УДК 004.056.52

Є. О. Марунчак

ЗАХИСТ САЙТІВ НА РІВНІ ВЕБ-СЕРВЕРУ З LINUX ОС

Вінницький національний технічний університет

Анотація

Розглянуто найпоширеніші веб-сервери, ціль їх використання та приведені приклади їх використання для захисту сайтів від DDoS-атак з-під окремих IP-мереж.

Ключові слова: веб-сервер, Apache, Nginx. Litespeed, DDoS-атака, захист інформації.

Abstract

A review of the most widely used web servers was carried out, the purpose of which was to use them to protect websites from DDoS attacks of IP networks.

Keywords*:* web server, Apache, Nginx. Litespeed, DDoS-attack, information protection.

Мета використання веб-серверів на серверах

Веб-сервер – це програмна частина серверу, що приймає HTTP-запити від клієнтів, зазвичай це веб-браузери, і видає їм HTTP-відповіді, як правило, разом з HTML-сторінкою, зображенням, файлами, медіа-потоком або іншими даними. Веб-сервером називають як програмне забезпечення, виконуючу функцію веб-сервера, так і безпосередньо комп'ютер, на якому працює необхідне програмне забезпечення. Користувач, яким зазвичай є веб-браузер, передає запити веб-серверу на отримання ресурсів, зазначених URL-адресами. Ресурси – це HTML-сторінки, файли або інші дані, які необхідні клієнту. У відповідь веб-сервер передає клієнту запрошені дані. Цей обмін відбувається по протоколу HTTP, або його захищеним розширенням HTTPS [1].

Веб-сервери можуть мати різні додаткові функції, наприклад:

- автоматизація роботи веб-сторінок;
- ведення журналу запитів користувачів до ресурсам;
- аутентифікація та авторизація користувачів;
- підтримка динамічних генерованих сторінок.
- Часто на комп'ютері разом із веб-сервером встановлюється також і поштовий сервер, щоб власник сайту міг створювати та користуватися поштовими скриньками.

Клієнти для звернення до веб-серверів можуть використовуватися різні програми та пристрої:

- веб-браузер, який працює на настільному комп'ютері або переносному пристрої (наприклад, кишеньковому ПК);
- різноманітні програми, що самостійно звертаються до веб-серверів для отримання оновлень або іншої інформації (наприклад, антивірус може періодично вимагати у певного веб-сервера оновлення своїх баз даних);
- мобільний телефон, який отримує доступ до ресурсів веб-сервера за допомогою протоколу WAP;
- інші цифрові пристрої чи побутова техніка.

Найпопулярніші веб-сервери

Станом на червень 2021 року, серед обраних одного мільйону сайтів, котрі є у вільному доступі, динаміка використання веб-серверів зображена в діаграмі на рисунку 1.

З наданої діаграми видно, що найпоширенішими серверами веб-контенту сайтів є Apache, Nginx, CloudFlare, Microsoft IIS, LiteSpeed та Google Servers з 1.1% [2].

Розглянемо дану інформацію та коротко охарактеризуємо веб-сервери:

1. Apache – відкритий веб-сервер з відкритими вихідними кодами, що розповсюджується у вигляді вільного софту (обмеження на скачування та копіювання відсутні). Перша версія веб-сервера була випущена у 1995 році, який розроблюється та підтримується спільнотою розробників відкритого програмного забезпечення під керівництвом Apache Software Foundation. В 1996 році Apache обійшов NCSA HTTPd і з того часу є найбільш популярним у світі [3].

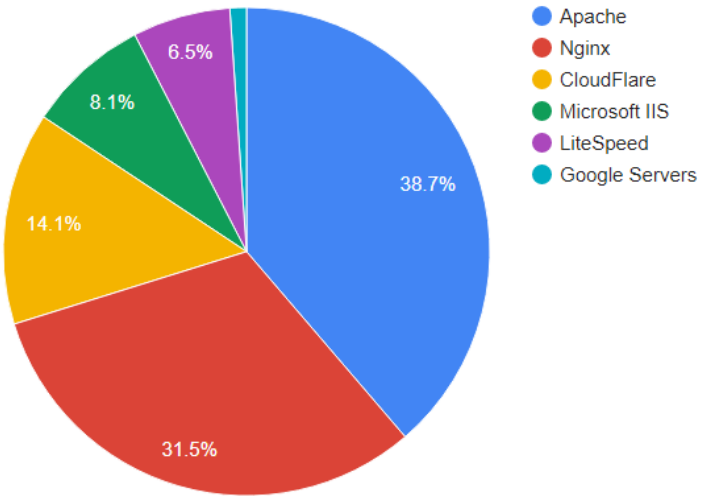

Рисунок 1 – діаграма поширення веб-серверів

Спочатку розроблявся як покращена версія NCSA HTTPd 1.3 (популярне серверне програмне забезпечення до появи Apache). Вибір на користь Apache обумовлений його перевагами: надійність, простота адміністрування, модульна структура, гнучкість та масштабованість.

