



<https://doi.org/10.21122/1683-6065-2022-1-89-90>
УДК 669

Поступила 18.01.2022
Received 18.01.2022

СИСТЕМА ФИЛЬТРАЦИИ WEB-ТРАФИКА

П. В. ПЕВНЕВ, ОАО «БМЗ – управляющая компания холдинга «БМК», г. Жлобин, Гомельская обл., Беларусь, ул. Промышленная, 37. E-mail: pv.pevnev@bmz.gomel.by; тел.: 8-02334-55747.

В статье приведен обзор системы фильтрации web-трафика с помощью программного пакета Squid на базе Linux. Система позволяет ограничивать пользователей в Internet и осуществлять сбор статистики без вмешательства в пользовательский компьютер, в том числе web-браузер.

Ключевые слова. Система фильтрации; Filtration system, iptables, Linux, NAT, Squid, Sams, vpn, proxy.

Для цитирования. Певнев, П. В. Система фильтрации web-трафика / П. В. Певнев // Литье и металлургия. 2022. № 1. С. 89–90. <https://doi.org/10.21122/1683-6065-2022-1-89-90>.

WEB-TRAFFIC FILTERING SYSTEM

P. V. PEVNEV, OJSC “BSW – Management Company of the Holding “BMC”, Zhlobin, Gomel region, Belarus, 37, Promyshlennaya str. E-mail: pv.pevnev@bmz.gomel.by, Tel.: +375-2334-55747.

The article provides an overview of the web traffic filtering system using the Linux-based Squid software package. The system allows you to limit users on the Internet and collect statistics without interfering with the user's computer, including the web browser.

Keywords. Filtering system, iptables, Linux, NAT, Squid, Sams, vpn, proxy.

For citation. Pevnev P. V. Web-traffic filtering system. Foundry production and metallurgy, 2022, no. 1, pp. 89–90. <https://doi.org/10.21122/1683-6065-2022-1-89-90>

В большинстве компаний тема фильтрации интернет-ресурсов является довольно актуальной. После анализа существующих систем выделен программный пакет *Squid* на базе *Linux OS*, который легко взаимодействует с *Active Directory Windows Server* путем аутентификации через *LDAP*.

Пользователи могут идентифицироваться по следующим параметрам:

- IP-адресу (или доменному имени узла).
- Переданным реквизитам (логин/пароль).
- Идентификатору пользовательского агента (браузера).

После установки пакета правильно настроенный фаервол *iptables* перенаправит исходящий веб-трафик на сервер *Squid*.

```
iptables -t nat -A PREROUTING -p tcp -m tcp -s 192.168.1.0/24 -dport 443 -j REDIRECT --to-ports 3129
iptables -t nat -A PREROUTING -p tcp -m tcp -s 192.168.1.0/24 -dport 80 -j REDIRECT --to-ports 3128
```

Squid анализирует полученный трафик, осуществляет сравнение *DNS* имени запроса с *ACL*-списками и определяет дальнейшую судьбу запроса.

Путь к файлу с белым списком *https* ресурсов:

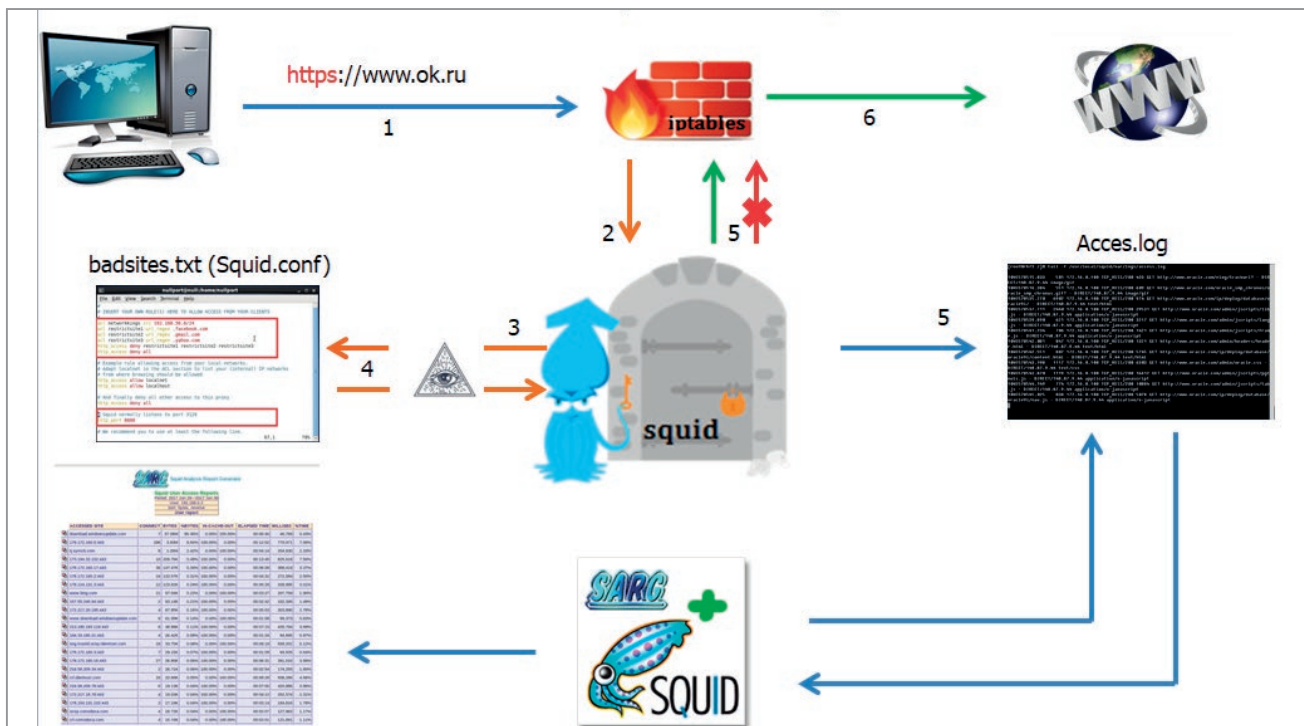
```
acl whitehttps ssl:: server_name "/etc/squid/white_https.txt"
```

Необходимо настроить *Squid* в режим невидимки, т.е. принимать автоматически перенаправленные пакеты и обрабатывать их. В разных версиях *Squid* за это отвечали разные команды. Настройка *Squid* версии 2.6.* выглядит так:

```
http_port 127.0.0.1:3128 transparent # Squid.
```

Для *Squid* существует веб-интерфейс *Sams*, который, кроме настройки прокси-сервера, может быть использован в качестве простейшего биллинга с различными удобными сортировками и выборками. На рисунке показан общий принцип работы *Squid* + *Sams*.

Squid прокси-сервер имеет свои положительные и отрицательные стороны.



Общий принцип работы Squid + Sams

Положительные стороны: Возможность устанавливать даже на слабые персональные компьютеры. Все зависит от количества сотрудников, но небольшая фирма может комфортно работать и через ПК с посредственными характеристиками.

Кеш сохраняется не только на диске, но и в оперативной памяти. Это позволяет значительно ускорить работу. Здесь важно учитывать, что потребуется большой объем оперативной памяти в вашем компьютере.

Поддерживает несколько вариантов авторизации. Настраиваются дополнительно по IP, MySQL, NTLM, через базу LDAP.

Негативные стороны прозрачного прокси: В прозрачном режиме не работает с SSL. Это значит, что вы не сможете зайти на сайт с адресом https://... в режиме аутентификации может работать на протоколах HTTP, SSL, FTP.

Не умеет работать сразу в двух режимах: аутентификации и прозрачном – доступ в интернет без всяких настроек, логинов и прочего. Режим аутентификации – когда пользователю необходимо ввести логин/пароль или другие настройки, предусмотренные администратором.

Не умеет работать с почтовыми серверами POP3, SMTP, IMAP. Вы не сможете принять или отправить почту через прокси Squid.