ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА ПРОТИДІЇ РОЗПОДІЛЕНИМ АТАКАМ СПРЯМОВАНИМ НА ВІДМОВУ В ОБСЛУГОВУВАНІ»

Виконав: студент 6 курсу, групи БСДМ-62
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)

Рогозільніков О.О.
(прізвище та ініціали)

Керівник Довженко Н.М.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2021

РЕФЕРАТ

Текстова частина магістерської роботи: 80 сторінок, 13 рисунків, 2 таблиці, 29 джерел.

Об'єкт дослідження – процес виявлення та протидії розподіленим атакам спрямованим на відмову в обслуговувані.

Предмет дослідження – технології виявлення та протидії розподіленим атакам спрямованим на відмову в обслуговувані.

Мета роботи – підвищення ефективності виявлення розподілених атак спрямованих на відмову в обслуговувані та розробка рекомендацій щодо протидії ним.

Методи дослідження – опрацювання літератури за даною темою, системний аналіз, дослідження технологій та програмного забезпечення.

В роботі досліджено методи, призначені для захисту від DDoS атак та виведено таксономію атак на відмову в обслуговуванні. Виокремлено рішення та механізми, які необхідні для виявлення та реагування на DDoS атаки.

Проведено детальний аналіз технологій функціонування та особливостей налаштування сервісу захисту сайтів та доменів від DDoS атак від вендора Qrator Labs. Досліджено технічний алгоритм підключення клієнтів, що включає перенаправлення трафіку користувача на вузли фільтрації Qrator. Приведено особливості налаштування фільтрування HTTPS (в тому числі з розкриттям та без розкриття ключів (PCI-DSS ready)). Досліджено особливості блокування IP-адрес з використанням методів Qrator API та налаштування двоетапної автентифікації (з використанням Google Authenticator). Розроблено рекомендацій щодо протидії DDoS атакам для користувачів та клієнтів.

Галузь використання – кібербезпека.

DDOS, QRATOR LABS, МЕРЕЖА, БЕЗПЕКА, PCI-DSS, HTTPS, ЗАГРОЗИ, ІНФОРМАЦІЯ, МЕТОД, GOOGLE AUTHENTICATOR.

ABSTRACT

Master's thesis: 80 pages, 13 figures, 2 tables, 29 sources.

Object of research – the process of detecting and counteracting DDoS attacks.

Subject of research – the technologies for detecting and countering DDoS attacks.

The aim of research – to increase the effectiveness of detection of DDoS attacks and the development of recommendations to counter them.

Research methods – elaboration of literature on the topic, systems analysis, technology research and practical software.

The paper investigates methods designed to protect against DDoS attacks and derives a taxonomy of denial of service attacks. The solutions and mechanisms needed to detect and respond to DDoS attacks are highlighted. It is noted that one of the disadvantages of these mechanisms is that customers need to know about protection and install special software.

A detailed analysis of the functioning technologies and features of setting up the service of protection of sites and domains from DDoS attacks from the vendor Qrator Labs is presented. The paper gives a detailed analysis of the technical algorithm of client connection which includes redirection of user traffic to Qrator filtering nodes. Features of HTTPS filtering configuration (including with and without key opening (PCI-DSS ready)) are given. The peculiarities of blocking IP addresses using Qrator API methods and setting up two-stage authentication (using Google Authenticator) are proposed. Guidelines for countering DDoS attacks for users and customers are developed.

Field of use – cybersecurity.

DDOS, QRATOR LABS, NETWORK, SECURITY, PCI-DSS, HTTPS, THREATS, INFORMATION, METHOD, GOOGLE AUTHENTICATOR.

ЗМІСТ

ВСТУП

Актуальність дослідження. Атака розподіленої відмови в обслуговуванні (DDoS) — це тип кібератаки, під час якої зловмисник прагне відмовити в наданні послуг у мережі/сервері, заповнюючи трафік мережі/сервера зайвими запитами, що робить його нездатним обслуговувати запити від легальних користувачів.

Існує багато видів DDoS-атак. Вони можуть орієнтуватися на різні рівні OSI і використовувати різні методи. Під час DDoS-атаки зловмисники знаходять уразливі місця і можуть, наприклад, запустити вірус на веб-сайт і викрасти дані користувачів чи клієнтів.

За даними Corero Network Security (постачальник захисту та пом’якшення DDoS-атак), у третьому кварталі 2020 року організації в усьому світі зазнавали в середньому 237 спроб DDoS-атак на місяць, що в середньому становить 8 DDoS-атак щодня. Це на 35% більше, ніж у другому кварталі того року, і на 91% більше, ніж у першому кварталі. Згідно з іншим дослідженням Incapsula, DDoS-атака коштує бізнесу в середньому 40 000 доларів США на годину.

Незважаючи на величезні зусилля дослідників і експертів з безпеки, спрямовані на вирішення цієї проблеми, атаки відмови в обслуговуванні в мережі Інтернет все ще залишаються невирішеною проблемою.

Існує комерційно доступне програмне забезпечення, яке виявляє та пом’якшує DDoS-атаки, але висока вартість цього програмного забезпечення ускладнює його доступність для малого та середнього бізнесу.

Основні функції рішення DDoS включають виявлення ранніх стадій атаки, масштаб поглинання обсягу трафіку та можливість пом’якшити джерело атаки. Це можна зробити за допомогою статичних або користувацьких правил або за допомогою набору захисних дій, що розвиваються, коли атака переходить на додаткові цілі.

Найскладніші для нейтралізації – інтелектуальні DDoS-атаки на рівні додатків, їм приділяють особливу увагу та вважають їхню нейтралізацію однією із

ключових компетенцій. Помилково вважати, що проблема розподілених мережних атак стосується лише «гігантів» мережі Інтернет та великих компаній. Цілі зловмисників непередбачувані, і їхні інтереси можуть зачіпати не тільки комерційні сфери: часто атаки організуються на благодійні, політичні організації, ЗМІ та ін.

Об'єкт дослідження – процес виявлення та протидії розподіленим атакам спрямованим на відмову в обслуговувані.

Предмет дослідження – технології виявлення та протидії розподіленим атакам спрямованим на відмову в обслуговувані.

Мета роботи – підвищення ефективності виявлення розподілених атак спрямованих на відмову в обслуговувані та розробка рекомендацій щодо протидії ним.

Відповідно до мети наукового дослідження були поставлені та розв'язані наступні завдання:

– досліджено методи, призначені для захисту від DDoS атак;

– виокремлено рішення та механізми, які необхідні для виявлення та реагування на DDoS атаки;

– досліджено вендорів, що здійснюють надання послуг щодо захисту від DDoS;

– проведено детальний аналіз технологій функціонування та особливостей налаштування сервісу захисту сайтів та доменів від DDoS атак від вендора Qrator Labs.

– розроблено рекомендацій щодо протидії DDoS атакам для користувачів та клієнтів.

Методи дослідження – опрацювання літератури за даною темою, системний аналіз, дослідження технологій та програмного забезпечення.

1 АНАЛІЗ РОЗПОДІЛЕНИХ АТАК СПРЯМОВАНИХ НА ВІДМОВУ В ОБСЛУГОВУВАНІ

1.1. Передумови та формулювання проблеми

Мережа Інтернет складається з мільйонів комп'ютерів у всьому світі, і багато людей користуються ним щодня. Атака «Відмова в обслуговуванні» (DoS) — це атака, яка має на меті відмовити передбачуваним користувачам у використанні мережевого ресурсу, такого як Інтернет-сервіс.

Атака з розподіленою відмовою в обслуговуванні (DDoS) — це скоординована атака на доступність послуг у певній цільовій системі або мережі, яка запускається опосередковано через багато скомпрометованих обчислювальних систем.

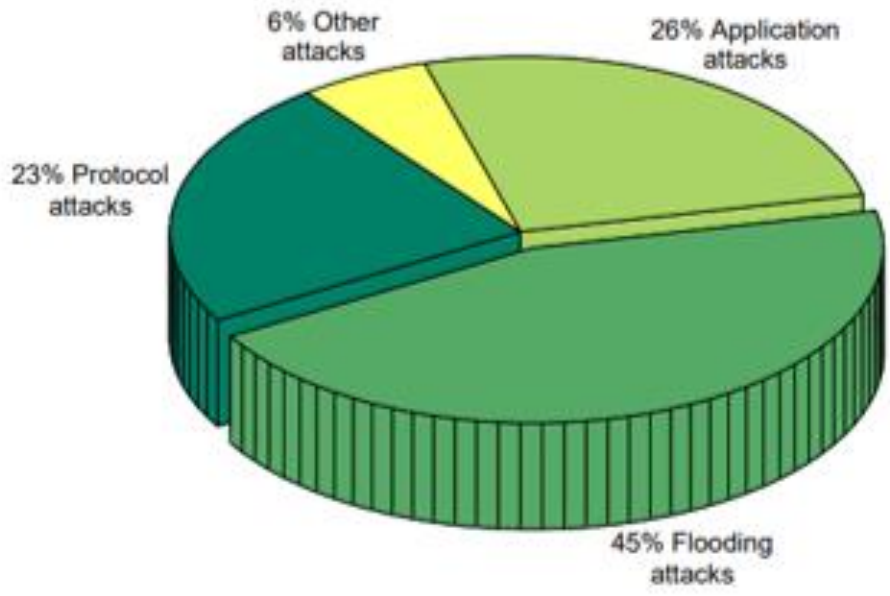

Рис.1.1. Типи DDoS-атак

DDoS-атаки загалом поділяються на дві категорії: атаки на виснаження пропускної здатності та атаки на виснаження ресурсів [1]. Атака на виснаження пропускної здатності має на меті наповнити мережу жертви небажаним трафіком, не даючи легальному трафіку досягти системи жертви. Наприкад, атаки на основі

flooding з використанням пакетів UDP або ICMP ехо-запитів. Атака виснаження ресурсів призначена для зв'язування ресурсів системи жертви шляхом націлювання на сервер або процес всередині системи, унеможливлюючи законні запити на отримання послуги.

Flooding TCP SYN є найбільш поширеною атакою і є ідеальним прикладом атаки на виснаження ресурсів. Як показано на рис. 1.1, найпоширенішим типом DDoS-атаки є атака на виснаження пропускної здатності [2].

1.2. Тенденції щодо розповсюдження атак DDoS

Відповідно до звіту Symantec Internet Security [3], нова атака запускається в середньому кожну хвилину кожного дня. Інструменти для атак з часом стають все більш досконалими, і вони легко знаходять нові недоліки безпеки на дірках у підключених до Інтернет ПК та інших ресурсах. Таким чином, залучення великої кількості атакуючих зомбі не є складним завданням, а широкомасштабні DDoS-атаки є проблемою, що швидко виникає.

Основною причиною поширеності атак DDoS є те, що Інтернет спочатку був розроблений для відкритості та масштабованості без особливого уваги до безпеки. Шкідливі користувачі використовують недоліки дизайну мережі Інтернет та розробляють інструменти для атаки, щоб легко здійснити DDoS-атаку.

Багато інструментів для атак засновані на неправильному використанні звичайних мережевих протоколів. Багато хостів в мережі Інтернет вразливі до атак DDoS, особливо хости, на яких або не встановлено антивірусне програмне забезпечення, або застаріле антивірусне програмне забезпечення, або ті, які не були належним чином виправлені.

У звіті Symantec Internet Security показано, що 61% шкідливих сайтів є звичайними веб-сайтами, які були скомпрометовані та заражені шкідливим кодом, тому щомісяця створюється понад 250 000 зомбі. В результаті майже всі Інтернет-сервіси вразливі до розподілених атак «відмова в обслуговуванні» у достатньому масштабі. У більшості випадків достатнього масштабу атаки можна досягти

шляхом компрометації достатньої кількості кінцевих хостів або маршрутизаторів і використання цих скомпрометованих хостів для запуску атаки. В принципі неможливо відрізнити DDoS-атаку від флеш-натовпу. Немає загальних характеристик потоків DDoS, які можна використовувати для їх виявлення та фільтрації. Зловмисники досягають бажаного ефекту, збільшуючи обсяг пакетів атаки, і можуть змінювати всі поля пакетів, щоб уникнути характеризації. Співпраця розподілених джерел ускладнює боротьбу з DDoS-атаками або їх відслідковування. Несподівано інтенсивний і нешкідливий трафік має той самий ефект, що й DDoS-атака [4].

1.3. Узагальнені вимоги до систем захисту від DDoS

Серйозність проблеми DDoS та збільшення частоти та потужності атак призвели до широкого спектру захисних механізмів.

Вимоги до систем захисту. Розробка ефективної системи захисту від DDoS містить значну проблему для успішного виявлення та припинення атак, водночас збереження продуктивності мережі. Нижче наведено загальноприйняті вимоги, яким повинна задовольняти хороша система захисту від DDoS:

1. Раннє виявлення атак. DDoS-атаки переповнюють жертви небажаними пакетами. Це означає, що під час нападу постраждалі не можуть звернутися за допомогою до когось іншого. Отже, будь-яка потенційна реакція може бути ініційована, якщо напад буде виявлено на ранніх стадіях. Зазвичай транспортний потік збільшується раптово і без будь-якого попередження [5]. З цієї причини захисні механізми повинні виявляти та швидко реагувати, щоб уникнути побічної шкоди жертві;
2. Надійне виявлення атак. Система повинна виявляти всі атаки, що відбуваються, і не генерувати помилкові тривоги;
3. Незалежне виявлення атак і відповідь. Система повинна працювати незалежно від жертви, і повинна реагувати незалежно від жертви;

4. Низький вплив на вартість продуктивності. Вартість продуктивності є важливим фактором при розробці системи захисту. Вимоги до ресурсів системи захисту не повинні погіршувати продуктивність мережі, що розгортається;

5. Ефективна відповідь. При виявленні атаки система повинна брати участь у відповіді, яка значно знижує ефективність атаки, незалежно від характеристик атаки;

6. Реалістичний дизайн. Системи захисту повинні мати практичне розгортання в мережі Інтернет. Таким чином система повинна вимагати незначних змін або зовсім не змінювати існуючу інфраструктуру Інтернету [6].

7. Висока безпека. Система захисту від DDoS-атак повинна гарантувати, що її не можна використовувати для погіршення якості або відмови в обслуговуванні клієнтів. Вона також повинна бути стійкою до спроб зловмисників обійти або вимкнути її.

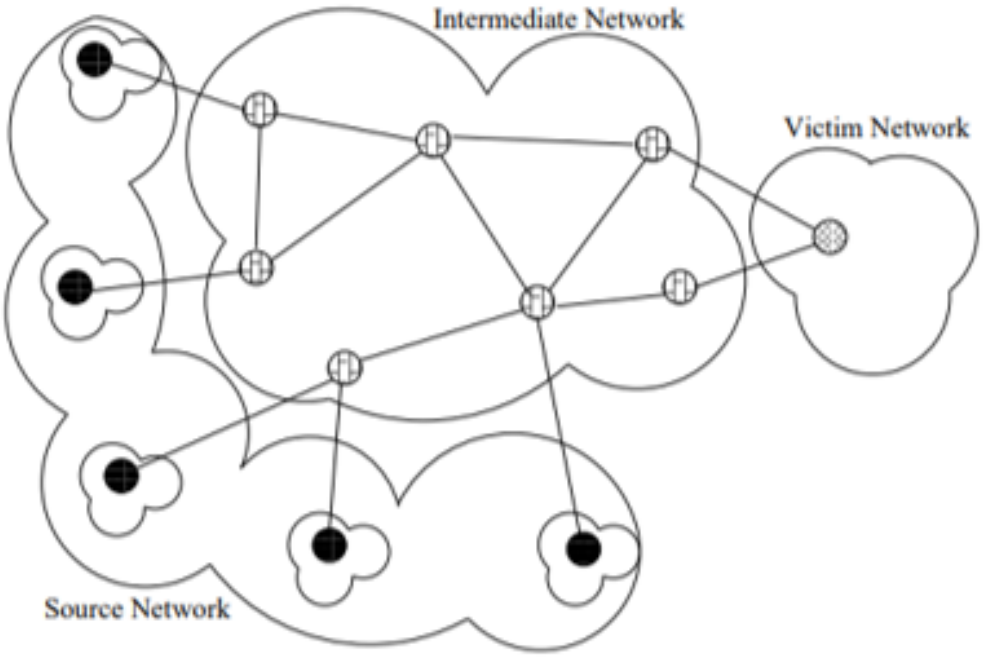

Рис.1.2. Спрощена мережа, яка ілюструє різні місця для розгортання захисту від DDoS

Як показано на рис.1.2, атакуючі вузли можуть знаходитися в мережі жертви, або в проміжній мережі чи у кінцевій мережі (мережі джерела). Мережа жертви — це адміністративний домен, який містить жертву атаки. Проміжна мережа — це

адміністративний домен, що пересилає атакуючі пакети жертві, а кінцеві мережі — це адміністративний домен, який містять більшість атакуючих вузлів.

Захист мережі жертви. Більшість систем захисту для боротьби з DDoS-атаками працюють з боку жертви. Захист жертви зазвичай не може повністю гарантувати повний захист від атак DDoS, оскільки сама система захисту може бути перевантажена атакуючим трафіком. Більшість із запропонованих систем намагаються виокремити атакуючий трафік та встановити правила фільтрації в маршрутизаторах, що перебувають у верхній частині мережі-жертви. У деяких випадках це може успішно захистити від наслідків атаки. Наприклад, веб-сервер, який перебуває під атакою UDP flood, може попросити відфільтрувати весь UDP-трафік. Однак ця технологія не працює, коли обсяг трафіку достатньо високий, щоб спричинити відставання механізму фільтрації в маршрутизаторі вище по потоку. Крім того, ядро мережі Інтернет має набагато більші ресурси, ніж його окремі мережі, і, таким чином, DDoS може повністю використовувати основні ресурси, щоб перевантажити мережу-жертву та вичерпати її обмежені ресурси [7].

Захист проміжної мережі. Ці типи захисту від DDoS розгортаються в проміжній мережі. Відповідь на DDoS-атаку з боку проміжної мережі, очевидно, ефективніша, ніж відповідь Victim-End Defense, оскільки великі обсяги трафіку атаки можна легко обробити, а атаки можна відстежити до джерел. Це пояснюється тим, що вузли захисту не настільки перевантажені, як вузли мережі жертви. Однак існує кілька проблем, які заважають широкому розгортанню цих підходів. Наприклад, виникають труднощі з виявленням атаки та ідентифікацією зловмисників, оскільки вузли захисту в проміжній мережі зазвичай спостерігають лише часткові наслідки атаки. Крім того, серйозними проблемами є відсутність міждоменного співробітництва, а також витрати на розгортання.

Захист кінцевої мережі (Source-End Defense). Цей тип захисту від DDoS розгортається в мережах, де розміщено деякі з машин для атаки, потенційно на самих машинах. Системи захисту Source-End можуть контролювати вихідний трафік із цих мереж і контролювати трафік атаки. Крім того, системи захисту Source-End забезпечують дуже вибіркову відповідь на DDoS-атаки і майже не

завдають шкоди легітимному трафіку. Проте розподілені витрати на комунікацію є найвищими з цих трьох стратегій розміщення; потенційно потребує численних комунікацій по всій мережі Інтернет.

У таблиці 1.1 порівнюються переваги систем захисту з різними місцями розгортання. У порівнянні з системами захисту жертви, розподілені системи захисту, які можна розгорнути в проміжних мережах або на кінцевій мережі, можуть виявляти атаки більш вчасно, оскільки кілька вузлів можуть обмінюватися інформацією та приймати точне рішення про атаку.

Таблиця 1.1

Порівняння систем захисту на основі місць розгортання

Характеристика	Мережа жертви	Проміжна мережа	Кінцева мережа
розподілений	зазвичай ні	так	так
простота виявлення	легка	помірна	жорстка
співпраця	не потребує	автономні системи	організації і користувачі
розгортання	тільки у жертві	в апаратному забезпеченні маршрутизатора	відстеження ПК і шлюзів
вибірковість	немає	деякі	високавибірковість
масштабованість	мала	велика	велика
раннє виявлення	немає	помірне	миттєве
накладні витрати	немає	середні	високі

Компоненти розподіленої системи захисту можуть співпрацювати один з одним для боротьби з атаками. Здебільшого розподілені системи захисту розміщують свої захисні вузли або на граничних маршрутизаторах, або в основних маршрутизаторах. Розподілений захист в ядрі Інтернету має певну перевагу над одноточковим захистом.

Хоча деякі поточні рішення можуть успішно виявляти та відкидати атакуючі пакети, не існує комерційних рішень, які дають будь-які гарантії продовження обслуговування легальних клієнтів жертви під час атаки. Крім того, більшість пропонованих рішень є централізованими та ізольованими системами, які використовуються для захисту однієї цілі або мережі. Централізовані системи захисту в основному розгортаються поблизу жертви через економічні причини і для того, щоб атаки можна було ідентифікувати за допомогою більш точних характеристик атаки.

1.4. Побудова моделі вектора атаки DoS і DDoS

За визначенням DDoS-атака надходить із розподілених джерел атаки (наприклад, зомбі-комп'ютерів), що говорить про те, що розподілений механізм захисту є найкращим для повного захисту. Розподілені системи захисту, які розташовані або на проміжному, або на вихідному кінці, потенційно можуть виявити атаку до того, як атакуючі пакети досягнуть жертви. Хоча виявлення атаки ефективніше ближче до мережі жертви, відповіді на атаку є більш вибірковими ближче до джерела. Як правило, розподілені системи захисту виявляють атаку в кількох точках і об'єднують рішення щодо атаки з кожної точки, щоб прийняти глобальне рішення про те, проводиться атака чи ні. Це зменшує пропускну здатність і спричиняє затримки зв'язку. Однак такий тип спільного прийняття рішень зменшує ймовірність помилкових тривог у розподіленій системі та підвищує ймовірність виявлення атаки.

Трафік атаки, як правило, координований для початку одночасно. Довжина чорної стрілки вказує, як далеко трафік проходить через мережу за короткий проміжок часу (рис.1.3.).

