КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.17.91111
УДК 004.49

Лактіонов Ілля Олександрович
Студент спеціальності “Кібербезпека”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-0562-2306
illia.laktionov.kb.2020@lpnu.ua

Кміть Андрій Юрійович
Студент спеціальності “Кібербезпека”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8854-818X
andrii.kmit.kb.2020@lpnu.ua

Опірський Іван Романович
д.т.н., проф., професор кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Гарасимчук Олег Ігорович
к.т.н., доц., доцент кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ ЗАХИСТУ ІНТЕРНЕТ-РЕСУРСІВ ВІД DDOS-АТАК ПІД ЧАС КІБЕРВІЙНИ

Анотація. На сьогоднішній день інформаційні технології проникли у всі сфери життя суспільства. У зв’язку із стрімким розвитком науково-технічного прогресу змінюються і традиційні методи введення війн, які тепер ведуться не лише на полях боїв але й в кібернетичному просторі суспільства. Сучасний світ характеризується активними війнами у кіберпросторі де одними із найбільш поширених атак є DDoS-атаки, зокрема й на об’єкти критичної інфраструктури. Це в першу чергу пов’язано із надзвичайною щільністю інтегрування у життя та діяльність суспільства різноманітних гаджетів, електронних пристроїв та Інтернету, порушення нормального функціонування яких здатне завдати значної шкоди – як психологічної, так і матеріальної, а також нанести значної шкоди ворогу зсередини. Одним із найпростіших та найпопулярніших методів для порушення такого нормального функціонування є застосування перевантаження ресурсів, що може привести навіть до їх повної недоступності. Одним із способів такого перевантаження є застосування DDoS-атаки – атаки на відмову сервісу. Масове надсилання зовнішніх запитів на ресурс, що атакується призводить до того що такий ресурс в короткий проміжок часу намагається опрацювати значну кількість запитів внаслідок чого його робота буде значно сповільненою або навіть це може призвести до повної зупинки ресурсу. Дана робота присвячена дослідженню методів за допомогою яких проводяться DDoS-атаки. Детально розглянуті найбільш поширені методи їх здійснення та базові способи захисту від них. В цій роботі детально розглянуто технології та методи захисту від DDoS-атак, проаналізовано і порівняно існуючі готові рішення компаній щодо надання захисту. Але оскільки інформаційні технології стрімко розвиваються, розвиватимуться і DDoS-атаки. Тому питання захисту від них є актуальним, особливо в умовах кібернетичної війни.

Ключові слова: DoS, DDoS, DDoS-атака, інтернет, інтернет-ресурс, кібервійна, гібридна війна.

ISSN 2663 - 4023

ВСТУП

В сучасному світі, окрім звичайних збройних конфліктів, країни воюють і в кіберпросторі. Одним з популярних засобів кібервійни є DDoS-атаки.

Багато століть війна обмежувалась лише збройними конфліктами на полі бою, які еволюціонували від луків і мечів до танків і ракет. Науково-технічний прогрес розвивається неймовірно стрімко, а разом з ним змінюються і методи ведення війни. Гаджети, електроніка та Інтернет все щільніше інтегруються в функціонування суспільства, тому сьогодні бойові дії ведуться не тільки на землі, а й у кіберпросторі. Оскільки багато сфер життя переноситься в онлайн, то порушення роботи необхідних сервісів здатне завдати значної шкоди – як психологічної, так і матеріальної.

Простий і популярний метод привести щось в негідність – перенавантаження. Так, можна навантажити деякий веб-ресурс, поки він не стане недоступний. Це якраз і є DOS-атака (англ. *Denial of service attack* – атака до відмови сервісу).

Суть DDoS-атаки полягає в масовому надсиланні на атакований комп'ютер або мережеве обладнання великої кількості зовнішніх запитів. Вони можуть не мати сенсу або бути сформульованими неправильно – головне, аби ціль прийняла запит і обробляла. І через те, що атаковане устаткування в короткий проміжок часу намагається опрацьовувати величезні кількості запитів, то його робота значно уповільнюється або повністю припиняється.

Є два варіанти досягнути відмови сервісу:

1. Примус атакованої цілі до зупинки роботи апаратної та/або програмної частини, або до значних витрат ресурсів, що ускладнює або унеможливлює подальшу роботу.

2. Заняття каналів зв'язку між користувачами та атакованою ціллю, внаслідок чого втрачається сполучення з користувачами та устаткуванням.[4]

Звичайно, як з появою мечів з'явилися лати, так і з появою DDoS-атак з'явився і захист від них.

Основні методи захисту від DDoS-атак:

1. Зменшення доступних для атаки зон

Цей засіб значно звужує простір, який можна атакувати. Необхідно переконатись, що доступ до сервісу закритий в тих місцях, в які не повинні потрапляти користувачі – порти, протоколи, додатки, API. Таким чином, зменшення кількості точок атаки дозволяє зосередити зусилля на них, підвищуючи рівень безпеки.

2. Масштабування

Спираючись на два варіанти досягнення відмови сервісу, що наведені вище, можна відповідно виділити два варіанти протидії:

– Обчислювальна потужність серверу

Більшість DDoS-атак вимагають значних апаратних ресурсів, тому важливо мати змогу швидко збільшувати та зменшувати обсяги потужності своїх серверів. Якщо DDoS-атака буде слабша за сервер, то він вистоїть, хоч і з можливими перебоями та уповільненням в роботі. Великі хостинг-провайдери розподіляють апаратні ресурси між своїми клієнтами, збільшуючи потужність при DDoS-атаках та зменшуючи при їх відсутності.

– Пропускна потужність

При проєктуванні сервісу необхідно переконатись, що постачальник послуг хостингу забезпечує надлишкову пропускну здатність при підключення до мережі Інтернет, а також дозволяє опрацьовувати великі об'єми трафіку. Оскільки метою DDoS-атаки є вплив на доступність веб-ресурсів, то розміщувати їх необхідно не тільки поруч

з кінцевими користувачами, а й в крупних вузлах обміну міжмережевого трафіку. Це легко забезпечить користувачам доступ до сервісу навіть при великих об'ємах трафіку

3. Інформація про типовий та нетиповий трафік

Щоразу при виявленні підвищених об'ємів трафіку, що потрапляють на хост, в якості орієнтиру можна взяти максимально можливий об'єм, який здатен обробити хост без погіршення доступності. Таку концепцію називають обмеженням швидкості. Більш просунуті методи захисту здатні інтелектуально аналізувати окремі пакети трафіку і приймати тільки дозволені.

4. Фаєрвол

Проти атак, які намагаються використовувати вразливості додатку, рекомендується застосовувати WAF – Web Application Firewall. Через унікальність таких атак власники атакованного сервісу повинні бути в змозі самостійно нейтралізувати заборонені запити. Їх можна виявляти через підозрілі IP-адреси, географічні регіони тощо.[2]

Постановка проблеми. Інформаційні технології щільно інтегрувалися з нашим життям. І мова не лише про переписки молоді в месенджерах і фотографії котиків, а буквально про усе на світі. Комп'ютери зараз абсолютно всюди, в кожній сфері життя. Замість голубиної пошти – e-mail, замість стопок паперів – електронні документи, замість телеграфних ліній – оптоволокно.

Багато з нас вважають Інтернет та комп'ютерні технології найвеличнішими винаходами людства. І так історично склалося, що деякі люди з певних причин прагнуть нанести шкоди іншим. Так людство створило інший винахід. Він жахливий, жорстокий, через нього назавжди зникали цілі цивілізації. Цей винахід – війна. І коли стоїть ціль завдати максимальної шкоди, агресори вдаються до всіх можливих і неможливих способів. Поки одні армії руйнують міста, що вони ззовні стають схожими на справжнє пекло, інші армії руйнують життя соціуму зсередини.

