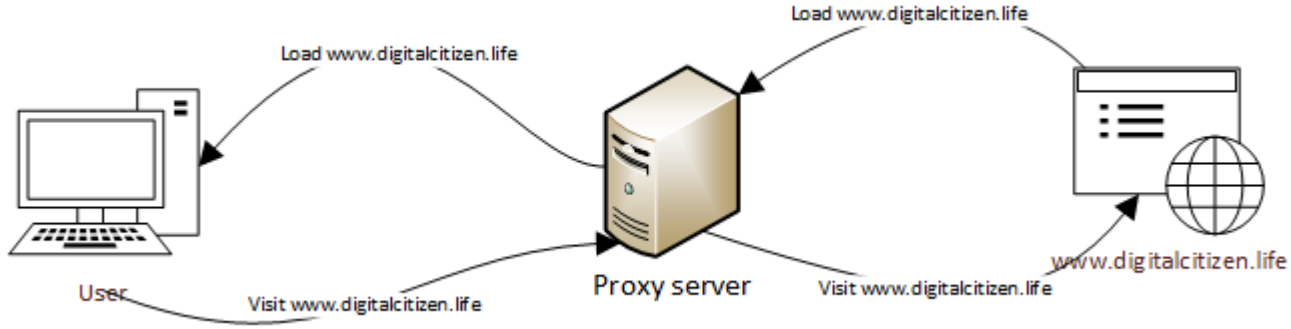
ЛАБОРАТОРНА РОБОТА 7

Інсталяція та налаштування proxy серверу на ОС Linux

Мета: ознайомитись з основами налаштування proxy серверу на базі ОС Linux

Теоретичні відомості

Proxy-сервер — це виділений комп'ютер або програмна система, що працює на комп'ютері, який діє як посередник між кінцевим пристроєм, таким як комп'ютер, та іншим сервером, з якого користувач або клієнт запитує послугу. Proxy-сервер може існувати на тому самому комп'ютері, що й сервер брандмауера, або він може бути на окремому сервері, який пересилає запити через брандмауер. В англійській мові proxy означає "повірений, уповноважений".



Перевагою proxy-сервера є те, що його кеш може обслуговувати всіх користувачів. Якщо один або кілька Інтернет-сайтів часто запитуються, вони, ймовірно, будуть у кеші proxy-сервера, що покращить час відповіді користувача. proxy також може реєструвати свої взаємодії, що може бути корисним для усунення несправностей. Коли proxy-сервер отримує запит на Інтернет-ресурс (наприклад, веб-сторінку), він переглядає свій локальний кеш попередніх сторінок. Якщо він знаходить сторінку, він повертає її користувачеві без необхідності пересилати запит в Інтернет. Якщо сторінки немає в кеші, proxy-сервер, діючи як клієнт від імені користувача, використовує одну зі своїх власних IP-адрес для запиту сторінки з сервера в Інтернеті. Коли сторінка повертається, proxy-сервер пов'язує її з вихідним запитом і пересилає її користувачеві.

На підприємстві proxy-сервер використовується, серед інших цілей, для забезпечення безпеки, адміністративного контролю або служб кешування. У контексті персональних комп'ютерів proxy-сервери використовуються для забезпечення конфіденційності користувача та анонімного перегляду. proxy-сервери також можна використовувати для протилежних цілей: для моніторингу трафіку та порушення конфіденційності користувачів.

Для користувача, що використовує proxy-сервер, усі Інтернет запити та повернуті відповіді видаються безпосередньо з адресованого Інтернет-сервера, тобто подібно до прямої роботи з ресурсами Інтернет. Користувач для використання proxy-серверу вказує його IP адресу як параметр конфігурації браузера або іншої програми, що використовує протоколи proxy-серверу.