Жертвою може бути мережевий сервер, клієнт або маршрутизатор, мережеве посилання або ціла мережа, постачальник послуг Інтернет або країна [8].

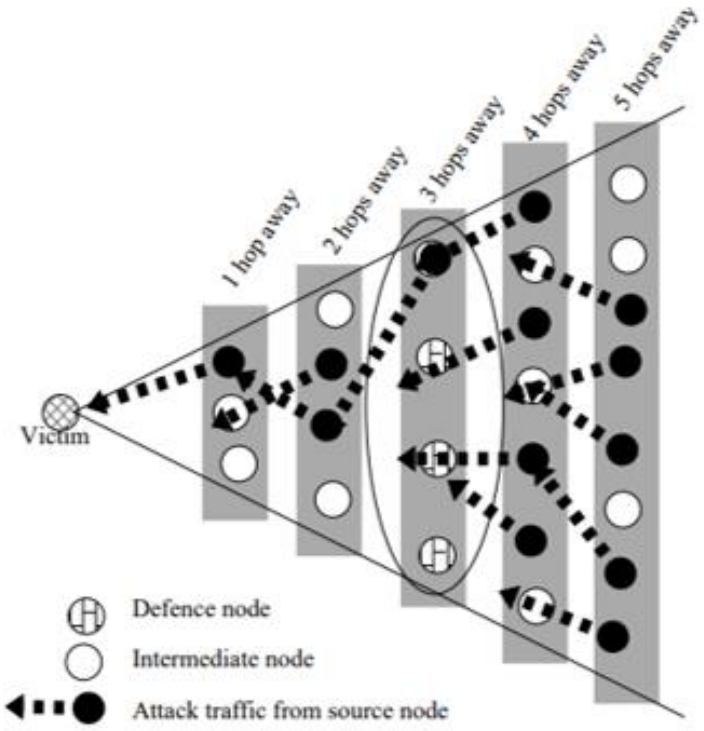

Рис.1.3. Вектор атаки в мережі, спрямований на жертву

Модель Agent-Handler DDoS-атаки складається з клієнтів, обробників та агентів, як показано на рис.1.4. Зловмисник спілкується з рештою системи DDoS-атаки. Обробники — це програмні пакети, розташовані по всій мережі Інтернет, які зловмисник використовує для спілкування з агентами.

Програмне забезпечення агента існує в зламаних системах, які в кінцевому підсумку здійснить атаку. Зловмисник спілкується з будь-якою кількістю обробників, щоб визначити, які агенти запущені та запущені, коли планувати атаки чи оновлювати агенти. Машина, на якій працюють агентські системи, не знає, що система зламана, і може взяти участь у DDoS-атаці.

Під час DDoS-атак програми зловмисник намагається перешкодити програмі виконувати завдання, змушуючи вичерпати ресурс. Ресурсами для додатків може бути максимальна кількість процесів та одночасних з'єднань, які програма може створити, тощо.

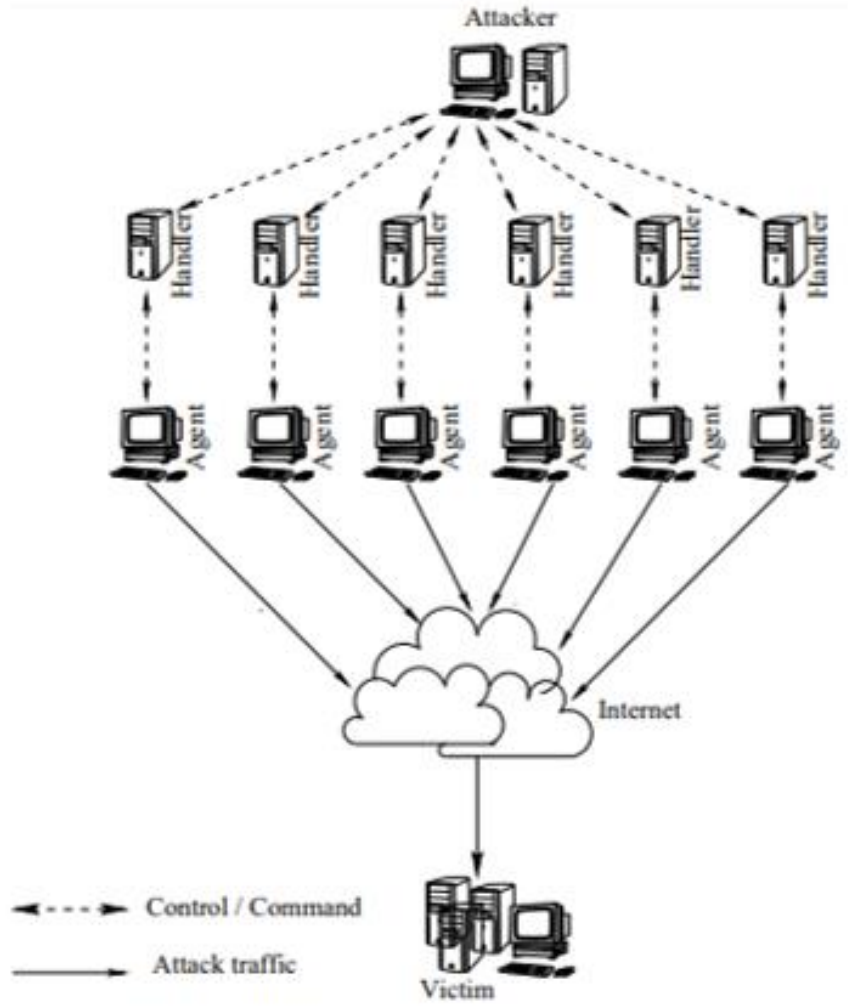

Рис.1.4. Модель атаки Agent-Handler DDoS

Приклади DDoS-атак на рівні програми включають: спроби завантаження веб-додатків, блокування доступу користувача через повторювані недійсні спроби входу, відкриття величезних кількість з'єднань програми з базою даних за запитами SQL.

DDoS-атаки на операційні системи. DDoS-атаки, направлені на операційні системи дуже схожі на DDoS-атаки, що спрямовані на додатки. Добре відомою DDoS-атакою на операційну систему є атака SYN flooding TCP. Зловмисник надсилає жертві потоки пакетів TCP, не завершивши з’єднання TCP, тим самим виснажуючи пам’ять стану з’єднання жертви[9].

DDoS на маршрутизаторі. Багато з DDoS-атак можуть бути запущені проти IP-маршрутизатора. Найпростіша атака на маршрутизатор — це перевантажити таблицю маршрутизації достатньо великою кількістю маршрутів, що призводить

до того, що у маршрутизатора не вистачає пам’яті, або у маршрутизатора недостатньо потужності ЦП для обробки маршрутів.

DDoS на поточне підключення. Замість атаки на кінцеву мережу зловмисник може спробувати порушити поточний підключення. Якщо зловмисник може спостерігати TCP-з'єднання, то досить легко підробити пакети, щоб або скинути це з'єднання, або десинхронізувати його, щоб не було подальшого прогресу.

DDoS на посилання. Найпростішою формою DDoS-атаки на посилання є надсилання достатньої кількості неконтрольованого перевантаженням трафіку (наприклад, UDP-трафіку), так що посилання стає надмірно перевантаженим, а легітимний трафік зазнає неприпустимо високих втрат пакетів.

Багато комунікаційних систем залежать від певної інфраструктури для своєї нормальної роботи. Наприклад, інфраструктура може бути глобальною системою доменних імен або глобальною інфраструктурою відкритих ключів, або може бути локальною інфраструктурою Ethernet або точкою безпроводового доступу. Наприклад, заборона доступу до DNS-сервера фактично забороняє доступ до всіх служб, таких як Інтернет, електронна пошта, відкриті ключі та сертифікати тощо, які обслуговуються цим DNS-сервером.

DDoS на брандмауерах і брандмауерах. IDS призначені для захисту систем, що стоять за ними, від зовнішніх загроз шляхом обмеження трафіку передачі даних до захищених систем. Брандмауери також можна використовувати для захисту від атак відмови в обслуговуванні. Між тим, самі брандмауери можуть стати ціллю DDoS-атак.

1.5. Проблеми захисту мережі від DDoS

Незважаючи на величезні зусилля дослідників і експертів з безпеки, спрямовані на вирішення проблеми відмови в обслуговуванні, атаки відмови в обслуговуванні в мережі Інтернет все ще залишаються невирішеною проблемою. Існують різні технічні та нетехнічні проблеми, які необхідно зрозуміти, щоб розробити гарні рішення. Спочатку, необхідно дослідити принципи дизайну мережі

Інтернет та її вплив на проблему відмови в обслуговуванні. Також необхідно розглянути інші технічні проблеми та те, як вони впливають на вирішення проблеми відмови в обслуговуванні.

Проблеми, засновані на архітектурі мережі Інтернет. Розглядаючи особливості організації та побудови вузлів мережі Інтернет, необхідно зазначити, що Інтернету — це засіб комутації пакетів, у якому мережі з'єднані між собою за допомогою зберігання та пересилання пакетів. Пакетна комутація виділяє посилання для використання на вимогу серед користувачів. У такому середовищі користувач, який погано себе поводить, може порушити обслуговування інших користувачів, займаючи більшу частину спільних ресурсів. Такий розподіл ресурсів на основі запитів користувачів створює залежність між користувачами. Один із принципів проектування полягає в тому, що Інтернет повинен підтримувати простими основними мережами та просувати будь-яку складність на кінцеві хости. Це означає, що проміжні маршрутизатори або основні маршрутизатори повинні доставляти лише IP-пакети без необхідності розуміти служби вище мережевого рівня. Більшість змін в Інтернеті впроваджуються на кінцевих хостах. Це стимулює розробку нових протоколів і, отже, інструментів DDoS.

Багатошляхова маршрутизація. Інфраструктура маршрутизації мережі Інтернет розроблена з можливістю маршрутизації пакетів альтернативними шляхами, які обходять несправні частини мережі. Можливість багатошляхової маршрутизації зменшує здатність маршрутизаторів визначати підроблену адресу джерела, що ускладнює відстеження походження пакетів атаки в мережі Інтернет.

Децентралізоване управління. Інтернет складається з численних мереж, з'єднаних між собою, щоб забезпечити глобальний доступ кінцевим користувачам. В мережі Інтернет відсутнє центральне управління, і кожна взаємопов'язана мережа керується локально. Такий підхід до управління дозволяє мережі швидко розвиватися. Однак це також надало зловмисникам доступні ресурси та зробило спільний захист від DDoS-атак у кількох підмережах. Багато підходів захисту від

DDoS необхідно розгорнути в багатьох місцях, щоб бути ефективними. Однак забезпечити глобальне розгортання в мережі Інтернет надзвичайно важко.

На додаток до архітектурних проблем, описаних вище, існує кілька інших проблем, від яких важко захиститися від DDoS в мережі Інтернет.

1. Труднощі розрізнення шкідливих запитів. Важко відрізнити шкідливі запити від легітимних. Це справедливо для пакетів, мережевих потоків, сегментів транспортного рівня або повідомлень із запитом на служби програми.

2. Проблеми дослідження DDoS. Розвиток досліджень захисту від DDoS були тимчасово призуминені через брак інформації про атаку, відсутність стандартизованої оцінки та складність широкомасштабного тестування. Вони стверджують, що дуже обмежена інформація про інциденти DDoS є загальнодоступною через небажання організацій розкривати факт атаки, щоб уникнути пошкодження ділової репутації жертви. Без детального аналізу реальних DDoS-атак важко розробити хороші рішення проблеми.

3. Відсутність загальних характеристик потоків DDoS. Немає загальних характеристик потоків DDoS, які можна використовувати для їх виявлення та фільтрації. Атаки досягають бажаного ефекту, збільшуючи обсяг пакетів атаки, і можуть дозволити собі змінювати всі поля пакетів, щоб уникнути характеризації. На додаток до цього, зловмисники стежать за досягненнями у сфері безпеки та коригують свої інструменти, щоб обійти нові системи захисту безпеки.

4. Відсутність співпраці між адміністративними доменами. Співпраця розподілених джерел ускладнює боротьбу з DDoS-атаками або їх відслідковування. У той же час відсутня співпраця між адміністративними доменами-учасниками (джерелом, цільовим та проміжним доменами, які передають DDoS-трафік), що забезпечило б швидку, ефективну та розподілену відповідь на атаку.

5. Автоматизовані інструменти. Код атаки DDoS та автоматизовані інструменти для поширення та розгортання можна легко завантажити з мережі. Таким чином, навіть нетехнічні зловмисники можуть здійснювати потужні атаки.

6. Прихована особистість учасників. Зловмисники використовують підробку вихідної IP-адреси, щоб приховати ідентичність атакуючих машин, і використовують машини-обробники, щоб приховати свою власну ідентичність.

7. Діри в безпеці в Інтернет-хостах. Існують легко завантажувані патчі для більшості дір у безпеці, які використовуються зловмисниками для компрометації машин агентів. Тим не менш, існує величезна спільнота користувачів Інтернету, які недостатньо технічно складні та не знають про безпеку, щоб застосувати ці виправлення.

1.6. Різновиди DDoS атак

Обізнаність про прийоми та методи DDoS є основним ключем до впровадження системи захисту для боротьби з цими атаками. Багато експертів намагалися класифікувати механізми захисту від DDoS, щоб прояснити їх. Ця класифікація дає користувачам загальне уявлення про ситуацію і допомагає розробникам захисних механізмів співпрацювати проти загрози.

DDoS-атаки загалом поділяються на дві категорії: атаки на виснаження пропускної здатності та атаки на виснаження ресурсів [10].

Атаки на виснаження пропускної здатності. Атака, пов’язана зі зменшенням пропускної здатності, або атака на основі флудингу заповнює мережу жертви небажаним трафіком, що перешкоджає легальному трафіку досягти системи жертви. Атаки зменшення пропускної здатності можна розділити на два типи: атаки flood та атаки посилення:

– Атаки flood. Передбачає, що зомбі надсилають великі обсяги трафіку до системи жертви, щоб перевантажити пропускну спроможність мережі жертви IP-трафіком. Система жертви сповільнюється, виходить з ладу або страждає від насиченої пропускної здатності мережі, що перешкоджає доступу легальних користувачів. Атаки Flood були запущені з використанням пакетів UDP (User Datagram Protocol) і ICMP (Internet Control Message Protocol). Коли ICMP

використовується для заповнення жертви, зловмисник використовує зомбі, щоб відправити великі обсяги пакетів ICMP ECHO REPLY (ping) до системи жертви.

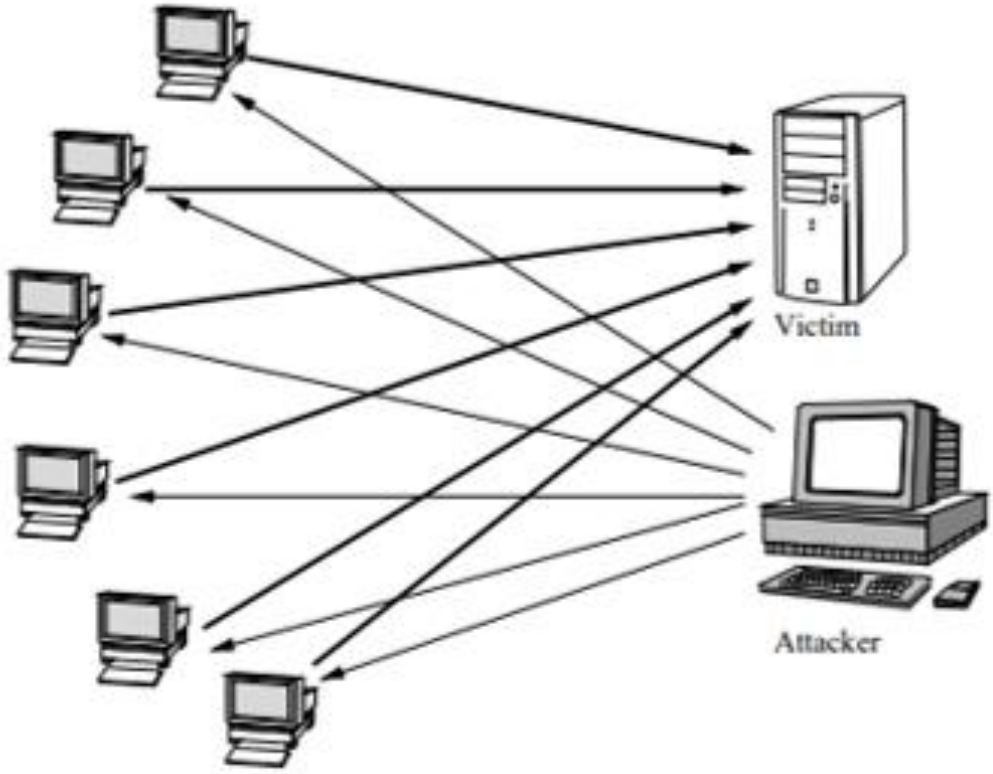

Рис.1.5. Простий приклад відбивача DDoS

– Атаки посилення. Як показано на рис.1.5., зомбі посилають повідомлення на широкомовну IP-адресу, щоб змусити всі системи підмережі, охопленої широкомовною адресою, надіслати відповідь системі-жертві. У цій атаці широкомовна IP-адреса використовується для посилення та відображення трафіку атаки і, таким чином, для зменшення пропускної здатності системи жертви. Атака Smurf є прикладом атаки посилення, коли зловмисник надсилає пакети до мережевого підсилювача – системи, яка підтримує широкомовну адресацію, з адресою повернення, підробленої на IP-адресу жертви. Іншим прикладом є атака DDoS Fraggle. Атака DDoS Fraggle подібна до атаки Smurf, оскільки зловмисник надсилає пакети на мережевий підсилювач. Fraggle відрізняється від Smurf тим, що Fraggle використовує пакети UDP ECHO замість пакетів ICMP ECHO.

*Атаки виснаження ресурсів. З*в'язують ресурси системи-жертви, що робить жертву не в змозі обробити легітимні запити на послуги. Зловмисник під час атак

на виснаження ресурсів надсилає пакети, які неправильно використовують зв’язок мережевого протоколу або мають неправильний формат

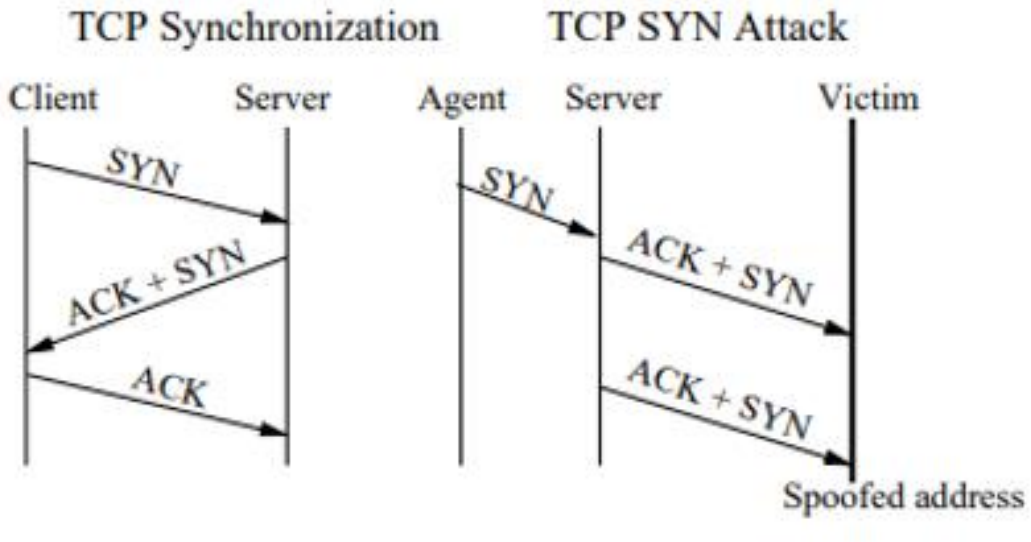

Рис.1.6. Модель атаки TCP SYN

Атаки зловживання протоколом. Неправильне використання пакету TCP SYN (синхронізація протоколу керування передачею), зловживання протоколом PUSH+ACK та підробка IP є прикладами такого типу атаки.

Під час атаки DDoS TCP SYN, як показано на рис.1.6, зловмисник інструктує зомбі надсилати фіктивні запити TCP SYN на сервер-жертву, щоб зв’язати ресурси процесора сервера і, отже, не дати серверу відповідати на законні запити. Під час атаки PUSH+ACK атакуючі агенти надсилають пакети TCP з бітами PUSH і ACK, встановленими в одиницю.

Ці тригери в заголовку пакету TCP дають вказівку системі-жертві вивантажити всі дані в буфері TCP і надіслати підтвердження після завершення. Якщо цей процес повторюється з кількома агентами, система-отримувач не зможе обробити великий обсяг вхідних пакетів, і система-жертва вийде з ладу. Під час підроблених IP-атак зловмисник надсилає DNS-запити на сервер DNS, щоб відповісти жертві, як показано на рис.1.7.

