### МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

> Коновалов Д.В. Булгаков Е.В.

### Перечень модулей

Вв	едение		4
1.	Спосо	бы 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.	Орган	изация локальной сети школы.	12
	2.1.	Организация локальной сети с контролируемым доступом в сеть интерне, на основе ALT Linux.	12
	2.1.1.	Организация локальной сети с контролируемым доступом в сеть интерне, 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.	Устан конте	овка и настройка программного обеспечения для организации нт-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.	Орган на осн	изация электронного журнала работы пользователей в сети Интернет юве SARG и Light Squid.	63

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

#### 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. Заключить договор 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 ложиться 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»:



Выбираем сетевой интерфейс и нажимаем кнопку «Изменить»:

0

Название	Последнее подключение	ф Добавить
Auto etho	2 минуты назад	<u>е И</u> зменить

(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:

😣 Измене	ние А	uto eth0		
<u>Н</u> азвание сое	единен	ния: Auto eth0		
Подключа	аться а	втоматически		
Проводные	Защи	та 802.1х Парамет	гры IPv4 Парамет	ры ІРv6
<u>П</u> рофиль:	Авто	матически (DHCP, 1	голько адрес)	<b>_</b>
Адреса				
Адрес		Маска сети	Шлюз	Добавить
Серверы <u>Д</u> омены и ID <u>к</u> лиен <sup>-</sup> ☑ Требо	<u>D</u> NS: поиска та DHC вать а,	81.176.72.82 :: :Р: дресацию IPv4 для	этого соединения	М <u>а</u> ршруты
☑ Доступно	всем г	тользователям	<b>Ж</b> О <u>т</u> менить	<u>Сохранить</u>

(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

용 <b>NetPolice</b> Яищу	Найти	
Безопасное использование Интернета дома О безопасном Интернете для преподавателей О безопасном Интернете для учащихся	ССССССССССССССССССССССССССССССССССССС	47

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

Беспроводные	<ul> <li>Защита беспроводно</li> </ul>	й сети Параметры IPv4	Параметры IPv
Профиль: 🛛	Автоматически (DHCP, т	голько адрес)	\$]
Addresses			
Адрес	Маска сети	Шлюз	<u> </u>
			<u> </u>
Серверы <u>D</u> I	NS: 81.176.72.82		
<u>Д</u> омены по	иска:		
ID <u>к</u> лиента	DHCP:		
🗹 Требова	ть адресацию IPv4 для	этого соединения	
			Routes

(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 контентфильтрации 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:

<ul> <li>Автоматически определять на</li> <li>Использовать системные наст</li> </ul>	стройки прокси для этой сет ройки прокси	И	
• Рұчная настройка сервиса про	кси:		
НТТР прок <u>с</u> и:	localhost	П <u>о</u> рт:	3128
	🗹 Использовать этот проко	си-с <u>е</u> рвер для всех прото	околон
SSL про <u>к</u> си:	localhost	Порт:	3128
FTP прокс <u>и</u> :	localhost	Порт:	3128
У <u>з</u> ел SOCKS:	localhost	Порт.	3128
	O SOCKS <u>4</u>		
Не использовать прокси <u>д</u> ля:	localhost, 127.0.0.1		
	Пример: .mozilla-russia.org	, .net.nz, 192.168.1.0/24	

(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 проксисервера.

"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 интерне, 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 cepвepa: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.

會 Альт Ли	нукс 5.0	Школьный Сервер 🖡 Ethernet-интерфейсы
Система	Mar Imate Interna	school-septer
Доверительные отношения Удостоверяющий Центр	Интерфейсы	- (awww.awawe
дата и время Системные журналы Виртуальные машины	eth0 eth1	Ceveras rapta: Intel Corporation 805408N Gigabit Ethernet Controller провод подсоеднием
Системные службы		Конфигурация: Вручную
Системные ограничения		IP-agpec: 192 168 0.4
Веб-интерфейс Резеление колитование		Маска сети: (/24 (255.255.255.0) 🔅
Выключение компьютера		Шлюз по умолчанию: [192.168.0.100
Crivedia vincularia SSI		DNS-cepsepsi: 80.247.96.65
ri pasiterine michani Soc		Домены поихока: (80.247.97.18
repaepu		(несколько значений записываются через пробел)
ЭНСР-сервер Сервер обновлений Сервер ситевых установок ПР-сервер Служба катапогов LDAP	Применить	Дополнительно

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

Система Доверительные отношения	Имя компьюте	pa: (ssbeel	astivat			
удостовержодии центр Дата и время Системные журнаты Виртуальные машины	Интерфейсы eth0 [eth1		Cerebas sapra: In Sthernet Controll mposog mogcoegiosé	ntel Corporation 825 er M	40EM Gigabit	
Виртуальные машины Системные службы Обновление системы Системные ограничения Вебчинтерфейс Резервное колифование Выспочение компьютера Службы хілеtd Управление ключами SSL Серверы	8	3	Конфигурация: IP-адрес: Маска сети: Шлюз по умолчанию: DNS-серверы: Домены помоса:	Вручную 192.168.56.2 /24 (255.255.255.0)		۵
DHCP-сервер Сервер обновлений Сервер сетевых установок FTP-сервер Служба каталогов LDAP Прокон-сервер DNS-сервер Dom/PPI-селвер	Применит	Верн	уть	Дополнительно		

(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=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):

🍵 Альт Ли	нукс 5.0 Школы	ный Сервер   Внешние сети
Система		· · · · · · · · · · · · · · · · · · ·
Доверительные отношения	Выберите режим работы:	poyrep 0
Удостоверяющий Центр		
дата и врама Систамала мольсты	своерете внешние интерфенсы.	Cetto (Intel Corporation 82540EM Gigabit Ethernet Controller ) 192.168.0.4
Вирткальные машины		Leth1 (Intel Corporation 82540EM Gigabit Ethernet Controller ) 192.168.56.2
Системные службы		U venet0
Обновление системы		
Системные ограничения		
Вер-интерденс Резеленсе кольторании	Разрешить входящие соединени	я на внешних интерфейсах:
Выключение компьютера	CHINEH	
Службы xinetd	C. G. WORL	✓ Центр управления системой (www)
Управление ключами SSL		Система печати CUPS
Серверы		DHOP
		DNS
Censen officialeada		Передача файлов (FTP)
Сервер сетевых установск		Почтовый сервер (ЗМАР)
FTP-cepeep		LDAP
Cnyx6a katanoroa LDAP		D OpenVPN
Прокси-сервер		Почтовый сервер (РОРЗ)
LMC-cepsep		Прокси-сервер

(Рис. 13. Настройка работы сервер 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 интерне, 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).

System eth0 (default)	
Интерфейс:	Ethernet (eth0)
МАС-адрес:	08:00:27:CA:CD:C3
Драйвер:	e1000
Скорость:	1000 Мбит/с
Защита:	Нет проверки подлинност
IP-адрес:	192.168.56.54
Широковещательный адрес:	192.168.56.255
Маска подсети:	255.255.255.0
Шлюз по умолчанию:	192.168.56.2
Первичный DNS:	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 системы).

Интерфейсы			
eth0	Сетевая карта: Intel ( Controller провод подсоединён	Corporation 82540EM Gigabit Ethernet	< .
	Конфигурация:	Вручную	0
	IP-адрес: 192.	192.168.56.54	
	Маска сети:	/24 (255.255.255.0)	0
	Шлюз по умолчанию:	192.168.56.2	
	DNS-серверы:	192.168.56.2	
	Домены поиска:		
	11	(несколько значений записываются через г	пробел)

(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.

🏦 Альт Ли	инукс 5.0 Школьный Сервер   онср-сервер
Система	
Доверительные отношения	Общие настройки
удостовержидни центр Дата и время Системные журналы	Включить службу DHCP
Виртуальные машины Обновление системы	Интерфейс: eth1 (192.168.56.1 - 192.168.56.254)   \$
Резервное копирование Выключение компьютера	(максинально дотустиный диагазон адоксов)
Серверы	Начальный IP адрес: 192.168.56.20
DHCP-cepsep	Koneu-aux IP addec: [192.168.56.55
Сервер обновлений	Срок действия адреса: 1 месяц 0
Сервер сетевых установок Прокои-сервер ОрепVPN-сервер	Информация, предоставляемая клиентам
Пользователи	Шлюз по умолчанию: 192.168.56.2
Использование диска Администратор системы	Применить Вернуть

(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).

	Нов компьютера	♦ MAC-appec	٠	IP-адрес	¢	Годен до
2	NewLife	08:00:27:4x a8:6c		192.168.56.55		Thu Feb 16 12:46:37 NOVT 2012
2	junior	06:00:27:cs:cd:c3		192.168.56.54		Thu Feb 16 12:50.16 NOVT 2012

(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.

Апплет для работы с сетью	🧔 Приложения Переход Система	🥹 📃 📥 Англ	📑 🖗 🖂 02:33 🔲 ubuntu 🖉	9
Апплет для работы с сетью				
		Апплет дл	я работы с сетью	

(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»:

Название	Последнее подключение	📥 Добавить
Auto eth1	1 минута назад	
Auto eth0	1 минута назад	
		🧧 <u>У</u> далить
		₽

(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».

