**Лабораторна робота №15**

**Тема:** Створення  та налаштування шлюзу Інтернет . Листи  доступу.

**Мета:** Набути практичних вмінь та навиків при роботі та конфігуруванні Інтернет шлюзу під Лінукс та Windows на базі проксі-сервера Squid.

**Порядок виконання роботи:**

1. **Встановити та сконфігурувати проксі-сервер Squid  під Linux для свого комп’ютера.**

**Крок 1: Встановлення та конфігурація Squid**

1. Встановив Squid з репозиторіїв свого дистрибутиву. Наприклад, для Ubuntu це може виглядати так:

sudo apt update

sudo apt install squid

1. Налаштував конфігураційний файл Squid, який зазвичай знаходиться в **/etc/squid/squid.conf**. Редагував цей файл відповідно до своїх потреб.

**Крок 2: Тестування роботи проксі-сервера**

1. Запустив службу Squid:

sudo systemctl start squid

1. Відкрив веб-браузер та налаштував його для використання проксі-сервера. Зазвичай це можна зробити у налаштуваннях браузера.
2. Переконався, що я можу виходити в Інтернет через проксі.

**Крок 3: Створення листа доступу**

1. Додав до конфігураційного файлу Squid лист доступу, що виглядає приблизно так:

acl allowed\_network src <IP-адреса комп'ютера>

http\_access allow allowed\_network

**Крок 4: Фільтр для блокування сайтів із забороненими словами**

1. Додав фільтр у конфігураційний файл Squid:

arduino

acl bad\_sites dstdomain "/etc/squid/bad-sites"

http\_access deny bad\_sites

1. Створив файл **/etc/squid/bad-sites** та додав туди сайти із забороненими словами.

**Крок 5: Фільтр для блокування банерів**

1. Використав фільтр для блокування банерів у конфігураційному файлі Squid:

arduino

acl ads url\_regex "/etc/squid/ads"

http\_access deny ads

1. Створив файл **/etc/squid/ads** та додав туди регулярні вирази для виявлення URL банерів.

**Крок 6: Дозвіл доступу певному комп'ютеру**

1. Додав до конфігураційного файлу Squid правило для дозволу доступу певному комп'ютеру на певний час:

php

acl allowed\_pc src <IP-адреса комп'ютера>

http\_access allow allowed\_pc TIME <Початок>-<Кінець>

**Крок 7: Перевірка працездатності**

1. Перезапустив службу Squid:

sudo systemctl restart squid

Перевірив, чи працює ваш проксі та чи виконуються всі правила, які я налаштував.

2. **Виконати тестування роботи проксі –сервера.**

**Крок 1: Перевірте стан служби Squid**

1. Відкрив термінал.
2. Використав команду для перевірки статусу служби Squid:

sudo systemctl status squid

1. Переконався, що служба працює без помилок.

**Крок 2: Перевірте доступ до проксі-сервера з браузера**

1. Відкрив веб-браузер.
2. Перейшов до налаштувань браузера та знайшов розділ про проксі-сервер або мережеві налаштування.
3. Ввів IP-адресу та порт, на який слухає Squid, відповідно до налаштувань у конфігураційному файлі.
4. Зберіг зміни та перезапустив браузер.
5. Спробував відкрити будь-яку веб-сторінку.

**Крок 3: Перевірив журнали Squid для виявлення помилок**

1. Відкрив термінал.
2. Використав команду для перегляду журналів Squid:

sudo tail -f /var/log/squid/access.log

1. Спробував знову відкрити веб-сторінку через браузер.
2. Перевірив журнал для будь-яких записів про запити та можливі помилки.

**Крок 4: Перевірив обмеження доступу**

1. В конфігураційному файлі Squid створив обмеження доступу для певних IP-адрес або мереж.
2. Перезапустив службу Squid.
3. Спробував відкрити веб-сторінку з комп'ютера, що не входить у обмежену мережу.
4. Перевірив журнали для виявлення блокованих запитів.

**Крок 5: Перевірив фільтрацію вмісту (опційно)**

1. Якщо я налаштував фільтрацію вмісту (наприклад, блокування певних сайтів чи ключових слів), перевірив, чи це фільтрується.

Спробував відкрити різні види веб-сторінок, щоб переконатися, що фільтрація працює.

3. **Створіть лист доступу по якому буде відкрито доступ до мережі комп, ютеру, що знаходиться справа від Вас, і заборонено – тому що зліва від Вас.**

**Крок 1: Додайте ACL до конфігураційного файлу Squid**

1. Відкрив конфігураційний файл Squid у текстовому редакторі:

sudo nano /etc/squid/squid.conf

1. Додав наступні рядки до свого конфігураційного файлу:

plaintext

acl right\_network src <IP-адреса комп'ютера справа>

acl left\_network src <IP-адреса комп'ютера зліва>

http\_access allow right\_network

http\_access deny left\_network

Замінив **<IP-адреса комп'ютерів>** на фактичні IP-адреси комп'ютерів зліва та справа від мене.