Як вже було зазначено, наше життя наскрізь пронизано інформаційними технологіями: зв'язок, новини, банкова справа, економіка. Саме тому бойові дії розповсюдились не лише на окопи, а й на кібернетичний простір суспільства. Найжахливіший винахід еволюціонував і приніс в світ кібервійну. На превеликий жаль, вона не оминула і Україну.

Аналіз останніх досліджень і публікацій. 23 грудня 2015 року росією було успішно атаковано та виведено з ладу три енергопостачальні компанії України. Сотні тисяч людей та підприємства залишились без електроенергії. Наступна успішна кібератака на енергетичну систему відбулася буквально через рік, в ніч на 18 грудня 2016 року [1]. І через ще менший період часу, в червні 2017 року відбулася найбільш відома хакерська атака на Україну – вірусом NotPetya [3].

Цифрове протистояння не стихає ні на мить. І після повномасштабного вторгнення росії в Україну 24 лютого 2022 року кібератак стало тільки більше.

Однією з найпопулярніших кібератак є DDoS – це ніби артилерійський обстріл. Якщо атака ведеться з великої кількості IP-адрес, то вона стане розподіленою атакою до відмови сервісу (англ. *Distributed Denial of service attack*) – DDoS.[4]. Зрозуміло, що питання захисту стоїть особливо гостро. Сьогодні, звичайно, існують засоби відгородити себе від такого роду небезпеки, але одного універсального найкращого рішення не існує. Тому розробки необхідного програмного забезпечення в цьому напрямку є вкрай актуальними і необхідними. Ми провели дослідження методів і технології захисту від DDoS-атак, розглянули та проаналізували існуючі інструменти оборони.

Мета статті. Метою статті є дослідження методів проведення DDoS-атак та дослідження наявних засобів захисту від них.

№ 1 (17), 2022
ISSN 2663 - 4023

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Здійснення DDoS-атак

DDoS-атака – це розподілена атака до відмови сервісу в обслуговуванні на комп'ютерний ресурс з метою вивести його з ладу, зробити недоступним для користувачів. Цей тип атаки може бути спрямований не тільки на веб-сайти, а й на програмні комплекси, електронну пошту, голосову пошту, різного типу комп'ютерні мережі.

Оскільки атака є розподіленою (distributed), то це означає, що вона здійснюється з величезної кількості дистанційно керованих комп'ютерів шляхом спрямування потоків хибного мережевого трафіку до цілі. Внаслідок цього обчислювальні потужності цілі перевантажені опрацюванням запитів від атакуючих комп'ютерів так, що не мають ресурсів і часу для обробки та надання відповідей на запити реальних користувачів. В результаті відбуваються або значні затримки між запитами та відповідними відповідями, або повна відмова системи - "падіння".

Розподіленість атаки

Як зазначалось вище, DDoS-атаки потребують великої кількості комп'ютерів, з яких буде вестись атака, і це можливо досягти двома способами:

1. Ботнет

Ботнет, тобто мережа ботів, це комп'ютери, що заражені спеціальними програмами, які дозволяють зловмиснику, власнику ботнета, дистанційно надавати інструкції зараженим, керуючи ними наче справжньою армією.

Переваги:

Використовуються реальні користувачі з різними комп'ютерами – так запити під час атаки виглядають максимально правдоподібно. Також, використовуючи ботнет, зловмисник не обтяжує себе захистом (наприклад, proxy) на випадок, якщо атакована ціль захоче знайти кривдників – в такому разі в двері постукають саме до власника зараженого комп'ютера.

Недоліки:

– Оскільки DDoS-атаки потребують деякої потужності, користувач може помітити, що його комп'ютер працює повільніше, ніж раніше. Після цього користувач може або придбати новий "чистий" комп'ютер, або перевірити свою систему антивірусним ПЗ, що призведе то -1 боту в мережі.

– З попереднього пункту випливає обмеженість використання потужностей комп'ютерів, що негативно впливає на ефективність DDoS.

2. Флешмоб

Флешмоб – це узгоджена робота великого числа користувачів із здійснення атак. Якщо ботнет порівнювати з примусовою армією, то флешмоб – це добровільна служба.

Переваги:

– Не виникає проблем з законом через зараження вірусом.

– При чинній мотивації обсяги флешмобу будуть набагато більші, ніж з ботнетом, і будуть набагато швидше зібрані.

– На відміну від ботнету, який орієнтується на зараження комп'ютерів з ОС Windows, флешмоб можна застосовувати на macOS, Linux, та будь-де, де цього захоче сам користувач.

– Більша потужність атаки:

- Комп'ютери, які беруть участь в DDoS, можуть бути увімкненим 24/7 для цілодобової атаки.

- Використання потужних серверів (оскільки майже всі сервери на Linux, то заразити їх ботнетом є досить непростою задачею),
- Використання комп'ютеру так, як би цього не дозволили можливості вірусу та антивірусного ПЗ (наприклад, з правами адміністратора).

Яскравим прикладом потужного флешмобу є масові DDoS-атаки на російські сервіси під час повномасштабної війни росії проти України в 2022 році. Внаслідок роботи десятків тисяч українців, в росії "падали" новинні сайти з пропагандою, банківські системи, системи бухгалтерського обліку тощо.

Флуд

Найпоширеніший тип DDoS-атак заснований на ідеї флуда, інакше кажучи, завалення цілі дуже великою кількістю пакетів.

Флуд буває різним:

– ICMP

– SYN

– UDP

– HTTP

Сучасні інструменти DDoS можуть застосовувати всі ці види флуду водночас, тому варто заздалегідь попіклуватися про надійний захист. [4]

Види флуду та захист від них

1. ICMP-флуд

Це дуже примітивний метод засмічення пропускної смуги і навантаження мережевого стеку через звичайнісіньку відправку запитів ICMP ECHO – просте пінгування.[4 – 5]

Приклад виконання:

ping -i 0 -s 10000 -l 100 -q example.com

-i – Інтервал часу між надісланими пакетами. Встановлювати інтервал менше 200 мс може тільки адміністратор (sudo).

-s – Розмір пакету в байтах. За замовчуванням 54, максимум 65507 байт.

-l – Кількість пакетів, які надсилаються без очікування відповіді.

-q – Виведення на екран лише результатів.

Цей флуд легко виявити, проаналізувавши потоки трафіку в обидві сторони – при атаці ICMP вони майже ідентичні.

Захист

Спосіб простий і майже не має побічних ефектів – відключення відповідей на запити ICMP ECHO:

sysctl net.ipv4.icmp_echo_ignore_all=1

Також, можна використати брандмауер:

iptables -A INPUT -p icmp -j DROP --icmp-type 8

2. SYN-флуд

Це один з популярних методів аби не лише засмітити канал зв'язку, а ще й ввести мережевий стек ОС в такий стан, що він буде не здатний приймати запити на підключення. Цей спосіб базується на ініціалізації великої кількості одночасних TCP-з'єднань надсиланням SYN-пакету із зворотною адресою, якої насправді не існує. Після декількох спроб надіслати ACK-пакет у відповідь на неіснуючу адресу більша частина ОС ставлять це невдале з'єднання в чергу, і лише після деякої n-ої спроби все-таки закривають з'єднання. І через те, що потік пакетів ACK дуже великий, черга швидко заповнюється, і ядро ОС дає відмову на відкривання нових з'єднань. Найбільш просунуті інструменти DDoS, окрім всього, ще додаткового аналізують систему перед тим, як почати атаку, аби надсилати запити тільки на відкриті особливо важливі порти.

