные/разрешенные адреса сайтов, фразы, типы файлов. Посмотреть содержимое файла можно при помощи команды `cat`:
- ```
cat /etc/dansguardian/dansguardian1.conf
```
- 8) Также имеется возможность использовать другие файлы с запрещенными/разрешенными сайтами, созданными самостоятельно. Для этого предназначена директива `.include`.
- 9) Перечислим некоторые файлы, на которые следует особо обратить внимание:
- `bannerdsitelist` блокирует целые домены;
  - `bannedurllist` – только некоторые их части;
  - `urlregexplist`, напротив, разъясняет DansGuardian, как прозрачно подменять одни URL другими, (теоретически) более безопасными.
  - Особое внимание уделите всем файлам, имена которых начинаются с “`exception`”. В них перечислено все – от расширений файлов до IP-адресов – что должно быть исключено из фильтрации. `Exceptionsitelist` и `exceptionsurllist`, например, содержат все безгрешные сайты или подразделы сайтов соответственно: в последнем случае вы можете разрешить.
- 10) После каждого редактирования файлов DansGuardian необходимо перезапустить службу:
- ```
service dansguardian restart
```

3.3.2. Установка и настройка контент-фильтра на основе DansGuardian в Ubuntu.

Принципиально установка и настройка контент-фильтра в Ubuntu ничем не отличается от установки и настройки в ALT Linux:

1. Запускаем приложение Терминал (Приложения — Стандартные - Терминал).
2. Устанавливаем пакет `dansguardian`: **`sudo apt-get install dansguardian`**

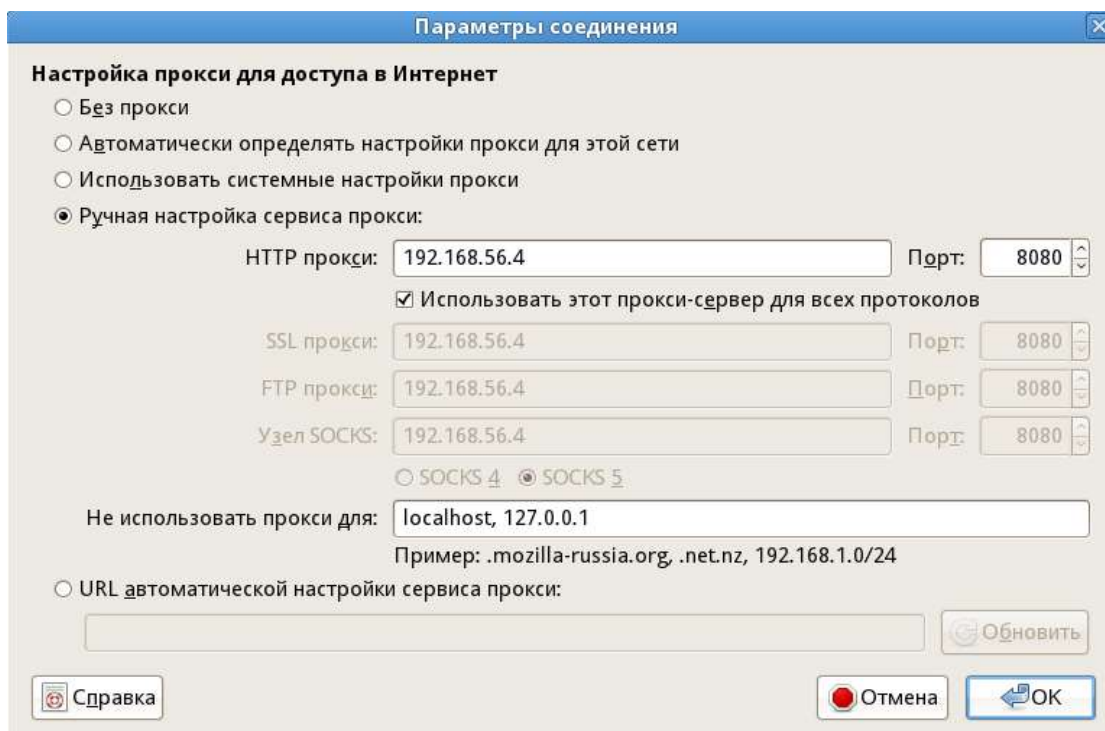
```
ubuntu@ubuntu:~$ sudo apt-get install dansguardian
[sudo] password for ubuntu:
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
 clamav clamav-base clamav-freshclam libclamav6 libtommath0
Предлагаемые пакеты:
 clamav-docs libclamunrar6
НОВЫЕ пакеты, которые будут установлены:
 clamav clamav-base clamav-freshclam dansguardian libclamav6 libtommath0
обновлено 0, установлено 6 новых пакетов, для удаления отмечено 0 пакетов, и 249
Необходимо скачать 35,8 МБ архивов.
После данной операции, объём занятого дискового пространства возрастёт на 45,6 М
Хотите продолжить [Д/н]? Д
Получено:1 http://ru.archive.ubuntu.com/ubuntu/ natty/main libtommath0 i386 0.39
Получено:2 http://ru.archive.ubuntu.com/ubuntu/ natty-updates/main libclamav6 i3
```

(Рис. 79. Установка DansGuardian в Ubuntu)

3. После установки отредактируем конфигурационный файл DansGuardian: **`sudo gedit`**

/etc/dansguardian/dansguardian.conf

4. Изменяем следующие параметры:
 1. Параметру language присваиваем значение «russian-1251»(**language = 'russian-1251'**)
 2. Порт на котором работает контент-фильтр: **filterport = 8080**
 3. Указываем порт, на котором работает прокси-сервер squid: **proxyport = 3128**
 4. Закомментируем строку, содержащую: UNCONFIGURED - т. е. поставим перед строкой знак #
 5. Сохраняем изменения.
 6. Запускаем DansGuardian: **sudo /etc/init.d/dansguardian start**
 7. В настройках браузера на локальной машине в сети указываем следующие параметры прокси-сервера:



(Рис. 80. Настройка браузера Firefox для работы с DansGuardian)

8. Проверяем работу контент-фильтра. Для этого введем в адресной строке браузера ресурс, не соответствующий задачам образования, например <http://www.dosug.cz> . Если все настроено верно, то браузер выдаст следующее сообщение:

Доступ запрещён!

Доступ к интернет ресурсу:

<http://www.dosug.cz/servlet/ru/barnaul/>

... запрещён по следующим причинам:

Превышен взвешенный предел фразы.

Вы видите эту ошибку, потому что, сделали попытку доступа к ресурсу содержащему или помеченному как содержащий, материал, который считается несоответствующим или инфицированным вирусами.

Если у Вас есть вопросы обратитесь к системному администратору сети вашей организации .

изготовитель [DansGuardian](#)

Ваша организация

(Рис. 81. Проверка работы контент-фильтрации на основе DansGuardian)

9. Также как и в случае с настройкой DansGuardian в ALT Linux для более детальной настройки необходимо заглянуть в файл `dansguardianf1.conf`. В нем перечислены файлы, в которых указаны запрещенные/разрешенные адреса сайтов, фразы, типы файлов. Посмотреть содержимое файла можно при помощи команды `cat`:
`cat /etc/dansguardian/dansguardian1.conf`
10. Также как и было описано ранее в пункте 3.3.1 в Ubuntu имеется возможность использовать другие файлы с запрещенными/разрешенными сайтами, созданными самостоятельно. Для этого предназначена директива `.include`.
11. После каждого редактирования файлов DansGuardian необходимо перезапустить службу: **`sudo /etc/init.d/dansguardian restart`**

3.4. Установка и настройка контент-фильтра на основе Redirector (Rejik).