1. Зберіг зміни та вийшов з текстового редактора.

**Крок 2: Перезапустив службу Squid**

1. Після внесення змін у конфігураційний файл, перезапустив службу Squid:

sudo systemctl restart squid

**Крок 3: Перевірив роботу ACL**

1. Використав браузер або інші інтернет-засоби для намагання відкрити веб-сторінки з комп'ютера справа і зліва.
2. Переконався, що доступ до Інтернету дозволений з комп'ютера справа, але заборонений з комп'ютера зліва.

Перевірив журнали Squid, щоб виявити блоковані запити і переконався, що правила ACL діють вірно.

4. **Створіть фільтр для блокування сайтів із забороненими словами.**

**Крок 1: Редагування конфігураційного файлу Squid**

1. Відкрив конфігураційний файл Squid у текстовому редакторі:

sudo nano /etc/squid/squid.conf

1. Додав наступні рядки у ваш конфігураційний файл:

plaintext

acl bad\_sites url\_regex "/etc/squid/bad-sites"

http\_access deny bad\_sites

**Крок 2: Створення файлу зі забороненими словами**

1. Створив файл **/etc/squid/bad-sites**:

sudo nano /etc/squid/bad-sites

1. Додав заборонені слова, використовуючи регулярні вирази, наприклад:

plaintext

.\*заборонене\_слово.\*

.\*інше\_заборонене\_слово.\*

Замінив **заборонене\_слово**, **інше\_заборонене\_слово**, тощо, на реальні слова чи фрази, які я хочу заборонити.

**Крок 3: Збереження та перезапуск Squid**

1. Зберіг зміни та вийшов з редактора.
2. Перезапустив службу Squid:

sudo systemctl restart squid

**Крок 4: Тестування**

1. Відкрив браузер і спробував відкрити веб-сторінки, які містять заборонені слова.

Перевірив журнали Squid, щоб виявити блоковані запити.

5. **Створіть фільтр для блокування банерів**.

**Крок 1: Редагування конфігураційного файлу Squid**

1. Відкрив конфігураційний файл Squid у текстовому редакторі:

sudo nano /etc/squid/squid.conf

1. Додав наступні рядки у свому конфігураційний файл:

plaintext

acl ads url\_regex "/etc/squid/ads"

http\_access deny ads

**Крок 2: Створення файлу з URL-адресами банерів**

1. Створив файл **/etc/squid/ads**:

sudo nano /etc/squid/ads

1. Додав URL-адреси банерів у цей файл, використовуючи регулярні вирази. Наприклад:

plaintext

.\*\.doubleclick\.net/.\*

.\*\.googleadservices\.com/.\*

Замінив ці URL-адреси на реальні адреси банерів, які ви хочете заблокувати.

**Крок 3: Збереження та перезапуск Squid**

1. Зберіг зміни та вийшов з редактора.
2. Перезапустив службу Squid:

sudo systemctl restart squid

**Крок 4: Тестування**

1. Відкрив браузер і відвідав веб-сторінки, де можуть бути розміщені банери.

Перевірив журнали Squid, щоб переконатися, що запити до URL-адрес, які я вказав,

блокуються.  
6. **Дозволив доступ комп’ютеру 192.168.44.8 на час моєї пари.**

**Крок 1: Редагування конфігураційного файлу Squid**

1. Відкрив конфігураційний файл Squid у текстовому редакторі:

sudo nano /etc/squid/squid.conf

1. Додав наступні рядки у ваш конфігураційний файл:

plaintext

acl allowed\_host src 192.168.44.8

acl access\_time time MWF 10:00-12:00

http\_access allow allowed\_host access\_time

http\_access deny all

У цьому прикладі, **MWF** вказую на "Понеділок, Середа, П'ятниця", а **10:00-12:00** вказую на час від 10:00 до 12:00.

**Крок 2: Збереження та перезапуск Squid**

1. Зберіг зміни та вийшов з редактора.
2. Перезапустив службу Squid:

sudo systemctl restart squid

**Крок 3: Тестування**

1. Відкрив браузер і спробував відвідати веб-сайти з комп'ютера з IP-адресою 192.168.44.8 під час визначеного часу доступу.

Перевірив журнали Squid, щоб побачити, чи дотримуються правила часового доступу.

7. **Перевірте працездатність системи.**

**Крок 1: Перевірка статусу служби Squid**

Відкрив термінал та ввів команду:

sudo systemctl status squid

Переконався, що служба Squid працює та не має помилок.

**Крок 2: Перевірка журналів доступу**

1. Відкрив термінал та ввів команду для перегляду журналів Squid:

sudo tail -f /var/log/squid/access.log

1. Спробував здійснити доступ до Інтернету з комп'ютера з правильними або неправильними умовами доступу.
2. Перевірив журнали для записів про доступ та можливі помилки.