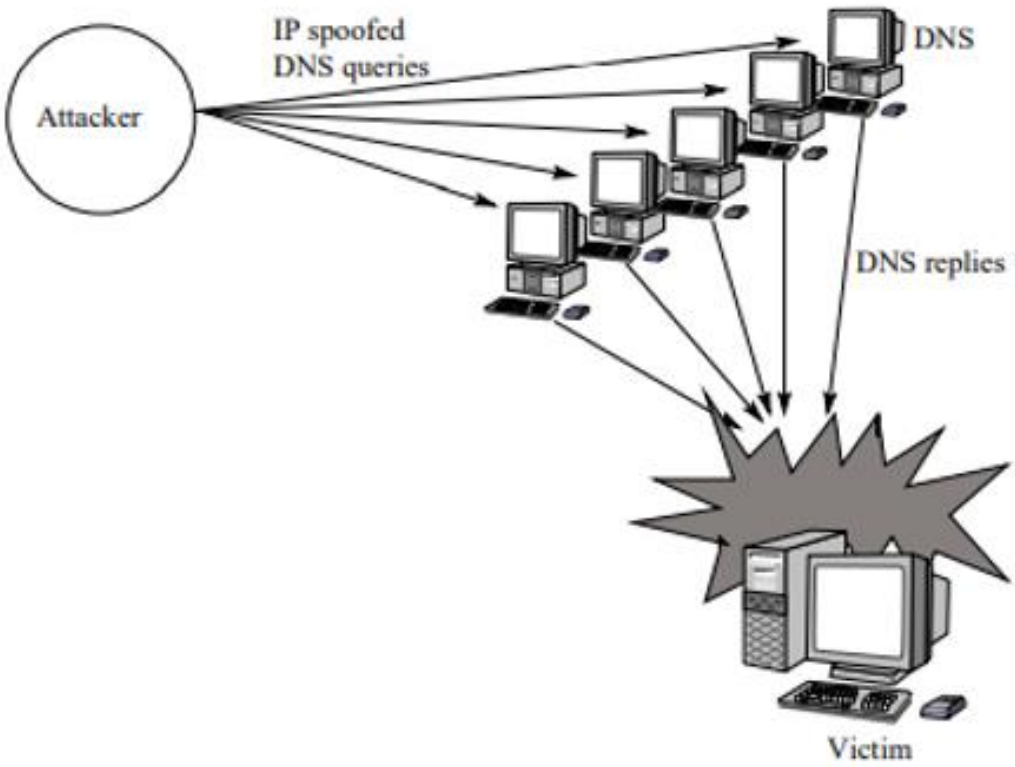

Рис.1.7. Тип підробленого IP для DDoS атаки

Атаки із неправильними пакетами. У цьому типі атаки зловмисник інструктує зомбі надіслати неправильно сформовані IP-пакети до системи-жертви, щоб зруйнувати її. Існує принаймні два типи атак із неправильним сформованим пакетом. При атаці на IP-адресу пакет містить однакові IP-адреси джерела та призначення. Це може заплутати операційну систему системи-жертви та призвести до збою системи-жертви. Під час атаки з параметрами IP-пакетів пакет із неправильною формою може рандомізувати необов’язкові поля в IP-пакеті та встановити всі біти якості обслуговування в один, так що система-жертва повинна використовувати додатковий час обробки для аналізу трафіку. Якщо ця атака буде множиною, вона може вичерпати можливості обробки системи-жертви.

1.7. Таксономія атак DDoS

Таксономія дозволяє розмірковувати про атаки та надає узагальнену класифікацію, яка ідеально пропонує способи пом'якшення атак шляхом

запобігання, виявлення та відновлення. Це може допомогти в управлінні ризиками, виявляючи вразливі місця та чітко визначаючи характеристики зловмисників. На основі попередніх обговорень різних типів атак було виведено таксономію атак на відмову в обслуговуванні. Рис.1.8. ілюструє таксономію атак відмови в обслуговуванні.

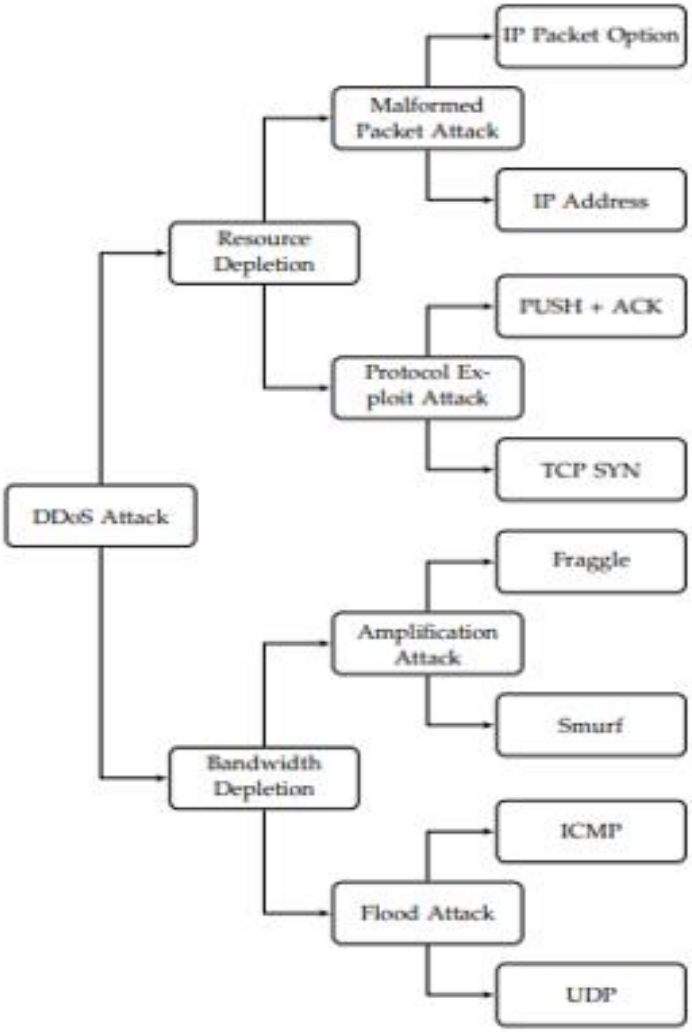

Рис.1.8. Таксономія атак DDoS

Пом'якшення DDoS-атак можна розділити на чотири етапи: запобігання, виявлення, ідентифікація джерела та відповідь. Підходи до запобігання намагаються виключити можливість DDoS-атак або запобігти завданню атаки будь-якої значної шкоди. Виявлення атак відстежує та аналізує події в системі, щоб виявити зловмисні спроби спричинити відмову в обслуговуванні. Це важливий крок, перш ніж спрямовувати подальші дії для протидії нападу. Ідентифікація

джерела атаки має на меті знайти джерела атаки незалежно від того, чи містить поле адреси джерела шкідливих запитів інформацію про підробку. Механізми реагування зазвичай запускаються після виявлення атаки.

Висновки до першого розділу

Зазначено, що багато рішень для запобігання DDoS-атак спрямовані на використання певних особливостей поточних атак. На жаль, зловмисники уважно стежать за подіями у сфері безпеки та можуть обійти систему безпеки.

Представлено три категорії, а саме: захист мережі жертви, захист проміжної мережі, захист кінцевої мережі, і описано сильні та слабкі сторони кожного методу.

Підкреслено, що системи захисту з одноточковим розгортанням або системи захисту жертви не можуть досягти успішного захисту від розподілених атак відмови в обслуговуванні. Проблема DDoS вимагає розподіленого рішення, в якому захисні вузли розташовані по всій мережі Інтернет та співпрацюють для досягнення кращого загального захисту.

Виокремлено, що системи захисту на основі аномалій є кращими перед системою захисту на основі сигнатур, оскільки вони можуть виявляти нові невідомі атаки.

Виведено, на основі попередніх обговорень різних типів атак, таксономію атак на відмову в обслуговуванні.

2 ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ЗАПОБІГАННЯ АТАКАМ DDOS

Механізми запобігання DDoS мають на меті зупинити атаки до того, як вони фактично завдадуть збитків підприємтсву чи організації. Механізми запобігання включають фільтрацію підроблених пакетів, самосертифікацію адрес і безпечні накладення.

2.1. Особливості функціонування механізму фільтрації підроблених пакетів для запобігання DDoS

Майже всі зловмисники DDoS підробляють IP-адресу, щоб приховати походження атаки. Методи атаки відображення та посилення покладаються на підробку IP-адреси. Механізми фільтрації призначені для того, щоб заборонити трафік DDoS-атаки з підробленими вихідними адресами досягати цілі шляхом відкидання пакетів з помилковими IP-адресами.

1. *Вхідна/вихідна фільтрація.* Мета вхідної/вихідної фільтрації полягає в тому, щоб дозволити трафіку входити або залишати мережу, лише якщо його вихідні адреси знаходяться в межах очікуваного діапазону IP-адрес. Вхідна фільтрація відноситься до фільтрації трафіку, що надходить у мережу, а вихідна фільтрація відноситься до фільтрації трафіку, що залишає мережу. Використання фільтрації вхідної мережі для протидії DDoS-атакам представлено в RFC 2827 як найкраща сучасна практика.

2. *Фільтрація на основі маршруту.* Підхід до фільтрації підроблених пакетів на основі фільтрації розподілених пакетів (DPF) на основі маршруту використовує інформацію про маршрутизацію, щоб визначити, чи дійсний пакет, що надходить на маршрутизатор з AS, щодо його позначених адрес джерела/призначення. DPF використовує інформацію про топологію маршрутизації BGP для фільтрації трафіку з підробленими адресами джерела.

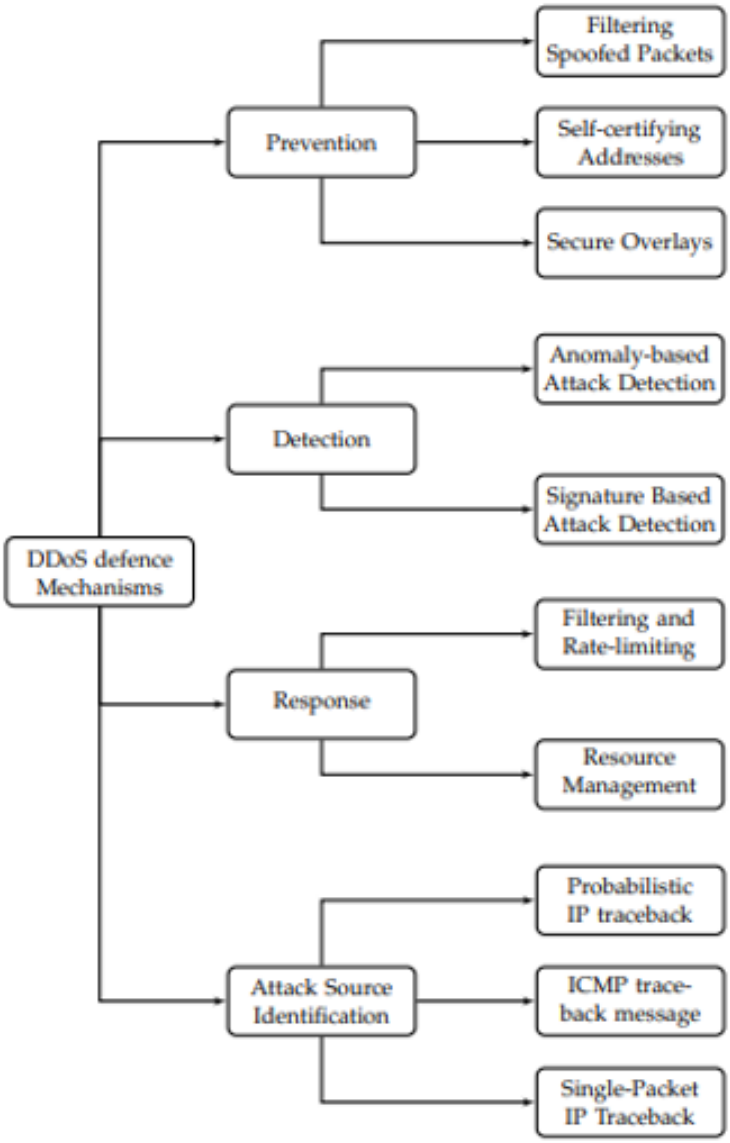

Рис.2.1. Таксономія механізмів пом'якшення DDoS

3. *Протокол перевірки валідності вихідної адреси (SAVE)*. Щоб подолати недоліки фільтрації на основі маршруту, був запропонований протокол перевірки валідності вихідної адреси. SAVE постійно поширює повідомлення, що містять дійсну інформацію про адресу джерела, від джерела до всіх місць призначення. Таким чином, кожен маршрутизатор в маршруті створює вхідну таблицю, яка пов’язує кожне посилання маршрутизатора з набором дійсних блоків адрес джерела. Коли пакет надходить на інтерфейс, маршрутизатор звертається до своєї вхідної таблиці, щоб визначити, чи надходить цей пакет з правильного напрямку.

4. Фільтрація кількості стрибків (HCF). HCF запроваджує фільтрацію пакетів із підробленими IP-адресами за допомогою методу, який називається

фільтрацією лічильника стрибків. Вони стверджують, що хоча зловмисник може підробити будь-яке поле в заголовку IP, він не може фальсифікувати кількість стрибків, які потрібно IP-пакету, щоб досягти місця призначення. Вони пропонують метод, щоб вивести цю інформацію про кількість стрибків із значення Time to Live (TTL) у заголовку IP. Використовуючи метод обчислення кількості стрибків на основі TTL, жертва створює таблицю зіставлення IP-адрес джерела. Коли жертва отримує пакет, вона обчислює кількість стрибків для своєї IP-адреси і порівнює його з кількістю стрибків, що зберігається в таблиці зіставлення, щоб ідентифікувати підроблені адреси пакети. Перевага HCF полягає в тому, що він вимагає розгортання на жертві, що набагато легше розгорнути в порівнянні з підходами до фільтрації на основі мережі. Більше того, потенційна жертва має набагато сильніший стимул до розгортання механізмів захисту, ніж проміжні постачальники мережевих послуг. Однак HCF страждає від високої кількості хибнопозитивних і хибнонегативних результатів.

5. *IPv4 Source Guard.* IP Source Guard забезпечує фільтрацію адреси вихідної IP-адреси версії 4 (IPv4) на порту рівня 2, щоб запобігти підробці IP-адрес зловмисним хостом. IP Source Guard відстежує призначення адреси DHCP і використовує статичні прив’язки джерела IPv4, щоб автоматично налаштувати кожен порт рівня 2 для відкидання трафіку, якщо IP-адреса джерела відрізняється від IP-адреси, призначеної цьому порту.

6. *Passport.* Passport — це структура перевірки вихідної адреси, яка має на меті гарантувати, що жоден хост або AS не зможе підробити адресний простір AS, яка розгортає Passport. Коли пакет залишає вихідну AS, прикордонний маршрутизатор ставить штамп по одному коду аутентифікації повідомлення (MAC) для кожної AS на шляху до місця призначення. Кожен MAC обчислюється за допомогою секретного ключа, спільного між вихідною AS і AS на шляху. Коли пакет потрапляє в AS на шляху, прикордонний маршрутизатор перевіряє відповідний MAC за допомогою секретного ключа, спільного з вихідною AS.

2.2. Особливості функціонування механізму самосертифікуючих адрес (self-certifying addresses) для запобігання DDoS

Підзвітність IP-адрес є однією з головних проблем, які необхідно вирішувати для запобігання DDoS-атаки. Host Identity Protocol і Accountable Internet Protocol є запропонованим рішенням для підзвітності IP.

1. *Host Identity Protocol (HIP).* Архітектура HIP пропонує новий простір імен, який називається простір імен Host Identity, і новий рівень протоколу під назвою Host Identity Protocol між мережею Інтернет і транспортними рівнями. Простір імен Host Identity складається з ідентифікаторів хосту (HI), де ідентифікатор хоста є відкритим ключем симетричної пари ключів. Архітектура HIP ефективна для запобігання підробці IP-адреси та запобігання DDoS.

2. *Підзвітний протокол Інтернету (AIP).* AIP забезпечує підзвітність рівня мережі Інтернет за допомогою самосертифікованих адрес. AIP розроблено для вирішення проблеми відсутності безпечної прив'язки хоста до його IP-адрес, а також відсутності безпечної прив'язки номера AS до префіксів IP, що належать цій AS. AIP роблять його дуже привабливим кандидатом для Інтернет-протоколів майбутнього покоління. Однак масштабованість маршрутизації та масштабованість інженерії трафіку AIP при схемі адресації для використання в Інтернеті є дуже серйозною проблемою.

Стратегія запобігання захищеному накладенню захищає жертву шляхом маршрутизації трафіку до захищеної мережі через накладену мережу, яка побудована поверх IP. Оскільки оверлейна мережа допускає лише авторизованих користувачів, і зловмисникам важко викликати DDoS на захищених серверах або мережах. Захищена жертва відокремлюється від мережі Інтернет шляхом приховування IP-адрес захищеної жертви або використанням розподілених брандмауерів для фільтрації всього вхідного трафіку до захищеної жертви, за винятком цього трафіку, що надходить від довірених вузлів у накладеній мережі. Secure Overlay Service і Secure-i3 є двома прикладами захисту від DDoS на основі безпечного накладання. Служби Secure Overlay Services (SOS) запобігають атакам

«відмова в обслуговуванні» на критичні сервери, перенаправляючи запити від попередньо аутентифікованих клієнтів на ці сервери через мережу накладання. Усі інші запити фільтруються за допомогою накладання. SOS — це розподілена система, яка пропонує чудовий захист зазначеної цілі за ціною модифікації комп'ютерів клієнтів, щоб вони усвідомлювали накладення та використовували його для доступу до цілі. Захищене накладення створюється шляхом вибору набору вузлів, розподілених по всій мережі, і логічно пов'язаних.

Як показано на рис.2.2, весь вихідний трафік перевіряється безпечною точкою доступу накладання (SOAP). Аутентифікований трафік буде перенаправлено на спеціальний накладений вузол, який називається маяком. Потім маяк направляє трафік на інший спеціальний вузол накладання, який називається секретним сервлетом для подальшої аутентифікації, а секретний сервлет направляє перевірений трафік до жертви

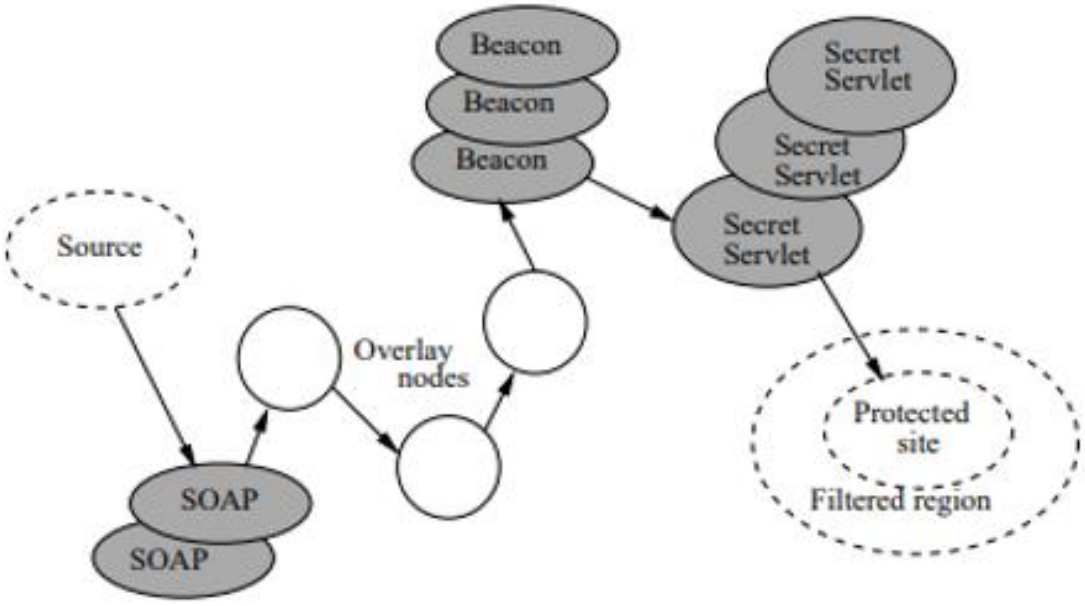

Рис.2.2. Зв'язок між авторизованим джерелом і захищеним сайтом у SOS

Особистість секретного сервлета розкривається лише маяку і залишається таємницею для зловмисника. SOS надійний проти DDoS-атак через наступні причини:

- якщо точку доступу атакують, джерело може вибрати альтернативну точку доступу.
- якщо ідентичність секретного сервлета виявлена зловмисниками, захищений сайт може вибрати альтернативний набір секретних сервлетів.

Основним недоліком SOS є те, що він не підходить для загальнодоступної служби, наприклад веб-сервера. Клієнти сервера, захищеного SOS, повинні зареєструвати свою особу, перш ніж вони зможуть підключитися, і потрібна велика кількість накладених вузлів, щоб зробити систему стійкою до DDoS-атак. Крім того, SOS не захищає від інсайдерських атак. Крім того, розгортання також є відносно складним. Secure Overlay Forwarding System (SOFS) є розширенням SOS, спрямованим на опір інтелектуальним атакам DDoS.

SOS використовує трирівневу архітектуру, тоді як SOFS використовує більше трьох шарів і, таким чином, забезпечує більший захист жертві. Розгортання SOFS вимагає багатьох змін у системі мережі. Secure-i3 — це назва накладеного мережевого рішення. Наскрізний зв'язок між двома хостами маршрутизується в межах накладання на основі ідентифікаторів замість IP-адрес. Secure-i3 використовує мережу накладання i3 як засіб приховування IP-адрес кінцевих хостів. Існує кілька проблем із Secure-i3. Припущення, що IP-адреси кінцевих хостів і частини вузлів i3 невідомі зловмиснику. Зловмисник може отримати таку інформацію за допомогою різних методів, таких як відбиток і сканування. Secure-i3 вимагає великої кількості потужних вузлів i3 з достатньою пропускною здатністю для розгортання в Інтернеті, що додає дуже високі додаткові витрати. Оскільки маршрутизація в накладеній мережі Secure-i3 створює додатковий рівень опосередкованості, вона збільшує наскрізну затримку та зменшує продуктивність мережі[20].

2.3. Дослідження стратегій виявлення DDoS атак

Стратегії виявлення DDoS поділяються на три типи: виявлення на основі сигнатур, виявлення на основі аномалій та гібридні системи. Методи на основі

сигнатур здійснюють пошук шаблонів або сигнатур у мережевому трафіку (який досліджується), які відповідають відомим сигнатурам атак із бази даних. Методи, засновані на аномалії, порівнюють параметри спостережуваного мережевого трафіку зі звичайним трафіком, і, отже, можливе виявлення нових атак. Однак, щоб уникнути помилкових тривог, модель звичайного трафіку повинна постійно оновлюватися, а поріг категоризації аномалії повинен бути належним чином налаштований. Нарешті, гібридні системи поєднують обидва ці методи. Гібридні системи зазвичай оновлюють свою базу даних сигнатур за допомогою атак, виявлених шляхом виявлення аномалій. У таблиці 2.1 показано порівняння виявлення атак на основі сигнатур і аномалій.