Программа проста в установке и настройке. Однако при этом достаточно эффективна и позволяет отсекают баннеры, организовать фильтрацию по "черным" и "белым" спискам. Разграничить доступ к ресурсам по логину или IP.

Squid позволяет в своей конфигурации указать внешнюю программу редиректор. Эта программа выполняет функцию фильтрации запросов клиентов.

Каждый раз, когда кто-то загружает файл через Ваш прокси, на стандартный вход редиректора передаются данные о запросе. Редиректор эти данные анализирует, при выполнении некоторых условий изменяет и выдает ответ на стандартный выход.

3.4.1. Установка и настройка контент-фильтра на основе Redirector (Rejik) в ALT Linux Школьный сервер 5.0

Первое что нужно сделать - это установить программу:

```
#apt-get install redirector
```

Указываем в конфигурационном файле `/etc/squid/squid.conf`, что будет использоваться программа-редиректор:

```
url_rewrite_program /usr/sbin/redirector /etc/squid/redirector/redirector.conf
```

Далее приступаем к настройке программы фильтрации.

Редактируем конфигурационный файл `/etc/squid/redirector/redirector.conf`. По умолчанию в нем выделено 4 категории для фильтрации:

- **<BANNER>** - раздел для блокирования баннеров
- **<PORNO>** - сайты содержащие порнографические материалы
- **<MP3>** - раздел для блокирования файлов музыки
- **<JS>** - раздел для блокирования js-скриптов

В нашем случае достаточно произвести замену адреса `http://127.0.0.1` на ip-адрес нашего веб-сервера (или его доменное имя). Например:

```
<BANNER>
```

```
ban_dir /var/lib/redirector/banlists/banners
```

```
url http://192.168.0.4/ban/1x1.gif
```

И разместить соответствующие файлы замены в директории веб-сервера. Файлы замены скачать можно здесь: http://www.rejik.ru/index_ru_11_1.html.

Для того чтобы добавить соответствующие сайты для блокирования, необходимо редактировать файлы банлистов в директории `/var/lib/redirector/banlist/` Например, для того чтобы заблокировать сайт `http://www.odnoklassniki.ru` нужно добавить запись в файл `/var/lib/redirector/banlist/porno/urls` - `odnoklassniki.ru` и перезапустить squid для того, чтобы изменения вступили в силу.

```
#service squid reload
```

Таким образом в нашей сети будет производиться фильтрация по "черным" спискам. Однако все ресурсы, не отвечающие задачам образовательного учреждения заблокировать достаточно сложно и если задаться целью, то попасть на такой ресурс возможно, что и

приводит к многочисленным претензиям со стороны надзорных органов. Поэтому имеет смысл ограничить доступ учащихся к ресурсам сети Интернет "белыми" списками. Для этого необходимо создать в `/etc/squid/redirector/redirector.conf` еще один раздел, отвечающий за доступ пользователей по "белым" спискам.

<WHITELIST>

ban_dir /var/lib/redirector/banlists/whitelist

url http://192.168.0.4/ban/whitelist.html

И добавить соответствующие файлы в директории `/var/www/html/` и `/var/lib/redirector/banlists/` аналогично уже имеющимся. Осталось только наполнить содержимым файл `/var/lib/redirector/banlists/whitelist/urls` теми ссылками, которые удовлетворяют образовательным задачам учебного заведения.

Список можно скачать и принять участие в их наполнении здесь:

• <http://catalog.iot.ru/>

• <http://www.spo.akipkro.ru/index.php/whitelist.html>

Соответственно списки должны быть утверждены школой для использования.

Иногда имеет смысл разграничить доступ. Например, запросы учителей и администрации фильтруются по "черным" спискам, а учащихся - по "белым".

Для этого в раздел `<WHITELIST>` необходимо добавить соответствующую запись (примеры):

• **work_ip f:/var/lib/redirector/banlists/class_ip** - применять фильтр по "белым" спискам группе пользователей с ip - указанными в файле **class_ip**.

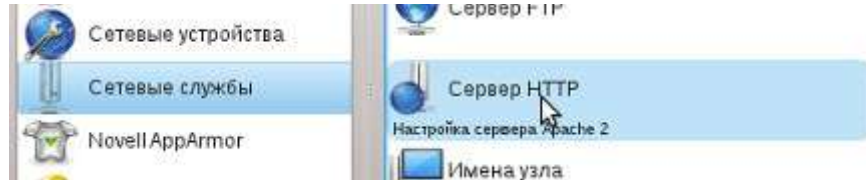
• **allow_id f:/var/lib/redirector/banlists/login** - не применять фильтр по "белым" спискам к пользователям с логинами, указанными в файле **login**.

3.4.2. Установка и настройка контент-фильтра на основе Redirector (Rejik) в OpenSuse.

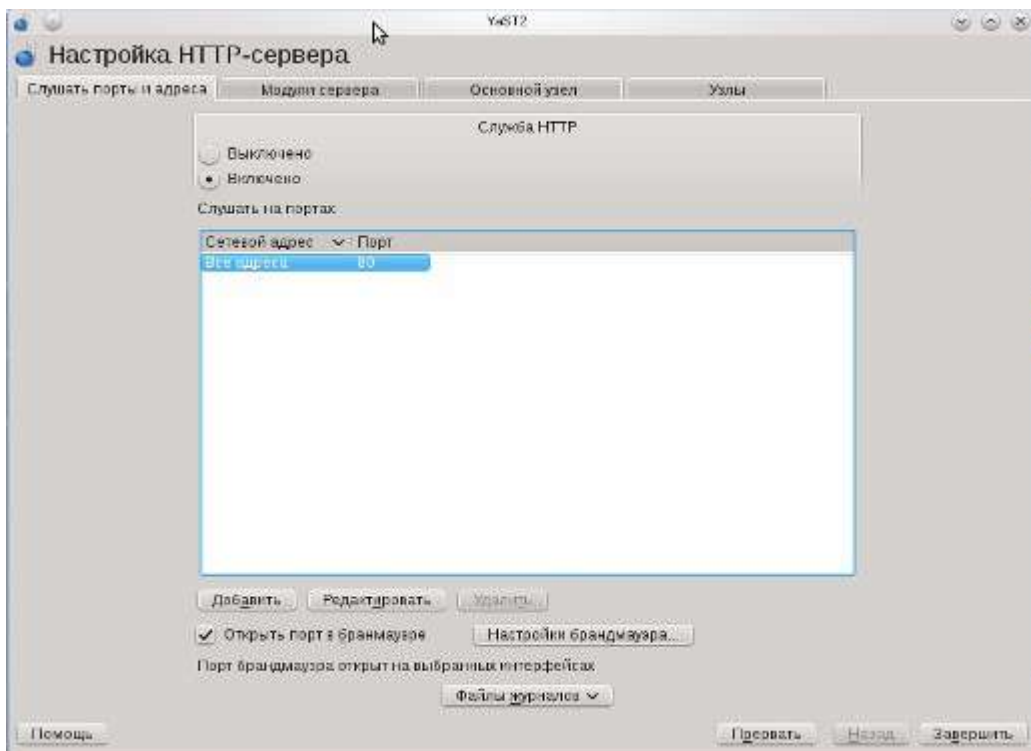
Установка.