**Крок 3: Перевірка фільтрів**

1. Спробував відкрити веб-сторінки, які містять заборонені слова або банери.
2. Перевірив, чи застосовуються фільтри, і чи блокуються вказані вами контенти.

**Крок 4: Перевірка обмеження доступу за часом**

1. Спробував здійснити доступ до Інтернету з комп'ютера, який має обмежений час доступу.
2. Переконався, що обмеження за часом працює вірно.

**Крок 5: Перевірка блокування сайтів та банерів**

1. Спробував звертатися до заборонених сайтів чи сайтів з банерами.
2. Переконався, що ці запити блокуються відповідно до мого конфігурації.

**Крок 6: Загальна перевірка працездатності**

Спробував взаємодіяти з Інтернетом через свій проксі-сервер і переконався, що всі налаштування працюють, як очікується.

8. **Оформити звіт.**

**Контрольні запитання .**

1. Призначення проксі-серверів.
2. Порядок установки проксі-сервера squid.
3. Основні можливості squid.
4. Який файл використовується для конфігуруванн Squid?
5. Які правила використовуються для доступу користувачів?
6. Як запустити проксі-сервер Squid?
7. Як зупинити проксі-сервер Squid?
8. Як перезапустити проксі – сервер Squid?
9. По якому порту як правило працює проксі-сервер Squid?
10. Для чого застосовують фільтри?
11. Як створюється фільтр?
12. Які типи фільтрів існують?
13. Як добавити фільтр на інтерфейс?
14. Як продивитися існуючий фільтр?
15. Як заборонити доступ по певній службі?
16. Як дозволити доступ по певній службі?
17. Як заборонити  доступ всіх користувачів окім вибраних?

**Відповіді на запитання:**

1. **Призначення проксі-серверів:** Проксі-сервери використовуються для проміжного посередництва між користувачем і Інтернетом. Вони слугують для збереження анонімності, фільтрації контенту, контролю доступу, зберігання кешу для прискорення доступу до веб-сайтів та інших завдань.
2. **Порядок установки проксі-сервера Squid:**
   * Встановіть Squid з допомогою пакетного менеджера (наприклад, в Ubuntu: **sudo apt-get install squid**).
   * Змініть налаштування у конфігураційному файлі **/etc/squid/squid.conf**.
   * Запустіть службу Squid (**sudo systemctl start squid**).
   * Налаштуйте автозапуск при старті системи (**sudo systemctl enable squid**).
3. **Основні можливості Squid:**
   * Кешування веб-сторінок.
   * Керування доступом.
   * Фільтрація контенту.
   * Захист від атак та шкідливого вмісту.
4. **Який файл використовується для конфігурації Squid?**
   * Основний файл конфігурації Squid розташований за адресою **/etc/squid/squid.conf**.
5. **Які правила використовуються для доступу користувачів?**
   * В Squid використовуються ACL (Access Control List) для визначення правил доступу користувачів.
6. **Як запустити проксі-сервер Squid?**
   * Команда для запуску: **sudo systemctl start squid**.
7. **Як зупинити проксі-сервер Squid?**
   * Команда для зупинки: **sudo systemctl stop squid**.
8. **Як перезапустити проксі – сервер Squid?**
   * Команда для перезапуску: **sudo systemctl restart squid**.
9. **По якому порту як правило працює проксі-сервер Squid?**
   * По замовчуванню, Squid працює на порту 3128.
10. **Для чого застосовують фільтри?**
    * Фільтри використовуються для обмеження або фільтрації контенту, який може бути доступний користувачам через проксі-сервер.
11. **Як створюється фільтр?**
    * Фільтр створюється за допомогою ACL та правил доступу в конфігураційному файлі Squid.
12. **Які типи фільтрів існують?**
    * Типи фільтрів включають URL-фільтри, фільтри за ключовими словами, фільтри за часом і т.д.
13. **Як добавити фільтр на інтерфейс?**
    * Фільтри додаються до конфігураційного файлу Squid у розділі ACL та http\_access.
14. **Як продивитися існуючий фільтр?**
    * Ви можете переглянути конфігураційний файл Squid (**/etc/squid/squid.conf**) для існуючих ACL та http\_access правил.
15. **Як заборонити доступ по певній службі?**
    * Використовуйте ACL та http\_access правила для блокування конкретних служб або доменів.
16. **Як дозволити доступ по певній службі?**
    * Використовуйте ACL та http\_access правила для дозволу конкретних служб або доменів.
17. **Як заборонити доступ всіх користувачів окім вибраних?**

Використовуйте ACL та http\_access правила для блокування всіх користувачів, крім тих, які вам потрібні.

**Висновок:** набув практичних вмінь та навиків при роботі та конфігуруванні Інтернет шлюзу під Лінукс та Windows на базі проксі-сервера Squid.