🛞 Измене	ние Аи	to eth0		
<u>Н</u> азвание сое	единен	ия: Auto eth0		
Подключа	ться ав	томатически		
Проводные	Защит	а 802.1х Парамет	ры IPv4 Параметр	ры ІРv6
<u>П</u> рофиль:	Вручн	ую		<b>.</b>
Адреса				
Адрес		Маска сети	Шлюз	ф Добавить
10.0.2.15	5	255.255.255.0	10.0.2.2	<u>Э</u> <u>У</u> далить
і Серверы <u>Д</u> омены г	<u>D</u> NS: тоиска:	217.8.237.53		
ID <u>к</u> лиен ⊡ Требов	га DHCi вать ад	":   ресацию IPv4 для :	этого соединения	<u>М</u> аршруты
🗹 Доступно	всем п	ользователям	<u>₿ От</u> менить	<u>С</u> охранить

(Рис. 21. Настройка сетевого интерфейса eth0)

Сетевому интерфейсу eth1 присваиваем параметры локальной сети школы:

🔘 Измене	ние Auto	eth1				
<u>Н</u> азвание со	еди <mark>нени</mark> я	Auto	eth1			
🖸 Подключа	аться <u>а</u> вто	матич	ески			
Проводные	Защита	802.1x	Параметрь	IPv4	Іараметр	ы ІРv6
<u>П</u> рофиль:	Вручнук	)				<b>.</b>
Адреса	-10				3	
Адрес 192.168.56.4		Маска сети 255.255.255.0		Шлюз 0.0.0.0	03	ф Добавить
					<u>В</u> <u>У</u> далить	
I Серверы	<u>D</u> NS:					
Домены	поиска:					
ID <u>к</u> лиен	та DHCP:					
🗹 Требо	вать <mark>ад</mark> ре	сацию	IPv4 для эт	ого соед	цинения	
0						<u>М</u> аршруты
🗹 Доступно	всем пол	ьзоват	елям	<u>ЖОт</u> м	енить	<u>е С</u> охранить

(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: ~	
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид П <u>о</u> иск <u>Т</u> ерминал <u>С</u> правка	
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	
<pre> 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</pre>	
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. Pacкомментируем cтроку net.ipv4.ip\_forward=1 и coxpaним 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
- 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</li>
- 6. Также нам понадобиться 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 <u>http://www.webmin.com/jcameron-key.asc</u>
  - 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-adpec сервера:10000 (в нашем случае <u>https://192.168.56.4:10000</u> или, если мы работаем на локальной машине — https://localhost:10000).

You mus	t enter a username and password to login to the Webmin server or 192.168.56.4
Username	ubuntu
Password	•
	Remember login permanently?

(Рис. 24. Вход в Webmin)

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

Login ubuntu	(An)	
Webmin		
System		s luenmin
Servers		3 000011111
Others		
Networking	System hostname	ubuntu.localdomain
Hardware	Operating system	Ubuntu Linux 11.04
Cluster	Webmin version	1.570
💷 Un-used Modules	Time on system	Sat Dec 3 07:19:39 2011
Search:	Kernel and CPU	Linux 2.6.38-8-generic on i686
	Processor information	Intel(R) Pentium(R) CPU P6100 @ 2.00GHz, 1 cores
🛆 View Module's Logs	System uptime	4 hours, 37 minutes
System Information	Running processes	136
Sefresh Modules	CPU load averages	0.00 (1 min) 0.03 (5 mins) 0.07 (15 mins)
O Logout	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.	

(Рис. 25. Стартовая страница Webmin)

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

Login: ubuntu Webmin	Change Language and Theme	
Backup Configuration Files Change Language and Theme Webmin Actions Log	This module can be used to change the language that modules are displayed in and the theme that controls Webr appearance, for your Webmin account only.	min's
Webmin Configuration Webmin Servers Index	Webmin Ul language Global language (English (US))  Personal choice Russian CP1251 (RU RU)	
System Servers	Webmin UI theme   Global theme (Blue Framed Theme)  Personal choice Old Webmin Theme	
<ul> <li>Others</li> <li>Networking</li> <li>Hardware</li> </ul>	Make Changes	
Cluster Un-used Modules		
Search:		
System Information		
U Logout		

(Рис. 26. Настройка русификации Webmin)

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

Login: ubuntu III Webmin III Система III Службы III Плачиса	E	webmin
Сеть	System hostname	ubuntu localdomain
Оборудование	Operating system	Ubuntu Linux 11.04
🗵 Кластер	Webmin version	1.570
💷 Неиспользуемые модули	Time on system	Sat Dec 3 07:30:56 2011
Search:	Kernel and CPU	Linux 2.6.38-8-generic on i686
	Processor information	Intel(R) Pentium(R) CPU P6100 @ 2.00GHz, 1 cores
🛆 View Module's Logs	System uptime	4 hours, 48 minutes
🕅 System Information	Running processes	136
🗳 Обновить модули	CPU load averages	0.00 (1 min) 0.01 (5 mins) 0.05 (15 mins)
🕘 Выйти	CPU usage	1% user, 2% kernel, 0% IO, 97% idle
	Real memory	496.09 MB total, 201.95 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. 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. <u>Click here</u> to have it downloaded and installed using APT.» Система сама установит необходимые пакеты:

Дисковые квоты     Меню Модуля     Установка пакета       Загрузчик Linux (GRUB)     Загрузчик Linux (GRUB)     Установка пакетов с пошещью кошанды арт-get -yforce-yes -f install dhcp3-server       Каталоги NFS     Конфигурация Sendmail     Peading package lists       Менеджер списков рассылки Мајогdomo     Pading sette information       Манедон служб МОN     The following extra packages will be installed: isc-dhcp-setwer	
Загрузчик Linux (GRUB)       Unpaska         Загрузчик Linux (LILO)       Установка пакетов с пошощью кошанды apt-get -yforce-yes -f install dhcp3-server         Каталоги NFS       Reading package lists         Конфигурация Sendmail       Building dependency tree         Менеджер списков рассылки       Reading state information         Маритор служб MON       The following extra packages will be installed:	
Sarpysuk Linux (LLO)       Установка пакетов с пошещью кошанды apt-get -yforce-yes -f install dhcp3-server         Каталоги NFS       Reading package lists         Конфигурация Sendmail       Building dependency tree         Менеджер списков рассылки       Reading state information         Маритор служб MON       The following extra packages will be installed:	
Salysank Linux (LLC)       Ycrahoska nakerose c nomoulubio komahdul apt-get -yforce-yes -f install dhcp3-server         Karanork NFS       Peading package lists         Kohdwirypauus Sendmail       Building dependency tree         Mahedawep cnuckos pacculuku       Peading state information         Majordomo       The following extra packages will be installed:         Mounton cnywfn MON       isc-dhcra-common isc-dhcra-cerver	
Каналони NFS     Reading package lists       Конфигурация Sendmail     Building dependency tree       Менеджер списков рассылки     Reading state information       Majordomo     The following extra packages will be installed:       Монитор служб MON     isc-dbrcn-common isc-dbrcn-server	
Конфитурация Sendmail Reading Package 1555 Менеджер списков рассылки Reading state information Majordomo The following extra packages will be installed: Mounton cnywf MON isc-diper-common isc-diper-center	
Meнеджер списков рассылки Majordomo The following extra packages will be installed: Mounton cnywf MON isc-dhorn-comeon isc-dhorn-cerver	
Majordomo The following extra packages will be installed:	
MOHNTON CRYWE MON isc-dhon-client, isc-dhon-server	
Wolling on we will be	
Hactpoğka Postfix Suggested packages:	
resolvconf isc-dhcp-server-ldap	
The following NEW packages will be installed:	
dcp3-server 1sc-dcp-server	
IIOTOBBIN QUADTO PTOCMAII Ine following packages will be upgraded.	
Tipokcu-cepsep Squid	
Сборщик почты Fetchmail Need to get 993 kB of archives.	
CepBep CVS After this operation, 1073 kB of additional disk space will be used.	
Get:1 http://ru.archive.ubuntu.com/ubuntu/ natty-updates/main isc-dhcp-client i386 4.1.1-Pl-15ubuntu9.1 [266 kB]	
Censen DNS BIND Get: 2 http://ru.archive.ubuntu.com/ubuntu/ natty-updates/main isc-dhcp-common i386 4.1.1-P1-15ubuntu9.1 [319 kB]	
Cappen IMAP/POD3 (Devect) Get 3 http://ru.archive.ubuntu.com/ubuntu/natty-updates/main isc-dhep-server i386 4.1.1-P1-1Subuntu9.1 [402 kB]	
General DAD Breaching ascharge	
Cepter LDAP Frechning parkages	
Cepsep OpenSLP (Reading database 148151 files and directories currently installed.)	
Cepsep PPP Preparing to replace isc-dhcp-client 4.1.1-Pl-15ubuntu9 (using/isc-dhcp-client 4.1.1-Pl-15ubuntu9.1_i386.deb	)
Cepsep ProFTP Unpacking replacement isc-dhcp-client	
Cepsep WU.FTP Preparing to replace isc-dhcp-common 4.1.1-P1-15ubuntu9 (using/isc-dhcp-common_4.1.1-P1-15ubuntu9.1_i386.deb	)
Ceppep 6as gathesk MvSQL Unpacking replacement isc-dhep-common	
Centren faz naluluz Umber faz naluluz	
PostgreSQ Selecting previously deslected package dhopserver_11.FrF130bulldu5.f_136e.ueb/	
Unpacking dhcp3-server (from/dhcp3-server 4.1.1-P1-15ubuntu9.1 all.deb)	
Concession and the set of the set	
сервер солощении запрег	

(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

Систешные парашетры	
Файл настроек сервера DHCP	/etc/dhcp/dhcpd.conf
Исполняешый файл сервера DHCP	/usr/sbin/dhcpd
Команда для запуска сервера DHCP	⊖ Программа запуска сервера ⊚ //etc/init.d/isc-dhcp-server
Кошанда для пришенения настроек	⊘ Убить и перезапустить ● //etc/init.d/isc-dhcp-server
Command to stop DHCP server	Kill process
Путь к файлу PID сервера DHCP	/var/run/dhcp-server/dhcpd
Файл аренды сервера DHCP	/var/lib/dhcp/dhcpd.leases
Тип интерфейса файлов	Debian 🔻
DHCP server version	Work out automatically

Сохранить

### (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

Подробная инфо	ормация подсети			
Subnet description	shool			_
Сетевой адрес	192.168.56.0		Сетевая маска	255.255.255.0
Диапазон алресов	192.168.56.5	- 192.168.56.45	🔲 Динамическо	e BOOTP?
			🔍 Динамическо	e BOOTP?