Apache також не позбавлений недоліків - велика кількість конфігураційних файлів та доступних параметрів, що зумовлюють зниження рівня безпеки та падіння продуктивності у разі різкого зростання трафіку.

2. Nginx – також програмне забезпечення з відкритим кодом для серверів, сумісне з UNIX-системами. Розроблявся як веб-сервер для обслуговування HTTP-запитів. Над проектом працював програміст Ігор Сисоєв, розробка програмного забезпечення почалася 2002 року, а реліз вийшов у грудні 2004 року [4]. Основна мета, яку ставив собою Сисоєв, – вирішення проблеми C10k, пов'язаної зі складністю обробки численних запитів (10.000 запитів та більше). Створений ним веб-сервер успішно справлявся з високими навантаженнями, чим і зумовлено його подальшу популярність, незважаючи на існування серйозного конкурента в особі веб-сервера Apache:

- Nginx демонструє високу швидкість обробки підключень статичного контенту. За цим показником він обходить найближчого конкурента вдвічі. Продуктивність під час роботи з динамічними сайтами в обох програмних продуктів приблизно однакова;
- є менш вимогливим до пам'яті, ніж веб-сервер Apache;
- підтримує багато популярних операційних систем. Однак він розроблявся для UNIX-систем. Сумісність з Windows реалізована слабо, тому швидкість роботи програмного забезпечення в цій системі досить низька.

Щоб об’єднати переваги обох найпопулярніших веб-серверів, почали використовувати зв'язок Apache + Nginx. Останній розгортається перед Apache для виконання функцій реверс-проксі. За обробку всіх запитів відповідає Nginx, здатний успішно справлятися з їх великою кількістю. Його основне завдання у цій конфігурації – обробка статичного контенту. Якщо потрібно виконання, наприклад, PHP-сценаріїв, запит надходить на Apache, де відбувається його обробка. Отриманий результат передається спочатку Nginx, а потім кінцевому користувачеві.

Таким чином, Nginx сортує запити на статичні та динамічні. З першими він успішно справляється сам, другі – адресує Apache. Цей підхід спричиняє часткове зниження навантаження на останній.

3. Cloudflare використовує CDN як інфраструктуру, через яку можна направити роботу домену між відвідувачем сайту та сервером, де він зберігається. Якщо відкрити такий сайт через браузер, то він визначить веб-сервер сайту як cloudflare, тому що від нього отримав відповідь на запит, але на сервері все-одно використовується одне з популярних програмних забезпечень. Тому, даний пункт вважаю доцільним вилучити з розгляду.

4. Microsoft IIS – це веб-сервер, розроблений компанією Microsoft для своїх операційних систем. Продукт повністю пропрієтарний та йде в комплекті з Windows. Перша версія з'явилася у Windows NT і продовжує розвиватись. За промовчанням IIS вимкнено в операційній системі. Для його активації необхідно зайти в панель керування та активувати як компонент [5].

5. LiteSpeed — веб-сервер, розроблений компанією LiteSpeed Technologies, який є альтернативою

веб-серверу Apache і сумісний із найбільш поширеними його можливостями. В першу чергу, LiteSpeed цікавий тим, що дозволяє прискорити роботу сайтів за рахунок використання спеціалізованих плагінів для різних CMS [6].

LiteSpeed технологія забезпечує високу продуктивність та можливість обробки великої кількості трафіку завдяки використанню нового принципу кешування – технології LSCache. Сайти завантажуються швидше, а кеш не потрібно налаштовувати додатково, тому що всі необхідні налаштування включені за замовчуванням в базову версію ПЗ.

Хоча популярність даного програмного забезпечення відносно малий, але на думку автора є найцікавішим серед інших веб-серверів.

6. Google Web Server (GWS) – веб-сервер розроблений компанією Google для підтримки власних онлайн сервісів, який працює на базі Linux систем. Сервер використовується компанією для власних застосувань, таких як Blogger, Google Docs, та Google App Engine. Дане програмне забезпечення не поширюється серед клієнтів для встановлення на своїх серверах, тому невідома реалізація захисту інформації.

Отже, з розгляду найпоширеніших веб-серверів в мережі інтернет, можна дійти висновку, що власники сайтів на серверах з операційними системами Linux використовують Apache, Nginx, LiteSpeed, та займають приблизно 85% ринку.

Захист сайтів по IP

В першу чергу розглянемо більш складну реалізацію захисту в Nginx. В даному прикладі потрібно редагувати конфігураційний файл на сервері, та якщо він неправильно записаний, сервіс Nginx може зупинити свою роботу з помилками і всі відвідувачі сайтів не матимуть доступ до сайтів, поки не відновиться робота веб-серверу. Тому, перед роботою з файлами рекомендуємо зберегти їх копії.

1. Відкриваємо встановленим редактором на сервері файл конфігурації веб-серверу, наприклад за допомогою vim:

```
vim /etc/nginx/nginx.conf
```

2. Прописуємо у секцію server наступну строку:

```
include /etc/nginx/blacklist.conf;
```

3. Створюємо новий файл blacklist.conf за вказаним шляхом та добавляємо в нього правила блокування:

```
deny 192.168.1.0/24;
deny 192.168.2.102;
```

В даному прикладі ми прописали цілу підмережу 192.168.1 та окремо IP-адресу 192.168.2.102, вказавши правило як deny, тобто заблокували. Також можна розблокувати окрему адресу з-під мережі, прописавши перед нею значення allow.