Идем на сайт <http://www.rejik.ru>, из раздела скачать скачиваем последнюю стабильную версию редиректора и распаковываем. Переходим в папку с файлами редиректора и устанавливаем:

1. Запускаем веб сервер (YaST->Сетевые службы-> Сервер HTTP)



(Рис. 82. Запуск http сервера)



(Рис. 83. Работы http-сервера)

2. Скачиваем и выкладываем на веб сервер (srv/www/htdocs) файлы, которыми будем заменять рекламу, порно, и.т.д. Файлы берем здесь: http://www.rejik.ru/index_ru_11_1.html
3. Проверяем доступность этих файлов (<http://localhost/www/porno.html>)
4. Необходимо узнать, под каким пользователем у Вас работает squid, и в какую группу входит этот пользователь. Для этого можно посмотреть, как у Вас прописаны в squid.conf опции `cache_effective_user` и `cache_effective_group`.
5. Редактируем Makefile. Как минимум нужно прописать переменные `SQUID_USER` и `SQUID_GROUP`, значения которых Вам должно быть известно из предыдущего пункта.
6. В диспетчере файлов выбираем **сервис-> открыть терминал** и вводим **make**
7. **make install**
8. Переходим в директорию `/usr/local/rejik3/`

9. Скачиваем и распаковываем бан-листы (берем в http://www.rejik.ru/index_ru_11_1.html)
10. Переименовываем **redirector.conf.dist** в **redirector.conf**
11. Проверяем, правильно ли прописаны пути в **redirector.conf**, в **url** прописываем пути к файлам которыми будем заменять рекламу, порно и т.д. на нашем веб сервере.
12. Добавляем в конфигурационный файл прокси сервера squid (/etc/squid/squid.conf) следующую строку: **url_rewrite_program /usr/local/rejik3/redirector /usr/local/rejik3/redirector.conf**. Таким образом мы указываем squid что будет использоваться редиректор.
13. Перезапускаем squid, читаем логи, пробуем открывать страницы в браузере.

Настройка.

Редиректор можно настроить для работы по «черным» и по «белым» спискам. Для того чтобы редиректор работал по «черным» спискам можно воспользоваться проектом DBL (распределенный бан лист). Раздел DBL на сайте <http://rejik.ru>.

Для работы редиректора по «белым» спискам необходимо следующее:

1. Создать в **/usr/local/rejik3/redirector.conf** еще один раздел, отвечающий за доступ пользователей по "белым" спискам.
<WHITELIST>
work_ip /usr/local/rejik3/ip
ban_dir /usr/local/rejik3/banlists/whitelist
url <http://localhost/www/whitelist.html>
reverse
2. Добавить соответствующие файлы в директории **/srv/www/htdocs/** и **/usr/local/rejik3/banlists/**
3. Наполнить содержимым файл **/usr/local/rejik3/banlists/whitelist/urls** теми ссылками, которые удовлетворяют образовательным задачам учебного заведения (<http://catalog.iot.ru/> <http://www.spo.akipkro.ru/index.php/whitelist.html>)
4. Указать в файле **/usr/local/rejik3/ip** ip адреса компьютеров к которым будет применима фильтрация по «белым» спискам.

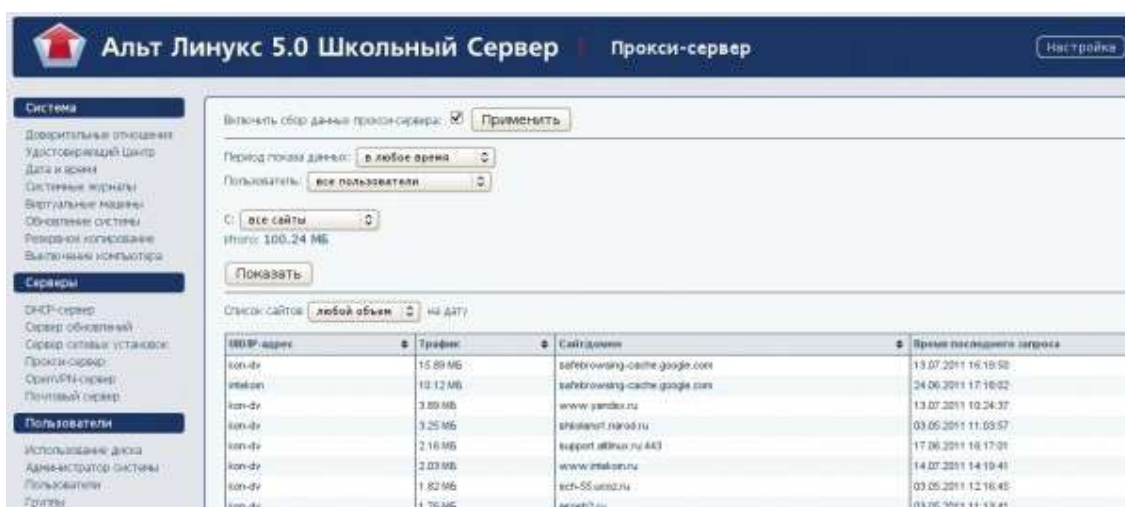
4. Организация электронного журнала работы пользователей в сети Интернет на основе SARG и Light Squid.

После того как мы полностью контролируем доступ в сеть Интернет, имеет смысл просматривать статистику работы пользователей в сети Интернет и вести журнал работы пользователей в сети. Тем более, что ведение журнала работы пользователей в сети Интернет - требование ко многим учебным заведениям. Вести журнал на бумажном носителе - очень трудоемко и не всегда удобно. Поэтому воспользуемся специальным программным обеспечением.

Существует множество программ для генерации отчетов работы пользователей в сети Интернет. Для организации электронного журнала воспользуемся программой SARG (Squid Analysis Report Generator) - генератор отчетов на основании анализа лог-файла прокси сервера Squid. Отчеты позволяют выяснить какой пользователь в какое время обращался к какому сайту. Суммарный отчет может оказать большую помощь в тарификации работающих через Squid пользователей, так как включает в себя суммарный трафик и число коннектов для каждого пользователя за определенный период времени.

4.1. Организация электронного журнала работы пользователей в сети Интернет на основе SARG в ALT Linux.

В ALT Linux в панели управления школьным сервером для этого создан раздел "Статистика", где можно просматривать статистику работы в сети Интернет пользователей школьной сети:



IP-адрес	Трафик	Сайт(ы)	Время последнего запроса
kon-dv	15.89 MB	safebrowsing-cache.google.com	13.07.2011 16:18:58
kon-dv	10.12 MB	safebrowsing-cache.google.com	24.06.2011 17:16:02
kon-dv	3.89 MB	www.panda.ru	13.07.2011 10:24:37
kon-dv	3.25 MB	shopart.larod.ru	03.05.2011 11:03:57
kon-dv	2.16 MB	support.altlinux.ru/Alt3	17.06.2011 16:17:01
kon-dv	2.03 MB	www.intel.com.ru	14.07.2011 14:19:41
kon-dv	1.82 MB	ict-55.com.ru	03.05.2011 12:16:45
kon-dv	1.76 MB	konf2.ru	03.05.2011 11:18:41

(Рис. 84. Просмотр статистики работы пользователей в сети Интернет при помощи панели управления школьным сервером)

Однако также можно воспользоваться программой генератора отчетов работы прокси-сервера Squid - SARG.