#### Нажимаем кнопку «Редактировать сетевой интерфейс»

Редактировать параметры клиента	Редактирование параметров клиента DHCP, относящиеся ко всем подсетям, разделяемым сетям, узлам и группам
Edit TSIG-keys	Edit TSIG-keys (used for authenticating updates to DNS servers)
Manually Edit Configuration	Edit configuration file manually text
Редактировать сетевой интерфейс	Установить сетевые интерфейсы для прослушивания сервером DHCPD при запуске.
Список арендованных адресов	Список арендованных (динамически назначенных) IP-адресов сервера DHCP.
Запуск сервера	Нажмите на эту кнопку для запуска сервера DHCP с использованием текущих настроек.

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

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

модуля 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
<del>年</del> 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 Configuracion» и в открывшемся окне вводим следующее:

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).

измене	елине А			
	аться а			
роводные	Защи	та 802.1х Парамет	ры IPv4 Парамет	гры ІРv6
<u>П</u> рофиль:	Авто	матически (DHCP)	1	'   <b>-</b>
Адреса				
Адрес		Маска сети	Шлюз	Добавить
				<b>у</b> далить
Серверы	<u>D</u> NS:			
Домены	поиска	:		
ID <u>к</u> лиен	ITA DHO	CP:		
🗹 Требо	вать а,	дресацию IPv4 для	этого соединени	я
				М <u>а</u> ршруты

(Рис. 31. Настройка получения настроек сети автоматически)

Просмотрим полученные настройки:

<u>.</u>	активные подключения	
U	Auto eth0 (default)	
	Общие	
	Интерфейс:	Ethernet (eth0)
	МАС-адрес:	08:00:27:F7:C6:C2
	Драйвер:	e1000
	Скорость:	1000 Мбит/с
	Защита:	Нет
	IPv4	
	ІР-адрес:	192.168.56.5
	Широковещательный адрес:	192.168.56.255
	Маска подсети:	255.255.255.0
	Шлюз по умолчанию:	192.168.56.4
	Первичный DNS:	192.168.56.4
	IPv6	
	Игнорировано	

(Рис. 32. Просмотр настроек сети)

Осталось только запустить браузер и проверить доступ в сеть Интернет:

🚭 Приложения Переход Система	1	Англ	<b>E 4</b>	18:23	ubuntu	$(\bigcirc)$
😣 🖨 🖨 🛛 Google - Mozilla Firefox						
<u>Ф</u> айл <u>П</u> равка <u>В</u> ид <u>Ж</u> урнал <u>З</u> акла	дки <u>И</u> нструменты	<u>С</u> правка				
🚼 Google 🛛 👫						•
📀 \gg 🛐 http://www.google.ru/			ି <b>•</b> ୯	Soogle ₹	Q	
	Go	og	е			<u>*</u>
	Поиск в Google	Мне пове:	ëT!	₩.		
iGoogle Изменить фон	Рекламны	е программы	Решения д	ля предприятий Всё о Google	Конфиденці Google.com	иалі in E I

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

### 2.3 Организация локальной сети с контролируемым доступом в сеть интерне, 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»

Xo	Центр управления YaST @ school	808
Пон <u>с</u> к	Восстановление системы	î
Программное абеспе В Оборудование	чени Системные службы (Уровень запуска)	
Система	Естонье устройства	
🥥 Сетевые устройства	OSL	-
Сетевые службы	ISDN	
1 NovellAppArmor		
🤔 Безопасность и польз	воват Модемы	
🚛 Виртуализация	Сетевые настройки	
Поддержка.	Сетевые службы	
Разное		
Гатово		

(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.

	Параметры настроики DSL-соединения
Режим РРР	
PPP over Ethernet	
	Режимозависимые настройки РРР
VPI/VCI	
	THE SECOND STREET
	Ethernet-Kapta
IC Plus IP100A Inte	tegrated 10/100 Ethernet MAC + PHY Изменить устройство
Ceresan mara	- DHCF - adher
	<u>Н</u> астроить сетевые карты
Имя или Р-адрес сер	BeDa
10.0.0 138	
Включить устройство	
Во время загрузки систе	емы 🗸
Разрешить управлени	ие устройством пользователям не-администраторам через Qinternet

(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.

		YaST2	8 9 8
Настройка сетевой н	карты		
Общий	<u>А</u> дрес	Оборудование	
Тип устройства	н	азвание Конфилбалии	
Ethernet	<u> </u>	ith2	
🔵 Без IP-адреса (для объединяем	ых устройств) 📃 Испал	ьзовать значения IBFT	
Динамический адрес	V (DHCP	обенх версий 4 и б 🖌	
<ul> <li>Статически присвоенный IP-адр</li> </ul>	ec		
Р-адрес	Маска под <u>с</u> ети	Имя <u>у</u> зла	
192.168.1.1	/24		
	(E. 200 a)		
Имя псевдонима \vee IP-адре	допол	нительные адреса	_
Имя псевдонима \vee IP-адре	допол	: ∴	
Имя псевдонима У IP-адре Добавить Редактировал	с Сетевая маска	нительные адреса.	

(Рис. 37. Настройка сетевого адреса)

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

P (4) 1	Ye512	6 6 6
Настройки сети		
Общно параметры Обхор	Именухова/295 Каршрутизация	
	Имп узла и имп домена	
лын ухин	Имн урганна	
school	(716361)	1
Измонить ныя узлачоров ОНСР		
Назнанить имя узла IP "обратной петли"		
Изменль настообке ОМЯ	Hardport in apparentiment and	
Исплоковать политику по умолнанию 🗸	( )	
	Список зерверсе имен и доменое приске	
Сертер имён 1	Домен поиска	
To the second		
Conton Hada 2		
	187	
Censer week 3		
1	10.	
di di seconda di secon		
Помещь		OTRANA I LOK

(Рис. 38. Настройка имени узла и DNS)

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

26	VaST2	808
<ul> <li>Настройки сети</li> </ul>		
Общие параметры	D6359 Икм узла/ <u>D</u> 5.5	Маршрутнаацея
Шлюз Реч по умолчание		straction
There was no build and the		11 · • •
Street State State State		
	Таблица марырунзации	
Назначение У Шлюз	Маска Устройстве Парамотры	
	[	ini i
<ul> <li>Волючить (Р-переадря</li> </ul>	Callino,	
(Datas)		The same of the second
Tronoup		OTWERE DK

(Рис. 39. Маршрутизация)

Нажимаем «ок» и «далее»

Department of the processing of the second of the sec	Выбор интернет-провайлер	a (ISP)	
Crosse Crosse	<ul> <li>percent nu chuci-uboeanteb</li> </ul>	a (13F)	
E trans Transmo Messes Messes Messes Restrondersmannn Restrondersmann Restrondersmann Restrondersmannn Restrondersma	Construction of the second sec	(poseduste)	
Antenna Instante Instante Hanger-uta Hanger-uta Hanger-uta Car Car	Closure	Line of the line o	
Transland Transland Brand Market Brand Brand Hongery Auto Hongery Brand C JA	PACT2-III	11(1)	
Tapanan Basi ani Hang Astan Jan Cananan Cananan Can	10s-saige		
Cardinal Science Scien	Tappisone,		
Hindup Carlos Consented Carlos Carlos	Devi pui		
C di A	History Bolton (2019)		
Hapel	CALL HOUSE		
Hapit			
Hingeld			
Hatel			
Hope			
. Hegelt			
Haget			
Planet			
Hogeit			
		Haget	

(Рис. 40. Выбор провайдера)

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

(e)	YaST2	303
Параметры провайдера		
idua gra nacopa -icinação 🛛 orior carà		
Имя подвайдара		) (
	APTOPRIM 1/2	
தின் பலங்களை சான	Banna	
1		
	A gearfy santamana u	apon.
Towards		Отмена Назад Далея

(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 dsl0 будет внешней зоной, eth1 внутренней.

- W	Yasitti	00
Jarytk	🔄 🚰 Настройка брандмауэра: И	нтерфейсы
Faapeulenus covelu	Интераройсь ор	тнампира
Трактеция сетция драго Шителобацияны - екрасти интелобацияны - екраст Прав из гользователя Прав из гользователя	Victoria         Victoria         Unrepue/Cr           BST732         Ciguit Etherral Control         eF1           DSL         BST732         eff           Ciguit Etherral Control         eF1           UST732         eff         eF1           DSL         Etherral Control         eF1           Ciguit Etherral Control         eF2         eF1           Ciguit Etherral Control         eF2         eF2           Ciguit Plant P100A tributes 15/150         eF2         eF2	ити трана, Грастронный з Вофранции кола Вонации кола Вонации кола Вонации кола Вонации кола Водовници кола
	Нименитьактронть.	
	Revolue	Onvena and Baree

(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 nlockmgr). 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 блокированы. 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.