Захист

Розпізнати такий флуд досить просто: необхідно спробувати під'єднатися до одного з сервісів. Захисні дії включають в себе:

– Збільшення черги недовідкритих (невдалих) TCP-з'єднань:

sysctl -w net.ipv4.tcp_max_syn_backlog=1024

– Зменшення часу тримання недовідкритих з'єднань в черзі:

sysctl -w net.ipv4.tcp_synack_retries=1

– Застосування механізму TCP syncookies:

sysctl -w net.ipv4.tcp_syncookies=1

– Обмеження максимальної кількості недовідкритих з'єднань з однієї IP-адреси до одного порту:

iptables -i INPUT -p tcp --syn --dport 80 -m iplimit --iplimit-above 10 -j DROP

3. UDP-флуд

Це типовий метод заповнення смуги пропускання. Він базується на нескінченному надсиланні пакетів UDP на порти різних UDP-сервісів.

Захист

Усунути цей вид флуду можна досить легко – просто відділити такі сервіси від зовнішнього світу й встановити обмеження на кількість з'єднань за одиницю часу до DNS-сервера на стороні шлюзу:

iptables -i INPUT -p udp --dport 53 -j DROP -m iplimit --iplimit-above 1

4. HTTP-флуд

HTTP-флуд є одним з найпоширеніших на сьогоднішній день. Засновується на безперервному надсиланні HTTP GET-запитів на порт 80 щоб перевантажити WEB-сервер настільки, щоб він не зміг опрацьовувати запити від користувачів. Часто метою HTTP-флуду є не корінь веб-сервера, а лише один із скриптів, які виконують ресурсоємні задачі або працюють з базами даних. Про початок атаки сигналізує аномально стрімке зростання логів веб-сервера.

Захист

Для захисту проти флуду HTTP використовується модифікація веб-сервера і баз даних для зниження впливу атаки, а також фільтрація DDoS-користувачів різними прийомами:

– Збільшення максимальної кількості з'єднань з базами даних одночасно.

– Встановити перед веб-сервером Apache легкий і ефективний nginx, який буде кешувати запити і видавати статику. Це рішення є просто найнеобхіднішим, бо воно не лише знижує ефект від DDoS-атак, а й загалом дозволяє серверу витримувати великі навантаження. Наприклад:

```
# vi /etc/nginx/nginx.conf
# Збільшення максимального числа використовуваних файлів worker_rlimit_nofile 80000;
events {
# Збільшення максимального числа з'єднань
worker_connections 65536;
# Використання ефективного методу epoll для обробки з'єднань
use epoll;
}
http {
gzip off;
# Відключення таймауту на закриття з'єднань keep-alive
keepalive_timeout 0;
# Не надавати версію nginx в заголовку відповіді
server_tokens off;
# Скидати з'єднання після таймауту
reset_timedout_connection on;
```

```
}
# Стандартні налаштування для роботи як проксі
server {
listen 111.111.111.111 default deferred;
server_name host.com www.host.com;
log_format IP $remote_addr;
location / {
proxy_pass http://127.0.0.1/;
}
location ~* \.(jpeg|jpg|gif|png|css|js|pdf|txt|tar)$ {
root /home/www/host.com/httpdocs;
}
```

Готові рішення захисту від DDoS

Оскільки усі готові рішення використовують одні і ті ж методи захисту від DDoS-атак, доречно буде порівнювати не рішення, а саме технології які вони використовують. Найпопулярніші технології захисту від DDoS-атак надають захист від атак 3, 4 та 7 рівня.

Для того, щоб зрозуміти що таке атаки DDoS рівня 7, нам необхідно зрозуміти що означає цей рівень. Рівень 7 належить до атак прикладного рівня моделі OSI (Open System Interconnection). Цей рівень є верхнім шаром та використовується різними додатками на сервері.

Атаки рівня 7 зосереджені на особливостях цього шару таких як HTTP (HyperText Transfer Protocol), SNMP (Simple Network Management Protocol), FTP (File Transfer Protocol) та інших. Атаки рівня 7 потребують набагато меншої смуги пропускання та пакетів, ніж для атак мережевого рівня щоб пошкодити роботу сервісів. Наприклад, атака мережевого рівня, така яка SYN-потік потребує великої кількості пакетів для ефективної реалізації. Слід враховувати що обмежена кількість пакетів може виконати DDoS-атаку у великих масштабах. HTTP потоки є найпомітнішими елементами DDoS-атак на рівні додатку. Коли HTTP запит відправляється на сервер він використовує значні ресурси, отже обмежена кількість цих пакетів може задіяти усі ресурси сервера.

Атаки на потоки HTTP, як правило, зосереджені на додатках, які використовують багато ресурсів, як правило це веб-додатки. Дуже важко ідентифікувати атаку рівня 7, оскільки пакети на сервері є обмежені. Коли пакети падають на сервер ви не можете відрізнити справжній запит від атаки. HTTP атаки як правило використовують POST запити, тому що саме вони використовують найбільше ресурсів сервера та можуть призвести до збою в роботі додатку.

DDoS-атака рівня 3 атакує цільовий рівень 3 у моделі OSI. Мета атаки рівня 3 полягає в тому, щоб уповільнити або призвести до збою програми, служби, комп'ютера чи мережі або заповнити ємність, щоб ніхто інший не міг отримати послугу. DDoS-атаки рівня 3 зазвичай досягають цього, націлюючись на мережеве обладнання та інфраструктуру.

Існує кілька важливих відмінностей між DDoS-атаками рівня 3 і атаками на вищих рівнях:

– Атаки рівня 3 спрямовані на мережевий рівень, а не на процеси транспортного або прикладного рівня (як це роблять атаки рівня 4 і рівня 7 DDoS)

– Атаки рівня 3 не повинні спочатку відкривати TCP-з'єднання з ціллю

– Атаки рівня 3 не спрямовані на певний порт

Рівень 3 OSI називається мережевим рівнем. Рівень 3 містить протоколи та технології, які роблять можливими взаємопов'язані мережі – іншими словами, Інтернет. На цьому рівні здійснюється маршрутизація між мережами. Дані, які перетинають мережі, поділяються на пакети, і ці пакети адресуються та відправляються до місця

призначення на рівні 3. Найважливішим протоколом для цього процесу є протокол Інтернету (IP).

Протоколи на рівні 3 не відкривають з'єднання, не забезпечують надійну доставку даних і не вказують, яка служба цільового пристрою має використовувати ці дані; це процеси 4-го рівня. Рівень 4 передбачає використання транспортних протоколів, таких як TCP і UDP. Пересилання пакетів через мережі без транспортного протоколу рівня 4 схоже на відправку листа на адресу, не переконавшись, що адреса правильна, включаючи ім'я конкретної особи за цією адресою, яка має відкрити лист, або використання авторитетної поштової служби доставки . Дані можуть надійти, а можуть і ні. Ось чому багато протоколів рівня 3 завжди використовуються разом із транспортним протоколом рівня 4, який забезпечує передачу даних у потрібне місце.

Проте все ще можна надсилати пакети даних до адресата мережі через IP без використання транспортного протоколу.

Оскільки рівень 3 не має з'єднання, DDoS-атакам рівня 3 не потрібно відкривати з'єднання через TCP або вказувати призначення портів. DDoS-атаки рівня 3 спрямовані на мережеве програмне забезпечення, яке працює на комп'ютері, а не на певний порт.

Як і у випадку з іншими типами DDoS-атак, зловмисник надсилає через ці протоколи великий обсяг небажаного мережевого трафіку. Існують різні методи для цього, залежно від протоколу. Сміттєвий трафік заважає законним запитам користувачів, сповільнюючи відповіді на них або взагалі блокуючи їх. Іноді є так багато небажаних даних, що вони перевантажують ресурси цілі, і ціль виходить з ладу.

Хоча можливі й інші атаки, включаючи атаки лише через IP, атаки на основі ICMP є найпоширенішими. Добре відомі атаки ICMP включають:

– *Ping flood*: під час DDoS-атаки ping flood зловмисник надсилає тисячі або навіть мільйони запитів ping на сервер одночасно.