Устанавливаем программу:

```
#apt-get install sarg
```

Настройка sarg также сводится к редактированию конфигурационного файла /etc/sarg/sarg.conf. Воспользуемся, уже знакомой нам командой, **mcedit /etc/squid/sarg.conf**

language Russian_UTF-8

Указываем где находятся лог-файлы squid:

access_log /var/log/squid/access.log

Включаем построение графиков

graphs yes

graph_days_bytes_bar_color orange

Указываем название отчета:

title "Отчет о работе в сети Интернет"

Каталог, в который помещаются отчеты:

output_dir /var/www/html/squid-reports

Удаляем временные файлы:

remove_temp_files yes

При генерации отчета перезаписываем старые файлы:

overwrite_report yes

Сохраняем изменения нажатием клавиши F2. F10 — выход.

Команда генерации отчетов:

sarg

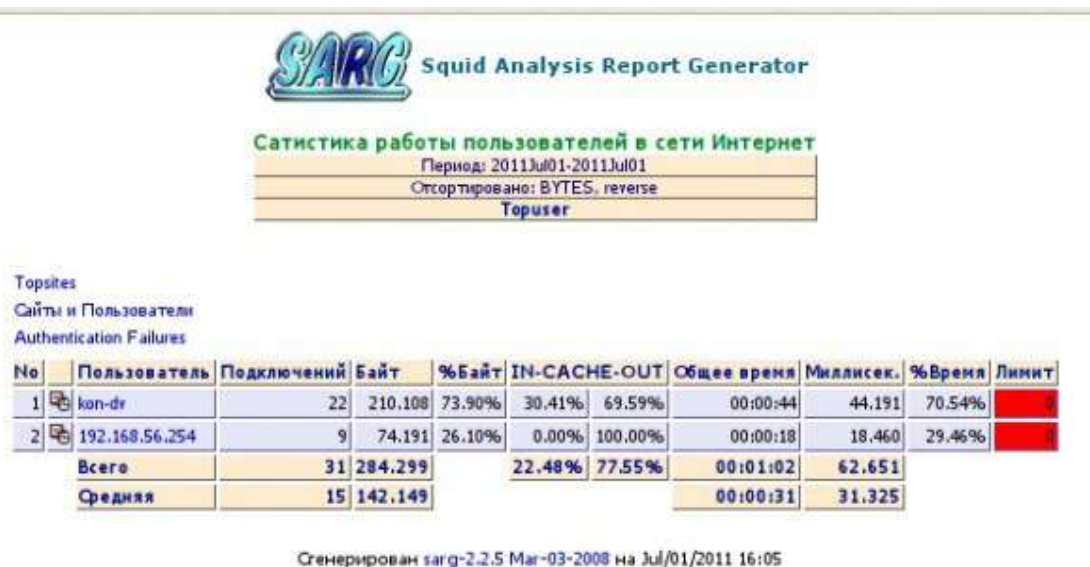
Теперь открываем браузер и заходим на страницу отчетов. Отчет будет доступен по адресу: **http://ip-адрес сервера/squid-reports/** в следующем виде:

Период	Дата создания	Пользователей	Байт	Средняя
2011Jul13-2011Jul13	Wed Jul 13 16:05:01 NOVST 2011	1	1.955.903	1.955.903
2011Jul01-2011Jul01	Fri Jul 1 16:05:01 NOVST 2011	2	284.299	142.149
2011Jun29-2011Jun29	Wed Jun 29 16:05:02 NOVST 2011	2	1.695.252	847.626
2011Jun28-2011Jun28	Tue Jun 28 16:05:02 NOVST 2011	1	6.227	6.227
2011Jun24-2011Jun24	Fri Jun 24 17:05:01 NOVST 2011	2	22.319.235	11.159.617
2011Jun23-2011Jun23	Thu Jun 23 18:05:01 NOVST 2011	2	719.103	359.551
2011Jun22-2011Jun22	Wed Jun 22 20:05:01 NOVST 2011	1	3.606.018	3.606.018
2011Jun17-2011Jun17	Fri Jun 17 18:05:01 NOVST 2011	3	15.528.051	5.176.017
2011Jun06-2011Jun06	Mon Jun 6 15:05:01 NOVST 2011	2	607.808	303.904
2011May30-2011May30	Mon May 30 16:05:02 NOVST 2011	2	3.622.480	1.811.240
2011May23-2011May23	Mon May 23 16:05:01 NOVST 2011	1	8.195.135	8.195.135
2011May10-2011May10	Tue May 10 17:05:01 NOVST 2011	1	2.337.928	2.337.928
2011May06-2011May06	Fri May 6 16:05:02 NOVST 2011	1	2.628.610	2.628.610
2011May03-2011May03	Tue May 3 17:05:01 NOVST 2011	1	34.012.175	34.012.175
2011Apr29-2011Apr29	Fri Apr 29 15:36:35 NOVST 2011	4	3.278.726	819.681

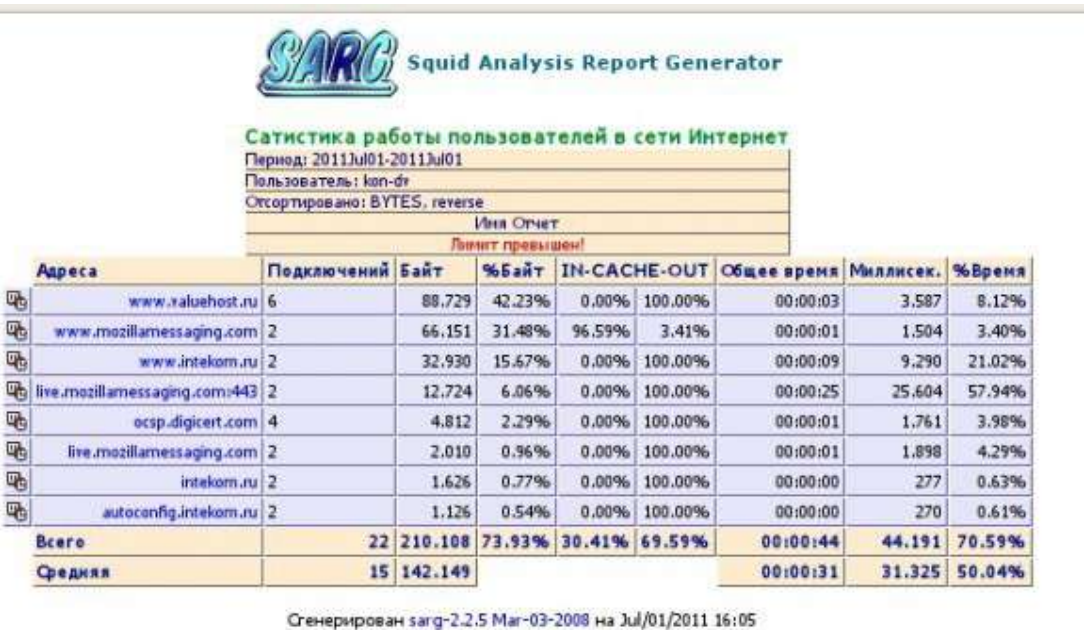
Сгенерирован sarg-2.2.5 Mar-03-2008 на Jul/13/2011 16:05