₽ 🔾	YaST2	0 0 0		
— Запуск Интерфейсы - Разрешённые службы	Настройка брандмауэра: Трансляци адресов	я сетевых		
— Широковещательная рассылка — Широковещательная рассылка — Уровень журналирования — Правила пользователя	Трансляция сетевых адресов 🕑 <u>Т</u> ранслировать сети			
	Перенаправить запрос на транслируемый IP			
	Сеть источника 🗸 Протокол Преб IP Треб Port	Перенапр. на IP		
	< Добавить Удали <u>т</u> ь			
	Отме	на Назад Далее		

(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 RPCслужб.

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 RPCслужбы. Эта запись необязательна.

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

	Magi S			THE COL
– Sanyok – Virreptiońcia	😽 Настройка бран	дмауэра: Правил	а пользовател	ศ
Разрешённые службы — Трансляция сетелькадросов — Шлосковещательнае рассылка — Урован журналирования — Преволлановополосом	На Зона бра-урануара Внадния зона	строенные разрешённые гу м	озанла	
	Сель источника — Прогр сод UDP сод UDP сод ТСР сод ТСР	хол Порт наанзинениет 4433 sintouetle (7500) smtp (25) pop3 (110)	Парт источника	
	Добавать Удилиць Помощь	10	Огмена і шкал	Лалее

(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.

• Тои <u>с</u> к ()	Сетевые устройства DSL	Ì
Программное обеспечени В Оборудование	ISDN	
Система	Модемы	
Сетевые устройства	Сетевые настройки	
Novell AppArmor	Настройка сетевой карты, имени узла и маршрутизации Сетевые службы	
Безопасность и пользоват	Сервер DHCP	
О Поддержка	Сервер DNS Настройка сервера DNS	
Разное	Сервер FTP	

(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.

<ul> <li>настроика сетевои кар</li> </ul>	ты		
О <u>б</u> щий	Адрес	Оборудова <u>н</u> ие	
Тип <u>у</u> стройства	Название	конфигурации	
Ethernet	✓ eth2		
Без IP-адреса (для объединяемых ус.)	тройств) 📃 Использовать	значения iBFT	
Динамический адрес	DHCP обенха	ерсий 4 и 6 🗸	
<ul> <li>Статически присвоенный IP-адрес</li> </ul>			
[Р-адрес	Маска подсети	Имя узла	
192.168.1.2	/24	com1	
Добавить Редактировать	Удалить		

(Рис. 49. Настройка сетевой карты: Адрес)

Нажимаем «Далее». Переходим на вкладку «Маршрутизация» и вводим IP адрес нашего сервера в поле «Шлюз IPv4 по умолчанию»
Настройки сети					
Общие параметры	Обзор	Имя узла/ <u>D</u> NS	Маршрутизация		
<u>Ш</u> люз IPv4 по умолчанию				Устройст	во
192.168.1.1				eth0	~
Шлюз IPv6 по умолчанию				Устройст	80
					$\overline{\mathbf{v}}$
		Таблица маршрутизации			
Назначение 🗸 Шлюз	Маска Ус	тройство Параметры			
		1477 (1777)			
	Добав	ить Редактировать У	Далить		
Включить ІР-переадрес	сацию				
Томощь				Отмена	
[]	Рис. 50. Нас	стройка сети: Мар	шрутизация)		

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

#### 3. Установка и настройка программного обеспечения для организации контентфильтрации.

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 <u>https://ip</u>-aдрес сервера:8080.

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

譮 Алі	ьт Лину	/кс 5.0 I	Школьнь	ій Сервер	Į.	
Пожалуйста, зарег	истрируйтесь					
Учётная запись:	root					
Пароль:						
Язык интерфейса:	Русский	٥				
1	Войти	L				

(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 потребуется. Это может существенно ускорить доступ к популярным сайтам и снизить потребляемый организацией трафик.

Система			
Доверительные отношения	Основные параметры		
Удостоверяющий Центр Дата и время	Основные параметры управления прокси-се	рвером	
Системные журналы Виртуальные машины		🔲 Включить сервис прон	си-сервера
Обновление системы	Выберите режим проксирования:	Прозрачный 🔻	
Резервное копирование Зыключение компьютера	Выберите способ аутентификации:	Без аутентификации 🔻	
Серверы	Порт прокси-сервера:	3128	N
ЭНСР-сервер			3
ервер обновлений			
сервер сетевых установок		Разрешённые сети	Разрешённые протоколы
Трокси-сервер			
Точтовый сервер		применить	
OpenVPN-сервер			

(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 использование 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:

Система			
Доверительные отношения	Разрешённые сети		
Удостоверяющий Центр	Запросы из указанных сетей будут об	бработаны. Запросы из д	аругих сетей будут промгнорированы.
Дата и время			
Системные журналы			
Виртуальные машины	127.0.0.0/8 (LOCALHOST)	Сеть ІР:	192.168.56.0/24
Обновление системы	102.100.00.024 (iai1)		
Резервное копирование			(ІР-адрес/биты подсети)
Выключение компьютера			
Серверы		Комментарий:	
DHCP-сервер		lan	
Сервер обновлений			
Сервер сетевых установок		Применить	Вернуть
Прокси-сервер			
Почтовый сервер	Coanath	Vacation	
OpenVPN-сервер	COSAND	удалить	
Пользователи			
Использование диска	Назад		

(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.

Система	
Доверительные отношения	Основные параметры
Удостоверяющий Центр Дата и время	Основные параметры управления прокси-сервером
Системные журналы	Включить сервис прокси-сервера
виртуальные машины Обновление системы	Выберите режим проксирования: Обычный 🔻
Резервное копирование Выключение компьютера	Выберите способ аутентификации: Кеrberos+РАМ 🔻
Серверы	Порт прокси-сервера: 3128
ОНСР-сервер	(номер порта)
Сервер обновлений	
Сервер сетевых установок	Разрешённые сети Разрешённые протоколы
Прокси-сервер	
Почтовый сервер	Применить
Onen//PN-censen	

(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 <a href="https://192.168.56.4:10000">https://192.168.56.4:10000</a> (или <a href="https://localhost:10000">https://localhost:10000</a> — если вы работает на локальной машине). Выполним вход в систему и в разделе «Неиспользуемые модули» выберем «Прокси-сервер Squid»:

Настройки QMail Почтовый фильтр Procmail Прокси-сервер Squid	Настройка Прокси-сервер Squid
Сборщик почты Fetchmail Сервер CVS	Исполняемый файл Squid squid не существует. Если у вас установлен Squid, то исправьте пути в настройках модуля.
Сервер DHCP Сервер DNS BIND Сервер IMAP/POP3 (Dovecot)	The Squid Proxy Server package can be automatically installed by Webmin. Click here to have it downloaded and installed using APT.

#### (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:

Denus v nort v denus vermeen envid	
полный путь к файлу настроек squid	/etc/squid/squid.conf
Кошанда для запуска squid	⊖ Автоматически 💩 /etc/init.d/squid start
Кошанда для остановки squid	⊘ Автоматически
Command to apply changes	Automatic I/etc/init.d/squid restart



#### Далее укажем параметры кеша:

Меню модуля Справка		Параметры кэша Приме изме Остановка		Применение изменений Остановка Squid		
Параметры кэширо	ования и запросов					
Каталоги кэша	⊖ По умолчанию (/var/spool/squid)	Перечисленные				
	Каталог	Тип	Раз∎ер (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

Имя ACL	shoolnet	
C IP	Ha IP	Маска сети
192.168.56.0		24
URL Отказа		
Store ACL value	es in file 💿 Squid	configuration 🎯 Separat
	🔲 Just us	e existing contents of file

Сохранить

< Вернуться к Список ACL | Вернуться к меню

(Рис. 59. Создание нового acl)

На вкладке «Ограничения прокси» разрешим новому acl доступ:

Меню модуля

## Создание ограничений прокси

Применение изменений Остановка Squid

Ограничения прокс	и	
Действие	💿 Разрешить \ominus Запретить	
Совпадающие ACL	Iocalhost to_localhost localnet SSL_ports Safe_ports purge CONNECT shoutcast apache shoolnet ▼	all ▲ manager localhost to_localhost localnet ≡ SSL_ports Safe_ports purge CONNECT shoutcast ▼
Сохранить		

🝬 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:

Меню модуля Справка		Управление доступом		Применение изменений Остановка Squid	
Списки управления доступом		Ограничения прокси	Ограничения ІСР	External ACL programs	Reply proxy restrictions
Добавить огран	ичение прокси				
Действие	ACL				Переместить
🗌 Разрешить	manager localh	iost			+
🗌 Запретить	manager				¢¢
🗌 Разрешить	purge localhos	t			*↑
🗌 Запретить	purge				*↑
🗌 Запретить	!Safe_ports				¢↑
🗌 Запретить	CONNECT ISSL	ports			*↑
🔲 Разрешить	shoolnet				*↑
🗌 Разрешить	localhost				*↑
🗌 Запретить	all				Ť
Добавить огран	ичение прокси				
Delete Select	ted Restriction	s			

(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 <u>http://www.webmin.com</u>, в разделе downloads ищем rpm пакет для OpenSuse, скачиваем и устанавливаем. После установки набираем в браузере <u>https://localhost:10000</u>, 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.