– *Атака Smurf*: ICMP не має заходів безпеки або перевірки, що дає можливість зловмиснику підробити IP-адресу в запиті ICMP. Під час DDoS-атаки Smurf зловмисник надсилає запити ping на тисячі серверів, підробляючи IP-адресу цілі в запитах ping, щоб відповіді надходили до цілі, а не до зловмисника. Більшість сучасного мережевого обладнання більше не вразливі до цієї атаки.

– Ping of death: під час атаки ICMP ping of death зловмисник надсилає цілі запит на пінг, який перевищує максимально допустимий розмір. Маршрутизатори на шляху до цілі фрагментують ping на менші пакети, щоб ціль приймала їх, але коли вона намагається зібрати великий пакет з менших фрагментів, розмір пакета перевищує максимальний і збиває ціль. Сучасні пристрої не вразливі до цієї атаки.

Рівень 4 моделі OSI, також відомий як транспортний рівень, керує мережевим трафіком між хостами та кінцевими системами, щоб забезпечити повну передачу даних. Протоколи транспортного рівня, такі як TCP, UDP, DCCP і SCTP, використовуються для керування обсягом даних, куди вони надсилаються та з якою швидкістю.

Забезпечуючи стандартизований доступ до комунікаційних послуг, таких як зв'язок, орієнтований на з'єднання, надійність, контроль потоків і мультиплексування, рівень 4 усуває потребу, щоб рівні 5-7, орієнтовані на застосування, розглядали характеристики самої комунікаційної мережі. Рівень 4 також відповідає за наскрізне відновлення помилок.

Оскільки рівень 4 координує передачу даних без видимості вмісту повідомлень, балансування навантаження рівня 4 може приймати рішення щодо маршрутизації без необхідності дешифрування або перевірки мережевого трафіку. Це робить балансування навантаження рівня 4 швидким та ефективним підходом до балансування навантаження на рівні пакетів на основі простих алгоритмів, таких як циклічна маршрутизація.

Для маршрутизації трафіку на основі типу медіа, правил локалізації, програми або інших критеріїв, де потрібна перевірка повідомлень, необхідно використовувати балансування навантаження рівня 7.

DDoS-атаку рівня 4 часто називають SYN-флудом. Він працює на рівні транспортного протоколу (TCP). З'єднання TCP встановлюється за допомогою так званого тристороннього рукостискання. Клієнт надсилає пакет SYN, сервер відповідає SYN ACK, а клієнт відповідає на це ACK. Після завершення «тристороннього рукостискання» з'єднання TCP вважається встановленим. Саме в цей момент програми починають надсилати дані за допомогою протоколу рівня 7 або прикладного рівня, такого як HTTP.

SYN flood використовує притаманне стеку TCP очікування, щоб перевантажити сервер, посилаючи потік SYN-пакетів, а потім ігноруючи SYN ACK, повернуті сервером. Це призводить до того, що сервер витрачає ресурси, очікуючи налаштований проміжок часу для очікуваного підтвердження ACK, яке має надійти від законного клієнта. Оскільки веб-сервери та сервери додатків обмежені в кількості одночасних TCP-з'єднань, які вони можуть відкрити, якщо зловмисник надсилає на сервер достатню кількість пакетів SYN, він може легко обробляти дозволену кількість TCP-з'єднань, таким чином запобігаючи відповіді на законні запити з боку сервера.

Потоки SYN досить легко виявити для доставки додатків на основі проксі та продуктів безпеки. Оскільки вони проксі-з'єднання для серверів і, як правило, засновані на апаратному забезпеченні з набагато вищим лімітом TCP-з'єднань, рішення на основі проксі може обробляти великий обсяг з'єднань без перевантаження. Оскільки рішення на основі проксі-сервера зазвичай розриває TCP-з'єднання (тобто це «кінцева точка» з'єднання), воно не зможе передати з'єднання на сервер, поки не завершить трьохстороннє рукостискання. Таким чином, SYN flood зупиняється на проксі-сервері, і легітимні з'єднання швидко передаються на сервер.

Як правило, зловмисникам зупиняється переповнення мережі за допомогою файлів cookie SYN. Файли cookie SYN використовують криптографічне хешування, і тому є дорогими з точки зору обчислень, тому бажано дозволити рішенням проксі/доставки з апаратним прискоренням криптографічних можливостей обробляти цей тип заходів безпеки. Сервери можуть впроваджувати файли cookie SYN, але додаткове навантаження на сервер значно полегшує виграш, досягнутий шляхом запобігання SYN flood, і часто призводить до доступних, але неприпустимо повільних серверів і сайтів.[13]

Clean Pipes

Clean Pipes (“Чиста труба”), мабуть, є найпоширенішою технікою пом’якшення DDoS-атак. Основний принцип чистого каналу – як випливає з назви – досить простий: весь вхідний трафік повинен проходити через центр «чистої труби», який також відомий як «центр очищення», де система ідентифікує та блокує шкідливий трафік, дозволяючи лише легітимний трафік. щоб отримати доступ до сервера.

“Чиста труба”є ефективною для пом’якшення DDoS-атак і запобігання помилкових спрацьовувань (блокування законного трафіку), вона також відома своєю складністю в реалізації. Для цього знадобиться маршрутизатор BGP (Border Gateway Protocol) і спеціальний пристрій, здатний завершити тунель GRE.

Крім того, є деякі ключові обмеження методу “чистої труби”:

– Це не завжди актуальне рішення. Коли буде виявлено вектор атаки, знадобиться деякий час, щоб перенаправити трафік до центру очищення, для чого знадобиться щонайменше кілька хвилин, перш ніж почнеться фактичне пом’якшення.

– Незважаючи на те, що техніка чистої труби ефективна при обробці об'ємних DDoS-атак, вона не дуже ефективна в обробці атак на основі вразливостей.

– Ваш IP-префікс не прихований, тому теоретично зловмисник може виявити вашого провайдера та проаналізувати вашу інфраструктуру, щоб знайти вразливі місця.

– Через його складність може знадобитися людське втручання.

Однак, незважаючи на свої слабкі сторони, техніка чистої труби дуже універсальна. Можна вважати її майстром на всі руки техніки пом'якшення DDoS. Вона підтримує майже всі програми в стеку IP, але не має розширеного захисту для будь-якого конкретного випадку використання. Прекрасний варіант, якщо необхідне грамотне рішення.[6-8]

CDN Dilution

Мережа доставки вмісту (CDN Dilution) – це велика розподілена система серверів, які безпечно доставляють веб-сторінки, зображення та інший онлайн-контент користувачам залежно від його географічного розташування.

Цей тип техніки пом'якшення DDoS використовує CDN для зменшення трафіку ботів. Основний принцип полягає в тому, що CDN використовує віртуальний сервер для розповсюдження вмісту користувачеві з місця, яке набагато ближче до користувача, ніж вихідний сервер.

З огляду на це, техніка розведення CDN використовує величезну пропускну здатність, яку пропонує технологія CDN, для пом'якшення та поглинання DDoS-атак, особливо об'ємних (рівень 3 і рівень 4) DDoS-атак. Граничні сервери в мережі CDN працюють як зворотний проксі для веб-додатка: усі запити обробляються та фільтруються граничним сервером, перш ніж вони будуть відправлені назад до джерела.

Ключовою перевагою методу розведення CDN є те, що він залежить від контексту, тому дуже ефективний у захисті веб-додатків. Однак основним недоліком є те, що він застосовний лише до веб-додатків, а не до власних виділень TCP/UDP. Це постійне рішення, яке не потребує часу на виконання, що робить його дуже повним захистом від DDoS для веб-програм.[8-10]

TCP/UDP Proxy DDoS Protection

Якщо ваш веб-сайт або платформа складається із служб TCP/UDP, таких як електронна пошта (SMTP), доступ по SSH, ігрові послуги та інші, варто пам'ятати, що їхні відкриті порти можуть означати вразливість до DDoS-атак.