(Рис. 85. Просмотр статистики работы пользователей в сети Интернет, сгенерированного при

помощи SARG)



(Рис. 86. Просмотр статистики работы пользователей в сети Интернет, сгенерированного при помощи SARG)



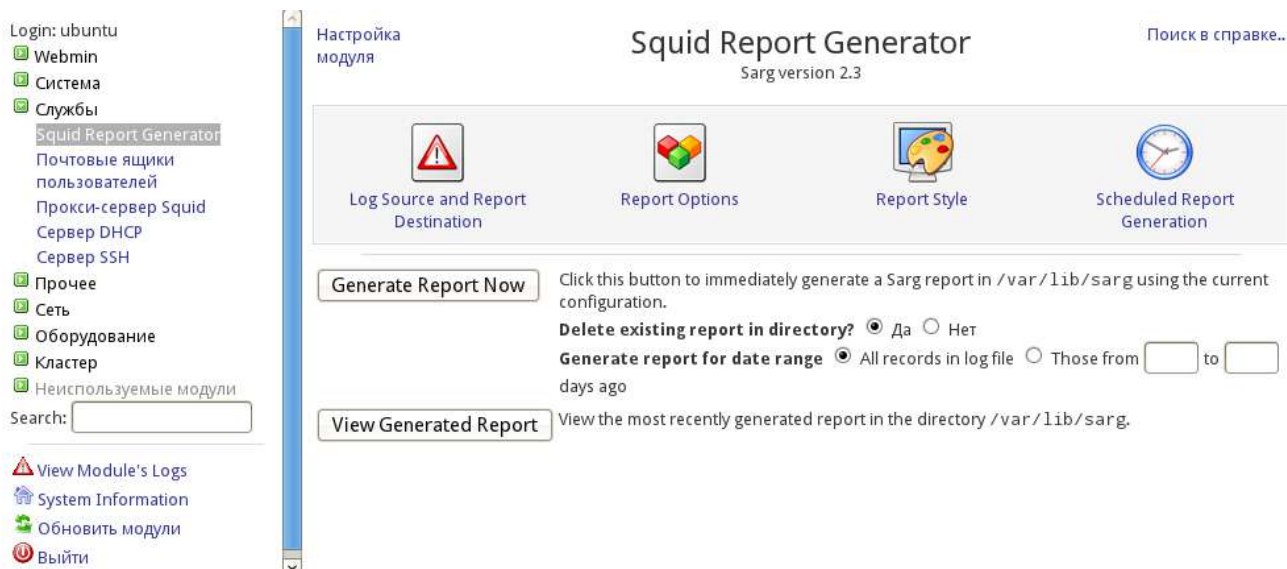
(Рис. 87. Просмотр статистики работы пользователей в сети Интернет, сгенерированного при помощи SARG)

При желании такой журнал можно распечатать и предоставить проверяющим.

4.2. Организация электронного журнала работы пользователей в сети Интернет на основе SARG в Ubuntu.

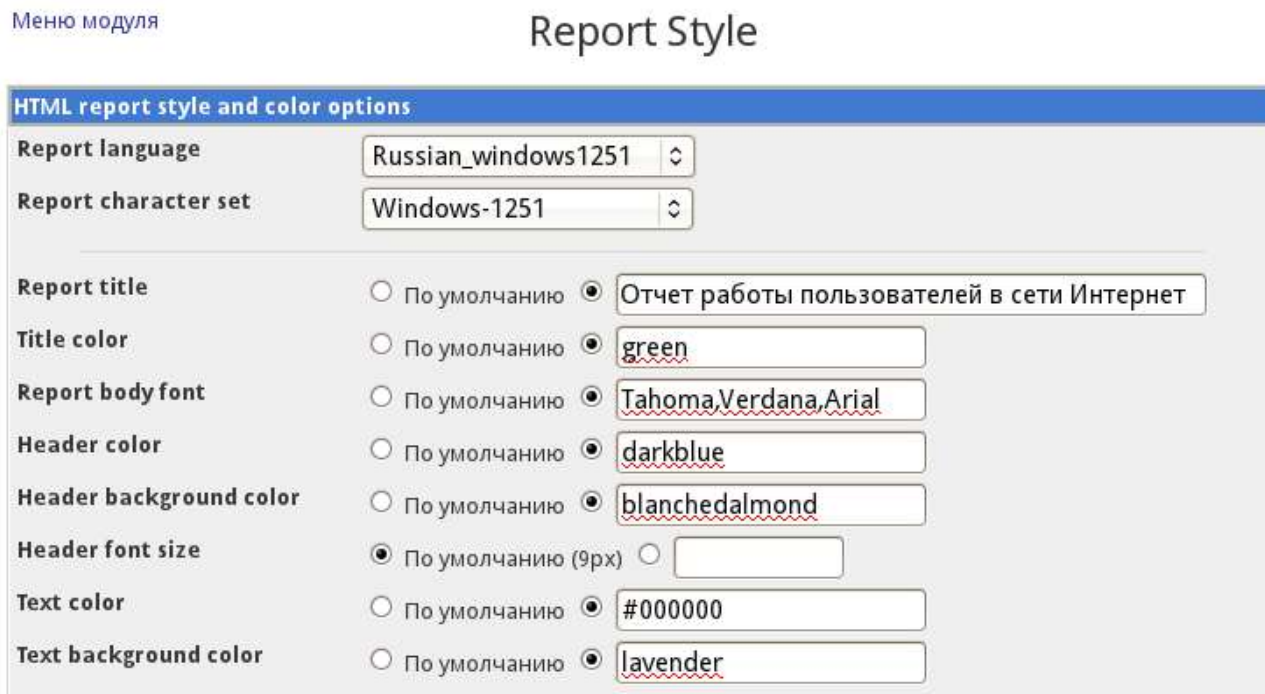
Для того чтобы установить SARG в Ubuntu запустим приложение «Терминал» и введем команду: **sudo apt-get install sarg**

После окончания установки в панели управления webmin в разделе Службы - Squid Report Generator:



(Рис. 88. Управление SARG при помощи Webmin)

В разделе Report Style укажем язык формирования отчета Russian_windows1251 и заголовок отчета «Отчет работы пользователей в сети Интернет»:



(Рис. 89. Настройка отчета SARG)

Сохраняем изменения при помощи кнопки «Сохранить» и генерируем отчет при помощи кнопки «Generate Report Now»:

Меню модуля

Generate Report

Now generating Sarg report from Squid log file /var/log/squid/access.log and all rotated versions ..

```
sarg -l /var/log/squid/access.log  
SARG: Unknown option language Russian_windows1251
```

.. done

[View completed report.](#)

[← Вернуться к module index](#)

(Рис. 90. Генерация отчета SARG при помощи Webmin)

Просмотреть сгенерированный отчет можно при помощи кнопки «View Generated Report»:

Меню
модуля

SARG report



Squid Analysis Report Generator

Отчет работы пользователей в сети Интернет

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2011Dec03-2011Dec04	Sun Dec 4 12:58:25 2011	3	10.69M	3.56M