Користувачі можуть отримати доступ до веб-proxy-серверів онлайн або налаштувати веб-браузери на постійне використання proxy-сервера. Параметри веб-браузера включають автоматично визначені та ручні параметри для proxy-серверів HTTP, SSL, FTP і SOCKS. Proxy-сервери можуть обслуговувати багато користувачів або лише одного. Ці параметри називаються спільними та виділеними proxy відповідно. Існує кілька причин для proxy-серверів, тому є кілька типів proxy-серверів.

Forward proxy — проксі-сервери, що пересилають запити клієнта. Користувачі отримують доступ до "forward proxy" при звичайному прямому перегляді Інтернет ресурсів за адресою або налаштувавши параметри доступу до Інтернет. Forward proxy дозволяють обходити брандмауери

та підвищувати конфіденційність і безпеку користувача, але іноді можуть використовуватися для завантаження незаконних матеріалів.

Reverse proxy — проксі-сервери, що прозоро обробляють усі запити на ресурси на цільових серверах, не вимагаючи додаткових дій з боку запитувача.

Reverse proxy використовуються:

- для увімкнення непрямого доступу, коли веб-сайт забороняє прямі підключення із міркувань безпеки;
- для забезпечення балансування навантаження між серверами;
- для передачі внутрішнього вмісту користувачам Інтернету;
- для вимкнення доступу до сайту, наприклад, коли є необхідність заблокувати певний веб-сайт.

Сайти можуть бути заблоковані з більш-менш поважних причин. Зворотні проксі можуть використовуватися для запобігання доступу до аморального, незаконного або захищеного авторським правом вмісту. Іноді ці причини виправдані, а іноді ні. Зворотні проксі-сервери іноді використовують для обмеження доступу до небажаних керівництвом (певної держави або підприємства) новинних сайтів, запобігають доступу користувачів до сайтів, де вони можуть розкрити інформацію про дії уряду чи галузі, тощо.

Transparent proxy - це прозорі для використання проксі-сервери, які зазвичай знаходяться біля виходу з корпоративної мережі. Ці проксі централізують мережевий трафік. У корпоративних мережах проксі-сервер пов’язаний із сервером-шлюзом, який відокремлює мережу від зовнішніх мереж (як правило, Інтернету), і брандмауером, який захищає мережу від зовнішнього вторгнення та дозволяє сканувати дані з метою безпеки перед доставкою клієнту в мережі. Ці проксі-сервери допомагають контролювати та адмініструвати мережевий трафік, оскільки комп’ютери в корпоративній мережі зазвичай є безпечними пристроями, яким не потрібна анонімність для типових повсякденних завдань.

Anonymous proxy — проксі-сервери, що використовують для приховування IP-адреси клієнта, за допомогою них можна отримати доступ до матеріалів, які заблоковані брандмауерам, або обійти заборону IP-адреси. Вони також можуть використовуватися для покращення конфіденційності та/або захисту від атак.

Highly anonymous proxy - підвид анонімних проксі-серверів, що приховують навіть той факт, що вони використовуються клієнтами, і надають публічну IP адресу, яка не є проксі-сервером. Тож вони не лише приховують IP-адресу клієнта, який їх використовує, але й дозволяють доступ до сайтів, які можуть блокувати проксі-сервери. Прикладами “highly anonymous proxy” є I2P та TOR.

Proxy-сервери Socks 4 і 5 забезпечують проксі-сервіс для даних UDP і операцій пошуку DNS на додаток до веб-трафіку. Деякі проксі-сервери пропонують обидва протоколи Socks.

DNS-proxy пересилають запити служби доменних імен (DNS) із локальних мереж на DNS-сервери в Інтернеті, одночасно кешуючи для підвищення швидкості.

Squid — це проксі-сервер, який найчастіше використовується на базі Linux. Проксі-сервер Squid використовується для фільтрації трафіку, безпеки та пошуку DNS.