Щоб вирішити цю проблему, розміщується проксі-сервер на основі TCP/UDP, який працює подібно до захисту на основі розведення CDN. У цьому методі пакети даних надсилаються на зворотний проксі-сервер TCP/UDP, який потім відфільтрує шкідливий трафік і пакети.

Як і у двох попередніх методів захисту від DDoS, цей метод має недоліки:

– IP джерела зміниться для бекенда. Оскільки ми не можемо отримати IP-адресу реального відвідувача, це може бути додатковою вразливістю.

– Конфігурація проксі-сервера TCP/UDP базується на кожній програмі, а не на основі домену (як у розведенні CDN).

– Він більш схильний до хибно-позитивних результатів порівняно з розведенням CDN (в цьому аспекті дуже схожий на метод Clean Pipe).

– Не пропонує деталізації мереж.

Зворотний проксі-сервер TCP/UDP є досить універсальним і точним, оскільки він може дозволити певним портам отримати доступ, а не відкривати всі порти. Крім того, він досить добре поглинає повільну DDoS-атаку [11].

Враховуючи все вище описане можна скласти таку порівняльну таблицю, виділивши ключові параметри.

Таблиця 1

	Clean Pipes	**Proxy DDoS Protection**	**CDN Dilution**
Тип	Тунельний	Проксі	Зворотний проксі
Застосовується для	Будь-яких додатків	TCP/UDP додатки	Лише веб додатки
Вимоги	BGP роутер та підтримка 24 підмаски мережі	Пропускна здатність Інтернету	Пропускна здатність Інтернету
Конфігурація	За префіксом	За додатком	За доменом
Час виконання	Дні	Хвилини	Хвилини
Захист від атак 3/4 рівня	Не завжди ввімкнено	Так	Так
Захист від атак 7 рівня	Середній	Середній	Високий
Балансування навантаження	Не підтримує	Є	Є
Помилкові спрацьовування	Відносно високі	Середньої частоти	Майже немає
Ключові переваги	Не потрібно змінювати додатки в більшості випадків	Балансування навантаження на бекенд (можлива підтримка декількох портів на тому ж ім'я хоста)	Кеш вмісту, WAF можливості
Ключові обмеження	Відносно висока ймовірність хибного спрацювання	Початковий сервер не може побачити справжній IP, оскільки його буде замінено на довірений-вихідний NAT IP	Застосовується лише до веб-додатків

Для власника ресурсу існує декілька готових рішень для захисту від DDoS-атак, які використовують вищезгадані способи захисту.

1. Cloudflare CDN

Cloudflare – це мережа серверів, поширена по всьому світу, і ця мережа виступає свого роду посередником між вами та сервером, на якому зберігається веб-сайт, який ви хочете відвідати. Переходячи між серверами, Cloudflare захищає від зловмисних DDoS-атак, низької швидкості завантаження та простоїв між запитами за допомогою CDN.

№ 1 (17), 2022
ISSN 2663 - 4023

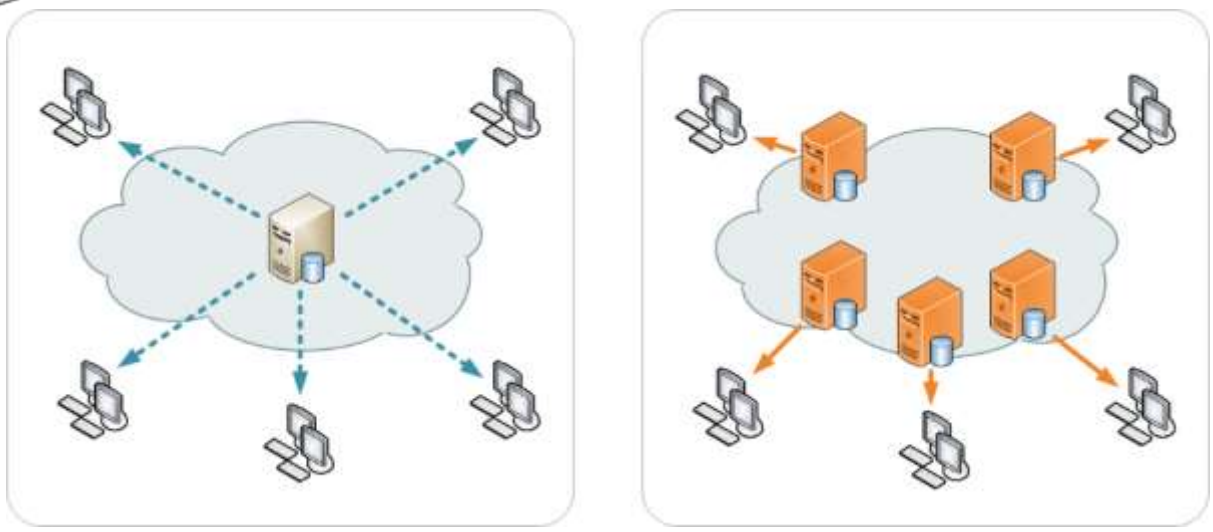

Рис. 1. Мережа серверів Cloudflare

CDN вирішує проблему затримки (затримка перед передачею даних, тобто тривалий час очікування). У сучасну епоху Інтернету сторінка, завантаження якої займає більше кількох секунд, як правило, закривається та забувається. Отже, якщо ви купуєте Cloudflare для свого веб-сайту, CDN, який пропонує Cloudflare, усуває цю проблему.

Рис. 2. Організація обміну даними без CDN

Рис. 3. Організація обміну даними з CDN

Cloudflare працює, кешуючи ваш веб-сайт і його файли на своїх серверах по всьому світу, а потім, коли хтось намагається отримати доступ до вашого сайту, його запит спрямовується на найближчий до них сервер. Це гарантує, що ваша веб-сторінка буде швидко завантажуватися незалежно від трафіку.

Cloudflare працює інакше, ніж стандартний CDN, оскільки він позбавляє від суєти та клопоту під час налаштування CDN. Все, що потрібно зробити – це оновити DNS (систему доменних імен), щоб перейти до Cloudflare. Потім Cloudflare попросить вибрати два сервери імен Cloudflare для вашого домену. Це можна зробити через реєстратора, у якого було придбано оригінальний домен.

Їх прискорення працює завдяки використанню Cloudflare Anycast (технології мережевої маршрутизації), яка направляє початковий пошук вашого домену до центру обробки даних і серверу, найближчому до відвідувача. Центр обробки даних, який отримує запит, надсилає відповідь, яка потім спрямовує відвідувача на найкращий для нього сервер. Оскільки Cloudflare має центри майже в 200 містах, можна бути впевненим, що швидкість ніколи не буде проблемою.

Після обробки початкового запиту на пошук сервер, що знаходиться поблизу відвідувача, починає обслуговувати фактичний веб-сайт. Завдяки цьому витягу інформації Cloudflare працює як CDN, але з кількома додатковими функціями. Коли використовується Cloudflare як хостинг-платформа, велика частина даних вашого веб-сайту кешується на кожному сервері, щоб відвідувач міг швидко отримати доступ. Як бонус, однією з додаткових функцій Cloudflare є те, що центр обробки даних також перевіряє кожну вхідну IP-адресу, яка намагається отримати доступ до вашого сайту. Цей скринінг діє як захист від DDoS-атак та інших загроз для вашого сайту.