Generated by sarg-2.3 Jun-21-2010 on Dec/04/2011 12:58

[← Вернуться к module index](#)

(Рис. 91. Просмотр сгенерированного отчета SARG при помощи Webmin)

Меню модуля

SARG report for 2011 Dec 03-2011 Dec 04



Squid Analysis Report Generator

Отчет работы пользователей в сети Интернет

Period: 2011 Dec 03—2011 Dec 04

Sort: BYTES, reverse

Top users

[Top sites](#)

[Sites & Users](#)

[Downloads](#)

[Denied accesses](#)

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE	OUT	ELAPSED TIME	MILLISEC	%TIME
1	192.168.56.5	366	6.64M	62.11%	2.09%	97.91%	00:30:17	1,817,455	34.29%
2	192.168.56.1	393	3.24M	30.35%	1.79%	98.21%	00:52:30	3,150,796	59.44%
3	127.0.0.1	86	806.39K	7.54%	0.00%	100.00%	00:05:32	332,211	6.27%
TOTAL		845	10.69M	1.84%	98.16%		01:28:20	5,300,462	
AVERAGE		281	3.56M				00:29:26	1,766,820	

Generated by sarg-2.3 Jun-21-2010 on Dec/04/2011 12:58

[← Вернуться к module index](#)

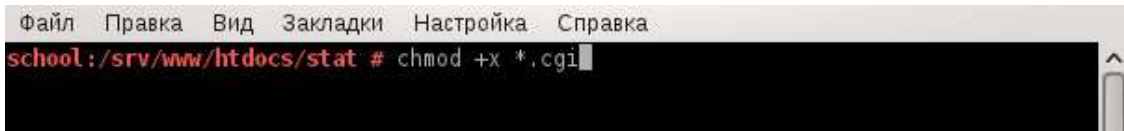
(Рис. 92. Просмотр отчет SARG при помощи Webmin)

4.3. Организация электронного журнала работы пользователей в сети Интернет на основе Light Squid в OpenSuse.

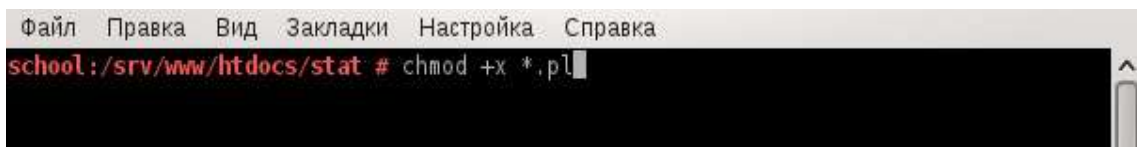
Установка.

1. Создаём с помощью менеджера файлов каталог, где у нас, непосредственно, и будет расположен lightsquid. Назовем его немного короче **stat** (**srv/www/htdocs/stat**)
2. Скачиваем и распаковываем в созданный каталог последнюю версию lightsquid (берем тут: <http://lightsquid.sourceforge.net/>)
3. Делаем скрипты программы исполняемыми.

```
# chmod +x *.cgi  
# chmod +x *.pl
```

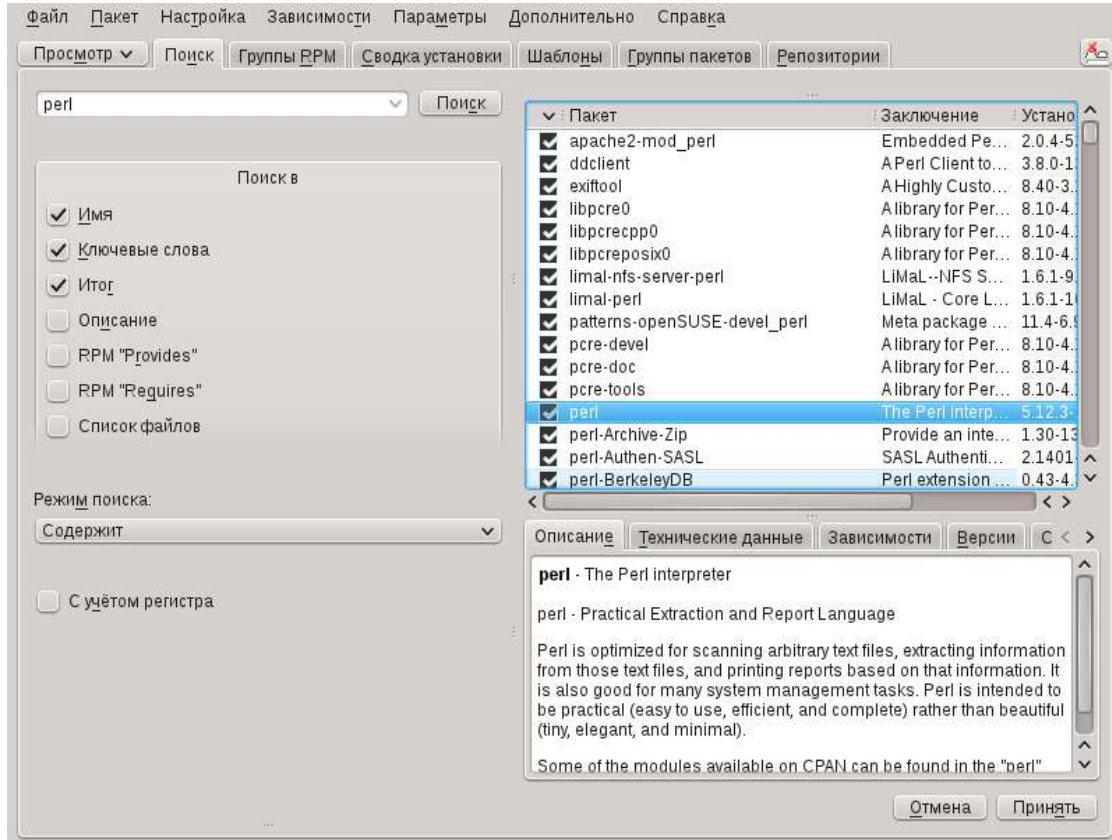


(Рис. 93. Ввод команды chmod +x *.cgi)



(Рис. 94. Ввод команды chmod +x *.pl)

4. Ставим зависимые пакеты, без которых программа работать не будет (**libgd-gd2-perl** отвечает за показ графиков)



(Рис. 95. Установка дополнительных пакетов)

Настройка.

1. Для того, чтобы Apache правильно обрабатывал *.cgi*-скрипты отредактируем файл `/etc/httpd.conf` и добавим в него следующие строки:

```
<Directory "/srv/www/htdocs/stat">
  Options +ExecCGI
  AddHandler cgi-script .cgi
  DirectoryIndex index.cgi
  AllowOverride All
</Directory>
```

Затем, для применения новых настроек перезапустим Apache.