Defa	ult (usually 3128) 🕚 Lister Divisi y ma/Appec IP — U All U	d below. Options fer p	ort		
Defa Hopr 3129	ult (usually 3128) Имя утла/Адрес IP АI 192 (68.6.2	d below Options for p	ort		
3129	Иня узла/Адрес IP	Options for p	ort		
3128	All 3				
3128	1921697.2	The second second second second second			
	protected and the set of the set of the	transparent			
		-			
3128		transparent			
a state and	192.168.1.1	A DESCRIPTION OF			
	- (• all -				
	-				
	100 H 10 1	1			
SSL addresses and Usually 3128) Usted below.					
Порт	Имя узла/Адрес IP	Options for p	ort		
	• All				
		_			
3	1				
• По у	молчанию	Исходящий	🖲 любой 🥥		
		адрес ТСР			
ес 🐮 Люб	uo No	Входящия	💌 любой 🥥		
		адресорр			
TIGHEN P		приема ТСР	🙂 ОС по умолчанию 🤍 🗌		
1		Allow	50 U.V.		
nesin 🖱 Да	- Her	underscore in	🗢 Да 🥌 Нет		
		hostnames?			
- Decis	Dure .				
	nd Defs Парт © Поу ес люб льные nes in © Да	I 197, 168, 1.1 All • Default (usually 3120) Uster Порт Има узла/Адрес IP • All • По умолчанию по умолчанию по умолчанию по умолчанию по умолчанию по умолчанию вес льные Вкл. • Вылл.	nd Default (usually 3128) Usted below Порт Има узла/Адрес IP Options for р АШ С По умолчанию С По умолчани		

### (Рис.63. Параметры портов и сети)

### Далее настроим параметры кэша.

Расписание заданий								
Cron	раметры каши	рования и запросов						
Резеряное Ка	талоги кэша	De une su sun la sete chate	will . Tana					
копирование		<ul> <li>По умолчанию (ver)cache/s</li> </ul>	iquid/ intepe	численны	c.	Encourse and a second s		<u>11</u>
Системный журнал		Karanor	THE		Размер	Katanoru Iro	Katanoru Zro	Паранетры
Страницы		A STATE OF A			LIMUT	уросля	уровла	COLORY INCOME.
ручеводства		/var/cache/squid	UFS	×	8192	16	256	8
Файловые системы		1	UFS		1	10		
Службы			1 area					
SpamAssassin Mail	2000.002			10040304444				
Def control Anacha	едний	• Designer the states of the	14 12	Obseki	ов на	. On unions instan	1.000	
Hen repaire pa	знер	С по унолнанию С	NO V	узел		с тар унолганию		
Sendmail 00	benta			200				
Почтовые зника	кошировать	all	Incelhort	Максин	чальное	• Пр уколчанию		
пользователей	C LUIS MCL	all manager	- Incarriese	время	0.02444.0			
Почтовый фильто		to localhest localnet	localnet1	Kamp	and the second			
Procmail								
Прекси-сервер Squid		SSL_partsSafe_ports	no-mra.					
Сборщик почты								
Fetchmail		no-mral CONNECT	informatika					
Cepsep CVS								
Cepnep DHCP		mail						
Cepter DNS BIND Ma	ксимальный	1. I 20000 200000 1 I I I	1102-0101	Максии	чальный	7. • • • • • • • • • • • • • • • • • • •	100 mm	122-0-0-0-0
Cepeep OpenSLP	зиер тела	○ По умолчанию	KU V	разнер		О По умолчанию		KE V
Cepsep SSN 3at	ipoca			заголо	вка			
Сервер баз данных				sanpoc	a			
MySQL	ximum client	· De suma ma angres	1.46	Вреия			Luc lu	
Файл-сервер Samba //ее	id-ahead gap	Contraction Contraction	in v	кэшири	ования	Contraction and the second	Sec. 10	×.
Прочев				Sanbor	a			
Сеть	vinum tenhy	PERSONAL PROPERTY AND INCOME.						
Оборудование во	dv sizes	Size (kb)   For requests mate	hing ACLs fiea	ve empt	y for all!			
Кластер					1			
Неистользуемые модули				Berner				
arch	CH3 HRDODAHUG	С Пе умолчанию	NAL V	преня	OLINOKH	С По умолчанию		
50	ODCDEN DNS	CE CONTOURNED BESTELLE		провер	KH DNS		· · · · · · · · · · · · · · · · · · ·	
Re Re	CM8			Backs				
View Module's Logs	млания	🕙 Пе умолнанию 🔾 👘	Hac Q	ожила	HARN.	. По умолчанию	0	ic v
Sector Information Y 100	слинения			чтення				
	225							

(Рис.64. Параметры кэша)

Заполним таблицу согласно рисунку и нажмем сохранить.

Использование памяти.

A - Ka neamost int	tps://ocainostiloove		-5.*	C M + For the workgroup Pist	12Here II
Процесс А инициализации lint) Процессы Расписание заханий	Меню модуля Справка	Использо	вание памяти	Octa	Трименение маменений новка Squa
Расписание заданий	Параметры использ	ования паняти и диска			
Резервное копирование Системный журнал	Ограничение использования памяти	— По умолчанию 🕚 256 <u>М6 у</u>	Размер каша У FQDN	🕖 По умолчанию 🕚 🔟	(
Страницы руководства Файловые системы	Верхняя граница использования диска	🕞 По унолчанию 🕚 95 🗌 %	Нижияя граница использования диска	🕖 По умолчанию 🕑 😥 🥱	
E Службы SpamAssassin Mail Filter	Максинальный разнер кэшируеного объекта	По унслиания (С) (КС	Размер кзшировання адреса IP	😂 Пе умолчанию 🙏 🔟 2024 — 3	пементы
Kondurypayus Sendmail	Верхняя граница использования кэша IP	👃 По умелчанию 🕚 😏 🐂	Нижняя граница использования кэша IP	💛 По умолчанию 🐮 😡 🛸	
пользователей	Политики замены диска	По уполчанию	Политики замены	По умолчанию	×
Procmail Прокси-сервер Squid Сборцик почты Рессіятаl	Сохраните Вернуться к меню	squid			

(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.

🏟 🧼 🚷 localhost htt	ps://localhos	t:10000		ି 🗙 ୯ ୯ 🖳 🔊 🗸 · f	or the workgroup MSOSH <b>M</b>
Процесс инициализации linit) Процессы Расписание заланий	Меню моду. Справка	ля	Управление дост	упом	Применение изменений Остановка Squid
Расписание заданий	Списки у	правления доступом	Ограничения прокси Ограничения ІСР	External ACL programs	Reply proxy restrictions
Cron	ling	Тип	Соврадение		
Резервное	manager	Destor on UPI	cache object		
копирование	Incalhoet	A ROAC K RINGHT 3	127.0.0.1/821		
Системный журнал	to localhos	tAppec Raficensens	127.0.0.0/8.0.0.0/321		
Страницы	localnet	Апрас и пианта	102 168 1 0/24		
руководства	localnet1	Адресклиента	192.168.0.0/24		
Файловые системы	CCL north	Dept 101	1/12		
Службы	Safe ports	Dear URL	445		
SpamAssassin Mail	Sale_ports		21		
Filter	Sale_porca	Berungsuse supervision	and component i mrim(0,018) maily nu		
Be6 cepsep Apache	no-mral	Регулярное выражение и	seb cepsepa-i mrimt\ mail.ru		
Конфигурация	Cofe porte	Перт ЦО			
Sendmail	Sale_ports	Deer UDI	70		
Почтовые ящики	Safe ports		210		
пользователей	Sale_ports	Dear URI	1025 65535		
Почтовый фильтр	Safe ports	Deet UDI	1015-05555		
Dearce contran Sauid	Safe_ports	Deet URI	100		
Проксичеервер зации	Sale_ports		400		
Eetchmail	Safe ports	Dept URI	777		
Cephen CVS	CONNECT	Sadboc Matora	CONNECT		
Capped DHCP	Sofa porto	Барт ЦВІ	7500		
Cepsen DNS BIND	Safe ports	Deer URI	1422		
Cepses OpenSLP	Sale_ports	Deer URI	4433		
Censen SSH	Safe ports	Deet UPI	110		
Сервер баз данных	informatika	A Deck Breuts	103 169 1 4 103 169 1 19/33		
MySOL	mormalika	Адресклиента	im mail ru im1 mail ru im2 ma	ul nu lim3 mail ru lim4 mai	l ru iim5 mail ru iim6 mail ru
Файл-сервер Samba	mail	Имя узлавеб-сервера	jim7 mail ru jim8 mail ru jim9 m	ail ru jim10 mail ru jim11	mail ru jim12 mail ru
Прочее	Costasking	HORADO ACI External Prove			
Сеть	создание	External Frogr	V		

(Рис. 66. Управление доступом)

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

Адрес клиента	ACL		
Имя ACL C IP	Ha IP	Маска сети	
URL Отказа Store ACL value	s in file 💽 s	quid configuration O Separate file	] [

(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**.