Після того, як Cloudflare гарантує, що відвідувач не є загрозою, він отримує доступ до кешу вашого сайту і починає обслуговувати його. Cloudflare зберігає лише статичні частини вашого сайту, наприклад зображення, Javascript і CSS. Cloudflare намагається бути консервативним у тому, що вони кешують, не боячись зіпсувати динамічні функції, такі як HTML. Лише близько 50% будь-якого веб-сайту зберігається в кеші, але Cloudflare часто оновлює свій кеш, щоб гарантувати, що кеш завжди оновлюється. Хороша новина полягає в тому, що якщо більша частина вашого сайту є статичною і зберігається на їхніх серверах, то Cloudflare доставить сайт надзвичайно швидко.

У випадку, якщо запит відвідувача не кешується, сервер починає перетягувати веб-сайт на локальний сервер зі свого вихідного сервера. Через велику кількість серверів відвідувачеві все одно надається преміальний «маршрут» до вашого сайту, який, як правило, набагато швидший, ніж спроба отримати доступ безпосередньо до оригінального сервера.[12]

2. Cisco Clean Pipes

Сучасну концепцію захисту від DDoS-атак розробила Компанія Cisco Systems. Розроблена концепція Cisco отримала назву Cisco Clean Pipes ("очищені канали"). У детально розробленій вже майже 10 років тому концепції досить докладно описувалися основні принципи та технології захисту від аномалій у трафіку, більша частина яких використовується і сьогодні, зокрема іншими виробниками.

Концепція Cisco Clean Pipes передбачає такі принципи виявлення та придушення DDoS-атак.

Вибираються точки (ділянки мережі), трафік у яких аналізується щодо виявлення аномалій. Залежно від того, що ми захищаємо, такими точками можуть бути пірінг-з'єднання оператора зв'язку з вищими операторами, точки підключення нижчестоящих операторів або абонентів, канали підключення центрів обробки даних до мережі.

Спеціальні детектори аналізують трафік у цих точках, будують (вивчають) профіль трафіку у його нормальному стані, з появою DDoS-атаки чи аномалії – виявляють її, вивчають і динамічно формують її характеристики. Далі інформація аналізується оператором системи, і в напівавтоматичному чи автоматичному режимі запускається процес придушення атаки. Придушення полягає в тому, що трафік, призначений

"жертві", динамічно перенаправляється через пристрій фільтрації, на якому до цього трафіку застосовуються фільтри, сформовані детектором, що відображають індивідуальний характер цієї атаки. Очищений трафік вводиться в мережу та відправляється одержувачу (тому і виникла назва Clean Pipes – абонент отримує "чистий канал", що не містить атаки).

Таким чином, весь цикл захисту від DDoS-атак включає наступні основні стадії:

– Навчання контрольним характеристикам трафіку (профілювання, Baseline Learning);

– Виявлення атак та аномалій (Detection);

– Перенаправлення трафіку з метою його пропуску через пристрій очищення (Diversion);

– Фільтрування трафіку з метою придушення атак (Mitigation);

– Введення трафіку назад у мережу та надсилання адресату (Injection).

Водночас рекомендується використовувати механізми захисту інфраструктури мережі, що передбачені концепцією Network Foundation Protection, що дозволить підвищити рівень захищеності в цілому.

Таблиця 2

<table>
<tr><td rowspan="2">Cisco DDoS Protection Solution</td><td>Detection

Ідентифікувати та класифікувати атаки на підставі характеристик трафіку</td><td>Diversion/Injection

Перенаправити весь трафік, призначений для певної мети; повернути очищений трафік назад у мережу щоб він досяг мети</td><td>Mitigation

Аналіз трафіку та видалення пакетів DDoS-атаки</td></tr>
<tr><td colspan="3">Network Foundation Protection

Захист фундаменту мережі</td></tr>
</table>

Як детектори можуть використовуватися два типи пристроїв:

1. Детектори виробництва Cisco Systems – сервісні модулі Cisco Traffic Anomaly Detector Services Module, призначені для встановлення у шасі Cisco 6500/7600.

2. Детектори виробництва Arbor Networks – Arbor Peakflow SP CP.

Як пристрій очищення трафіку Cisco рекомендує використовувати сервісний модуль Cisco Guard, який встановлюється в шасі Cisco 6500/7600 і за командою, що отримується з детектора Cisco Detector або Arbor Peakflow SP CP здійснюється динамічне перенаправлення, очищення і зворотне введення трафіку в мережу. Механізми перенаправлення – це або BGP апдейти у бік вищих маршрутизаторів, або безпосередні керуючі команди у бік супервізора з допомогою пропрієтарного протоколу. При використанні BGP-апдейтів вищестоящому маршрутизатору вказується нове значення nex-hop для трафіку, що містить атаку – так, що цей трафік потрапляє на сервер очищення. При цьому необхідно подбати про те, щоб ця інформація не спричинила організацію петлі (щоб нижчестоящий маршрутизатор при введенні на нього очищеного трафіку не намагався знову загорнути цей трафік на пристрій очищення). Для цього можуть використовуватися механізми контролю поширення BGP-апдейтів за параметром community або використання GRE-тунелів при введенні очищеного трафіку.[6]

ISSN 2663 - 4023

3. NGIX/NGIX Plus

Nginx – це веб-сервер з відкритим вихідним кодом, який надає такі можливості, як зворотній проксі-сервер, кешування, балансування навантаження, потокове передавання мультимедіа тощо. Він починався як веб-сервер, розроблений для максимальної продуктивності та стабільності. На додаток до своїх можливостей HTTP-сервера, NGINX також може функціонувати як проксі-сервер для електронної пошти (IMAP, POP3 і SMTP), а також як зворотний проксі-сервер і балансувальник навантаження для протоколів HTTP/2, TCP і UDP.

Nginx використовує архітектуру, керовану подіями, і обробляє запити асинхронно. Він був розроблений для використання неблокуючого алгоритму обробки підключень, керованого подіями. Отже, його процес може обробляти тисячі з'єднань (запитів) в межах 1 потоку обробки. Такі модулі процесу з'єднань дозволяють Nginx працювати дуже швидко і широко з обмеженими ресурсами. Крім того, можна використовувати Nginx для обробки більш ніж 10 000 одночасних з'єднань з низькими ресурсами (ЦП і пам'ять) під великим навантаженням запитів.

Зворотний проксі-сервер Nginx діє як проміжний сервер, який перехоплює клієнтські запити і пересилає їх на відповідний верхній серверний сервер, а потім пересилає відповідь від сервера назад клієнту. Зворотний проксі-сервер надає різні переваги як абстрактний рівень над вищими сервісами.

Балансування навантаження: рівномірне балансування навантаження Nginx для клієнтського запиту до кількох вищестоящих серверів, що покращує продуктивність і забезпечує резервування в разі збою сервера. Це допомагає підтримувати програму в постійному стані, щоб обслуговувати запити клієнтів і забезпечити кращу угоду про рівень обслуговування для програми.

Безпека: сервер Nginx забезпечує безпеку серверам, які існують у приватній мережі, приховуючи їх ідентичність. Внутрішні сервери невідомі клієнту, який робить запити. Він також забезпечує єдину точку доступу до кількох серверів, незалежно від топології мережі.

Кешування: Nginx може безпосередньо обслуговувати статичний вміст, як-от зображення, відео тощо, і забезпечувати кращу продуктивність. Це зменшує навантаження на сервер, обслуговуючи статичний вміст безпосередньо замість того, щоб пересилати його на внутрішній сервер для обробки.

Ведення журналів: Nginx забезпечує централізоване ведення журналів для запитів та відповідей на сервер, що проходять через нього, і надає єдине місце для аудиту та журналу для усунення проблем.

Підтримка TLS/SSL: Nginx забезпечує безпечний зв'язок між клієнтом і сервером за допомогою TLS/SSL-з'єднання. Дані користувача залишаються захищеними та зашифрованими під час передачі по дротовій мережі за допомогою з'єднання HTTPS.

