**Лабораторная работа №13.**

**Прокси-сервер в Linux.**

**Цель** – установить, настроить, изучить работу прокси-сервера.

Squid – 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 неблокируемый процесс ввода/вывода. Используется в UNIX-системах и в операционных системах семейства Windows NT.

Имеет возможность взаимодействия с Active Directory Windows Server путём аутентификации через LDAP, что позволяет использовать разграничения доступа к интернет-ресурсам пользователей, которые имеют учётные записи на Windows Server, также позволяет организовать «нарезку» интернет трафика для различных пользователей. Сервер Squid развивается в течение уже многих лет. Обеспечивает совместимость с большинством важнейших протоколов Интернета

**Задание 1**. Установите и выполните начальные настройки squid.

1. Для установки squid запустите в терминале следующую команду:

*sudo apt-get install squid*

1. Конфигурация для squid находится в файле /etc/squid/squid.conf.
2. Измените правила. Для аутентификации пользователей добавьте следующие строки:

auth\_param basic program /usr/lib/squid/ncsa\_auth /etc/squid/internet\_users

auth\_param basic children 5

auth\_param basic realm Enter Login/Password

auth\_param basic credentialsttl 2 hours

auth\_param basic casesensitive off

В директории /usr/lib/squid/ncsa\_auth находится программа, для аутентификации; в директории /etc/squid/internet\_users – список пользователей и их пароли в зашифрованном виде. Текст «Enter Login/Password» обозначает приглашение к аутентификации.

1. Добавьте строку http\_access allow localnet. Это имя правила. Теперь напишите сами правила:

alc localnet src 10.0.0.0/8 #RFC1918 possible internal network

alc localnet src 172.16.0.0/12 #RFC1918 possible internal network

alc localnet src 192.168.0.0/24 #RFC1918 possible internal network

1. Аналогичным образом добавим правило с именем «password» и его описание:

acl password proxy\_auth REQUIRED

1. После этого сохраняем файл-конфигурации и перезапускаем squid следующей командой:

*sudo service squid restart*

**Задание 2**. Проверьте работу нашего прокси-сервера. Например, создайте ещё одну виртуальную машину с любой операционной системой. К примеру, будем использовать Windows XP.

1. Поменяйте настройки виртуальной машины с Linux Ubuntu: в категории «Сеть» добавляем второй адаптер. При этом тип подключения «Внутренняя сеть», имя: «intnet».
2. Поменяйте настройки виртуальной машины с Windows XP (или другой любой операционной системой): в категории «Сеть» для адаптера 1 тип подключения «Внутренняя сеть», имя: «intnet».
3. В самих операционных системах припишите статический IP-адрес, например, для Linux Ubuntu 192.168.0.1, для Windows XP – 192.168.0.2.
4. Далее, в Windows XP необходимо использовать подключение к LAN через прокси-сервер. В браузере Internet Explorer это можно сделать следующим образом:

Сервис > Свойство обозревателя > Подключение > Настройка LAN. Далее выделить пункт «Использовать прокси-сервер». В адресе прописать IP-адрес Ubuntu (192.168.0.1) и порт, который был прописан в файле-конфигурации squid (3128).

**Задание 3**. Создайте новое правило работы Squid: разрешить доступ подсети 192.168.0.0/24.

**Задание 4**. Измените предыдущее правило работы Squid: доступ подсети 192.168.0.0/24 должен быть разрешен в период рабочего времени (с 8.00 до 17.00) и только в рабочие дни (понедельник, вторник, среда, четверг, пятница).

**Задание 5**. Создайте новое правило работы Squid: запретить доступ к сайтам vk.com, youtube.com.

**Задание 6**. Выясните, как просмотреть и изменить список портов, разрешенных для использования Squid.