Лабораторная работа №7
Прокси-сервер Squid

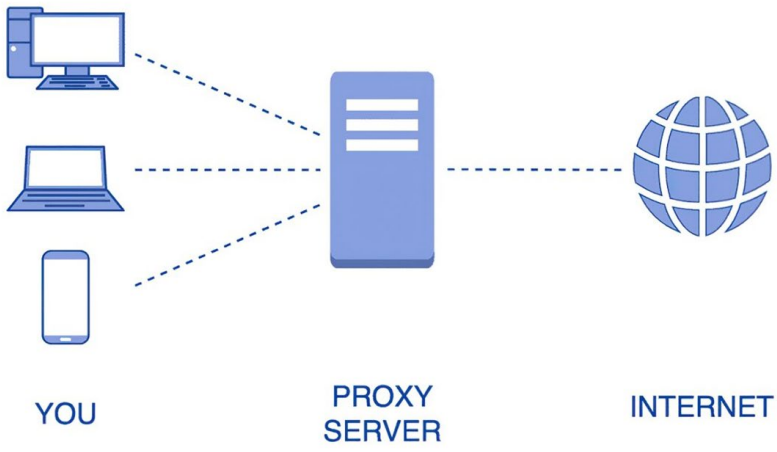
1. Теоретическая часть

1.1. Прокси-сервер

Прокси-сервер (от англ. proxy — представитель, уполномоченный; часто просто прокси, сервер-посредник) — это программные и аппаратные средства в компьютерных сетях, выполняющие роль посредника между пользователем и целевым сервером.

Прокси-сервер принимает и пересылает запросы на подключение, а затем возвращает данные для этих запросов. Он использует анонимный сетевой идентификатор вместо фактического IP-адреса клиента (то есть скрывает IP-адрес клиента), так что фактический IP-адрес клиента не может быть раскрыт.

Сначала клиент подключается к прокси-серверу и запрашивает какой-либо ресурс (например e-mail), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу, используя свой IP-адрес, и получает ресурс у него, либо возвращает ресурс из собственного кэша (если прокси-сервер является кеширующим).



При этом стоит иметь в виду, что прокси-сервер анализирует пакеты на прикладном уровне модели OSI, в то время как Firewall — на уровнях ниже. Поэтому для большей эффективности применяют связку Proxy-Firewall, которые в полной мере предоставляют возможности для контроля трафика.

В качестве функции прокси-сервера указана подмена локального IP-адреса своим собственным. Это похоже на технологию NAT, которая так же сопоставляет множеству локальных адресов одному IP-адресу для выхода в сеть. Однако эта технология, которая поддерживается маршрутизаторами, работает только на сетевом уровне модели OSI и не занимается анализом трафика.

В качестве правил, которыми руководствуется прокси-сервер, могут выступать условия пакетной фильтрации. Правила могут быть достаточно сложными, например в рабочие часы блокируется доступ к тем или иным узлам и/или прилопсжениям, а доступ к другим узлам разрешается только определенным пользователям, причем для FTP-серверов пользователям разрешается делать лишь загрузку, а выгрузка запрещается. Прокси-серверы могут также фильтровать почтовые сообщения по типу пересылаемого файла (например, запретить получение сообщений формата MP3) и по их контенту. К разным пользователям могут применяться разные правила фильтрации, поэтому часто на прокси-серверы возлагается задача аутентификации пользователей.

Наиболее популярным прокси-сервером является ***Squid (англ. squid — «кальмар»)*** — программный пакет, реализующий функцию кэширующего прокси-сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS.

Для его установки применяется команда

```
sudo apt install squid
```

Конфигурационный файл лежит по пути **/etc/squid/squid.conf**. Проанализируем его структуру.

В файле настраиваются правила доступа клиентов к прокси-серверов. Это делается с помощью списков управления доступом **ACL (Access Control List)**.

Общий формат списка управления доступом:

```
acl имя_списка параметр содержимое
```

Параметром может быть одно из следующих:

- **src addr1-addr2/mask** — диапазон IP-адресов источников запросов;
- **dstdomain [-n] .foo.com ...** — домен из URL в запросе;
- **dstdom_regex [-n] [-i] \.foo\.com ...** — регулярное выражение для домена из URL запроса;
- **url_regex [-i] ^http:// ...** — регулярное выражение для URL запроса:
- **time [day-abbrevs: MTWHFAS] [h1:m1-h2:m2]** — установка времени.