Действие	ACL	Перемести
Разрешить	manager localhost	+
Разрешить	manager	<b>↓↑</b>
Запретить	!Safe_ports	<b>↓</b> ↑
Запретить	mail	<b>↓↑</b>
Запретить	no-mra	<b>↓</b> ↑
Запретить	no-mral	††
Запретить	CONNECT ISSL_ports	††
Разрешить	localnet	₩Ť
Разрешить	localnet1	¢¢
Разрешить	localhost	<b>↓</b> ↑
Разрешить	localhost	<b>↓</b> ↑
Запретить	all	Ť

(Рис. 68. Настройка ограничений прокси)

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

Совпадающие ACL	all manager localhost localnet localnet localnet SSL_ports Safe_ports	ACL all manager localhost to_localhost localnet localnet1 SSL_ports Safe_ports
-----------------	--	---

- 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. Проксисервер 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 настройки производятся аналогично).
- 2. В главном меню «Правка» «Настройка» «Дополнительные» вкладка «Сеть» -

)	Настройки Firefox						
(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			Вангожания			Ö	
Общие Сет	ъ Обновл	ения Шифрова	ние				
Соедине	ние						
Настрой	те параме	тры соединения	я Firefox с Интер	онет		😟 На <u>с</u> троить)	
		(D	II		-)		

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

<ul> <li>Без прокси</li> <li>Автоматически определять на</li> <li>Использовать системные наст</li> <li>Ручная настройка сервиса про-</li> </ul>	стройки прокси для этой с ройки прокси «си:	сети	
Н <u>⊤</u> ТР прокси:	192.168.0.2	П <u>о</u> рт:	3128 🛟
	🗹 Использовать этот про	кси-с <u>е</u> рвер для всех пр	отоколов
SS <u>L</u> прокси:	192.168.0.2	Порт: (	3128 🗘
ЕТР прокси:	192.168.0.2		3128
<u>G</u> opher прокси:	192.168.0.2	Порт: (	3128
Узел S <u>O</u> CKS:	192.168.0.2	Пор <u>т</u> :	3128
	O SOCKS <u>4</u> ● SOCKS <u>5</u>		
Не использовать прокси <u>д</u> ля:	localhost, 127.0.0.1, 192.1	68.0.0/24, asosh2.lan	
OURL автоматической настройки	Пример: .mozilla-russia.org и сервиса прокси:	, .net.nz, 192.168.1.0/24	ţ
O URL автоматической настройки	и сервиса прокси:	C	О <u>б</u> новит