2. Открываем на редактирование конфигурационный файл `lightsquid.cfg` и правим пути в секции `GLOBAL VARIABLES`

```
$cfgpath      ="/srv/www/htdocs/stat";
$tplpath      ="/srv/www/htdocs/stat/tpl";
$langpath     ="/srv/www/htdocs/stat/lang";
$reportpath   ="/srv/www/htdocs/stat/report";
$logpath      ="/var/log/squid";
$ip2namepath  ="/srv/www/htdocs/stat/ip2name";
```

В секции `WEB VARIABLES` выставляем нужный язык интерфейса. В данном случае русский.

```
$lang      = "ru";
```

3. Закрываем и сохраняем. Теперь с помощью скрипта **check-setup.pl** можем проверить правильность сделанных настроек. Никаких ошибок быть не должно.

```
# ./check-setup.pl
```

4. Открываем файл `realname.cfg` и прописываем там IP пользователей и их реальные имена, которые будут отображаться в отчётах `lightsquid`

```
192.168.1.2  com1
192.168.1.4  com2
192.168.1.5  com3
192.168.1.6  com4
192.168.1.7  com5
192.168.1.8  com6
```

Теперь можно вручную сгенерировать отчеты и заодно проверить как работает `lightsquid`:

сервис->открыть терминал и ввести `./lightparser.pl`

После того как отчет сгенерирован открываем браузер и вводим в адресной строке:
`http://ip_вашего_сервера/stat`

Отчёт по использованию интернета, прокси-сервер Squid.
 Отчётный период: Май 2011

Календарь											
2011											
01	02	03	04	05	06	07	08	09	10	11	12

Популярные сайты	Всего	Групп
ГОД	ГОД	ГОД
МЕСЯЦ	МЕСЯЦ	МЕСЯЦ

Дата	Группа Пользователей	Превысили	Байт	В среднем	Cache Hit %
31 Май 2011	груп.	25	2	641.2 М	25.6 М 3.25%
30 Май 2011	груп.	19	2	597.2 М	31.4 М 5.01%
29 Май 2011	груп.	3	0	3.3 М	1.1 М 0.00%
28 Май 2011	груп.	17	0	94.0 М	5.5 М 8.10%
27 Май 2011	груп.	18	2	528.0 М	29.3 М 3.88%
26 Май 2011	груп.	18	3	809.5 М	45.0 М 3.90%
25 Май 2011	груп.	25	1	438.8 М	17.6 М 9.26%
24 Май 2011	груп.	33	1	796.3 М	24.1 М 15.63%
23 Май 2011	груп.	27	2	1.2 G	44.9 М 2.49%
22 Май 2011	груп.	2	0	3.0 М	1.5 М 0.04%
21 Май 2011	груп.	27	1	468.1 М	17.3 М 19.38%
20 Май 2011	груп.	30	5	2.6 G	89.6 М 4.47%
19 Май 2011	груп.	33	3	2.4 G	74.2 М 3.16%
18 Май 2011	груп.	38	4	1.8 G	47.8 М 7.92%
17 Май 2011	груп.	33	2	900.4 М	27.3 М 9.86%
16 Май 2011	груп.	32	3	956.2 М	29.9 М 14.20%
15 Май 2011	груп.	4	0	3.3 М	862 878 0.00%
14 Май 2011	груп.	5	0	7.4 М	1.5 М 12.07%
13 Май 2011	груп.	38	1	1.1 G	28.3 М 8.97%
12 Май 2011	груп.	39	3	1.7 G	43.9 М 15.07%
11 Май 2011	груп.	34	5	1.2 G	37.4 М 15.15%

(Рис. 96. Главная страница lightsquid)

Отчёт по использованию интернета, прокси-сервер Squid.

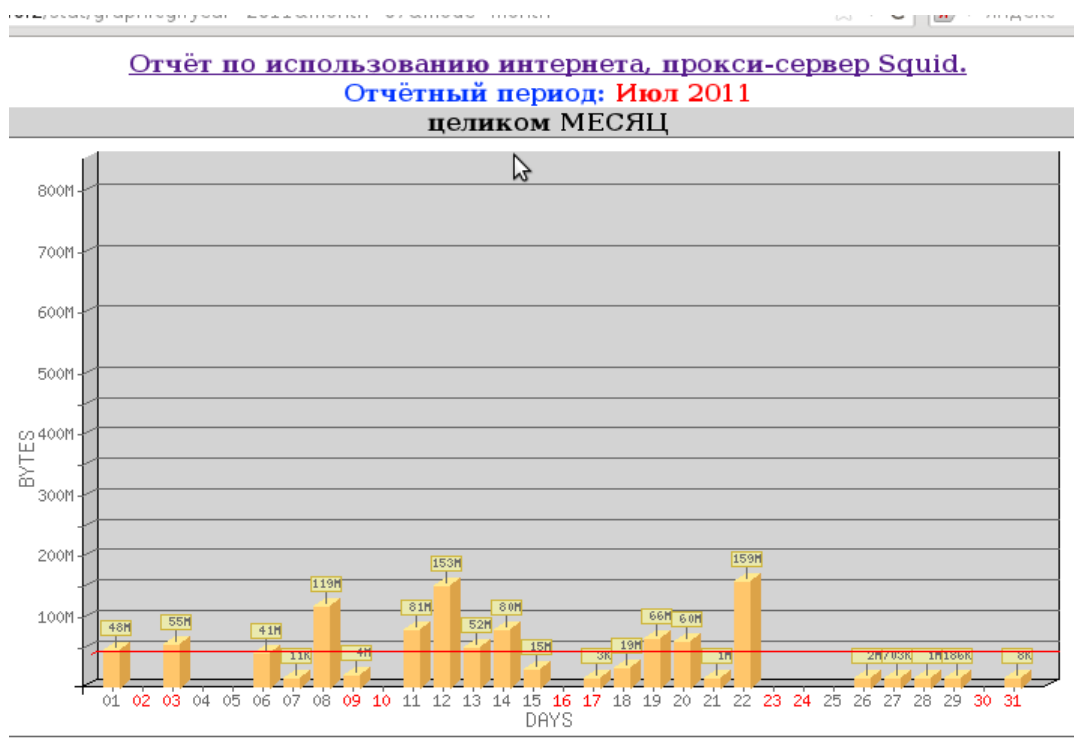
Дата: 29 Сен 2011 (Обновлено :: 20:46 :: 2 Окт 2011)

Популярные сайты (отчёт)

Кто скачал БОЛЬШИЕ файлы (отчёт)

№	Время	Пользователь	Ф.И.О	Соединений	Байт	%	Группа
1	192.168.0.48	geograf-t		5 327	660.9 М	43.7%	?
2	192.168.0.33	Bbiblioteka		5 492	174.1 М	11.5%	?
3	192.168.0.52	BUNGALTER		1 111	135.4 М	8.9%	?
4	192.168.0.45	glavbuh		1 041	95.2 М	6.3%	?
5	192.168.0.37	obj-t		1 549	67.8 М	4.4%	?
6	192.168.0.7	Kom4		3 460	37.4 М	2.4%	?
7	192.168.0.3	Admin		6 833	33.9 М	2.2%	?
8	192.168.0.36	izo		988	32.7 М	2.1%	?
9	192.168.0.41	uchitelskaya2		575	26.3 М	1.7%	?
10	192.168.0.9	Kom6		2 587	26.3 М	1.7%	?
11	192.168.0.6	Kom3		3 387	25.5 М	1.6%	?
12	192.168.0.12	Kom9		2 895	24.8 М	1.6%	?
13	192.168.0.4	Kom1		3 340	24.7 М	1.6%	?
14	192.168.0.13	Kom10		2 037	20.7 М	1.3%	?
15	192.168.0.15	?		1 032	19.3 М	1.2%	?
16	192.168.0.50	Kom		254	14.7 М	0.9%	?
17	192.168.0.5	Kom2		1 991	14.3 М	0.9%	?
18	192.168.0.10	Kom7		1 099	10.6 М	0.7%	?
19	192.168.0.44	zavuch		1 574	10.1 М	0.6%	?
20	192.168.0.47	istoriya-t		1 226	9.8 М	0.6%	?