Підтримка протоколу: Nginx підтримує HTTP, HTTPS, HTTP/1.1, HTTP/2, gRPC – гіпертекстовий транспортний протокол разом із IP4 та IP6 Інтернет-протоколами.

NGINX та NGINX Plus мають ряд функцій, які разом з характеристиками DDoS атаки, можуть зробити їх цінною частиною рішення для пом'якшення DDoS-атак. Ці функції спрямовані на DDoS-атаку як шляхом регулювання вхідного трафіку, так і шляхом контролю трафіку, коли він передається на бекенд сервери.

NGINX розроблено як «амортизатор» для вашого сайту чи програми. Він має неблокуючу, керовану подіями архітектуру, яка справляється з величезною кількістю запитів без помітного збільшення використання ресурсів.

ISSN 2663 - 4023

Нові запити з мережі не переривають NGINX в обробці поточних запитів, а це означає, що NGINX має можливість застосовувати описані нижче методи, які захищають ваш сайт або програму від атак.

Користувач може обмежити швидкість, з якою NGINX і NGINX Plus приймають вхідні запити, до значення, типового для реальних користувачів. Наприклад, ви можете вирішити, що реальний користувач, який отримує доступ до сторінки входу, може робити запит лише кожні 2 секунди. Ви можете налаштувати NGINX і NGINX Plus, щоб дозволити одній IP-адресі клієнта намагатися ввійти лише кожні 2 секунди (еквівалентно 30 запитам на хвилину):

```
limit_conn_zone $binary_remote_addr zone=addr:10m;

server {
    # ...
    location /store/ {
        limit_conn addr 10;
        # ...
    }
}
```

Рис. 4. Приклад налаштування обмежень швидкості

Директива limit_req_zone налаштовує зону спільної пам'яті, яка називається one, для зберігання стану запитів для вказаного ключа, у цьому випадку IP-адресу клієнта ($binary_remote_addr). Директива limit_req у блоці розташування для /login.html посилається на зону спільної пам'яті.

Ви можете закрити з’єднання, які занадто рідко записують дані, що може означати спробу зберегти з’єднання відкритими якомога довше (таким чином зменшуючи здатність сервера приймати нові з’єднання). Прикладом такого типу атаки є Slowloris. Директива client_body_timeout контролює, скільки часу NGINX чекає між записами тіла клієнта, а директива client_header_timeout контролює, скільки часу NGINX чекає між записами заголовків клієнта. За замовчуванням для обох директив є 60 секунд.

```
server {
    client_body_timeout 5s;
    client_header_timeout 5s;
    # ...
}
```

Рис. 5. Приклад налаштування NGINX на очікування не більше 5 секунд між записами від клієнта для заголовків або тіла

Якщо ви можете ідентифікувати IP-адреси клієнта, які використовуються для атаки, ви можете заборонити їх перерахувати за допомогою директиви deny, щоб NGINX та NGINX Plus не приймали їхні з’єднання чи запити. Наприклад, якщо ви визначили, що атаки надходять з діапазону адрес від 123.123.123.1 до 123.123.123.16:

ISSN 2663 - 4023

```
location / {
    deny 123.123.123.0/28;
    # ...
}
```

Рис. 6. Приклад заборони IP-адрес клієнта

Або якщо ви визначили, що атака відбувається з IP-адрес клієнта 123.123.123.3, 123.123.123.5 і 123.123.123.7:

```
location / {
    allow 192.168.1.0/24;
    deny all;
    # ...
}
```

Рис. 7. Директива deny all блокує всі IP-адреси клієнта, які не знаходяться в діапазоні, визначеному директивою дозволу

Можна налаштувати NGINX і NGINX Plus для поглинання значної частини сплеску трафіку, який є результатом атаки, увімкнувши кешування та встановивши певні параметри кешування для розвантаження запитів із серверної частини.

Деякі з корисних налаштувань:

– Параметр оновлення до директиви proxy_cache_use_stale повідомляє NGINX, що коли йому потрібно отримати оновлення застарілого кешованого об'єкта, він повинен надіслати лише один запит на оновлення та продовжувати обслуговувати застарілий об'єкт клієнтам, які запитують його протягом потрібного часу. щоб отримати оновлення від серверного сервера. Коли повторювані запити на певний файл є частиною атаки, це різко зменшує кількість запитів до серверів.

– Ключ, визначений директивою proxy_cache_key, зазвичай складається з вбудованих змінних (ключ за замовчуванням, $scheme$proxy_host$request_uri, має три змінні). Якщо значення включає змінну $query_string, атака, яка надсилає випадкові рядки запиту, може спричинити надмірне кешування. Ми рекомендуємо не включати змінну $query_string до ключа, якщо у вас немає для цього особливої причини.

Можна налаштувати NGINX або NGINX Plus для блокування кількох видів запитів:

– Запити на певну URL-адресу, яка може бути ціллю.

– Запити, у яких для заголовка User-Agent встановлено значення, яке не відповідає звичайному клієнтському трафіку.

– Запити, у яких для заголовка Referer встановлено значення, яке може бути пов'язане з атакою.

– Запити, в яких інші заголовки мають значення, які можуть бути пов'язані з атакою.

Наприклад, якщо ви визначите, що DDoS-атака спрямована на URL-адресу /foo.php, ви можете заблокувати всі запити до сторінки:

ISSN 2663 - 4023

```
location /foo.php {
    deny all;
}
```

Рис. 8. Приклад блокування усіх запитів до сторінки

Або якщо ви виявите, що запити DDoS-атаки мають значення заголовка User-Agent foo або bar, ви можете заблокувати ці запити.

```
location / {
    if ($http_user_agent ~* foo|bar) {
        return 403;
    }
    # ...
}
```

Рис. 9. Приклад блокування окремих запитів

Змінна http_name посилається на заголовок запиту, у наведеному вище прикладі на заголовок User-Agent. Подібний підхід можна використовувати з іншими заголовками, які мають значення, які можна використовувати для ідентифікації атаки.

Екземпляр NGINX або NGINX Plus зазвичай може обробляти набагато більше одночасних підключень, ніж бекенд-сервери, на яких він балансує навантаження. За допомогою NGINX Plus можна обмежити кількість підключень до кожного мережевого сервера.

```
upstream website {
    server 192.168.100.1:80 max_conns=200;
    server 192.168.100.2:80 max_conns=200;
    queue 10 timeout=30s;
}
```

Рис. 10. Обмеження NGINX Plus встановленням не більше 200 підключень до кожного з двох серверів у верхній групі веб-сайту

NGINX і NGINX Plus можна використовувати як цінну частину рішення для пом’якшення DDoS, а NGINX Plus надає додаткові функції для захисту від атак DDoS і допомагає визначити, коли вони відбуваються.[7]

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Актуальний фронт сучасної війни - кібернетичний. Комп’ютерні технології проникли в наше повсякденне життя, використовуються в усіх сферах, в тому числі в критичній інфраструктурі країни. Ураження таких інформаційних систем здатні нанести

величезну шкоду ворогу зсередини. Україна у війні з росією пережила чисельні кібератаки, які вплинули на комунальну систему, банківську, інформаційну, тощо.

Одним з найпоширеніших видів кіберзброї є DDoS, тобто атаки до відмови сервісу. При таких атаках на цільові комп'ютери або комп'ютерні мережі через різні протоколи надсилається величезна кількість запитів, які ціль не здатна обробити. Таким чином, її робота значно уповільнюється або повністю унеможливлюється. Застосовуючи таку зброю в кібервійні, можна знищувати противника зсередини.