Таблиця 2.1

Порівняння виявлення атак на основі сигнатур і аномалій

Виявлення атак на основі сигнатур	Виявлення атак на основі аномалій
– Визначити атаки за допомогою відповідності шаблону або ознакам відомих атак; – Надійне та просте виявлення для вже відомих атак; – База даних сигнатур має постійно оновлюватися, щоб підтримувати надійність системи.	– Виявити атаки шляхом моніторингу змін обсягу трафіку або функцій; – Невідомі атаки можуть бути виявлені; – Оновлення моделей необхідно оновлювати зі змінами системи.

1. *Виявлення атак на основі сигнатур*. Система захисту на основі сигнатур намагається знайти відповідність шаблону або сигнатурі, які можуть дозволити виявити конкретні відомі атаки. В основному цей тип виявлення досліджує вміст пакетів і приймає рішення про атаку. Перевага цих методів полягає в тому, що вони можуть легко і надійно виявляти відомі атаки, але не можуть розпізнати нові атаки. Більше того, база даних підписів повинна постійно оновлюватися, щоб підтримувати надійність системи.

Bro — це система виявлення вторгнення в мережу для виявлення зловмисників у мережі в режимі реального часу шляхом моніторингу мережевого зв’язку. Система Bro є високошвидкісною, для моніторингу великого обсягу, з механізмами виявлення атак у реальному часі. Bro концептуально розділений на механізм подій, який підтримує стан для кожного з'єднання на основі вихідної IP-адреси, вихідного порту, IP-адреси призначення та порту призначення. Bro вимагає ручного створення сигнатур атак і сценаріїв обробки подій, що вимагає від адміністраторів безпеки докладних зусиль і сильного досвіду виявлення вторгнень [21].

Snort спирається на сигнатури, які визначають шаблони байтів відомих пакетів атаки. Вони забезпечують низький рівень помилкових позитивних результатів, але не можуть виявити раніше невідомі атаки. Snort — це легкий інструмент виявлення та запобігання вторгненню в мережу з відкритим вихідним кодом, а також широко розгорнуті системи виявлення та запобігання вторгненню в мережу по всьому світу.

2. *Виявлення атак на основі аномалій*. Механізми виявлення атак DDoS на основі аномалій аналізують нормальну поведінку в системі та мають на меті виявити атаки шляхом виявлення значних відхилень від нормальної поведінки. Здебільшого він виявляє атаки, відстежуючи зміни обсягу трафіку або функцій. Він ефективний проти DDoS-атак, які можна виявити. У порівнянні з підходами виявлення на основі сигнатур, ця стратегія може виявляти раніше невидимі атаки. Підходи, засновані на аномаліях, стикаються з проблемою під час визначення порогу для нової поведінки атаки. Механізми, які розгортають виявлення аномалій, мають модель нормальної поведінки системи, наприклад, модель нормальної динаміки трафіку або очікуваної продуктивності системи. Поточний стан системи періодично порівнюється з моделями для виявлення аномалій. Перевага виявлення аномалій перед виявленням шаблонів полягає в тому, що можна виявити невідомі атаки. Однак виявлення на основі аномалій має вирішувати дві проблеми:

- *Встановлення порогового значення*. Аномалії виявляються, коли поточний стан системи відрізняється від моделі на певний поріг. Встановлення

низького порогу призводить до багатьох помилкових спрацьовувань, тоді як високий поріг знижує чутливість механізму виявлення.

- *Оновлення моделі*. Системи та моделі комунікації розвиваються з часом, і моделі необхідно оновлювати, щоб відобразити цю зміну. Системи на основі аномалій зазвичай виконують автоматичне оновлення моделі, використовуючи статистику, зібрану в той час, коли атака не була виявлена. Такий підхід робить механізм виявлення вразливим до збільшення частоти атак, які можуть помилково розглянути моделі та затримати або навіть уникнути виявлення атак. Системи виявлення аномалій, такі як NSOM, відстежують мережевий трафік і шукають аномальну поведінку, застосовуючи нейронні мережі або механізми на основі порогових значень. Вони здатні виявляти раніше невідомі атаки за рахунок більш високого рівня хибнопозитивних і хибнонегативних результатів [22].

2.4. Аналіз методів ідентифікації джерела атаки DDoS

Після виявлення атаки відповідь на атаку є більш ефективною поблизу джерела атаки. На жаль, немає простого способу відстежити IP-трафік до його джерела. Це пояснюється двома характеристиками протоколу IP. По-перше, вихідні IP-адреси можуть бути підроблені. По-друге, IP-маршрутизація без стану, коли маршрутизатори зазвичай знають лише наступний стрибок для пересилання пакета. Далі буде представлено деякі методи ідентифікації джерела.

1. *Імовірнісне відстеження IP (PPM)*. Схема PPM відстежує анонімні атаки переповнення пакетів в Інтернеті до їх джерела. Основна ідея імовірнісного маркування пакетів полягає в тому, що кожен маршрутизатор імовірно кодує інформацію про відстань до одержувача та адресу маршрутизатора в поле маркування в заголовку пакета, а приймач реконструює шлях, який пройшов пакет із закодованої інформації.

2. *Повідомлення ICMP traceback*. Новий тип повідомлення ICMP під назвою iTrace packet використовується, щоб допомогти одержувачу відновити шлях, який проходять пакети через Інтернет. Кожен маршрутизатор генерує

повідомлення відстеження з дуже низькою ймовірністю для кожного пакету, який він пересилає, і надсилає повідомлення одержувачу. Перевага цієї схеми в тому, що вона проста і легко реалізується. Однак для захисту цілісності інформації, що міститься в повідомленні відстеження, йому потрібні цифрові підписи.

3. *Відстеження однопакетної IP-адреси (SPIE)*. SPIE ідентифікує джерело конкретного IP-пакету, надавши копію пакета, який слід відстежувати. Він знаходить IP-адресу та приблизний час отримання. SPIE вимагає від усіх маршрутизаторів зберігати хеш-дайджест нещодавно пересланих пакетів. Коли потрібне зворотне відстеження, запит надсилається до SPIE, який, у свою чергу, запитує у маршрутизаторів зведення пакетів за відповідні періоди часу. Основна перевага SPIE перед відстеженням PPM та ICMP полягає в тому, що одержувачу не потрібно отримувати велику кількість пакетів атаки для відстеження до джерела атаки. Однак SPIE вимагає великого обсягу пам'яті для зберігання дайджестів пакетів на маршрутизаторах.

4. *Схема зміни ентропії.* Для реалізації схеми зворотного відстеження використовується зміна ентропії мережевого трафіку. Різниця значень ентропії між звичайним трафіком і трафіком під час DDoS-атаки використовується для виявлення атаки. Після його виявлення починається відстеження через процедуру відстеження. Запропонована схема має перевагу перед традиційними схемами маркування пакетів з точки зору вимог до масштабованості та зберігання в потерпілих або проміжних маршрутизаторах. Метод зберігає лише короткочасну інформацію про ентропію трафіку для виявлення DDoS-атаки. Метод здатний реалізувати точне відстеження в сценарії масштабної DDoS-атаки протягом декількох секунд.

5. *Хмарний захист безпеки*. Для захисту від XML DoS-атаки використовується механізм, який включає детерміновану маркування пакетів і сервісно-орієнтовану архітектуру зворотного відстеження. Це механізм відстеження, який визначає джерело атаки та фільтрує його. У цій схемі використовуються хмарний трекбек і хмарний захист. Хмарна трасування назад

позначає вхідні пакети, а хмарний захист фільтрує пакети. Хмарний захист — це навчена нейронна мережа зворотного поширення.

6. *Відстеження з використанням нових інформаційних метрик*. Узагальнена метрика ентропії та метрика інформаційної відстані були запропоновані для виявлення низькошвидкісних DDoS-атак. Цей підхід має переваги з точки зору швидкості виявлення та частоти хибних позитивних результатів. Непрактичність цього підходу є досить невдалою, оскільки успішна реалізація покладається на отримання повного контролю над усіма маршрутизаторами в мережі [23].

2.5. Аналіз механізмів реакції на атаку DDoS

Після своєчасного застосування методів виявлення атаки та ідентифікації джерела атаки необхідні подальші дії для протидії атаці. Механізми реакції або реагування зазвичай запускаються після виявлення атаки, щоб усунути або мінімізувати вплив атаки. Популярними механізмами реакції є фільтрація, обмеження швидкості та управління ресурсами.

1. *Фільтрація та обмеження швидкості*. Механізми фільтрації та обмеження швидкості використовують характеристику шкідливого трафіку, яка надається механізмами виявлення, щоб відфільтрувати потоки атак або обмежити швидкість. Обмеження швидкості зазвичай використовується у випадках, коли виявлення має багато помилкових спрацьовувань або не може точно охарактеризувати трафік атаки. Алгоритм обмеження швидкості заснований на тому факті, що швидкість трафіку на кінці жертви є нормальною, якщо швидкість трафіку, що пересилається жертві всіма маршрутизаторами рівня k, нормальна. Одним з недоліків є те, що він використовує однаковий ліміт швидкості для всіх маршрутизаторів рівня k, і, отже, це несправедливо для тих маршрутизаторів, які передають мало або зовсім не передають атакуючий трафік. Супутній збиток для законного трафіку буде неминучим у цих маршрутизаторах. Розподілена захисна структура на основі накладання виявляє атаки на стороні жертви. Під час пошуку

джерела використовується SPIE. Щоб контролювати трафік атаки на кінці джерела, він поєднує історію потоку з обчисленням обмеження швидкості, визначаючи аргумент репутації.

Підробка DDoS-атаки може зробити алгоритм обмеження швидкості на основі потоку неефективним. Більше того, реалізація фреймворка потребує відносно великої модифікації поточної мережі. Фільтрація пакетів зазвичай виконується на маршрутизаторах на основі чітко визначених сигнатур атак, наприклад, явно неправильних адрес джерел. Загальним недоліком фільтрації пакетів є те, що її потрібно широко розгорнути, щоб захистити жертву, а трафік атаки неможливо відфільтрувати, якщо він використовує пакети, які запитують легітимні послуги.

Метод фільтрації Pushback high-bandwidth aggregates (ACC) - призначений для управління агрегатами високої пропускної здатності в мережі, де агрегат є набір пакетів від одного або кількох потоків, які мають деяку спільну властивість. ACC включає в себе локальний механізм для ідентифікації та керування агрегатом на одному маршрутизаторі, а також спільний механізм зворотного зв'язку, за допомогою якого маршрутизатор може запитувати маршрутизатори вище по потоку керувати агрегатом. ACC запускається лише тоді, коли в каналі спостерігається стійка серйозна перевантаженість, яку можна визначити, шукаючи тривалий період високої швидкості втрати пакетів. Після виявлення серйозного затору ACC визначає агрегати, які відповідають за перевантаження. На жаль, відмова кожного джерела у великій розподіленій DDoS-атаці, ймовірно, буде відносно дорогим з точки зору стану мережі, і вимагає окремого ідентифікації та відкидання кожного джерела.

StopIt. Це захисна структура від DDoS на основі фільтрів. StopIt прагне зупинити небажаний трафік, призначений одержувачу, не завдаючи шкоди законним хостам, які надсилають трафік цьому одержувачу. Сервер StopIt дізнається адреси інших серверів StopIt, прослуховуючи оновлення протоколу Border Gateway Protocol (BGP)[24].

2. *Управління ресурсами.* Фундаментальна проблема мережі Інтернет щодо DDoS-атак полягає в тому, що одержувач не контролює, хто може надіслати йому скільки трафіку. Зловмисник може просто ігнорувати будь-які сигнали контролю перевантажень і надсилати трафік з максимально можливою швидкістю. Рішення для реагування на DDoS на основі керування ресурсами мають на меті дозволити одержувачу зупинити неправильну поведінку відправників.

Фактично, DDoS є проблемою перевантаження ресурсів, підходи до обліку ресурсів можуть її вирішити. Одним з недоліків цих механізмів є те, що клієнти повинні знати про захист і встановлювати спеціальне програмне забезпечення, що дозволяє їм відповідати на тести на легітимність. Іншим недоліком є те, що облік ресурсів вимагає збереження стану на одного користувача, отже, вимоги до зберігання зростають із збільшенням кількості законних користувачів. Це означає, що система повинна бути встановлена в кінцевій мережі.

Захист жертв не може впоратися з великими атаками, які перевантажують систему захисту. Механізми примноження ресурсів забезпечують велику кількість ресурсів для протидії DDoS-загрозам. Наприклад, пул серверів з балансувальником навантаження і встановлює високопропускні зв'язки між собою та маршрутизаторами вище по потоку. Інший підхід — динамічне отримання ресурсів після виявлення атаки. Ці підходи, по суті, піднімають планку того, скільки машин має брати участь в атаці, щоб бути ефективною. Хоча не забезпечує ідеального захисту, для тих, хто може дозволити собі витрати, збільшення ресурсів часто виявляється достатнім. Іншим підходом є використання служб Akamai для розподіленого хостингу веб-сайтів. Запити користувачів на веб-сторінку, розміщену таким чином, перенаправляються на сервер імен Akamai, який потім розподіляє навантаження між кількома географічно розподіленими веб-серверами, на яких розміщуються репліки запитуваної сторінки. Фільтр інтернет-потоку без стану та архітектура перевірки трафіку — це дві добре відомі схеми керування ресурсами: фільтр Інтернет-потоку без стану (SIFF) SIFF вибірково зупиняє небажані потоки атак від досягнення мережі одержувача. SIFF передбачає два класи Інтернет-пакетів: привілейовані пакети, які підлягають контролю з боку

одержувача, і непривілейовані пакети, які використовуються в застарілому трафікі та при рукостисканні SIFF.

Протокол рукостискання SIFF використовується відправниками для отримання можливостей надсилати привілейований трафік. Відправник починає процес рукостискання, надсилаючи пакет запиту на можливості з ініціалізованим значенням його можливостей.

Архітектура перевірки трафіку (TVA) — це архітектура мережі, яка обмежує вплив DDoS-флудів. Архітектура TVA спирається на запропоновану раніше роботу щодо можливостей і намагається усунути обмеження попередніх механізмів можливостей, таких як SIFF. TVA має на меті подолати атаки, пов’язані з наповненням каналу налаштування можливостей, і атаки, які переповнюють приймач, використовуючи вже отримані можливості. Існує кілька недоліків схеми TVA. Наприклад, TVA припускає, що одержувач може відрізнити зловмисного відправника від законного. Отже, TVA покладається на метод ідентифікації атаки для фільтрації шкідливого трафіку, а ефективність його запобігання DDoS залежить від точності методу ідентифікації.

2.6. Опис узагальнених пропозиції щодо захисту від DDoS

1. *Захист мережі жертви.* Більшість систем для боротьби з DDoS-атаками працюють на стороні жертви. Як було описано раніше, захист жертв не може забезпечити повний захист від атак DDoS, оскільки сама система захисту може бути переповнена трафіком атаки.

Кілька систем захисту від DDoS здійснюють виявлення аномалій (зазвичай у мережі-жертві), спостерігаючи численні параметри трафіку та визначаючи діапазон дозволених значень на основі аналізу даних трасування пакетів. Відповідь на атаку полягає у встановленні невибіркового обмеження фіксованої швидкості для потоків-порушників, що, ймовірно, завдає шкоди законному трафіку.

У роботі [25] була запропонована система захисту на основі сигнатур шляху (PS). Система вимагає, щоб усі маршрутизатори повертали вибрані біти в полі

ідентифікації IP для всіх вхідних пакетів. На основі цих бітів маркування можна створити унікальний PS для всіх пакетів з одного місця. На стороні жертви система захисту відокремлює трафік на основі PS кожного пакету і виявляє DDoS-атаки шляхом моніторингу аномальних змін обсягу трафіку від PS. Потім для цього трафіку буде встановлено обмеження швидкості. Однак важко виявити DDoS-атаки, якщо різноманітність PS набагато більше, ніж реальна різноманітність вхідного трафіку маршрутизатора. Крім того, можливо, що PS був змінений після виявлення атаки. У цій ситуації не можна уникнути побічної шкоди для легітимного трафіку. Захисний фреймворк для DDoS-атак на основі flooding виявляє атаки на жертву за допомогою методів дистанційного захисту від DDoS і реагує на атаки на кінцях джерела. У схемі є дві проблеми: зв'язок із кінцевою мережею під час атаки, і виявлення атаки на мережу жертву не може заборонити пошкодження жертви.

2. *Захист проміжної мережі.* Розподілена система захисту на граничних маршрутизаторах або в основних маршрутизаторах має певну перевагу перед захистом однієї точки. Ідея спільного захисту від DDoS-атак була запропонована в ряді проектів.

- DefCOM є розподіленою кооперативною системою, яка поєднує різноманітні системи захисту для спільного реагування на DDoS. DefCOM містить три типи вузлів, а саме: вузли оповіщення, вузли ядра та вузли класифікатора. Вузли оповіщення виявляють атаки поблизу цілі та поширюють тривогу. Основні вузли та вузли класифікатора обробляють різні види трафіку, напр. Вузли класифікатора розрізняють легітимні та атакуючі пакети. Різні політики адміністрування мережі ускладнюють розгортання цієї системи захисту.
- MANAnet утворює кооперативні околиці захисних вузлів навколо жертви. Ці вузли штампують пакети, які вони пересилають, кодуючи шлях до жертви в заголовку пакета. Маршрутизатор на жертві пропонує значну частку ресурсів кожному закодованому шляху. Вихідні мережі можуть додатково розгорнути зворотний брандмауер, щоб запобігти вихідним атакам. MANAnet вимагає безперервного розгортання захисних вузлів поблизу жертви та внесення

змін до протоколу IP, щоб полегшити штампування пакетів. Обидві ці функції можуть перешкоджати широкому розгортанню.

- COSSACK — це розподілений підхід до виявлення та реагування на DDoS, який використовує програмну підсистему, відому як охоронний таймер. Кожна мережа повинна розгорнути власний охоронний таймер на вихідному маршрутизаторі. Пристрої виявляють атаки за допомогою існуючих систем виявлення вторгнень і діляться своїми рішеннями з іншими сторожовими, що підвищує впевненість виявлення. Багатоадресний зв'язок використовується для попередження інших сторожових. COSSACK покладається виключно на методи інших систем захисту для прийняття локальних рішень, а багатоадресний зв'язок споживає більше мережевих ресурсів, ніж протокол пліток, який ми використовували в нашій системі захисту.

- IDIP — це протокол прикладного рівня, який координує виявлення та відповіді множинних систем виявлення вторгнень. Вузли IDIP організовані в райони та спільноти. Скоординованим виявленням, відстеженням атак і реагуванням у спільноті керує компонент, який називається координатором виявлення. IDIP передбачає безперервне розгортання мікрорайонів, які обмінюються інформацією, і, таким чином, його здатність запобігати атакам обмежена в сценарії часткового розгортання. Через підробку IP-адрес у DDoS-атаках використовується багато підроблених IP-адрес.

- SIM — це схема виявлення на основі моніторингу IP-адреси джерела. SIM-карта розгортається на граничному маршрутизаторі, який забезпечує доступ до Інтернету до підмережі, в якій знаходиться ціль. SIM передбачає, що набір вихідних IP-адрес, які бачать під час нормальної роботи, є дещо постійними, і більшість раніше невидимих адрес, які з'явилися під час атаки, належать зловмисникам. Використовуючи попередньо створену базу даних IP-адрес, SIM відстежує частку раніше небачених вихідних IP-адрес і виявляє будь-які різкі зміни за допомогою алгоритму послідовного визначення точок зміни кумулятивної суми (CUSUM). Різка зміна частки нових вихідних IP-адрес позначається як серйозна

ознака DDoS-атаки. Вони також намагаються підвищити точність виявлення, одночасно відстежуючи швидкість трафіку на IP-адресу.

- Активна система безпеки (ASSYST) складається з захисних вузлів, розгорнутих у периферійних мережах. Після виявлення атаки вузли виявляють своїх однорангових за допомогою повідомлень-зондів і організовують себе в однорангову мережу. Запити на блокування потім поширюються на вищезазначені однорангові, а відповідь встановлюється якомога ближче до джерел. ASSYST не забезпечує відокремлення легітимних потоків від атак і, ймовірно, зменшить побічні збитки.

- Distributed Change-point Detection (DCD) використовує дерева агрегації змін (CAT) для виявлення DDoS шляхом співпраці між різними доменами в ISP. Кожен домен створює CAT на основі надпотоку трафіку маршрутизаторів. Завдяки співпраці між CAT кожного домену будується глобальне дерево CAT. Як тільки глобальне дерево CAT перевищує встановлений поріг, оголошується атака. Оскільки порогове значення кішки не є однаковим для всіх типів прикріплення, встановлення ідеального порогового значення в цій системі захисту є складним завданням, тоді як у нашій системі захисту ми приймаємо рішення на основі можливостей жертви.

- FireCol — це мережа спільного захисту для виявлення атак Flooding DDoS, розгорнута на рівні постачальників послуг Інтернету (ISP). Ця система захисту формує віртуальні захисні кільця навколо хостів для захисту та співпраці шляхом обміну вибраною інформацією про трафік.

Однак, як і в службах Secure Overlay Services (SOS), клієнт повинен зареєструватися заздалегідь, щоб отримати доступ до Інтернет-сервісів, захищених FireCol, а обмін інформацією про атаку в системі захисту є небезпечним.

3. *Захист у кінцевій мережі.* Система захисту від DDoS, яка може бути розгорнута в мережах, де розташована більшість джерел атаки, відома як система захисту в кінцевій мережі. D-WARD і MULTOPS є двома прикладами систем захисту Source-end.