4. Перевірити чи правильно запуститься веб-сервер з новими правилами можна за допомогою команди nginx -t, якщо все правильно, в консолі буде приблизно наступне повідомлення:

```
the configuration file /etc/nginx/nginx.conf syntax is ok
configuration file /etc/nginx/nginx.conf test is successful
```

В інакшому випадку потрібно перевіряти змінені файли та виправити помилки, щоб при перезапуску серверу або сервісу Nginx сайти працювали коректно.

5. Щоб нові правки вступили в силу, потрібно перезапустити Nginx за допомоги команди:

```
service nginx restart
```

Якщо з заблокованої IP-адреси перейти на сайт, який знаходиться на цьому сервері, в браузері отримуємо повідомлення, як зображено на рисунку 2.

Рисунок 2 – помилка доступу до сервісу на веб-сервері Nginx

Обмеження доступу до сайту на веб-серверах Apache та LiteSpeed налаштовуються легше та гнучкіше, тому що окремі правила можна добавляти для окремих сайтів у файли .htaccess.

.htaccess - це конфігураційний файл веб-сервера Apache/LiteSpeed, який дозволяє керувати роботою веб-сервера та налаштуваннями сайту за допомогою різних параметрів (директив) без зміни основного конфігураційного файлу веб-сервера.

Щоб заблокувати доступ до сайту:

1. Редагуємо файл .htaccess серед файлів сайту, якщо його нема, то створюємо:
   vim .htaccess
2. Підключаємо директиву order та описуємо логіку роботи обмеження:
   order deny, allow # - сповіщає серверу блокувати усі адреси окрім обраних
   order allow, deny # - сповіщає серверу дозволяти запити усіх адрес окрім обраних
3. З наступної строки прописуємо правила по порядку вказання операторів, наприклад, щоб заблокувати всі адреси окрім 192.168.0.1:
   order deny, allow
   deny from all
   allow from 192.168.0.1

На цьому алгоритм дій для блокування адрес за допомоги Apache/LiteSpeed закінчується. Сервіси непотрібно перезапускати, при допущенні помилок, доступ може зникнути тільки до обраного сайту поки не виправляться помилки у файлі .htaccess. Також даним методом можна заблокувати окремі директорії сайту або відповідні сторінки, надаючи доступ до всього іншого контенту.

Висновки

За останні 10 років об’єм інформації збільшився в мережі в 40 раз та питання захисту даних актуально як ніколи. Багато людей створюють веб-сайти для розгортання онлайн-магазинів, розповсюдженню новин або для ведення форуму про хобі. Нові додатки та сервіси дозволяють створювати громіздкі портали з великою кількістю даних без навичок та розуміння мов програмування. Такі сервіси найчастіше розташовують на поширених та безкоштовних веб-серверах Apache, Litespeed та Nginx. Дані програмні забезпечення підтримують блокування доступу до серверу за допомогою прописання правил у конфігурацію та власники сайтів таким чином можуть захищати доступ від небажаних гостей.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Вебсервер [Електронний ресурс]. – Режим до доступу: uk.wikipedia.org/wiki/Вебсервер (дата звернення: 20.04.2022). — Назва з екрана.
2. What Is the Most Popular Web Server Application? [Електронний ресурс]. – Режим до доступу: digitalintheround.com/what-is-the-most-popular-web-server (дата звернення: 20.04.2022). — Назва з екрана.
3. Apache [Електронний ресурс]. – Режим до доступу: freehost.com.ua/faq/wiki/apache-chto-eto (дата звернення: 20.04.2022). — Назва з екрана.
4. Nginx [Електронний ресурс]. – Режим до доступу: freehost.com.ua/faq/wiki/chto-takoe-nginx (дата звернення: 20.04.2022). — Назва з екрана.
5. IIS – Принцып работи [Електронний ресурс]. – Режим до доступу: itglobal.com/ru-ru/company/glossary/iis (дата звернення: 20.04.2022). — Назва з екрана.
6. LiteSpeed – переваги веб-сервера на віртуальному хостингу [Електронний ресурс]. – Режим до доступу:hyperhost.ua/info/uk/litespeed-perevagi-veb-servera-na-virtualnomu-khostingu (дата звернення: 20.04.2022). — Назва з екрана.

Марунчак Єгор Олександрович – студент групи КІТС-18б факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: EgorMarunhcak27@gmail.com.

Науковий керівник: ***Шиян Анатолій Антонович*** – доцент кафедри менеджменту та базпеки інформаційних систем, кандидат фізико-математичних наук.

Marunchak Yegor Oleksandrovych - faculty of management and information security, Vinnytsia National Technical University, Vinnytsia.

Scientific adviser: ***Shiyan Anatoly Antonovich*** - associate professor of management and security of information systems, candidate of physical and mathematical sciences.