Практична частина

Перед встановленням squid необхідно актуалізувати пакети операційної системи, для чого використовується наступна команда в терміналі:

```
~$ sudo apt update
```

Для початку інсталяції squid використовуємо команду:

```
~$ sudo apt install squid
```

Файл конфігурацій squid знаходиться в /etc/squid/squid.conf:

Для виконання редагування цього файлу його слід відкрити в редакторі із правами root, наприклад, наступною командою:

```
$ sudo mcedit squid.conf
```

Файл достатньо об’ємний — більше 8500 рядків, більша частина яких закоментовано символом #. Традиційно файл містить документацію до свого вмісту і прикладами параметрів. Тому навігацію по файлу можна роботи поступово рядок за рядком, або через пошук необхідного параметру.

У конфігураційному файлі SQUID використовується декілька різних типів директив.

Директиви з одним значенням. Це директиви, які приймають лише одне значення, тому при їх багатократному використанні у файлі конфігурації останнє значення директиви замінить усі попередні декларації. Наприклад, logfile_rotate слід вказувати лише один раз:

```
logfile_rotate 10
# Наступний рядок змінить попереднє значення
logfile_rotate 5
```

Логічні значення або директиви перемикання. Ці директиви також можуть мати тільки одне значення і зазвичай використовуються для увімкнення або вимкнення певної функції.

```
query_icmp on
log_icp_queries off
url_rewrite_bypass off
```

Директиви з декількома значеннями. Директиви цього типу зазвичай приймають одне або більше значень. Значення можна або вказати в одному рядку після директиви, або записати у кількох рядках, повторюючи директиву щоразу. Агрегація значень у директиві виглядає наступним чином:

```
hostname_aliases   proxy.exmaple.com    squid.example.com
```

Це саме можна зробити декількома окремими рядками:

```
dns_nameservers   proxy.example.com
dns_nameservers   squid.example.com
```

Директиви, що мають значення часу. Є кілька директив, які приймають значення одиниць часу. Squid розуміє слова секунди, хвилини, години тощо, і їх можна додати до числових значень, щоб визначити фактичні значення. Наприклад:

```
request_timeout 3 hours
persistent_request_timeout 2 minutes
```

Директиви зі значеннями розміру файлу або пам'яті. Значення, що передаються цим директивам, вказуються з одиницями розміру файлу або пам’яті: байтів, кБ, МБ або ГБ. Наприклад:

reply_body_max_size 10 MB
cache_mem 512 MB
maximum_object_in_memory 8192 KB

При налаштуванні Squid gершим необхідно знайти опцію http_port — номер порту, на який сервер приймає запити від клієнтів на ресурси Інтернет. Зазвичай цей рядок розкоментовано і параметр має значення 3128:

Номер цього рядку приблизно 1900.

Цей порт зазвичай передає трафік TCP. Якщо є потреба налаштувати трафік системи на інший порт, то його слід змінити саме тут. Типово для proxy-серверів використовують такі порти, як 3128, 8000, 8008, 8080, тощо. Але це значення не регламентується будь-якими стандартами, тому номером для squid може бути і інше значення.

Також можна вказати комбінацію IP-адреси та порту. Зазвичай це використовується, коли на комп’ютері є кілька інтерфейсів і необхідно, щоб Squid слухав тільки інтерфейс, який підключено до локальної мережі (LAN), наприклад:

http_port 192.0.2.25:3128

або у формі з використанням імені (або доменного імені):

http_port myproxy.example.com:8080

Ця директива може приймати кілька значень в окремих рядках. Наприклад:

http_port 192.0.2.25:8080
http_port lan1.example.com:3128
http_port lan2.example.com:8081

Ці рядки запустять Squid для прослуховування трьох адрес і портів. Це корисно, коли є клієнти в різних локальних мережах, які налаштовані на використання різних портів для проксі-сервера.

Squid також може мати режими роботи: intercept, tproxy, accel тощо.