- D-WARD — це система захисту від DDoS-атак на стороні джерела, яка автономно виявляє та зупиняє атаки, що походять із мережі джерела атаки. Атаки виявляють шляхом моніторингу потоків двостороннього трафіку між мережею та рештою Інтернету. Потоки, що відстежуються, періодично порівнюються з попередньо визначеними моделями звичайного трафіку, і ці потоки, які класифікуються як частина DDoS-атаки, мають обмежену швидкість. Моделі звичайного трафіку TCP, ICMP, UDP використовуються як моделі звичайного трафіку TCP, ICMP, UDP. Як тільки потік атаки буде ідентифікований, він буде контролюватися за граничним значенням швидкості. Хоча D-WARD може виявити деякі атаки на стороні джерела, виявлення може бути схильним до помилок через відсутність зв’язку між джерелом і кінцем жертви, а також координації між захисними системами джерела.
- MULTOPS — це евристика та структура даних, які мережеві пристрої можуть використовувати для виявлення атак DDoS. Кожен мережевий пристрій підтримує багаторівневе дерево, відстежуючи певні характеристики трафіку та зберігаючи дані у вузлах, що відповідають префіксам підмережі на різних рівнях агрегації. Дерево розширюється і стискається в межах фіксованого бюджету пам'яті.

Атака виявляється за ненормальними значеннями співвідношення пакетів, а швидкість потоків обмежена. Система розроблена таким чином, щоб вона могла працювати як система захисту від DDoS-атак на стороні джерела або як жертва. Потоки, не пов’язані з TCP, у системі, що використовує MULTOPS, можуть бути неправильно класифіковані як потоки атак, або визнані як спеціальні та обмежені фіксованим значенням. У першому підході шкода завдається законному потоку, тоді як у другому підході достатньо розподілена атака все ще може використовувати дозволену швидкість для досягнення ефекту.

Висновки до другого розділу

Досліджено методи, призначені для захисту від DDoS атак. Зазначено, що представлені методи є статичними за своєю природою і не включають внутрішнього процесу, що необхідний для забезпечення повноцінного захисту.

Проаналізовано матеріал, який вказує на виокремлену таксономію атак. Підкреслено послідовність у визначенні атак і впровадженні відповідного захисту.

Виокремлено рішення та механізми, які необхідні для виявлення та реагування на DDoS атаки. Зазначено, що одним з недоліків цих механізмів є те, що клієнти повинні знати про захист і встановлювати спеціальне програмне забезпечення. Це означає, що система повинна бути встановлена в кінцевій мережі.Іншим недоліком є те, що за останні роки відбулося прогресивне зростання кількості DDoS атак.

3 ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ТА ПРОТИДІЇ РОЗПОДІЛЕНИМ АТАКАМ СПРЯМОВАНИМ НА ВІДМОВУ В ОБСЛУГОВУВАНІ

Приблизно 20 років тому з’явився такий різновид атак як DoS або атака типу «відмова в обслуговуванні». Згодом DoS переріс на DDoS, тобто фактично «розподілений DoS» – атака спровокована не одним атакуючим, а розподіленою мережею. На той момент, а саме у 90-ті роки, навряд чи можна було правильно оцінити появу такої нової «кіберзброї», з огляду на невелику потужність тогочасних інформаційних систем. Але дуже швидко відбувся прорив у створенні веб-сервісів і великих хмарних платформ, які дали змогу без проблем адаптувати попит на якісні інфопослуги та великі обсяги обробки даних.

3.1. Аналіз найгучніших атак DDoS та векторів направленості

Існує багато видів DDoS-атак. Вони можуть орієнтуватися на різні рівні OSI і використовувати різні методи. Під час DDoS-атаки зловмисники знаходять уразливі місця і можуть, наприклад, запустити вірус на веб-сайт і викрасти дані користувачів чи клієнтів.

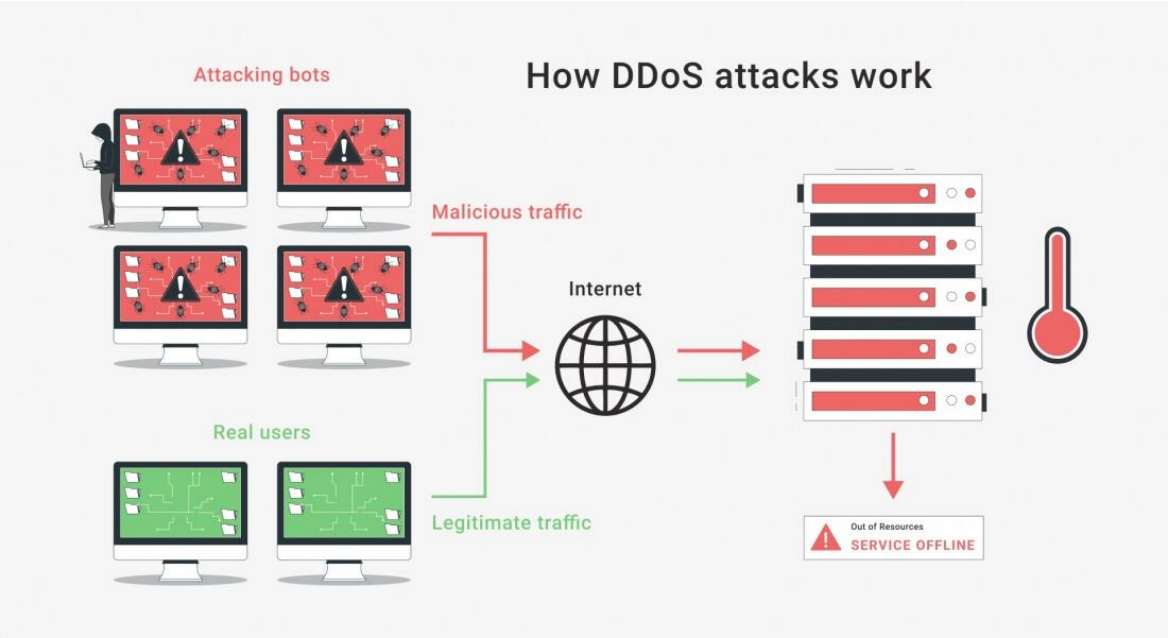

Рис.3.1. Узагальнена схема функціонування DDoS

Github атака. На початку березня 2018 року відбулася найпотужніша DDoS-атака в історії. Вона вразила GitHub, встановивши новий рекорд – 1,35 Тбіт/с, або 126,9 мільйона пакетів в секунду. Зловмисники навчилися використовувати для посилення DDoS-сервери Memcached, які можуть посилити атаку більш ніж у 50 000 разів.

Атака Eve online. У лютому 2020 року потужна DDoS-атака, яка тривала більше тижня, повністю паралізувала ігровий процес: чати, керування кораблем і ринкові транзакції були заблоковані.

Атака Takeaway.com. У березні 2020 року сталася велика DDoS-атака на мережу доставки їжі Takeaway.com. Ресторани могли отримувати замовлення, але не могли їх обробляти. Зловмисники вимагали від компанії 2 біткойни в якості оплати за припинення DDoS-атаки. Того ж дня генеральний директор опублікував у Твіттері скріншот їхнього повідомлення. Takeaway.com. вирішив не платити викуп, але сама DDoS-атака завдала серйозної шкоди. Вони повинні були повернути кошти всім користувачам, чиї замовлення були оплачені, але не доставлені.

Рис.3.2 Скріншот повідомлення зловмисників при атаці Takeaway.com

Аналітики Qrator Labs підвели підсумки другого кварталу 2021 року, опублікувавши статистику DDoS-атак та BGP-інцидентів. Повідомляється, що

найбільший ботнет зріс майже вдвічі, а основними векторами атак, як і раніше, є UDP-, IP- та SYN-флуд (рис.3.3).

Вектор атак. У другому кварталі 2021 року було зафіксовано серйозне зростання UDP flood атак, на частку яких припало більше половини нападів (53,04%). Саме UDP flood використовується для генерації великої кількості флуду через велику кількість вразливих серверів. Експерти пишуть, що зростання цього сегмента обумовлено збільшенням частки атак смугою 10-100 Гбіт/сек – клас високошвидкісних атак, для організації яких часто використовується техніка Amplification публічних UDP-сервісів.

Складніші атаки, такі як SYN flood, також не здають своїх позицій: їхня частка у другому кварталі склала 11,9%. Такі атаки небезпечні тим, що безладно інфраструктуру, «вимикають» окремі пристрої, і боротися з ними шляхом простого скидання трафіку не виходить – для цього потрібні «розумніші» методи фільтрації. Таким чином, три основні «чисті» вектори атак – це UDP-, IP- та SYN-флуд, на які припало 78% усіх DDoS-атак другого кварталу.

Тривалість. Медіанний час атаки склав 270 секунд, що близько до спостережень за 2020 рік, коли цей показник дорівнював 300 секунд. Порівняно з першим кварталом 2021 року, медіанний час атаки зріс значно – зі 180 секунд. Середній час атаки виріс ще суттєвіше - з ~700 секунд у першому кварталі до майже 2000 секунд у другому, збільшившись майже триразово. Велика тривалість була майже універсальним правилом атак другого кварталу 2021 року. Порівняно з першим кварталом, у другому навіть найкоротші атаки подвоїлися у тривалості.

Потужність. Середня пропускна спроможність всіх DDoS-атак другого кварталу становила 6,5 Гбіт/с. У першому кварталі ця цифра була трохи вищою – 9,15 Гбіт/с, тоді як у четвертому кварталі 2020 року цей показник становив лише 4,47 Гбіт/с. Розмір найбільшого ботнета, що спостерігається фахівцями, зріс практично вдвічі: з 73 892 машин у першому кварталі 2021 року до 137 696 - у другому. Більшість заблокованих IP-адрес, з яких складався даний ботнет, були з В'єтнаму, Індії, Індонезії та Таїланду.

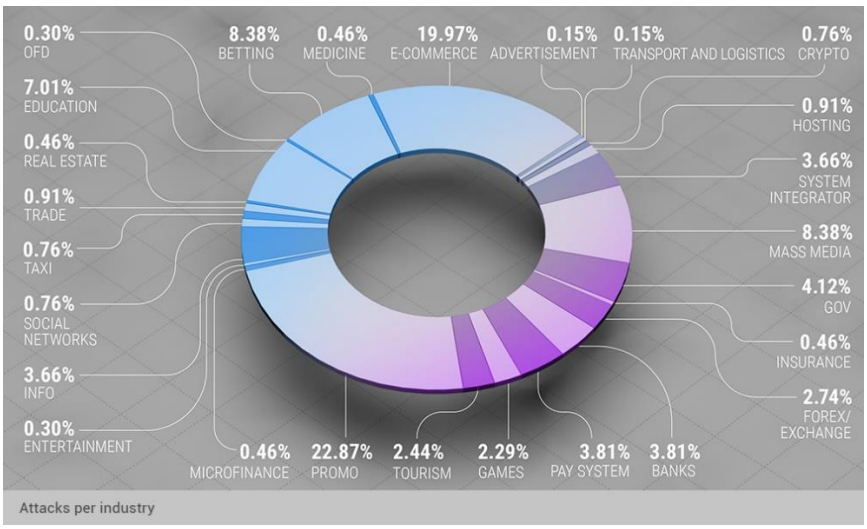

Рис.3.3. Розподіл атак по індустріям

Інциденти BGP. Кількість унікальних автономних систем, які брали участь у перехопленнях або витоках маршрутів BGP, трохи знизилася у другому кварталі 2021 року порівняно з першим, хоча кількість учасників у місяцях, що окремо спостерігаються, майже не змінилася. Крім цього, у травні та червні кількість перехоплюючих автономних систем значно зросла порівняно з попередніми місяцями. Так, травень став першим місяців, коли кількість унікальних автономних систем, що створювали перехоплення, перевищила 10 тисяч.

Кількість окремих інцидентів, пов'язаних із перехопленням або витіканням маршрутів, також зросла, порівняно з першим кварталом. Майже 10 мільйонів витоків маршрутів у другому кварталі – значна цифра, яка хіба що збільшуватиметься без значних заходів щодо їх запобігання. Кількість перехоплень була порівнянна з першим кварталом 2021 року [26].

3.2. Огляд сучасних технологічних рішень та механізмів світових вендорів для виявлення та протидії розподіленим атакам спрямованим на відмову в обслуговувані

Атаки розподіленої відмови в обслуговуванні (DDoS) можуть пошкодити організацію, мережу або навіть цілу країну. DDoS-атаки становлять значний відсоток загроз безпеці, а останні атаки були більш масштабними та складнішими,

ніж будь-коли. Хоча є деякі речі, які групи безпеки можуть зробити, щоб зменшити вплив DDoS-атак, зростаюча складність таких атак спричинила сильне зростання ринку рішень DDoS.

Перелічені тут постачальники отримали хороші результати у звіті Forrester DDoS Wave або у звіті Quadrant Knowledge Solutions DDoS – або в обох. Окрім обробки традиційних DDoS-атак, вони включають хмарні, мобільні та IoT-функції. Кожен підсумок постачальника посилається на детальний аналіз, включаючи цільові ринки та варіанти використання, функції, показники, розвідку, використання агентів, сертифікати безпеки, доставку продуктів (хмарне, програмне або апаратне забезпечення) та ціни.

Основні функції рішення DDoS включають виявлення ранніх стадій атаки, масштаб поглинання обсягу трафіку та можливість пом’якшити джерело атаки. Це можна зробити за допомогою статичних або користувацьких правил або за допомогою набору захисних дій, що розвиваються, коли атака переходить на додаткові цілі.

До найкращих постачальників послуг захисту від DDoS відносять: Akamai, Verisign, Radware DefensePro, Cloudflare DDoS, Arbor Networks APS, Nexusguard, DOSarrest, F5 Захист від DDoS, Neustar SiteProtect NG, FortiDDoS, Qrator Labs та ін.

1. Пом’якшення DDoS-атак від Akamai. Рішення Akamai для пом’якшення DDoS може включати очищення на основі CDN, розподілену відмову в обслуговуванні (DDoS) та/або компоненти DNS, залежно від вимог кожного клієнта. Компонент CDN працює як зворотний проксі-сервер HTTP/S, який автоматично відкидає весь трафік не на порт 80/443, включаючи будь-які DDoS-атаки рівня 3 і 4. Компонент очищення DDoS покладається на центр операцій безпеки Akamai (SOC) для застосування ряду цільових заходів пом’якшення на основі вектора атаки (наприклад, за допомогою IP або підпису атаки), включаючи пом’якшення для SYN-флудів, UDP-флудів та інших типів рівня. 3 і 4 DDoS атаки. Компонент DNS автоматично припиняє трафік, що не є DNS, включаючи DDoS-атаки рівня 3 і 4. Akamai пом’якшує DDoS-атаки на основі DNS (наприклад, посилення DNS), а також захищає служби DNS від DDoS-атак.

Рішення включає:

- Автоматичне керування тарифами, яке блокує трафік на основі порогових значень, налаштованих клієнтом або Akamai;
- Спеціальні правила брандмауера веб-програм (WAF), створені навколо певних сигнатур атак;
- Інструменти моніторингу, які надають сповіщення та дозволяють SOC переглядати та оцінювати шкідливий трафік на основі зразків пакетів у реальному часі;
- Інструменти для створення та зберігання профілів трафіку клієнтів, що дає змогу SOC отримати доступ до даних швидкого порівняння;
- Моніторинг заголовків HTTP в режимі реального часу на наявність аномалій у порівнянні з базовими показниками;
- Інструменти, що дозволяють SOC переглядати дампи/p-caps TCP майже в режимі реального часу, генерувати правила пом’якшення з точністю та оцінювати пом’якшення;
- Процеси роботи з клієнтами та уникнення надмірного пом’якшення, включаючи формалізовані Runbook для кожного клієнта, узгоджені методи для розуміння середовища клієнтів і спілкування в реальному часі під час будь-якої події DDoS;

Основними клієнтами Akamai є фінансові послуги, комерція, мовлення, видавництво, державний сектор, високі технології, SaaS, виробництво, охорона здоров’я, енергетика та ігри.

Akamai має сім центрів очищення по всьому світу, 3,5 Тбіт/с виділеної мережі (8 Тбіт/с до першого кварталу 2018 року). Також має 150 співробітників SOC, які фізично не розташовані в центрах очищення, а в п'яти окремих місцях SOC, а також 700 експертів з безпеки, які зосереджені на розвідці загроз і вдосконаленні автоматизованого захисту від загроз, що використовується політиками і правилами захисту.

Кваліфікація безпеки. ISO 27001, PCI DSS, GDPR, FedRAMP, HIPAA, FISMA, SOC 2

2. **Служби захисту від DDoS Verisign.** Коли монітори Verisign виявляють DDoS-атаку, персонал служби підтримки негайно сповіщає про це клієнтів і рекомендує стратегію пом'якшення. Окрім моніторингу, компанія пропонує пом'якшення наслідків на вимогу. Він також має OpenHybrid API, який дозволяє організаціям використовувати наявні системи безпеки для надсилання інформації про загрози до хмарної служби Verisign для можливого пом'якшення.

Verisign розпочав свою діяльність у 1995 році як центр сертифікації, але в 2010 році продав свій сертифікаційний бізнес Symantec. У 2000 році він придбав Network Solutions і почав працювати з реєстром доменів. Сьогодні компанія продовжує надавати послуги домену, але розширив свій бізнес, пропонуючи такі послуги безпеки, як брандмауер DNS, керований DNS, рекурсивний DNS і захист від розподіленої відмови в обслуговуванні (DDoS).

Verisign пропонує можливості моніторингу та пом'якшення наслідків на вимогу. Коли монітори компанії виявляють DDoS-атаку, персонал служби підтримки повідомляє клієнта про атаку та рекомендує стратегію пом'якшення. Якщо використовується стороння служба моніторингу або компанія контролює свою власну мережу, клієнт може повідомити Verisign, коли почати пом'якшення. Verisign також пропонує OpenHybrid API, який дозволяє організаціям використовувати наявні пристрої безпеки для надсилання інформації про загрози до хмарного рішення Verisign. Verisign має пропускну здатність мережі 1,7 Тбіт/с.

3. **Захист від Radware DefensePro.** Рішення для захисту від DDoS-атак Radware і пропозиції щодо безпеки веб-додатків забезпечують інтегровану безпеку програм і мереж. Рішення для пом'якшення атак – це гібридне рішення захисту від DDoS, яке об'єднує постійне виявлення та пом'якшення з хмарними об'ємними DDoS-атаками, очищенням, а також безпекою 24×7 кібератак і DDoS.

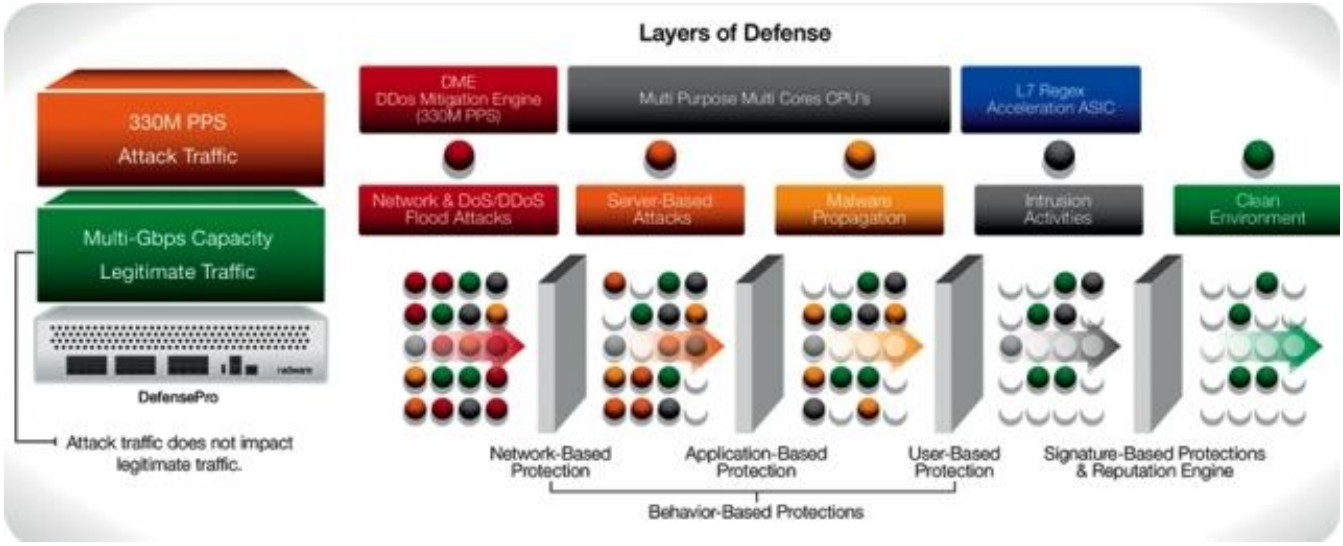

Рис.3.3. Рівні захисту Radware DefensePro

Radware DefensePro – система захисту та запобігання DDoS-атак, у тому числі, відображення IoT-ботнен атак у реальному часі, що забезпечує безпеку мережі та додатків від усіх відомих загроз та вразливостей «нульового дня» без порушення роботи легітимних користувачів. DefensePro дозволяє виключити простої та деградацію мережевої інфраструктури, запобігти розповсюдженню шкідливих програм, крадіжці інформації, захистити від атак на вразливості програм.

DefensePro є частиною системи відображення атак Radware AMS і забезпечує автоматичний захист від швидко поширюваних, великомасштабних, зашифрованих або дуже короткострокових загроз, включаючи IoT-ботнети, DNS, TLS/SSL-атаки, атаки типу "постійна відмова в обслуговуванні" (PDoS) та атаки з метою викупу (RDoS).

DefensePro включає повний набір механізмів захисту: система запобігання вторгненням (IPS), поведінковий аналіз мережі (NBA), захист від DDoS/DoS-атак, репутаційний механізм та захист від SSL-шифрованих атак.

DefensePro забезпечує захист від DDoS-атак шляхом аналізу користувальницької поведінки та запитів, накопичення та аналізу статистики, виявлення DDoS-атак на основі відхилень та аномалій у порівнянні зі штатними умовами роботи мереж і сервісів, що захищаються, блокування нелегітимного

трафіку методом динамічної фільтрації мережевих пакетів генерацією сигнатур DDoS-атаки у реальному часі.

На відміну від інших систем, які при захисті від атаки відключають непричетних до атак користувачів та цілі сегменти мережі від доступу до додатків та послуг, DefensePro забезпечує функціонування послуг під атакою та не перериває роботу легітимних користувачів.