Для настроенного списка с определённым названием отдельно устанавливается правило, имеющего вид:

```
http_access инструкция имя_списка
```

В качестве инструкции применяются **allow** (разрешить) или **deny** (запретить).

Конфигурация обрабатывается построчно как при работе правил Firewall. Если поставить запрещающую строку выше разрешающей, то работа будет неправильной.

Приведём пример конфигурационного файла:

```
acl eth port 80                          #Добавить в список номер порта
acl localnet src 172.102.0.100           #Добавить в список адрес
acl localnet src 172.1.0.1-172.1.0.255   #Добавить в список диапазон адресов
acl localnet src 172.16.0.0/12           #Добавить в список диапазон адресов
acl localnet srcdomain .mpsu.stu         #Добавить в список адрес домена от которого хотим подключиться

acl guestnet dst 172.16.0.11             #Добавить в список адрес машины к которой пытаемся осуществить доступ
```

acl guestnet dstdomain .temp.ru #Добавить в список адрес домена к которому хотим подключиться

http_access allow localnet #Разрешить доступ к списку с именем localnet
http_access deny all #Разрешить доступ из остальной сети

Проверка синтаксиса конфигурационного файла производится командой

```
squid -k check
```

После внесения изменений необходимо перезагрузить службу squid силами **systemctl**

```
squid -k reconfigure
```

Просмотр конфигураций, используемой прокси:

```
squid -k parse
```

В качестве примера запретим доступ к поисковой системе **ya.ru**.

Создадим файл **/etc/squid/block.txt** и запишем в него строку

```
.ya.ru
```

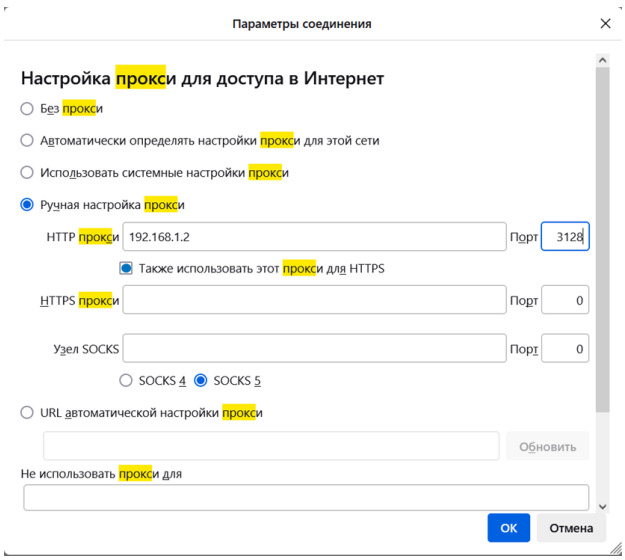
Затем в конфигурационный файл запишем строки:

```
http_port 3128

acl block-site dstdomain ”/etc/squid/block.txt”
http_access deny block-site
```

Примечание: ***http_port 3128*** *— порт, используемый клиентами для запросов к прокси.*

После перезагрузки Squid проверим работу прокси. Для этого зайдём в браузер и в его настройках укажем данные для подключения к прокси-серверу. На картинке показана настройка для Mozilla FireFox.



2. Практическая часть

2.1. Задание 1

2.4.1. Установите **Squid** на сервер.

2.4.2. Настройте прокси-сервер таким образом, чтобы был ограничен доступ к сайту **vk.com** в рабочее время, а остальные сайты запускались свободно.

2.4.3. Убедитесь, что из-под клиента имеется доступ к созданному вами сайту. Запретите клиенту подключение к сайту с помощью прокси-сервера.

Контрольные вопросы

1. Что такое HTTP?

2. Каким образом браузер получает WEB-страницу?

3. Для чего нужен межсетевой экран?

4. Зачем нужен прокси-сервер?

5. В чём разница между работой NAT и прокси-сервером?