(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

- 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)
```

- 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-aдрес cepвepa/cgi-bin/login.cgi Имя пользователя: root

Пароль: root

Админ	root
Пароль	
	Войти в систему

(Рис. 73. Вход в панель управления NetPolice)

 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

	CHINCOK				
администраторов					
Имя	Действие				
admin	Изменить пароль				

Тип	Название	Родители	Действие
General	admin		Подробно
General	teacher		Подробно
General	student	user	Подробно
Custom	my_student	student	Подробно Редактировать Удалить
Custom	my_teacher	admin teacher	Подробно Редактировать Удалить
General	user	student	Подробно

#### Пользователи и роли

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

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

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

Система	Новая учётная запись:	Создать
Доверительные отношения Удостоверяющий Центр Дата и время Системные журналы	student	✓ Учётная запись
Виртуальные машины Обновление системы Резервное копирование Выключение компьютера	user	Системное имя: Фамилия: Имя: Отчество:
Серверы DHCP-сервер Сервер обновлений Сервер сетевых установок		Пароль: Создать автоматически (введите фразу) (повторите фразу)
Прокси-сервер		<ul> <li>Работа</li> </ul>
OpenVPN-сервер		<ul> <li>Электронная почта</li> </ul>
Пользователи		<ul> <li>Дополнительная информация</li> </ul>
Использование диска Администратор системы Пользователи	,	Сохранить параметры Удалить пользователя

(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) интернетресурсов, 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 запрещённый ресурс (например, porno.ru). Страница заблокирована фильтром NetPolice! (при условии, что браузер настроен на работу с прокси-сервером)

# Страница заблокирована фильтром NetPolice! Сообщить о неверной категоризации ресурса

Найти

(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
21 юмор	студентам
22 интерьер	54 убийства, насилие, трупы
23 доступ в интернет	110 онлайн-казино
24 юридические услуги	102 социальные сети
25 литература	57 терроризм
26 СМИ	58 торговля
27 машиностроение	108 нижнее белье, купальники
28 металлургия	109 обеспечение анонимности, обход
29 мобильная связь	контентных фильтров
30 музыка	103 службы обмена сообщениями
31 общественные организации	104 файлообменные сети и сайты
113 компьютерные игры	106 табак
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 вебсайтам. 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, сводиться 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:
  - 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:

<ul> <li>О Автоматиче</li> <li>О Использова</li> </ul>	ески определять на ать системные наст	строики прокси для этои се ройки прокси	ти	
● Ручная наст	гройка сервиса прон	кси:		
	НТТР прок <u>с</u> и:	192.168.56.2	П <u>о</u> рт: [	8081
2		Использовать этот прок	си-с <u>е</u> рвер для всех пр	отоколо
2	SSL про <u>к</u> си:	192.168.56.2	Порт: [	8081
	ЕТР прокс <u>и</u> :	192.168.56.2		8081
	У <u>з</u> ел SOCKS:	192.168.56.2	TopI:	8081
		O SOCKS 4 @ SOCKS 5		
Не исполь:	зовать прокси <u>д</u> ля:	localhost, 127.0.0.1		
		Пример: .mozilla-russia.org, .	net.nz, 192.168.1.0/24	

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

6) Проверяем работу контент-фильтра. Для этого введем в адресной строке браузера ресурс, не соответствующий задачам образования, например <u>http://www.dosug.cz</u>. 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 помеченому как содержащий, материал, который считается несоответствующим или инфицированным вирусами.
	Если у Вас есть вопросы обратитесь к системному администратору сети вашей организации .
Ваша организация	изготовитель <u>DansGuardian</u>

(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:
  - $\circ$  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:
  - 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:

	Параметры соединения		
астройка прокси для доступа в	Интернет		
○ Б <u>е</u> з прокси			
○ А <u>в</u> томатически определять на	стройки прокси для этой сети		
○ Испо <u>л</u> ьзовать системные наст	ройки прокси		
• Ручная настройка сервиса про	кси:		
НТТР прок <u>с</u> и:	192.168.56.4	П <u>о</u> рт:	8080 🗘
	☑ Использовать этот прокси-серв	ер для всех протоколов	
<mark>SSL про<u>к</u>си:</mark>	192.168.56.4	Ποϼτι	8080
FTP прокс <u>и</u> :	192.168.56.4	Порт.	8080
У <u>з</u> ел SOCKS:	192.168.56.4	Порт	8080
	O SOCKS 4 @ SOCKS 5		
Не использовать прокси для:	localhost, 127.0.0.1		
	Пример: .mozilla-russia.org, .net.nz	, 192.168.1.0/24	
<ul> <li>URL автоматической настройк</li> </ul>	и сервиса прокси:		
		Go	<u>бновить</u>
<u>ө</u> С <u>п</u> равка		🖲 Отмена	<₽́ОК

(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 <u>http://www.dosug.cz</u>. Если все настроено верно, то браузер выдаст следующее сообщение:



(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 отсекать 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 фильтрования 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
- <МРЗ> 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 <u>http://192.168.0.4/ban/1x1.gif</u>

И разместить соответствующие файлы замены в директории веб-сервера. Файлы замены скачать можно здесь: <u>http://www.rejik.ru/index\_ru\_11\_1.html</u>.

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 смыл 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 <u>http://www.rejik.ru</u>, 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 НТТР)



(Рис. 82. Запуск http сервера)

лушать порты и адреса	Magneter	cepseua	Основной удел		Ухлы		
						- W - W	
	Пыклопена		служьани п				
	• Включено						
c	лушать на порт	ax					
1	Серевой аврес	× Dent				-	
i	Ble cupect	80					
	Rafianet.	Pensytamast	1 Vesterer 1				
	Добданть	Редактуровать					
	Дабалить Открыть пор	Редактуровать т в бранмаузов	и матеции Настосійни бра	ндчауара			

(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: <u>http://www.rejik.ru/index\_ru\_11\_1.html</u>
- 3. Проверяем доступность этих файлов (<u>http://localhost/www/porno.html</u>)
- 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 <u>http://www.rejik.ru/index ru 11 1.html</u>)
- 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.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 <u>http://rejik.ru</u>.

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 <u>http://localhost/www/whitelist.html</u> 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 (<u>http://catalog.iot.ru/ http://www.spo.akipkro.ru/index.php/whitelist.html</u>)
- 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:

🏦 Альт Ли	інукс 5.0 Шк	ольн	ый Сервер	О Прокси-сервер	(Настройка
истема	Витючить сбор даные с	ED LINE CHIP	нира: 🗷 Примения	6	
арадотонеронацие цанета дата и оржна Он технони мурилон Бата и оржна Он технони мурилон Он открыто надачна Он открыто и открытена Оностранов и открытена Каралование и открытена Серемона	Период проваз данно. Попызиванны — еее пол С. — есейты итипе: 100.24 МБ — Показать	D XODOC DODATEAN	аргия С) • С)		
OHCP-cepted	Crakcel califor noted	объем 🗅	на дату		
Сервер обновления Сервер селения установся:	URD IP- apper		7praduen: 0	Calif. Lowers	Result increasers targets
poszie-cepesp	son-th		15.89 MB	safebrowsing-caute google.com	 13.07.2011 16.18/58
pervPti-cepiedr	intelan		10.12 MB	safebrowsing-cache google com	24 26 3011 17 16 02
OALONPAS CADINID :	kon-dy		3.50.448	www.pandex.nz	13.07.2011 10.24:37
	ann du		32546	shisten: narod ru	an or serve as easily
ользователи	and the second sec		A LOUIS	V221525825920013972411	03.05.20111.03.57
ользователи	ion-de		2.16.305	tagport attinus ru/ A43	17.06.2011 16 17:01
олизователи спользованне диска вивнистратор системы	kon-dy		2.03 MB	support attinue rul 443 www.intelcon.ru	17 06.3011 14 17 01 14 07 2011 14 19 41
юлезоватили спользованне диска дивнистратор систены осъзоватили	kan-da kan-da kan-da		2.03.MB 1.03.MB 1.82.M6	tugpert attinus ry AKI www.intekon.ru ech-SS.umozna	17 26 201 11 15 37 17 26 201 10 17 01 14 27 201 14 10 41 03 26 2011 12 16 45

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

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

Устанавливаем программу:

#### **#apt-get install sarg**

Настройка sarg также сводиться 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-aдpec cepвepa/squid-reports/ в следующем виде:



#### Сатистика работы пользователей в сети Интернет

Период	Дата создания	Пользователей	Байт	Федняя
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	Eri Apr 29 15:36:35 NOVST 2011	4	3,278,726	819,681

Стенерирован 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)



			Сатистии	а работ	ты пол	asonate	лей в с	ети Интерне	T		
				Г	ериод: 20	0113ul01-20	11Jul01	CANADA CANADA CONTRACTOR AND			
				OT	сортиров	ano: BYTES	5, reverse				
						Topuser					
Fan	2										
op	snes	-									
	ты и	Гользователи									
	rens	ication Pandres				(					
No		Пользователь	Подключений	Байт	%Байт	IN-CAC	HE-OUT	Общее время	Миллисек.	%Время	Лимит
1	5	kon-dr	22	210,108	73.90%	30.41%	69.59%	00:00:44	44.191	70.54%	
2	5	192.168.56.254	9	74.191	26.10%	0.00%	100.00%	00:00:18	18,460	29.46%	i i
		Bcero	31	284.299		22.48%	77.55%	00:01:02	62.651		
		Средняя	15	142.149		1		00:00:31	31.325		

Сгенерирован sarg-2.2.5 Mar-03-2008 на Jul/01/2011 16:05

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

	C	атистика раб	боты по 20113ы01	льзоват	телей в	сети Ин	тернет		
	0	гсортировано: ВУ	TES. revers	e					
	_			View Orse	r				
	Amera	Полганиций	Four E a dire	нит превыи	IN-CAC	HELOUT	Ofman analys	Munnucar	% Baawa
а	www.valuehost.ru	6	88,729	42,23%	0.00%	100.00%	00:00:03	3.587	B.12%
ap.	www.mozillamessaging.com	2	66.151	31.48%	96.59%	3.41%	00:00:01	1.504	3.40%
	www.intekom.ru	2	32.930	15.67%	0.00%	100.00%	00:00:09	9.290	21.02%
-	live.mozillamessaging.com:443	2	12.724	6.06%	0.00%	100.00%	00:00:25	25.604	57.94%
-	ocsp.digicert.com	4	4.812	2.29%	0.00%	100.00%	00:00:01	1.761	3.98%
ъ	live.mozillamessaging.com	2	2.010	0.96%	0.00%	100.00%	00:00:01	1.898	4.29%
ъ	intekom .ru	2	1.626	0.77%	0.00%	100.00%	00:00:00	277	0.63%
ъ	autoconfig.intekom.ru	2	1.126	0.54%	0.00%	100.00%	00:00:00	270	0.61%
	Bcero	22	210.108	73.93%	30.41%	69.59%	00:00:44	44.191	70.59%
	Средняя	15	142.149				00:00:31	31.325	50.04%