На основі запатентованої технології створення сигнатур у реальному часі DefensePro автоматично генерує сигнатури DDoS-атак для запобігання та відбиття невідомих атак та загроз нульового дня. У межах 18 секунд DefensePro може виявити атаку, зняти характеристики та створити оптимальну сигнатуру для блокування раніше невідомих атак з мінімальним показником хибнопозитивних результатів.

Інтелектуальне рішення для відображення SSL-атак. Запатентоване рішення для відображення SSL-атак, що забезпечує захист від усіх типів зашифрованих атак із мінімальними показниками затримки. Підтримує системи з асиметричною архітектурою, включаючи хмарні середовища, мережі сервіс-провайдерів, корпоративні мережі з підключенням до кількох каналів зв'язку (multi-home).

Серед особливостей DefensePro треба зазначити велику кількість алгоритмів, за допомогою яких з-поміж великого обсягу трафіка можна виявити саме атаку типу «відмова в обслуговуванні». Справа в тому, що не завжди звичайний ICMP/TCP SYN flood — це те, що використовують кіберзлочинці. Часто атака може бути розтягнута за часом на день чи більший період, так звана Burst-атака, і стандартні методи боротьби, типу відправка SYN challenge або в принципі детектування даної активності — не працюють. Саме DefensePro і є тим проактивним захистом, що дає змогу впродовж усього циклу атаки створити антидію в режимі реального часу. Цей механізм є ключовим у цьому продукті. Насправді, тут йдеться про сигнатури, але не в класичному розумінні, а в сенсі створення прототипу трафіку. Алгоритми, які дають змогу цього досягти, якраз і є основою роботи даного рішення [27].

4. Захист від Cloudflare DDoS. Хмарна система захисту від DDoS від Cloudflare може боротися з атаками рівня 7, а також атак рівня 3 і рівня 4. Замість використання спеціального обладнання для захисту від DDoS кожна машина у своїй глобальній мережі бере участь у пом'якшенні DDoS. Він має ємність понад 15 Тбіт/с.

Мережа Cloudflare обробляє понад 10 трильйонів запитів на місяць, що становить майже 10 відсотків усіх запитів в Інтернеті для понад 2,5 мільярдів людей у всьому світі. Його підхід полягає в захисті та прискоренні Інтернет-додатків онлайн без додавання обладнання, встановлення програмного забезпечення або зміни рядка коду. Штаб-квартира компанії Cloudflare знаходиться в Сан-Франциско, штат Каліфорнія, офіси в Остіні, штат Техас; Шампейн, Іллінойс; Вашингтон, округ Колумбія.; Лондон; і Сінгапур. Семирічна компанія є приватною.

У Cloudflare завжди ввімкнена хмарна розподілена система захисту від відмови в обслуговуванні (DDoS). Замість використання спеціального обладнання для захисту від DDoS кожна окрема машина у своїй глобальній мережі бере участь у пом'якшенні DDoS. Маючи ємність понад 15 Тбіт/с, він може розширюватися для обробки найбільших DDoS-атак.

Оскільки зловмисники усвідомили, що старі об'ємні атаки L3/L4 ефективно борються, вони перемістилися вгору й переслідують програми на рівні HTTP/HTTPS безпосередньо (L7), це призвело до необхідності створення нових систем фільтрації.

Компанія обслуговує більшість вертикалей. Найбільша атака, яку спостерігала Cloudflare, була 600 Гбіт/с, але вона може обробляти 15 Тбіт/с. Cloudflare пом'якшує DDoS-атаки кожні три хвилини. Він бачить DDoS-атаки L3/L4 кожні шість хвилин, а L7 DDoS-атаки кожні вісім хвилин. (Атака кожні шість хвилин – це понад 80 000 атак на рік; кожні вісім хвилин – понад 60 000 на рік.)

Рішення Cloudflare DDoS побудовано на основі системи під назвою Gatebot, яка автоматично розпізнає та пом'якшує DDoS-атаки (як L3/L4, так і L7). Його

платформа машинного навчання вивчає поведінку IP-адрес і ботів і автоматично фільтрує поганий трафік.

Ціноутворення. Безкоштовний рівень $0/місяць; Pro $20/місяць; Бізнес $200/місяць. Ціни підприємства за запитом.

5. Arbor Networks APS. Arbor Networks використовує гібридні багаторівневі засоби захисту для захисту від усіх типів загроз DDoS. Внутрішній захист забезпечується за допомогою APS Arbor, який усуває атаки рівня додатків і TCP, що вичерпують стан. Він включає технологію виявлення та пом'якшення для швидкого автоматичного блокування атак.

Arbor Networks була заснована в Берлінгтоні, штат Массачусетс, у 2000 році. Tektronix Communications придбала компанію в 2010 році, а в 2013 році придбала австралійську компанію Packetloop. У 2015 році NETSCOUT придбала Arbor, і тепер вона вважається підрозділом безпеки NETSCOUT. Його продукти зосереджені на запобіганні розподіленої відмови в обслуговуванні (DDoS), глобальній розвідці загроз і видимості мережі.

Продукт Arbor APS постачається як пристрій, що забезпечує пом'якшення впливу до 40 Гбіт/с, або як віртуальна пропозиція, що підтримує хмарні середовища, такі як Amazon Web Services. Arbor використовує гібридні багаторівневі засоби захисту для захисту від усіх типів загроз DDoS. Це включає в себе хмарний захист для захисту від великих атак великого обсягу. Локальний захист також захищає від складних атак на рівні додатків і TCP, пов'язаних із вичерпанням стану. Гібридне рішення Arbor APS і Arbor DDoS Protection Service включає в себе технологію виявлення та пом'якшення, забезпечуючи перегляд мережевої діяльності та швидке автоматичне блокування атак, перш ніж вони вплинуть на критичні програми та служби.

Ринки та варіанти використання. Підприємства, уряд, фінансові послуги та малий та середній бізнес.

Arbor APS має здатність пом'якшення атак пристроїв до 40 Гбіт/с. Arbor Cloud має пропускну здатність мережі 7,6 Тбіт/с, розподілену по дев'яти центрам очищення по всьому світу. Усі продукти та послуги Arbor постійно озброєні Arbor

ATLAS Intelligence Feed, який може похвалитися видимістю 140 Тбіт/с світового інтернет-трафіку.

Кваліфікація безпеки

- Підтримка FIPS 140-2 рівня 2 і 3;
- Окреме адміністрування «Надійний шлях» для FIPS 140-2, рівень 3;
- Надійний корпус із захистом від несанкціонованого доступу;
- Ключі очищаються, якщо корпус порушено;

NETSCOUT Arbor має здатність обробляти об'ємні, TCP і DDoS-атаки прикладного рівня. На додаток до стандартних методів запобігання атак DDoS, NETSCOUT Arbor використовує свій канал глобальної розвідки загроз ATLAS та дані про репутацію від Arbor Security Engineering and Response Team (ASERT). Він також розширює, автоматизує та інтегрує захист у хмару за допомогою технології Cloud Signaling для підключення локального захисту з хмарними службами DDoS. APS можна налаштувати так, щоб сповіщати постачальників вищестоящих послуг, таких як провайдер або Arbor Cloud, коли більші атаки загрожують доступності, забезпечуючи швидке пом'якшення DDoS-атак до того, як вони переповнюють місцеві ресурси.

Ціноутворення. Arbor Networks не розголошує інформацію про ціни та пропонує кілька варіантів закупівлі CapEx та OpEx.

6. Nexusguard. Рішення Nexusguard пом'якшує всі типи DDoS-атак і кіберзагроз, забезпечуючи максимальний час безвідмовної роботи організаціям, які працюють в Інтернеті. Це охоплює захист від атак рівня 3-7, включаючи атаки DDoS, TCP SYN+ACK, TCP FIN, TCP RESET, TCP ACK, TCP PSH+ACK, TCP фрагмент, UDP, Slowloris, спуфінг, ICMP, IGMP, HTTP flood, грубий сила, з'єднання flood, ping of death, Smurf, відображені ICMP та UDP, SSL flood, атаки нульового дня тощо.

Ринки та варіанти використання. Фінансові послуги, електронна комерція, уряд, розваги, а також анти-DDoS рішення під ключ для постачальників послуг.

Компанія керує глобальною розподіленою мережею очищення. Прискорення та кешування визначає вміст, до якого часто звертаються, і порівнює його з кешом.

Якщо є збіг, вміст обслуговується з кешу, що зменшує використання пропускної здатності та прискорює доставку кінцевому користувачеві.

7. DOSarrest DDoS захист. DOSarrest – це зупинка DDoS-атак. Він зосереджений на HTTP/HTTP і захисті веб-сайтів, API та серверів мобільних додатків на портах TCP 80 і 443. Він пропонує повністю кероване хмарне рішення безпеки, яке складається із захисту від DDoS, брандмауера веб-додатків, CDN для підвищення продуктивності. , моніторинг та підтримка сайту. Усі вони інтегровані за допомогою його механізму аналізу великих даних. Він також відстежує веб-сайти за межами власної мережі з 10 різних місць по всьому світу. Крім того, він пропонує хмарне глобальне та локальне балансування навантаження.

У той час як багато компаній нещодавно відзначили зростання масштабів атак, DOSarrest помітив збільшення менших вторгнень на прикладний рівень.

Компанія виступає за кілька підходів або рівнів для ефективного захисту від DDoS. Захист від об'ємних атак сильно відрізняється від захисту від атак на прикладному рівні. Кожен підхід має свої вимоги. За словами Power, найкращий захист включає один рівень пом'якшення для об'ємних атак, який складається з пристроїв із великою пропускною здатністю та високою пропускною здатністю. Щоб захиститися від атаки на прикладному рівні, організаціям потрібні більш інтелектуальні системи, здатні глибоко перевіряти пакети та відстежувати сеанси.

Ринки та варіанти використання. Компанія захищає клієнтів у державній, електронній комерції, освіті, охороні здоров'я, фінансах, іграх та медіа.

Потужна пропускна здатність є оманливим показником. Він представляє лише один аспект одного стилю атаки. Крім того, додав він, цифри розраховуються як найкращі сценарії, коли атака ідеально розподіляється між найнадійнішими частинами оборони. Він вважає за краще відстежувати кількість атак, які зараз пом'якшуються, і каже, що його компанія може боротися з великою кількістю атак одночасно. Використовує машинне навчання як частину виявлення атак і аномалій.

Ціноутворення. DOSarrest пропонує два повністю керовані плани, починаючи з 700 доларів США на місяць.

8. F5 Захист від DDoS. F5 використовує чотирирівневий підхід до захисту від трафіку DDoS: хмара, мережа, програма та DNS. Він може досліджувати рівні мережі 3-7. Гібридний захист від DDoS-атак F5 забезпечує багаторівневий захист, який захищає від змішаних мережевих атак і атак складних додатків, одночасно забезпечуючи повне розшифрування SSL, можливості антиботів і розширені методи виявлення в одному пристрої. F5 Networks має пропускну здатність мережі 1 Тбіт/с, пропускну здатність 2 Тбіт/с і час відгуку менше секунди.

Ринки та варіанти використання. Підприємства, фінансові послуги та малого та середнього бізнесу.

Кваліфікація безпеки. Продукти F5 Networks Big-IP відповідають вимогам сертифікації загальних критеріїв, сертифікації відповідності IPv6, JITC PKE, NIST 800-53, UC APL і FIPS 140-2.

Негайний захист на швидкості лінії від відомих зловмисників і обмін інформацією між локальними розгортаннями та хмарою. Хмара, прилад і гібрид. Його пристрій інтегрується зі службою хмарного очищення Silverline.

Ціноутворення. F5 Networks не розкриває ціни.

9. Neustar SiteProtect NG. Neustar SiteProtect NG пропонує як локальні, так і хмарні варіанти. Завдяки ємності 4 Тбіт/с (збільшується до 10 Тбіт/с протягом наступних кількох місяців), його хмарна служба захисту від DDoS-атак очищає зловмисний трафік, щоб розслабити великі та складні атаки. Він може застосовувати контрзаходи, щоб обмежити доступ, захистити час роботи сайту та зберегти репутацію бренду. Neustar забезпечує автоматичне пом’якшення наслідків для кількох векторів атак. Нещодавно компанія запустила інтегроване рішення брандмауера веб-додатків (WAF), яке працює в парі з хмарним пом’якшенням DDoS-атак.

Ринки та варіанти використання. Фінансові послуги, технології, велика електронна комерція, роздрібна торгівля, комунальні послуги, ігри

Наразі Neustar здатний поглинати та захищати атаки зі швидкістю понад 4 Тбіт/с. До кінця року ця цифра зросте до 8 Тбіт/с, а до 1 кварталу 2019 року – до 10

Тбіт/с. Середній час пом’якшення становить менше 90 секунд. Операційний центр безпеки Neustar (SOC) використовує комбінацію аналітики загроз на основі його DNS-відбитку (10 відсотків авторитетного DNS проходить через Neustar), а також зовнішніх каналів загроз. Він також відстежує хакерські форуми/IRC, соціальні мережі та інші джерела розвідки, щоб підтримувати обізнаність про загрози, що розвиваються. Його SOC використовує захоплення пакетів у реальному часі та глибоку перевірку пакетів, щоб виявити аномальні тенденції та створювати дуже детальні пом’якшення, щоб позбутися лише небажаного трафіку.

Хмарна підтримка з локальними апаратними параметрами, які також можуть забезпечити гібридний захист від DDoS та брандмауер веб-додатків у його конфігураціях, що завжди ввімкнені (завжди маршрутизуються чи завжди проксі-сервер).

Ціноутворення. Neustar пропонує ціни на основі рівня ризику, а не традиційної атаки з оплатою за кожну атаку [28].

10. FortiDDoS. Серед кібератак, які постійно розвиваються, DDoS-атаки є одними з найпомітніших. FortiDDoS Protection Solution захищає корпоративні центри обробки даних від атак DDoS, використовуючи широку колекцію відомих методологій DDoS, створюючи багаторівневий підхід до пом’якшення атак. Він також аналізує поведінку даних для виявлення нових атак, що дозволяє зупинити загрози нульового дня. FortiDDoS включає:

- Багаторівневе рішення захисту від DDoS
- Виявлення машинного навчання. Захист від DDoS від Fortinet використовує архітектуру машинного навчання для вивчення поведінки пакетів даних. FortiDDoS блокує аномальні дії, захищаючи ваш сайт або додаток
- Безперервне навчання. FortiDDoS вивчає моделі трафіку, щоб розрізняти законний обсяг трафіку та атаки. З часом FortiDDoS може створювати профілі автоматично, заощаджуючи ваш час.
- Розширений захист DNS. FortiDDoS виконує повну перевірку вашого DNS-трафіку зі швидкістю до 12 мільйонів запитів в секунду (QPS), захищаючи вас від широкого спектру атак на основі програм DNS, об’ємних і аномальних атак.

- Автономне пом'якшення. FortiDDoS надає вам автономне пом’якшення, що означає, що член вашої IT-команди не повинен втручатися під час атаки. Усі необхідні пом’якшення відбуваються автоматично, незалежно від характеру чи розміру атаки.
- Центральний менеджер (CM). Організації з кількома пристроями FortiDDoS, розгорнутими в розподілених середовищах, можуть скористатися перевагами FortiDDoS-CM на вибраних моделях, дозволяючи адміністраторам отримати доступ до всіх своїх пристроїв на одному екрані керування.
- Потужна архітектура паралельної перевірки. FortiDDoS виконує 100% перевірку пакетів одночасно на трьох рівнях: 3, 4 і 7, незалежно від розміру, забезпечуючи вашу організацію комплексною системою запобігання загрозам.
- Постійна оцінка атак. Постійна оцінка поверхні атаки дозволяє FortiDDoS виявляти зміни загроз у мережевому трафікі, щоб пом’якшити загрози, захистивши ваш сайт або програму.
- Розширений захист NTP. FortiDDoS виконує 100% перевірку кожного запиту та відповіді протоколу Network Time Protocol (NTP) зі швидкістю до 6 мільйонів QPS.
- Гібридна локальна / хмарна підтримка. FortiDDoS інтегрується зі сторонніми службами пом’якшення DDoS, щоб захистити вашу організацію від широкомасштабних атак DDoS, не обмежуючи можливості розгортання.

3.3. Використання технології вендора QLabs для тестування протидії DDoS

DDoS-атака – це розподілена атака типу «відмова в обслуговуванні», метою якої є виведення сайту з ладу шляхом спрямування постійного потоку запитів із десятків і сотень тисяч заражених комп'ютерів, розкиданих по всьому світу. Якою б потужною не була інформаційна інфраструктура, яка обслуговує програми, вона не витримає навантаження, що перевищує норму на кілька порядків, і вийде з ладу. Це, як правило, призводить до дуже сумних наслідків: втрати грошей, втрати

репутації надійного партнера або провайдера послуг, переходу клієнтів до «надійніших» конкурентів, а то й зовсім до втрати всього бізнесу. Сьогодні вартість замовлення DDoS-атаки починається з 50$ за добу, що робить цей інструмент дуже популярним серед зловмисників.

Класифікація DDoS-атак. Мережеві атаки можна класифікувати залежно від того, які елементи інфраструктури вони спрямовані. Розглядаються такі рівні:

- Канальна ємність;
- Мережева інфраструктура;
- Стек протоколів;
- Додатки.

Найскладніші для нейтралізації – інтелектуальні DDoS-атаки на рівні додатків, їм приділяють особливу увагу та вважають їхню нейтралізацію однією із ключових компетенцій. Помилково вважати, що проблема розподілених мережних атак стосується лише «гігантів» мережі Інтернет та великих компаній. Цілі зловмисників непередбачувані, і їхні інтереси можуть зачіпати не тільки комерційні сфери: часто атаки організуються на благодійні, політичні організації, ЗМІ та ін.

Самостійний захист від DDoS-атак. Власник сайту може спробувати організувати захист мережі від DDoS-атак самостійно, встановивши засоби протидії на своєму сервері, але в більшості випадків це не дасть позитивного результату.

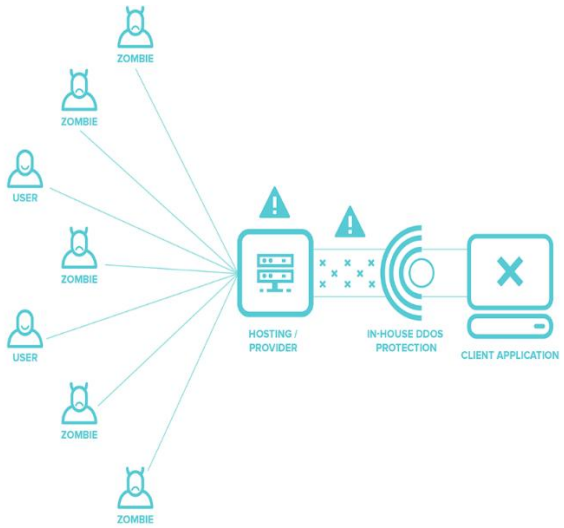

Рис.3.4. Приклад організації самостійного захисту

Безуспішність спроб захистити свою інфраструктуру від мережевої атаки в цьому випадку пов'язана з тим, що трафік може просто не дійти до обладнання фільтрації – є ймовірність, що DDoS-атака «паралізує» канали зв'язку жертви або її провайдера задовго до досягнення засобів захисту.

Захист від DDoS-атак на хостингу. У разі наявності у хостинг-провайдера спеціалізованих систем нейтралізації DDoS-атак захист мережі може бути ефективним. Однак із серйозною атакою провайдер не завжди може впоратися самостійно: мережі хостинг-провайдерів не проектуються під екстремальні додаткові навантаження і не можуть протистояти масованим атакам на відмову в обслуговуванні.

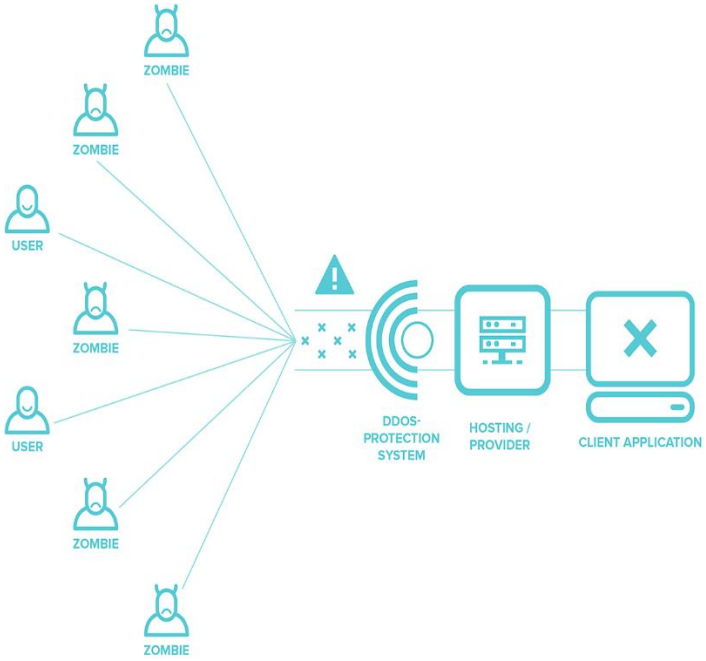

Рис.3.5. Захист від DDoS-атак на хостингу

Власник сайту в такому випадку може отримати таке повідомлення: «Зафіксовано DDoS-атаку, спрямовану на домен XXX.ua, розміщений на Вашому обліковому записі. Роботу домену було припинено, оскільки атака створювала аварійну ситуацію на сервері, де розміщується сайт із зазначеним доменом, і стабілізувати роботу сервера без припинення роботи домену було неможливо».

Захист мережі Qrator Labs. Мережа Qrator спроектована і побудована для роботи під постійним впливом великої кількості DDoS-атак. Вузли фільтрації

Qrator Labs підключені до каналів найбільших магістральних інтернет-провайдерів США, Західної та Східної Європи, Південно-Східної Азії. Таким чином, на відміну від мереж операторів хостингу (особливо, віртуального) мережа Qrator Labs спроектована для екстремальних навантажень, і атака на ресурс одного з наших клієнтів ніяк не впливає на працездатність сайтів інших клієнтів.