(Рис. 97. Отчет по дате)



LightSquid v1.8 (c) Sergey Erokhin AKA ESL

(Рис. 98. Отчет в виде графика)

Отчёт по использованию интернета, прокси-сервер Squid.
целиком МЕСЯЦ
Отчётный период: Дек 2011

№	Время	График	МЕСЯЦ	Пользователь	Ф.И.О	Соединений	Байт	%	Итого
1			[M]	192.168.0.41	uchitelskaya2	7 445	3.1 G	20.5%	3.1 G
2			[M]	192.168.1.13	Kom10	9 558	3.1 G	20.0%	6.2 G
3			[M]	192.168.0.40	uchitelskaya1	4 643	1.7 G	11.3%	8.0 G
4			[M]	192.168.0.36	izo	62 827	1.3 G	8.6%	9.3 G
5			[M]	192.168.0.48	geograf.t	9 479	458.9 M	2.9%	9.7 G
6			[M]	192.168.1.6	Kom3	23 294	413.4 M	2.6%	10.2 G
7			[M]	192.168.1.3	Kom	14 352	403.5 M	2.5%	10.5 G
8			[M]	192.168.0.35	russ1	18 609	395.8 M	2.5%	10.9 G
9			[M]	192.168.0.3	Admin	40 014	318.8 M	2.0%	11.2 G
10			[M]	192.168.0.33	Bbiblioteka	1 199	311.3 M	1.9%	11.5 G
11			[M]	192.168.0.39	kab6	9 669	309.4 M	1.9%	11.9 G
12			[M]	192.168.1.5	Kom2	14 466	305.7 M	1.9%	12.1 G
13			[M]	192.168.1.4	Kom1	19 348	275.1 M	1.7%	12.4 G
14			[M]	192.168.0.52	BUNGALTER	12 374	272.0 M	1.7%	12.7 G
15			[M]	192.168.0.49	kab2.t	6 039	257.6 M	1.6%	12.9 G
16			[M]	192.168.0.15	test	2 934	249.3 M	1.5%	13.2 G
17			[M]	192.168.0.47	istoriya.t	5 926	247.5 M	1.5%	13.4 G
18			[M]	192.168.1.9	Kom6	12 566	230.3 M	1.4%	13.6 G
19			[M]	192.168.0.14	inyaz1	7 287	204.4 M	1.3%	13.8 G
20			[M]	192.168.1.10	Kom7	12 335	203.0 M	1.2%	14.0 G
21			[M]	192.168.0.37	abi.t	10 394	199.4 M	1.2%	14.2 G

(Рис. 99. Отчет за месяц)

Для автоматизации генерирования отчётов добавляем в *cron* (*/var/spool/cron/tabs/root*) задание: `0,15,30,45 * * * * /srv/www/htdocs/stat/lightparser.pl`. Отчёты будут автоматом генерироваться через каждые 15 минут.

Для правильной генерации отчетов так же вынесем в *cron* ротацию логов сквида: `1 0 * * * /usr/sbin/logrotate /etc/logrotate.conf`.

Заключение.

Сегодня имеется очень много несогласных с применением контент-фильтрации в образовательном учреждении, особенно по "белым" спискам, но давайте на минуту задумаемся - а зачем на входе в школу дежурит охрана или вахтер? Не затем-ли, чтобы отфильтровать нежелательные проникновения и для поддержания порядка в школе? Так и сеть Интернет на сегодня изобилует ресурсами, посещение которых просто не соответствует образовательным задачам и посещение которых учащимися может привести к штрафам, судебным искам к образовательному учреждению как со стороны родителей, так и со стороны надзорных органов.

И мы не прибегая к дорогостоящим программ, сумели организовать работу и контент-фильтрации, и учета статистики работы пользователей в сети Интернет средствами свободного программного обеспечения, существенно сэкономив при этом бюджет школы.

Литература

1. DHCP-сервер на Ubuntu: [сайт]. URL: <http://448dmg.ru/dhcp-server-nubuntu-278> (Дата обращения 13.12.2011).
2. LightSquid Home Site : Installs: [сайт]. URL: <http://lightsquid.sourceforge.net/Installs.html> (Дата обращения 13.12.2011).
3. NetPolice. Руководство по установке и эксплуатации: [сайт]. URL: <http://netpolice.ru/filters/altlinux/help/> (Дата обращения 13.12.2011).
4. Open-SUSE.RU: [сайт]. URL:<http://open-suse.ru/modules/smartsection/> (Дата обращения 13.12.2011).
5. Portal:Документация: [сайт]. URL: <http://ru.OpenSuse.org/Portal:%D0%94%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F> (Дата обращения 13.12.2011).
6. Sarg - Squid Analysis Report Generator: [сайт]. URL: <http://www.opennet.ru/prog/info/1175.shtml> (Дата обращения 13.12.2011).
7. Ubuntu Server. Настраиваем контент-фильтр роутера (DansGuardian): [сайт]. URL:http://interface31.ru/tech_it/2010/03/ubuntu-server-nastraivaem-kontent-fil-tr-routera-dansguardian.html (Дата обращения 13.12.2011).
8. Ubuntu-ru: [сайт]. URL: <http://ubuntu.ru> (Дата обращения 13.12.2011)/
9. Webmin — система на кончиках пальцев: [сайт]. URL: <http://habrahabr.ru/blogs/linux/72325/> (Дата обращения 13.12.2011).
10. Альт Линукс 5.0 Школьный: [сайт]. URL: <http://www.altlinux.ru/products/5th-platform/school-box/> (Дата обращения 13.12.2011).
11. Настройка SQUID с помощью Webmin: [сайт]. URL: http://break-people.ru/cmsmade/index.php?page=unix_webmin_practice_squid_webmin (Дата обращения 13.12.2011).
12. Настройка фильтра NetPolice DNS (Для Ubuntu): [сайт]. URL:<http://rub-educ.ru/dock/informat/98-nastroyka-filtra-netpolice-dns.html> (Дата обращения 13.12.2011).
13. Подключение NetPolice DNS: [сайт]. URL: <http://www.netpolice.ru/filters/dns-filter/connect/> (Дата обращения 13.12.2011).
14. Сайт, посвященный проблеме блокирования рекламы, порно-сайтов, mp3 и т.д. средствами прокси сервера SQUID: [сайт]. URL: <http://www.rejik.ru/> (Дата обращения 13.12.2011).
15. Система контентной фильтрации. На базе Ubuntu: [сайт]. URL:<http://oiyt.ru/blog/sictema-kontentnoy-filtracii-na-baze-ubuntu> (Дата обращения 13.12.2011).
16. Установка и настройка Lightsquid в Debian Lenny: [сайт]. URL: <http://www.youisbee.ru/head/25-linux/69-lightsquid> (Дата обращения 13.12.2011).
17. Шлюз Интернета на базе Ubuntu-Server: [сайт]. URL: http://help.ubuntu.ru/wiki/sharing_internet (Дата обращения 13.12.2011).