Оскільки DDoS є поширеним, було розроблено методи захисту від нього. Вони блокують підозрілі запити, фільтрують аномальний трафік, розподіляють потужності, застосовують складні алгоритми для забезпечення надійного захисту інформаційних систем. В цій роботі нами було детально розглянуто такі технології, проаналізовано і порівняно існуючі готові рішення компаній щодо надання захисту. Але оскільки інформаційні технології стрімко розвиваються, розвиватимуться і DDoS-атаки. Тому питання захисту від них є актуальним, особливо в умовах кібернетичної війни.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Кібератака на енергетичні компанії України. https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0_%D0%BD%D0%B0_%D0%B5%D0%BD%D0%B5%D1%80%D0%B3%D0%B5%D1%82%D0%B8%D1%87%D0%BD%D1%96_%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8.

2 Методи боротьби з Dos або DDos атаками. https://wiki.tntu.edu.ua/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8_%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8_%D0%B7_Dos_%D0%B0%D0%B1%D0%BE_DDos_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC%D0%B8.

3 Російсько-українська кібервійна. https://uk.wikipedia.org/wiki/%D0%A0%D0%BE%D1%81%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%BE%D1%83%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B0.

4 DoS-атака. https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0.

5 Що таке DDoS-атака? https://cip.gov.ua/ua/news/sho-take-ddos-ataka.

6 Service Provider Solutions. DDoS Protection Solution. Enabling "Clean Pipes" Capabilities. https://www.cisco.com/assets/cdc_content_elements/networking_solutions/service_provider/ddos_protection_sol/ddos_protection.pdf.

7 F5 NGINX Plus. https://www.nginx.com/products/nginx/.

8 How does DDoS protection work? https://datadome.co/learning-center/how-does-ddos-protection-work/

9 Common DDoS mitigation methods and comparison. https://www.mlytics.com/blog/common-ddos-mitigation-implementation-strategies-and-comparison/.

10 CDN Security. What is a CDN? https://www.netacea.com/glossary/cdn-security/.

11 About the TCP-UDP-Proxy. https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/ proxies/tcp/tcp_udp_proxy_about_c.html.

12 What is Cloudflare and How Does a CDN Work? https://blog.101domain.com/business-development/what-is-cloudflare-and-how-does-a-cdn-work.

13 What is the OSI Model? https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/

14 Susukailo, V., Opirsky, I., Yaremko, O. (2022) Methodology of ISMS Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (eds) Future Intent-Based Networking. Lecture Notes in Electrical Engineering, 831. https://doi.org/10.1007/978-3-030-92435-5_15

15 Опірський, І.Р., Василишин, С.І., Сусукайло, В.А. (2021). Розслідування кіберзлочинів за допомогою приманок у хмарному середовищі. *Безпека інформації, 27*(1), 13-20. https://doi.org/10.18372/2225-5036.26.15574

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (17), 2022
ISSN 2663 - 4023

Laktionov Illia Oleksndrovych
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID*:* 0000-0002-0562-2306
illia.laktionov.kb.2020@lpnu.ua

Kmit Andrii Yuriyovych
Cybersecurity student
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8854-818X
andrii.kmit.kb.2020@lpnu.ua

Ivan R. Opirskyy
Dc.S., Professor, Professor of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

Harasymchuk Oleh Ihorovych
CScTech., Associate Professor., Associate Professor of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

RESEARCH TOOLS FOR PROTECTING INTERNET RESOURCES FROM DDOS-ATTACK DURING CYBERWAR

Abstract. To date, information technologies have entered all the spheres of society. Due to the rapid development of scientific and technological progress, the traditional methods of introduction of wars, which are currently underway not only in the field of hostilities, but also in the cybernetic space of society, are also changing. The modern world is characterized by active wars in cyberspace, where one of the most common attacks is DDoS-attack, including critical infrastructure. This is primarily due to the extreme density of integration into the life and activities of the society of various gadgets, electronic devices and the Internet, the violation of which can cause significant damage - both psychological and significant damage to the enemy from the inside. One of the simplest and most popular methods for violating such normal functioning is the use of resource overload, which can even lead to their complete inaccessibility. One of the ways of overload is the use of DDoS-attacks in case of refusal of service. Mass sending external requests to the attacked resource leads to the fact that such a resource in a short period of time is trying to develop a significant number of requests, which will lead to a significant slowdown in its work or even lead to a complete stop of the resource. This work is devoted to the study of the methods by which DDoS-atack are carried out. The most common methods for their implementation and the main methods of protection against them are considered in detail. This work has examined in detail the technologies and methods of protection against DDoS attacks analyzed and relatively existing solutions of ready-made companies for protection. But since information technologies are developing rapidly, DDoS attacks will develop. Consequently, the problem of protection against them is relevant, especially in the conditions of cyber.

Keywords: DoS, DDoS, DDoS-attack, Internet, Internet resource, cyberwar, hybrid war.

REFERENCES

1 Cyberattack for energy companies of Ukraine. https://uk.wikipedia.org/wiki/%%D0%9a%D1%96%D0%B1%B1%B5%D1%80%D0%B0%D1%82%D0%B0%B0%D0%BA%d0%b0_%d0%bd%d0%b0_%d0%d0%bd%d0%b5%d1%80%d0%b3%d0%b5%D1%82%d0%b8%d1%%%87%D0%BD%D1%96_%D0%BA%D0%D0%BC%D0%BF%D0%B0%D0%BD%D1%96%D1%97_%D0%A3%D0%BA%% D1%80%D0%B0%D1%97%D0%BD%D0%B8.

2 Methods for combating DOS or DDOS attacks. https://wiki.tntu.edu.ua/%D0%9C%D0%B5ING%D1%80%D0%be%D1%82%D1%8C%D0%D0%B8_%D

0%B7_DOS_%D0%D0%D0%D0%BE_DDOS_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC%D0%B8.
3 Russian-Ukrainian cyberwar. https://en.wikipedia.org/wiki/wiki/%D0%A0%D0%BE%D1%81%D1%96%96,D0%be%D1%83%D0%BA%D1%80%D0%D1%97%D0%BD%D1%81%D1%8C%D0%BA%D0%B0_%D0%BA%D1%96%D0%B1%D0%D1%80%D0%B2%D1%96%D0%B9%D0%BD%D0%B.
4 DOS-Attack. https://en.wikipedia.org/wiki/dos-%D0%B0%D1%82%D0%B0%D0%BA%BA%D0%B0.
5 What is a DDOS-Attack? https://cip.gov.ua/en/news/sho-take-dos-ataka.
6 Service Provider Solutions. DDOS Protection Solution. Enabling “Clean Pipes” Capabilities. https://www.cisco.com/assets/cdc_content_elements/networking_solutions/service_provider/ddos_protection_sol/ddos_protection.pdf.
7 F5 nginx Plus. https://www.nginx.com/products/nginx/.
8 How does ddos Protection Work? https://datadome.co/learning-center/how-does-dos-protection-work/
9 Common Ddos Mitigation Methods and Comparison. https://www.mlytics.com/blog/common-ddos-mitigation-implementation-strategies-and-Comparison/.
10 CDN Security. What is a cdn? https://www.netacea.com/glossary/cdn-security/.
11 About the TCP-UDP-PROXY. https://www.watchGuard.com/help/docs/Help-center/en-us/content/en-en-us/fireware/ proxies/tcp/tcp_udp_proxy_abut_c.html.
12 What is Cloudflare and How does a cdn work? https://blog.101Domain.com/business-development/what-is-cloudflare-and-does-a-cdn-work.
13 What is the osi model? https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
14 Susukailo, V., Opirskyy, I., Yaremko, O. (2022) Methodology of isms Establishment Against Modern Cybersecurity Threats. In: Klymash M., Beshley M., Luntovskyy A. (EDS) Future Incent-Based Networking. Lecture Notes in Electrical Engineering, 831. https://doi.org/10.1007/978-3-030-92435-5-5_15
15 Opirskyy, I.R., Vasylyshyn, S.I., Sukukailo, V.A. (2021). Cybercrime investigation with baits in the cloud environment. *Information safety, 27*(1), 13-20.