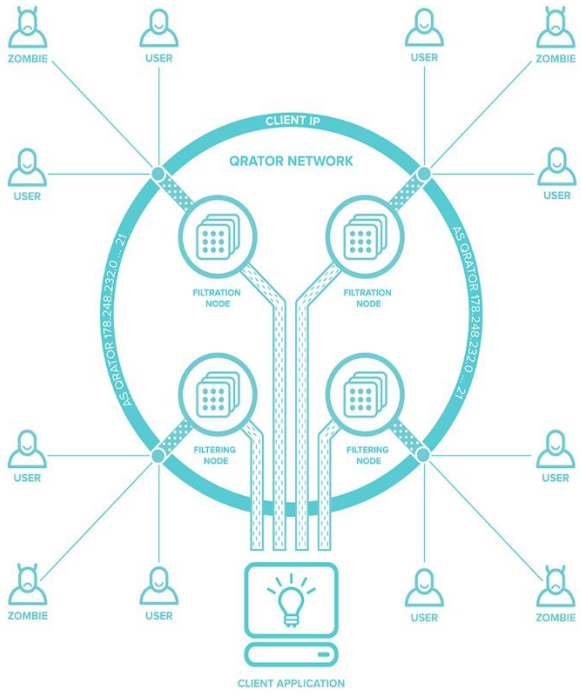

Рис.3.6. Приклад організації захисту Qrator Labs

Технічний алгоритм підключення клієнтів. Клієнти вносять зміни в записи DNS, що направляють трафік користувача на вузли фільтрації Qrator. Ці вузли використовують технологію BGP anycast для анонсування своїх адрес. У разі необхідності захисту підмереж клієнта до BGP anycast можуть бути додані і відповідні клієнтські префікси. Після підключення трафік клієнтів постійно, незалежно від наявності DDoS-атаки, надходить до мережі Qrator та аналізується. «Чистий» трафік перенаправляється на сайт, що захищається. Така схема роботи дозволяє вузлам фільтрації «розуміти», який профіль трафіку є нормою для кожного сайту окремо, та у разі будь-яких відхилень блискавично реагувати на це.

Всі вузли мережі Qrator працюють незалежно, і в разі виходу з ладу одного з них трафік сайту, що захищається, не загубиться, а автоматично буде перемаршрутизовано на інший найближчий вузол фільтрації.

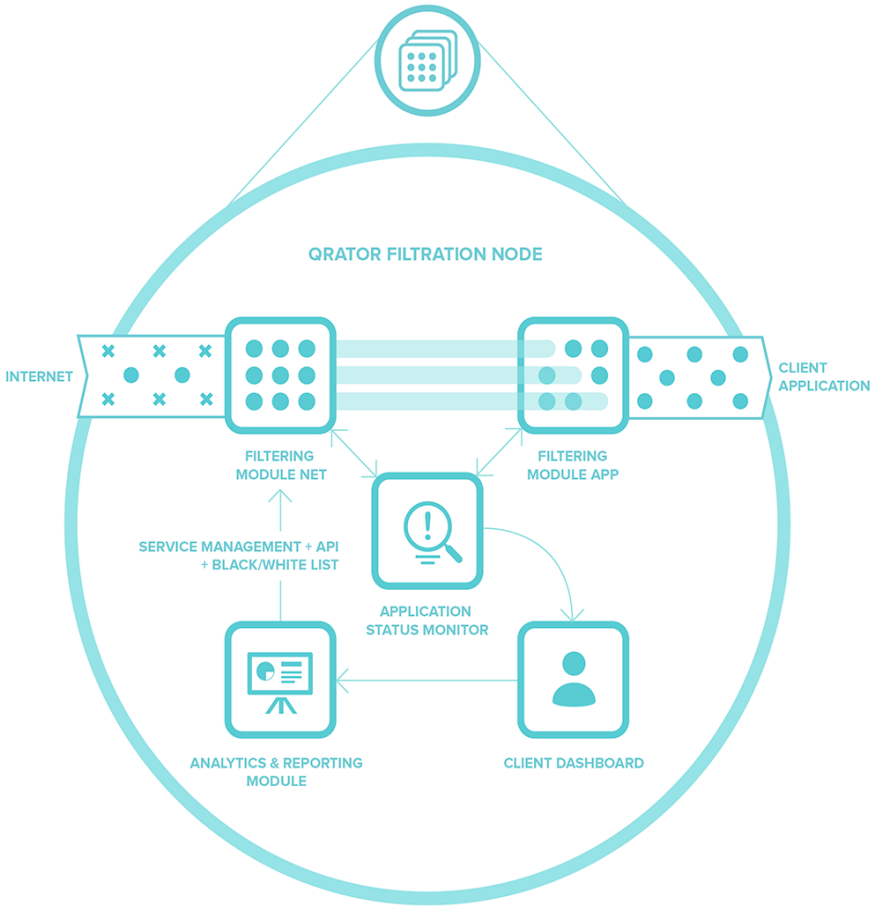

Рис.3.7. Схема роботи вузла Qrator Labs

Характеристики мережі Qrator Labs. Мережа Qrator має такі основні характеристики:

- близько 3000 Гбіт/с смуги пропускання, призначеної для фільтрації DDoS-атак;
- <5% хибних спрацьовувань у процесі нейтралізації DDoS-атаки;
- час навчання мережі з моменту підключення нового клієнта – менше 2 годин;
- час реакції мережі Qrator на DDoS-атак – від 30 секунд до 3 хвилин;
- доданий час затримки під час проксування трафіку – від 0 до 100 мс. У разі проксування HTTP-трафіку через використання persistent HTTP-з'єднань з сервісом, що захищається, можливе зниження мережевих затримок для сервісу, що захищається;
- кількість ЦОД, що захищаються, і сервісів – не обмежена.

Реєстрація акаунту та модерація в Qrator Labs. Клієнт реєструється в Особистому Кабінеті, отримує електронною поштою посилання на встановлення нового пароля.

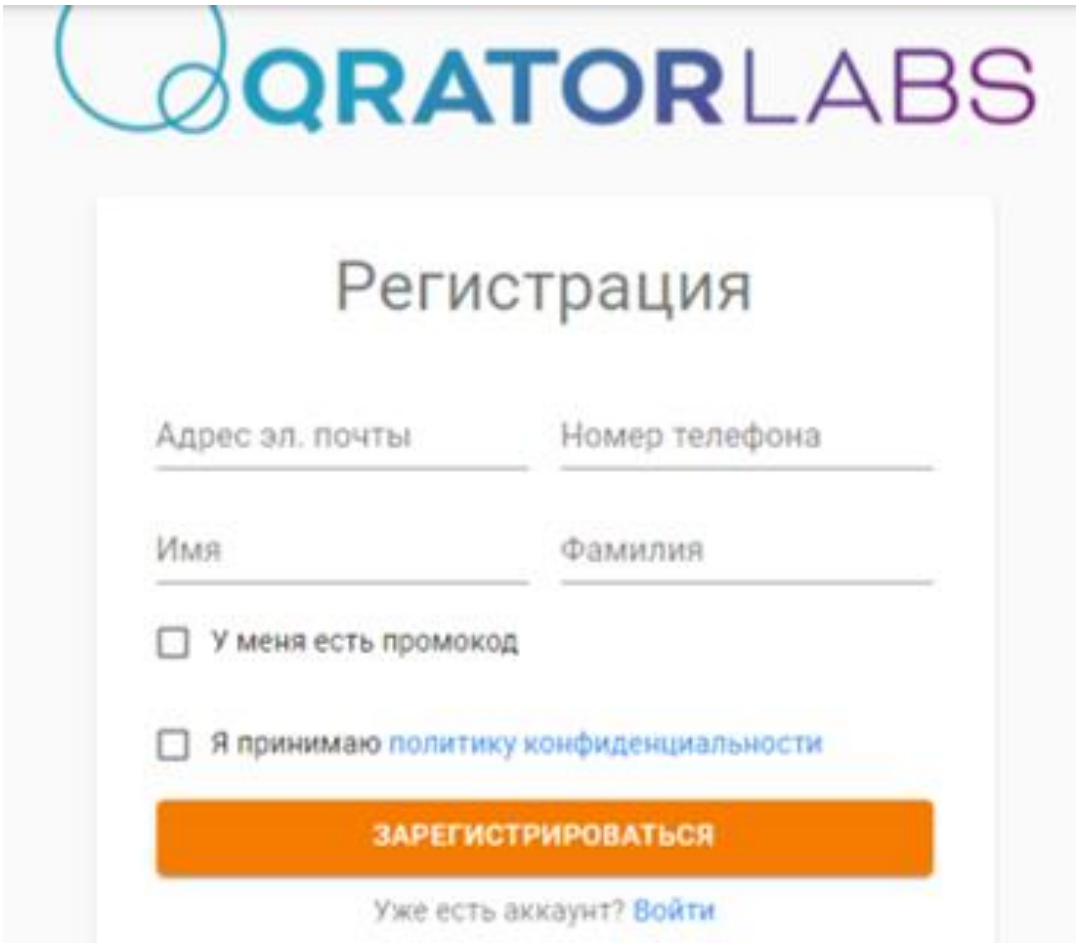

Рис.3.8. Рєстрація в Qrator Labs

Всі нові облікові записи та домени, створені в системі, проходять модерацію. Перевіряється інформація, надана в процесі реєстрації про компанію та ресурс, який використовуватиме послугу. Потрібно заповнити повне найменування організації, юридичну та фактичну адресу (докладна інформація про компанію може бути вказана пізніше), а також створити домен у системі та вказати найменування вебсайту, який буде використовувати послугу.

Рис.3.9. Активація облікового запису в Qrator Labs

Новий домен отримує налаштовані користувачем конфігурацію апстрімів, конфігурацію SSL (якщо були встановлені сертифікати), ідентифікаційний номер виду dXXXX і очікує на включення в статусі «На модерації».

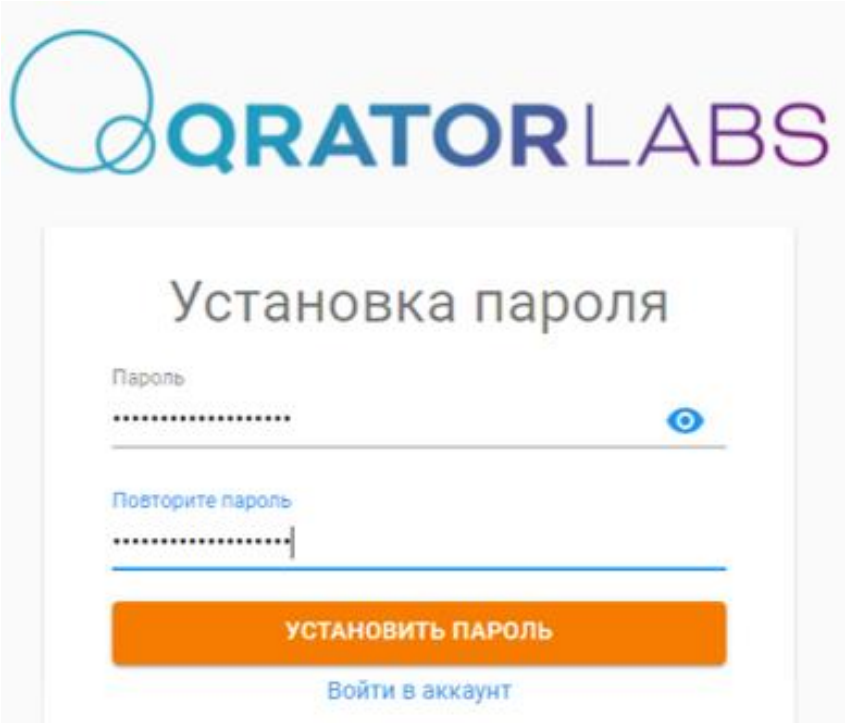

Рис.3.10. Налаштування пароля для доступу в Qrator Labs

Рішення про включення домену приймається відповідно до внутрішньої політики компанії, адже вона працює тільки з юридичними особами за договором та не надає послуги з фільтрації трафіку для неофіційних ігрових серверів, сайтів, які містять інформацію, заборонену до поширення на території країни.

Включення домену супроводжується призначенням йому Qrator IP, який повинен бути використаний для захисту трафіку користувача вебсайту.

Інструкції з підключення захисту надсилаються на поштову адресу контакту, яка була вказана при реєстрації та всім контактам з технічною роллю, якщо такі є в обліковому записі клієнта.

*Додаткові можливості особистого кабінету та рекомендації щодо роботи з сервісом. П*ісля основних етапів налаштування захисту рекомендується також:

- ознайомитись з розділом Real-IP, щоб налаштувати передачу заголовка X-Forwarded-For на сервері.
- налаштувати двофакторну аутентифікацію та персоналізувати контакти особистого кабінету Qrator.

Превентивний тест конфігурації послуги у Qrator. Перед тим, як перевести трафік на мережу фільтрації Qrator, рекомендується зробити кілька тестових запитів до обраного сервісу через налаштований домен у Qrator, щоб переконатися в його готовності обробляти виробничий трафік сервісу користувача відповідно до очікувань. Зробити це можна з використанням утиліти командного рядка curl із зазначенням прапора --resolve або з використанням звичайного браузера, додавши файл /etc/hosts/ запис з Qrator IP навпроти доменне ім'я ресурсу.

Приклад:

 # Приклад використання утиліти curl для дозволу доменного імені в Qrator IP

curl -I --resolve example.com:80:qrator_ip http://example.com/

curl -I --resolve example.com:443:qrator_ip https://example.com/

або

 # Додайте запис з вашим Qrator IP і доменом у файл /etc/hosts

178.248.2XX.XX example.com

 # Використовуйте утиліту curl з опцією -I, щоб перевірити, який HTTP код стану буде повертатися користувачу при проходженні трафіку через мережу фільтрації Qrator

curl -I example.com

Якщо в результаті тестового запиту користувач отримує помилку 502, то для встановлення можливих причин виникнення помилки рекомендується ознайомитися з розділами інформаційних матеріалів коди стану HTTP та налаштування firewall

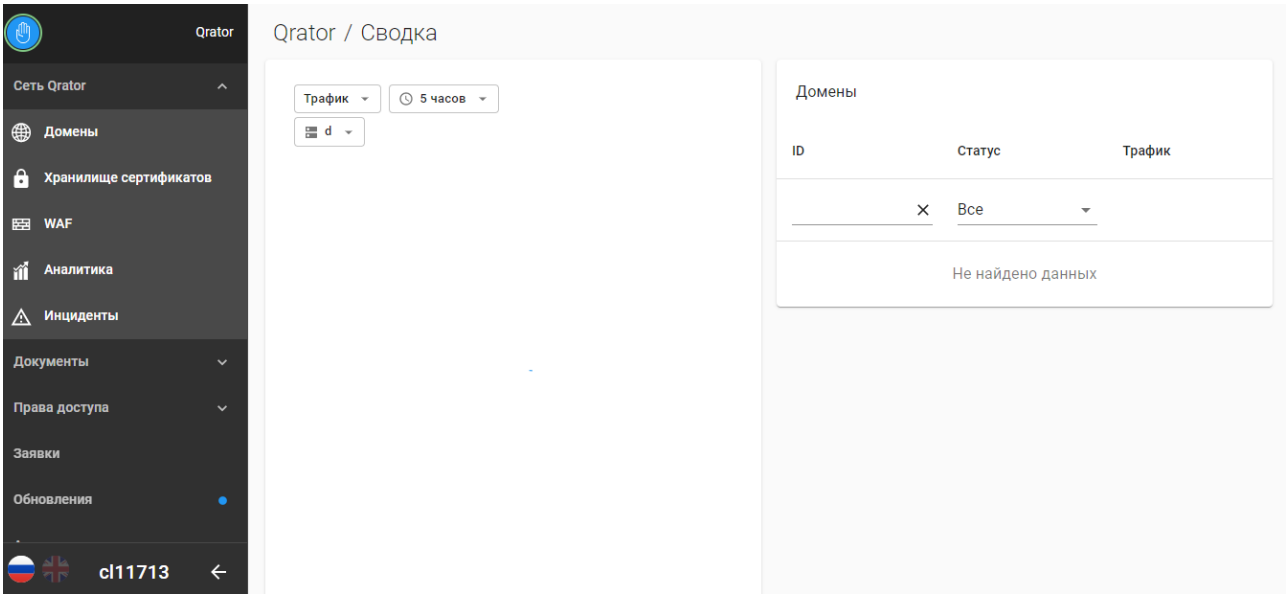

Рис.3.11. Підключення до Qrator

TTL A-запису DNS. Перед перекладом трафіку на сервіс Qrator необхідно перевірити поточне значення TTL A-запису користувацького домену та за необхідності змінити його на рекомендоване. Рекомендоване значення TTL для запису A 300 (або нижче). Щоб перенаправити трафік користувацького сервісу на мережу фільтрації Qrator, необхідно змінити поточну IP адресу в A-записі DNS користувацького ресурсу на Qrator IP, виділений домену в Qrator. У типовому випадку в DNS-зоні мають бути такі A-записи:

@IN A Qrator_IP

WWW IN A Qrator_IP

Після перебудови DNS запити на сайт повинні надходити лише від IP-адрес системи фільтрації трафіку QRATOR:

87.245.197.192

87.245.197.193

87.245.197.194

87.245.197.195

83.234.15.112

83.234.15.113

83.234.15.114

83.234.15.115

66.110.32.128

66.110.32.129

66.110.32.130

66.110.32.131

185.94.108.0/24

Лист з інструкціями з підключення надсилається також на пошту, вказану при реєстрації та іншим контактам з технічною роллю в особистому кабінеті Qrator, якщо такі є. Довідкова інформація про контакти в особистому кабінеті Qrator та доступні їм ролі викладена в інформаційному розділі контакти.

Підключення під атакою. При підключенні під атакою IP адреси ресурсу, що атакується, можуть бути відомі зловмисникам. Для виключення атаки безпосередньо на апстрім-сервери після підключення до Qrator, рекомендується запитувати нові IP адреси у хостингу, щоб використовувати їх як адреси, куди мережа Qrator буде направляти очищений трафік і обмежити доступ на серверах на рівні firewall по їх прямих IP з усіх адрес, крім списку довірених та IP адрес легітимних точок.

Фільтрування HTTPS. Після включення домену, клієнту надається послуга зі стандартною конфігурацією, де Qrator виступає як Reverse Proxy для ресурсу, що захищається, і здійснює фільтрацію вхідних HTTP запитів від користувачів по 80 порту Qrator IP. Для того, щоб Qrator IP почав приймати SSL з'єднання (за замовчуванням по 443 порту) і система фільтрації Qrator могла обробляти HTTPS

трафік необхідно налаштувати фільтрацію HTTPS на клієнтському домені Qrator на основі однієї з наступних технологій:

- *Фільтрування HTTPS із розкриттям ключів.* Клієнт завантажує файли з ланцюжком сертифікатів та закритим ключем у особистому кабінеті Qrator у сховище сертифікатів. Після цього завантажений ланцюжок сертифікатів стане доступним для встановлення в розділі «SSL» користувацького домену. Для встановлення сертифіката потрібно знайти потрібний сертифікат у списку доступних і натиснути «Встановити», вказавши одне або кілька доменних імен, для яких мережа фільтрації Qrator буде використовувати вибраний сертифікат, або поставивши галочку «Використовувати цей сертифікат за промовчанням для будь-якого домену». Якщо це необхідно - таким чином можна налаштувати інші сертифікати та доменні імена, які повинні використовуватися мережею фільтрації на даному домені. Для застосування вказаних налаштувань – натиснувши кнопку «Зберегти» в нижній частині екрану. Після того, як користувач встановить сертифікат(и) і відбудеться застосування змін на мережі, система фільтрації Qrator почне приймати SSL з'єднання і надсилати запити користувацькому серверу 443 портом. Необхідно зазначити, що для роботи послуги на користувацькому сервері також потрібно встановити сертифікат(-и) та налаштувати HTTPS. У режимі захисту на основі HTTP-проксі відсутня підтримка протоколу Web Socket. Якщо клієнт використовує цю технологію, то рекомендується розглянути можливість використання режиму захисту на основі тунелювання трафіку ресурсу, що захищається, при якій SSL з'єднання з відвідувачем буде встановлюватися на стороні користувача, що дасть можливість використовувати Web Sockets разом із захистом.

- *Фільтр HTTPS без розкриття ключів (PCI-DSS ready).* Між користувацьким сервером та мережею Qrator налаштовується IPIP (або GRE)-тунель. Пакети від користувачів сайт буде передавати у тунелі без зміни вмісту і відповіді (зазвичай використовують policy-based routing). У цій схемі фільтри не бачать вмісту запитів, тому захист здійснюється лише до рівня транспорту. Для реалізації захисту на рівні програми існують такі варіанти:

- Пересилання логів звернень з сервера, що захищається в Qrator по syslog. Вимагає додаткових налаштувань на стороні сервера та Qrator. Рекомендується проводити в рамках основної заявки на підключення послуги «фільтрація HTTPS без розкриття». На основі отриманих логів збирається необхідні дані для організації повноцінної фільтрації трафіку користувача аж до рівня програми;

- *Блокування IP-адрес з використанням методів Qrator API.* Доступ до API надається за допомогою токенів API або для необхідних IP адрес на запит через систему заявок. У цьому випадку користувач звертається до API Qrator із запитом про його блокування. Час, на який буде заблоковано IP-адресу, також вказується клієнтом в запиті.

Апстріми. Апстріми - реальні IP-адреси, що виділяються інтернет-провайдером серверам, на яких працюють користувацькі домени. Мережа фільтрації Qrator використовує ці адреси для передачі трафіку легітимних користувачів захищеним ресурсам. Для кожного домену має бути заданий хоча б 1 апстрім. Рекомендується отримати в інтернет-провайдера нові IP-адреси для використання з послугою захисту Qrator. Це важливо, тому що зловмисникам можуть бути вже відомі користувацькі поточні IP-адреси, і вони можуть організувати DDoS-атаку безпосередньо на них, минаючи систему захисту.