Сгенерирован sarg-2.2.5 Mar-03-2008 на Jul/01/2011 16:05

# (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:





В разделе Report Style укажем язык формирования отчета Russian\_windows1251 и заголовок отчета «Отчет работы пользователей в сети Интернет»:

Меню модуля

## Report Style

Report language	Russian_windows1251 🗢	
Report character set	Windows-1251	
Report title	О По умолчанию 🖲 Отчет работы пользователей в сети Интернет	
Title color	О По умолчанию 💿 green	
Report body font	О По умолчанию 💿 Tahoma,Verdana,Arial	
Header color	О По умолчанию 💿 darkblue	
Header background color	О По умолчанию 💿 blanchedalmond	
Header font size	• По умолчанию (9рх) •	
Text color	○ По умолчанию ● #000000	
Text background color	О По умолчанию 💿 lavender	

(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 -1 /var/log/squid/access log
SARG: Unknown option language Russian\_windows1251

.. done

View completed report.

속 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



С 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



놓 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: <u>http://lightsquid.sourceforge.net/</u>)
- 3. Делаем скрипты программы исполняемыми.

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

Файл	Правка	Вид	Закладки	Настройка	Справка	
school :	/srv/www	r/htdoo	cs/stat #	chmod +x *.e	cgi.	î
			(Рис. 93	3. Ввод ком	анды chmod +x *.cgi)	
Файл	Правка	Вид	Закладк	и Настройка	а Справка	
school	l:/srv/w	w/htd	ocs/stat a	≇ chmod +x *	4.pl	Î
			( <b>-</b> 0			

(Рис. 94. Ввод команды chmod +x \*.pl)

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

perl	<ul> <li>Пои<u>с</u>к</li> </ul>	✓ Пакет		Заключение	Устано	
		🗸 apache	2-mod perl	Embedded Pe	2.0.4-5	
2.29		ddclien	t	APerl Client to	. 3.8.0-1	
Поиск	B	🔽 exiftool		A Highly Custo	. 8.40-3.	
/ Имя		🔽 libpcre(	)	A library for Per.	8.10-4	
<u> </u>		🔽 libpcred	pp0	A library for Per.	8.10-4	
🖊 <u>К</u> лючевые слова		🔽 libpcrep	osix0	A library for Per.	8.10-4	
/ Итог		🔽 limal-ni	s-server-perl	LIMaLNFS S	1.6.1-9	
2		🔽 limal-p	erl	LiMaL - Core L.,	. 1.6.1-1	
_ Оп <u>и</u> сание		🔽 pattern:	s-openSUSE-devel_perl	Meta package	. 11.4-6	
PPM "Provides"		🔽 pcre-de	vel	A library for Per.	8.10-4	
		pcre-do	c	A library for Per.	8.10-4	
_ RPM "Re <u>q</u> uires"		pcre-to	ls	A library for Per.	8.10-4	
Список файлов		✓ peri		The Perl Interp.	5.12.3	
		perl-Arc	hive-Zip	Provide an inte.	. 1.30-1	
		peri-Au	nen-SASL	SASL Authenti	2.1401	
жи <u>м</u> поиска:		< peri-Be	rkeleyDB	Perlextension.	. 0.43-4	
одержит	<b>v</b>	Описани <u>е</u>	Технические данные	Зависимости Верси	и с <	
С учётом регистра		perl - The Perl interpreter perl - Practical Extraction and Report Language Perl is optimized for scanning arbitrary text files, extracting information from those text files, and printing reports based on that information. It is also good for many system management tasks. Perl is intended to				
		be practical (tiny, elegar	(easy to use, efficient, an t, and minimal).	d complete) rather than l	peautiful	

(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 lighsquid.cfg и правим пути в секции GLOBAL VARIABLES

="/srv/www/htdocs/stat";
="/srv/www/htdocs/stat/tpl";
="/srv/www/htdocs/stat/lang";
="/srv/www/htdocs/stat/report";
="/var/log/squid";
="/srv/www/htdocs/stat/ip2name";

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

\$lang ="ru";

- Закрываем и сохраняем. Теперь с помощью скрипта check-setup.plможем 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
  - 192.168.1.2com1192.168.1.4com2192.168.1.5com3192.168.1.6com4192.168.1.7com5192.168.1.8com6

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				Популяр	ные сайты	Всего	Групі
					Ī	од	ГОД	ГОІ
	01	01 02 03 04 05 06 07 08 09 1 0 1			ME	МЕСЯЦ	MEC5	
Дата	Группа	Пользователей	Превысили	Байт	В среднем	Cache Hit %		
<u>31 Май 2011</u>	груп.	25	2	641.2 M	25.6 M	3.25%		
<u>30 Май 2011</u>	груп.	19	2	597.2 M	31.4 M	5.01%		
<u>29 Май 2011</u>	груп.	3	0	3.3 M	1.1 M	0.00%		
<u>28 Май 2011</u>	груп.	17	0	94.0 M	5.5 M	8.10%		
<u>27 Май 2011</u>	груп.	18	2	528.0 M	29.3 M	3.88%		
<u>26 Май 2011</u>	груп.	18	3	809.5 M	45.0 M	3.90%		
<u>25 Май 2011</u>	груп.	25	1	438.8 M	17.6 M	9.26%		
<u>24 Май 2011</u>	груп.	33	1	796.3 M	24.1 M	15.63%		
<u>23 Май 2011</u>	груп.	27	2	1.2 G	44.9 M	2.49%		
<u>22 Май 2011</u>	груп.	2	0	3.0 M	1.5 M	0.04%		
<u>21 Май 2011</u>	груп.	27	1	468.1 M	17.3 M	19.38%		
<u>20 Май 2011</u>	груп.	30	5	2.6 G	89.6 M	4.47%		
<u>19 Май 2011</u>	груп.	33	3	2.4 G	74.2 M	3.16%		
<u>18 Май 2011</u>	груп.	38	4	1.8 G	47.8 M	7.92%		
<u>17 Май 2011</u>	груп.	33	2	900.4 M	27.3 M	9.86%		
<u>16 Май 2011</u>	груп.	32	3	956.2 M	29.9 M	14.20%		
<u>15 Май 2011</u>	груп.	4	0	3.3 M	862 878	0.00%		
<u>14 Май 2011</u>	груп.	5	0	7.4 M	1.5 M	12.07%		
<u>13 Май 2011</u>	груп.	38	1	1.1 G	28.3 M	8.97%		
<u>12 Май 2011</u>	груп.	39	3	1.7 G	43.9 M	15.07%		
<u>11 Май 2011</u>	груп.	34	5	1.2 G	37.4 M	15.15%		
			2					

### (Рис. 96. Главная страница lightsquid)

		Цата: 29 Сен 20	11 (Обновле	но :: 20:46 :: 2	2 OKT 20	)11)	
По	пулярні	<u>ые сайты</u> (отчёт)	1				
Kт	о скачал	<u>і БОЛЬШИЕ фай</u>	<u>лы</u> (отчёт)				
N⁰	Время	Пользователь	Ф.И.О	Соединений	Байт	%	Группа
1	Q	192.168.0.48	geograf-t	5 327	660.9 M	43.7%	2
2	Q	192.168.0.33	Bbiblioteka	5 492	174.1 M	11.5%	2
3	O	192.168.0.52	BUHGALTER	1 111	135 <b>.</b> 4 M	8.9%	2
4	Q	192.168.0.45	glavbuh	1 041	95.2 M	6.3%	2
5	Q	192.168.0.37	obj-t	1 549	67.8 M	4.4%	2
6	Q	192.168.0.7	Kom4	3 460	37.4 M	2.4%	2
7	Ø	192.168.0.3	Admin	6 833	33.9 M	2.2%	2
8	Q	192.168.0.36	izo	988	32.7 M	2.1%	2
9	Q	192.168.0.41	uchitelskaya2	575	26.3 M	1.7%	2
10	O	192.168.0.9	Kom6	2 587	26.3 M	1.7%	2
11	O	192.168.0.6	Kom3	3 387	25.5 M	1.6%	2
12	Q	192.168.0.12	Kom9	2 895	24.8 M	1.6%	2
13	Q	192.168.0.4	Kom1	3 340	24.7 M	1.6%	2
14	Q	192.168.0.13	Kom10	2 037	20.7 M	1.3%	2
15	Ø	192.168.0.15	?	1 032	19.3 M	1.2%	2
16	Q	192.168.0.50	Kom	254	14.7 M	0.9%	2
17	Q	192.168.0.5	Kom2	1 991	14.3 M	0.9%	2
18	Q	192.168.0.10	Kom7	1 099	10.6 M	0.7%	2
19	O	192.168.0.44	zavuch	1 574	10.1 M	0.6%	2
20	U	192.168.0.47	istoriya-t	1 226	9.8 M	0.6%	2

(Рис. 97. Отчет по дате)



Отчёт по использованию интернета, прокси-сервер Squid.



(Рис. 98.	Отчет в	виде	графи	xa)
-----------	---------	------	-------	-----

	On	чёт по	испол	ьзованию и	нтернета,	прокси-сер	овер S	quid.	_
				целико	M MEC	ЯЦ			
				Стчётный п	ернод: Дек 20	011			
Ne	время	График	месяц	Пользователь	Ф.И.О	Соединений	Байт	%	Итого
1	U	tila		192.168.0.41	uchitelskaya2	7 445	3.1 G	20.5%	3.1 G
2	10	16	IMI	192.168.1.13	Kom10	9 558	3.1 G	20.0%	6.2 G
3	C	<b>ulla</b>	IMI	192.168.0.40	uchitelskaya1	4 643	1.7 G	11.3%	8.0 G
4	Ø		[ <u>M</u> ]	192.168.0.36	izo	62 827	1.3 0	8.6%	9.3 0
Б	U	d	<u>[M]</u>	192.168.0.48	geograf-t	9 479	458.9 M	2.9%	9.7 G
6	Ø	<b>di</b> la	[ <u>M]</u>	192.168.1.6	Kom3	23 294	413.4 M	2.6%	10.2 G
7	Q		[M]	192.168.1.3	Kom	14 352	403.5 M	2.5%	10.5 G
δ	C	<b>M</b>	IMI	192.168.0.35	russ1	18 809	395.8 M	2.5%	10.9 G
9	0	da	[ <u>M]</u>	192.168.0.3	Admin	40 014	318.8 M	2.0%	11.2 G
10	O	<b>s</b> lu	[ <u>M]</u>	192.168.0.33	Bbiblioteka	1 199	311.3 M	1.9%	11.5 G
11	Q		[M]	192.168.0.39	kab6	9 669	309.4 M	1.9%	11.9 G
12	١		[M]	192.168.1.5	Kom2	14 466	305.7 M	1.9%	12.1 G
13	C	ille -	[M]	192.168.1.4	Kom1	19 345	275.1 M	1.7%	12.4 G
14	0		[ <u>M]</u>	192.168.0.52	BUHGALTER	12 374	272.0 M	1.7%	12.7 G
15	Ū	dla	[ <u>M]</u>	192.168.0.49	kab2-t	6 039	257.6 M	1.6%	12.9 G
16	۲	<b>s</b> la	[M]	192.168.0.15	test	2 934	249.3 M	1.5%	13.2 G
17	C		[M]	192.168.0.47	istoriya-t	5 926	247.5 M	1.5%	13.4 G
18	Ø	<b>pile</b>	IMI	192.168.1.9	Kom6	12 565	230.3 M	1.4%	13.6 0
19	0	uila	[M]	192.168.0.14	inyaz1	7 287	204.4 M	1.3%	13.8 G
20	Q	<b>B</b> la	[ <u>M]</u>	192.168.1.10	Kom7	12 335	203.0 M	1.2%	14.0 G
21	171	ell.	IMI	102 168 0 37	ohit	10 594	199.4 M	1.2%	1420
21	M	-	IMI (	192 168 0 37 Рис. 99. С	она	10 894 месяц)	199 4 M	1.2%	1420

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: 10 \* \* \* /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 контентфильтрации, 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: <u>http://448dmg.ru/dhcp-server-nubuntu-278</u> (Дата обращения 13.12.2011 ).
- 2. LightSquid Home Site : Installs: [сайт]. URL: <u>http://lightsquid.sourceforge.net/Installs.html</u> (Дата обращения 13.12.2011).
- 3. NetPolice. Руководство по установке и эксплуатации: [сайт]. URL: <u>http://netpolice.ru/filters/altlinux/help/</u> (Дата обращения 13.12.2011).
- 4. Open-SUSE.RU: [сайт]. URL:<u>http://open-suse.ru/modules/smartsection/</u> (Дата обращения 13.12.2011).
- Portal:Документация: [сайт]. URL: <u>http://ru.OpenSuse.org/Portal:%D0%94%D0%BE %D0%BA%D1%83%D0%BC%D0%B5%D0%BD</u>
  %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 poyrepa (DansGuardian): [сайт]. UPR:<u>http://interface31.ru/tech\_it/2010/03/ubuntu-server-nastraivaem-kontent-fil-tr-routeradansguardian.html</u> (Дата обращения 13.12.2011).
- 8. Ubuntu-ru: [сайт]. URL: <u>http://ubuntu.ru</u> (Дата обращения 13.12.2011)/
- 9. Webmin система на кончиках пальцев: [сайт]. URL: <u>http://habrahabr.ru/blogs/linux/72325/</u> (Дата обращения 13.12.2011).
- 10. Альт Линукс 5.0 Школьный: [сайт]. URL: <u>http://www.altlinux.ru/products/5th-platform/school-box/</u> (Дата обращения 13.12.2011).
- 11. Настройка SQUID с помощью Webmin: [сайт]. URL: <u>http://break-</u> <u>people.ru/cmsmade/index.php?page=unix\_webmin\_practice\_squid\_webmin</u> (Дата обращения 13.12.2011).
- 12. Настройка фильтра NetPolice DNS (Для Ubuntu): [сайт]. URL:<u>http://rub-educ.ru/dock/informat/98-nastroyka-filtra-netpolice-dns.html</u> (Дата обращения 13.12.2011).
- 13. Подключение NetPolice DNS: [сайт]. URL: <u>http://www.netpolice.ru/filters/dns-filter/connect/</u> (Дата обращения 13.12.2011).
- 14. Сайт, посвященный проблеме блокирования рекламы, порно-сайтов, mp3 и.т.д. средствами прокси сервера SQUID: [сайт]. URL: <u>http://www.rejik.ru/</u> (Дата обращения 13.12.2011).
- 15. Система контентной фильтрации. На базе Ubuntu: [сайт]. URL:<u>http://oivt.ru/blog/sictema-kontentnoy-filtracii-na-baze-ubuntu</u> (Дата обращения 13.12.2011).
- 16. Установка и настройка Lightsquid в Debian Lenny: [сайт]. URL: <u>http://www.youisbee.ru/head/25-linux/69-lightsquid</u> (Дата обращения 13.12.2011).
- 17. Шлюз Интернета на базе Ubuntu-Server: [сайт]. URL: <u>http://help.ubuntu.ru/wiki/sharing\_internet</u> (Дата обращения 13.12.2011).