Режим перехоплення підтримуватиме перехоплення запитів без необхідності налаштування клієнтських машин.

http_port 3128 intercept

Режим tproxy використовується для ввімкнення підтримки Linux Transparent Proxy для підробки вихідних з’єднань за допомогою IP-адреси клієнта.

http_port 8080 tproxy

Для того, щоб почати використовувати Squid необхідно знайти опцію http_access deny all. Її налаштовано на блокування всього HTTP-трафіку. Опцію необхідно замінити на:

```
http_access allow all
```

Перевірка роботи Squid робиться у декілька кроків.
Першим перевіряємо його роботу як сервісу, для чого використовуємо команду:

```
# systemctl status squid
```

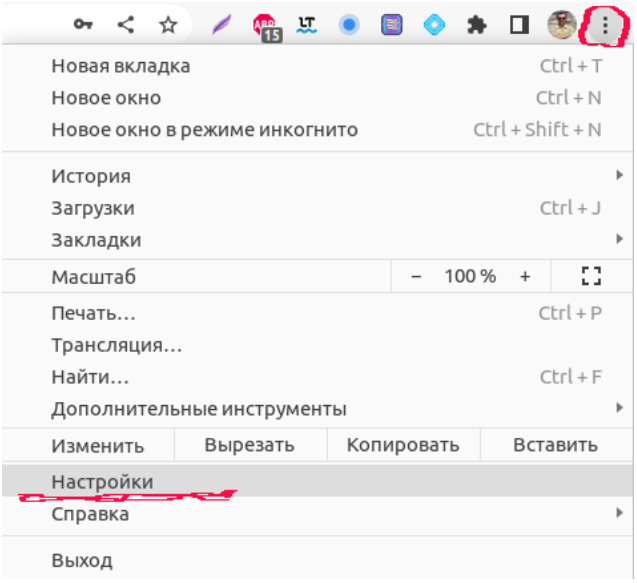
Якщо демон Squid працює, то відповідь повинна виглядати подібно до наступного:

```
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2022-11-22 08:54:15 EET; 2h 56min ago
       Docs: man:squid(8)
   Main PID: 1911 (squid)
      Tasks: 4 (limit: 19005)
     Memory: 25.0M
     CGroup: /system.slice/squid.service
             ├─1911 /usr/sbin/squid -sYC
             ├─1913 (squid-1) --kid squid-1 -sYC
             ├─1918 (logfile-daemon) /var/log/squid/access.log
             └─1920 (pinger)
```

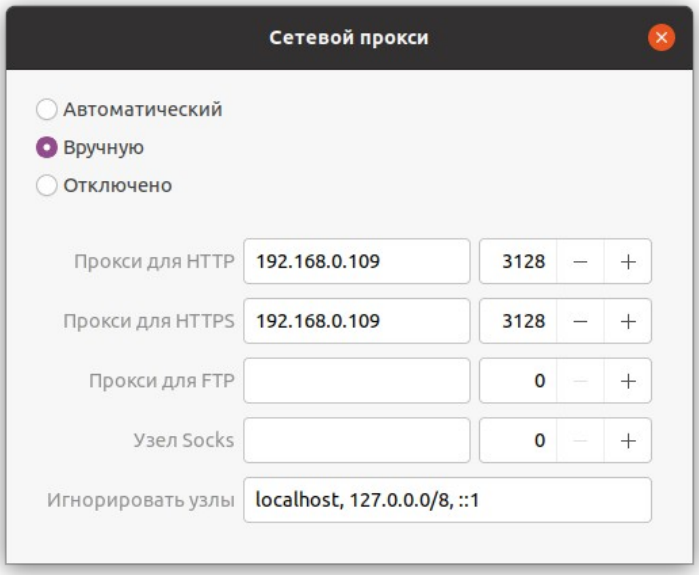
Якщо демон не працює слід спробувати його запустити командою:

systemctl start squid

Наступним налаштовуємо браузер на використання proxy-серверу. Зазвичай proxy-сервер встановлюється на окремому комп'ютері, тому для виконання налаштувань браузера слід взнати IP адресу цього комп’ютера, яку буде використовувати Squid. Усі браузери мають налаштування на використання proxy-серверу. Зазвичай за замовчуванням у браузері встановлено використання або автоматичних налаштувань, або системних. У браузері Google Chrome перейти до налаштувань виконується натисканням на кнопку, що позначено трьома точками:



У налаштуваннях натискаємо на “Система” -> “Відкрити налаштування проксі-серверу для комп’ютера” та задати відповідні параметри:



Списки контролю доступу (Access Control Lists — ACL)

Списки контролю доступу є базовими елементами для керування доступом і зазвичай використовуються в поєднанні з іншими директивами, такими як http_access, icp_access тощо, для контролю доступу до різних компонентів і веб-ресурсів через Squid.

ACL ідентифікує веб-транзакцію, а потім директиви, такі як http_access, кеш, а потім вирішує, чи слід дозволити транзакцію чи ні.

Також слід зазначити, що директиви, пов’язані з доступом до ресурсів, зазвичай закінчуються на _access.

Кожне визначення списку керування доступом має мати ім’я та тип, а потім значення для цього конкретного типу ACL:

```
acl ACL_NAME ACL_TYPE value
acl ACL_NAME ACL_TYPE "/path/to/filename"
```

Наприклад, ACL для доменного імені example.com:

```
acl example_site dstdomain example.com
```

де example_site — ім’я ACL із типом dstdomain, що вказує example.com є ім’ям домену.

ACL можуть задаватись у наступних спосіб:

1. Значення в одному рядку:
```
acl example_sites dstdomain example.com example.net example.org
```

2. Значення в кількох рядках:
```
acl example_sites dstdomain example.com example.net
acl example_sites dstdomain example.org
```

3. Значення з файлу: якщо кількість значень, які необхідно вказати, досить велика, то можна помістити їх у спеціальний файл, а потім наказати Squid читати значення з нього цього файлу:

acl example_sites dstdomain '/etc/squid/example_sites.txt'

Вміст файлу example_sites.txt має бути наступним:

Цей файл також може містити коментарі
#
example.net
example.org
example.com

ACL дозволяють організувати контроль доступу HTTP. ACL допомагають лише ідентифікувати запити на основі різних правил. ACL самі по собі не використовуються, їх слід поєднувати з директивами контролю доступу, щоб дозволити або заборонити доступ до різних ресурсів. http_access є однією з таких директив, яка використовується для надання доступу для виконання HTTP-транзакцій через Squid.

Загальний синтаксис http_access:
http_access allow|deny [!]ACL_NAME

Наприклад:
acl my_home_machine src 192.0.2.21
acl my_lab_machine src 198.51.100.86
http_access allow my_home_machine
http_access allow my_lab_machine

або
acl my_machines src 192.0.2.21 198.51.100.86
http_access allow my_machines

Завдання до лабораторної роботи

1. Виконайте вхід у систему під особистим логіном. Виконайте перемикання на акаунт root.
2. Встановіть в системі пакет серверу Squid та виконайте налаштування, користуючись наведеними вище вказівками у практичній частині. Налаштування адаптуйте до мережевої конфігурації власної локальної мережі.
3. Виконайте налаштування браузеру на використання Squid.
4. Перевірте роботу клієнту через Squid.
5. Складіть ACL та налаштуйте їх використання для: заборони певного ресурсу за його IP адресою; заборони певного ресурсу за його символьною адресою; заборони доступу до ресурсів, якщо зустрічається певний контент — за певним словом. Перевірте Роботу контролю доступу.
6. Підготуйте звіт, в якому наведіть screenshots етапів налаштування серверу Squid та результатів отримання або не отримання клієнтом доступу до ресурсів.

Контрольні питання

1. Для чого призначено proxy-сервер?
2. Які є типи proxy-серверів?
3. Яку мінімальну конфігурацію слід зробити для використання proxy-серверу?
4. Для чого призначено ACL?
5. Як заборони доступ до Інтернет ресурсу за певним вмістом у запиті?