Використання форми конфігурації апстрімів. Форма конфігурації апстрімів дозволяє додавати, видаляти, редагувати та переміщувати апстрими між основним та запасним списками. Кожен запис апстріму містить такі поля:

- Ім'я – це поле, яке користувач може задати для того, щоб запам'ятовувати та розрізняти апстрими у списку;

- IP-адреса користувацького сервера, на яку буде надіслано очищений трафік з мережі Qrator;

- Увімк. Необхідно поставити галочку, щоб почати використовувати той апстрім, або навпаки – вимкнути його (за замовчуванням вимкнено);

- Вага. У випадку, якщо опція «Вага апстрімів» увімкнена, це поле замінює собою поле. Значення може бути виставлене від 0 до 64. За замовчуванням воно дорівнює 1, при виставленні 0 трафік не надходитиме на вказаний апстрім;
- Алгоритм балансування. Цей блок дозволяє вибрати з двох наперед визначених методів для розподілу навантаження між декількома апстрімами;
- Round-robin. Кожен запит, що приходить, передається апстриму, що знаходиться у горі списку; після цього верхній апстрім переставляється в кінець списку, а його місце посідає за ним. Таким чином, апстрими циклічно змінюються для кожного наступного запиту, і кожен з них отримує однакову кількість запитів, що робить навантаження рівним для всіх апстрімів.
- IP Hash. Для кожного запиту обчислюється хеш від користувача IP-адреси. На основі значення цього хеша запит надсилається одному з апстрімів у списку. Таким чином, усі наступні запити від тих самих користувачів потраплять до одних і тих же апстрімів, які отримали вихідні запити від них.

Налаштування фаєрволу. Налаштування фаєрволу - обмеження доступу за прямою IP адресою програми, що захищається. При використанні захисту в proxy-based режимі (домени в Qrator, які не використовують технології для фільтрації HTTPS далі plain HTTP і технологія «фільтрація HTTPS з розкриттям ключів»), Qrator перенаправляє запити від користувачів на користувацький сервер, використовуючи наступні адреси як source ip:

66.110.32.128/30

83.234.15.112/30

87.245.197.192/30

185.94.108.0/24

Для запобігання атаці за прямою IP адресою користувацького сервера необхідно обмежити доступ на рівні міжмережевого екрана всіма адресами, крім перерахованих вище. Цей список може бути розширений адресами, які є для користувача довіреними (офіс, співробітники, автоматизований інструментарій), що виключить можливість їхнього блокування (неправдивих спрацьовувань) і зменшить кількість легітимного трафіку, що пропускається через мережу Qrator.

Універсальну інструкцію налаштування міжмережевого екрана зробити складно, т.к. найчастіше в iptables вже містяться правила, і навіть можуть бути різні особливості, як, наприклад, трансляція порту в контейнер.

Результат виконання цього скрипта сильно залежить від поточної конфігурації і застосування цих правил без змін може призвести до небажаних наслідків або не мати жодного ефекту.

Щоб попередити можливість здійснення DDoS атаки, націленої на пряму адресу користувацького сервера, необхідно в правилах iptables дозволити вхідні пакети на tcp порти 80 і 443 з адрес із зазначеного списку (а також можна розширити цей список довіреними адресами для цілей адміністрування або розробки) і далі заборонити (DROP) доступ до цих портів для решти.

Залежно від користувацької системи можна використовувати або тільки правила iptables для plain HTTP, або комбінувати їх з правилами iptables з підтримкою модулів conntrack і ipset. Рекомендується використовувати як conntrack, так і ipset, оскільки він робить набір правил iptables меншим (тим спрощуючи його обслуговування) і швидше (менше правил означає меншу кількість запитів на вхідному пакеті).

Приклад конфігурації IP tables для plain HTTP

```
#!/bin/sh
ADMIN_IPS="
127.0.0.1
" # Додамо ваші IP адреси та підмережі до списку довірених:
QRATOR_NODES="66.110.32.128/30
83.234.15.112/30
87.245.197.192/30
185.94.108.0/24
"
iptables -N qrator_ips
for IP in $ADMIN_IPS $QRATOR_NODES; do
   iptables -A qrator_ips -s $IP -j RETURN
```

```
done
iptables -A qrator_ips -j DROP

iptables -A INPUT -p tcp -m multiport --dports 80,443 -j qrator_ips
Приклад конфігурації для IP tables з підтримкою conntrack и ipset
#!/usr/bin/env bash
ADMIN_IPS="
127.0.0.1
" # Додавання ваших IP адрес та підмереж в список довірених:
QRATOR_NODES="66.110.32.128/30
83.234.15.112/30
87.245.197.192/30
185.94.108.0/24
"
# Створення довіреного спсику адрес:
ipset -N trusted_nodes hash:net
for ip in $ADMIN_IPS $QRATOR_NODES; do
   ipset -A trusted_nodes ${IP}
done

# Создание правил IP tables:
iptables -N qrator
iptables -A qrator -m set --match-set trusted_nodes src -j ACCEPT
iptables -A qrator -j DROP

iptables -I INPUT --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -p tcp -m multiport --dports 80,443 --state NEW -j qrator
```

Real-IP. При використанні захисту в proxy-based режимі всі HTTP(S) запити до сервера надходитимуть зі зміненими source IP на адреси вузлів фільтрації Qrator.

Реальні адреси відвідувачів передаються в заголовку X-Forwarded-For і рекомендується користувачеві налаштувати передачу цього заголовка у себе на сервері.

Налаштування XFF (Nginx). Якщо як веб-сервер користувач використовує Nginx, то можна розглянути можливість додавання наступного фрагмента в його конфігурацію. Таким чином веб-сервер зможе розпізнати заголовок X-Forwarded-For і відправити додатку реальну IP адресу відвідувача.

 # Додаємо адреси мережі Qrator до списку довірених:

set_real_ip_from 66.110.32.128/30;

set_real_ip_from 83.234.15.112/30;

set_real_ip_from 87.245.197.192/30;

set_real_ip_from 185.94.108.0/24;

 # Використовуємо заголовок "X-Forwarded-For" як джерело:

real_ip_header X-Forwarded-For;

 # Відправляємо реальну адресу відвідувача додатку в заголовку X-Real-IP header:

proxy_set_header X-Real-IP $remote_addr;

2FA. Двоетапна автентифікація. Qrator підтримує двоетапну аутентифікацію (2FA) для облікових записів користувачів як простий, але надійний засіб для підвищення безпеки особистих даних. Для цього використовується програма Google Authenticator на мобільних пристроях. З увімкненою 2FA користувач повинен ввести цифровий код, який генерується мобільним додатком Google Authenticator, у форму входу до Особистого Кабінету поряд з поштовою адресою та паролем. Цифровий код тимчасовий: кожні 30 секунд створюється новий код, старий стає непридатним для входу.

Налаштування двоетапної автентифікації

1. Встановлюється Google Authenticator на користувацький мобільний пристрій;

2. У розділі «Редагування контакту» необхідно поставити галочку «Увімкнути двоетапну автентифікацію». Користувач відразу бачить секретний ключ та QR-код;

3. Додається новий обліковий запис у мобільному додатку шляхом введення секретного ключа або сканування QR-коду. Тепер в основному екрані програми видно доданий обліковий запис і 6-значний ключ, який генерується для нього.

4. Налаштування завершено. Можна протестувати код у тестовій формі введення.

Підключення послуги. Для підключення послуги захисту від DDoS Qrator необхідно виконати такі дії:

- Перейти до панелі керування в розділі «Мережеві послуги».
- Натиснути кнопку «Замовлення послуг»;
- Обрати тип фільтрації трафіку Qrator та натиснути кнопку «Замовити»;
- Підтвердити оплату послуги у вікні.

Заявка на підключення послуг захисту від DDoS Qrator надсилається до служби технічної підтримки Selectel. Захищена IP-адреса, через яку проходитиме весь трафік, а також логін і пароль для входу в особистий кабінет Qrator надійдуть на пошту. У DNS потрібно додати A-запис, який буде вказувати захищений IP, дотримуючись інструкцій щодо зміни DNS-запису сайту з листа.

Змінити A-запис DNS сайту можна у розділі DNS-хостинг панелі керування Selectel за умови, що користувацький домен делегований на DNS сервери Selectel. До IP-адреси сервера повинен бути обов'язково прикріплений домен.

Після того, як від технічної підтримки прийде тикет про те, що послуга підключена, вона з'явиться у списку «Активні послуги» у розділі «Мережеві послуги» панелі керування Selectel. Підключення займає до 1 робочого дня.

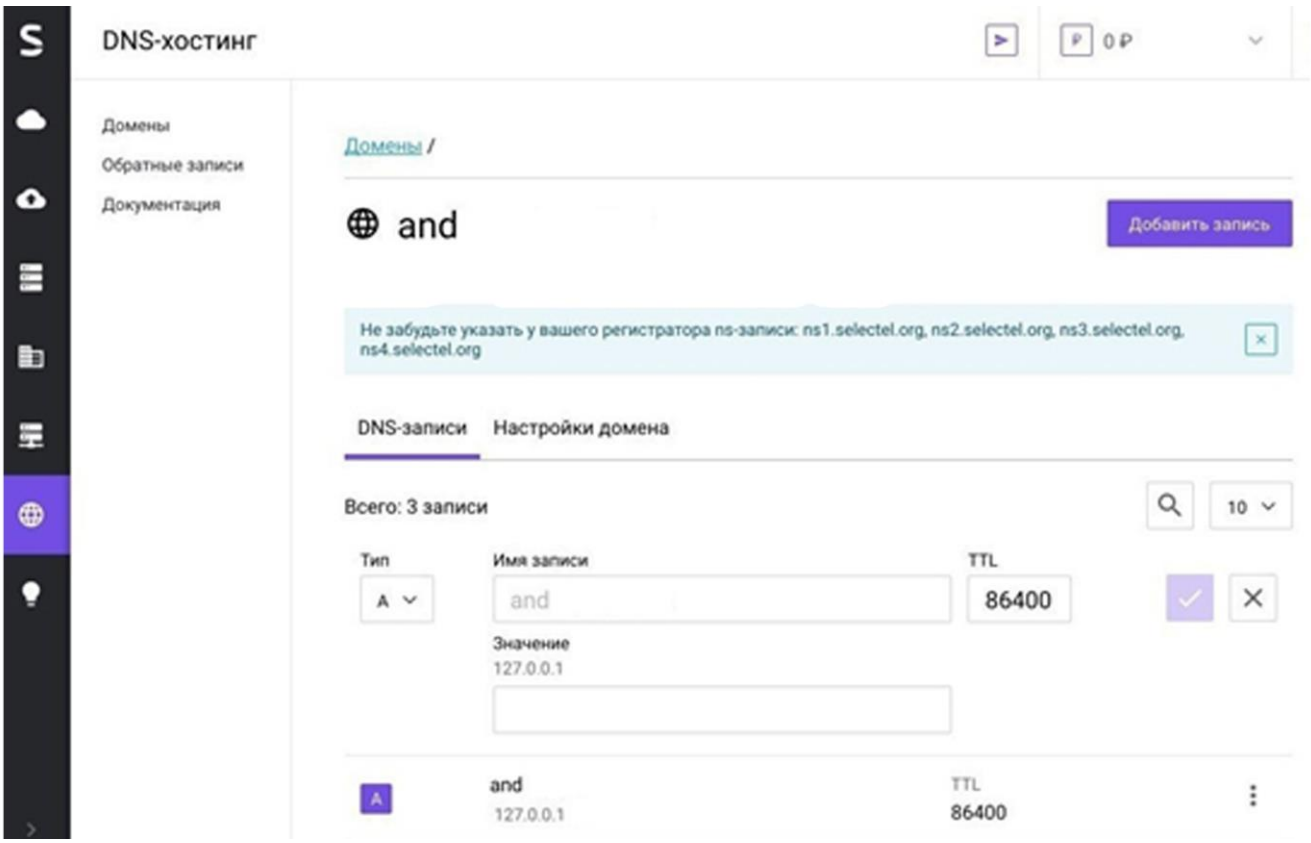

Рис.3.12. Внесення змін до функціонування А-записів DNS користувацького сайту

Статистика. У розділі статистики клієнт може переглянути загальний вхідний та пропущений (очищений) трафік. При побудові статистики можна використовувати фільтри:

- за типами (трафік, пакети, запити тощо);
- за часом (5 годин, 1 доба, тиждень, місяць тощо).

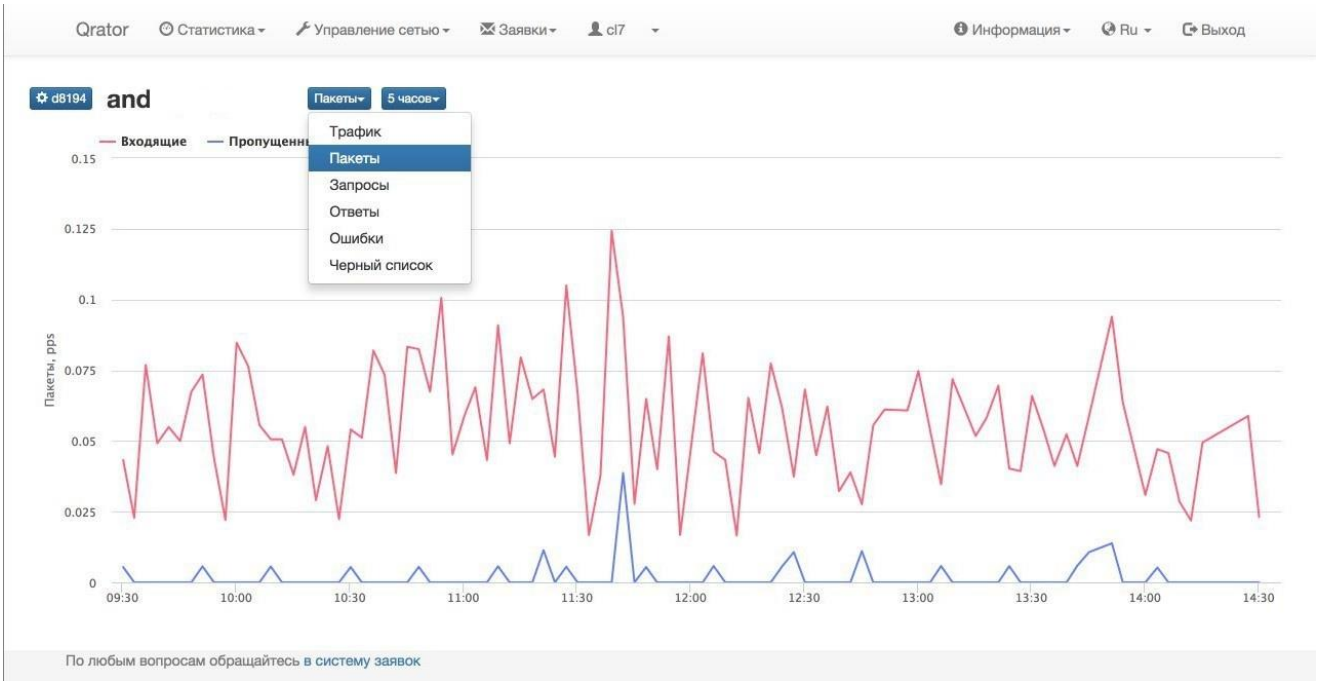

Рис.3.13. Статистичні дані щодо функціонування сайту

Додавання сертифіката. Якщо у користувача немає SSL-сертифіката, можна запросити підключення безкоштовного сертифіката від Let's Encrypt через тикет. Якщо у користувача вже є свій сертифікат, його можна підключити, завантаживши в особистому кабінеті. Для цього:

- необхідно перейти на вкладку «Керування мережею»;
- обрати пункт «Сертифікати»;
- натиснути кнопку «Додати сертифікат»;
- заповнити поля форми, що відкрилася;
- натиснути кнопку «Завантажити файли»;
- сертифікат додано.

Характеристики мережі Qrator

Мережа Qrator має такі основні характеристики:

- близько 1000 Гбіт/с пасивної лінії пропускання - детермінована обробка IP-пакетів без встановлення TCP-з'єднання;
- більше 300 Гбіт/с активної смуги пропускання - кожне вхідне TCP-з'єднання обробляється та аналізується;
- <5% помилкових спрацьовувань у процесі відображення DDoS-атаки;

- час навчання мережі від моменту підключення нового клієнта – менше 2 годин:
- у 33% випадків – до 4 хвилин;
- у 60% випадків – від 5 хвилин до 1 години.
- доданий час затримки при проксуванні трафіку – від 0 до 100 мс. У разі проксування HTTP-трафіку через використання persistent HTTP-з'єднань з сервісом, що захищається, можливий приріст швидкості роботи сервісу, що захищається;
- кількість ЦОД і сервісів, що захищаються, — не обмежена [29].

3.4. Розробка екстрених рекомендацій щодо протидії DDoS

При фіксуванні атаки, і не налаштованому жодному захисті для веб-сайту, можна виконати кілька дій.

1. Забанити IP-адреси, з яких здійснюється атака. Їх можна знайти в журналах. Щоб уникнути блокування кожного запиту вручну, можна використовувати grep. Це інструмент, який дозволяє знаходити певні елементи у файлі та виконувати з ними прості дії, наприклад, блокувати. Добре, якщо атака на сайт буде короткочасною. У цьому випадку можна відразу з’ясувати, звідки виник «сміттєвий» трафік, що дозволить заблокувати його. Але це малоймовірне явище, адже DDoS-атака може тривати кілька днів і спричиняти тисячі різних IP-адрес. Неможливо заблокувати їх усі, навіть використовуючи grep. Крім того, зупинка розумних атак шляхом блокування IP-адрес не дуже ефективна тактика. Якщо зловмисники використовують динамічні IP-адреси, жоден блок не врятує.

2. Блокувати запити за геолокацією. Цей метод працює лише в тому випадку, якщо фіксується, що багато запитів на веб-сайт надходить з певної частини світу. Наприклад, користувачі живуть у Східній Європі, але раптом величезна кількість трафіку надходить з Африки. Але знову ж таки, це рідкість. Більшість атак DDoS сьогодні є «розумними», і зловмисники, швидше за все, не зроблять такої помилки.

3. Блокування «важкого» розділу веб-сайту. Атака може бути спрямована не на весь веб-сайт, а на найбільш вразливу його частину, наприклад, на функцію пошуку. Якщо це не найважливіший елемент веб-сайту, можна просто вимкнути доступ до нього для всіх користувачів. Можливо, клієнти не зможуть користуватися пошуком, але все інше працюватиме нормально. Недоліком цього методу є те, що він марний для більшості атак.

Ці методи можуть допомогти зупинити деякі прості типи DDoS-атак. Крім того, всі вони призначені для відбиття атак на сервери і жодним чином не позбавлять від ботів на сайті, які також можуть викликати великі проблеми.

Наприклад, якщо обмежена кількість продуктів, зловмисник може запустити ботів, які додадуть усі продукти до своїх кошиків, не даючи реальним користувачам щось купувати. Крім того, навіть якщо вдасться відбити атаку, власник витратить час на вирішення проблеми. Це означає, що послуги деякий час будуть недоступні.

Щоб не вдаватися до екстрених заходів, краще з самого початку придбати хостинг із вбудованим захистом від DDoS-атак або включити платний захист від DDoS-атак для свого сервера.

Переваги використання спеціалізованого сервісу для захисту від DDoS-атак:

1. Захист на всіх рівнях. DDoS-атака може відбуватися на рівні мережі (L3), транспортного (L4) або прикладного (L7). Перераховані вище методи допоможуть у разі DDoS-атаки на одному рівні. Але напади бувають різними, а захистити всі рівні самостійно вкрай важко. Професійний захист — це добре розроблена платформа фільтрації, через яку проходить весь трафік і яка блокує підозрілі запити. «Сміттєві» пакети даних будуть зупинені на шляху до ресурсу.

2. Балансування навантаження. Хороша система безпеки зазвичай забезпечує рівномірний розподіл трафіку між вузлами. Це ускладнює для злочинців «збій» веб-сайту. Крім того, це також прискорить завантаження веб-сайту та допоможе з природним сплеском трафіку.

3. Захист уразливостей веб-додатків. Будь-який веб-сайт або додаток має слабкі місця, і зловмисники не соромляться використовувати їх. Вони виявляють

уразливості та використовують їх, щоб отримати доступ до конфіденційних даних користувачів. Брандмауер веб-додатків — це брандмауер, який приховує вразливості програм і блокує підозрілий трафік. Вибираючи брандмауер, важливо звернути увагу на те, як він працює. Добре вибрати «розумний» WAF з алгоритмами самонавчання. Такі екрани здатні аналізувати вміст пакетів і не блокувати реальних клієнтів разом з ботами.

4. *Гарантія повернення коштів.* Якщо виникла необхідність захистити веб-сайт будь-якими доступними інструментами, немає гарантії, що ці інструменти допоможуть. І навіть якщо власний захист поки що більш-менш впорався, завтра хакери можуть винайти новий тип DDoS-атаки, і всі методи будуть марними. З іншого боку, якщо користувач купуєте професійний захист, хороші компанії завжди надають гарантію повернення за свої послуги. Якщо захист не спрацює, можна повернути свої гроші. При цьому професійні системи постійно розвиваються і враховують появу нових DDoS-атак.

Висновки до третього розділу

Досліджено найкращих постачальників послуг захисту від DDoS (за версією звіту Quadrant Knowledge Solutions DDoS). До них відносять: Akamai, Verisign, Radware DefensePro, Cloudflare DDoS, Arbor Networks APS, Nexusguard, DOSarrest, F5 Захист від DDoS, Neustar SiteProtect NG, FortiDDoS, Qrator Labs та ін.

Підкреслено, що перелічені вендори окрім обробки традиційних DDoS-атак, включають хмарні, мобільні та IoT-функції, та проводять детальний аналіз цільових ринків, варіантів використання, функцій, показників, використання агентів та сертифікати безпеки.

Проведено детальний аналіз технологій функціонування та особливостей налаштування сервісу захисту сайтів та доменів від DDoS атак від вендора Qrator Labs. Мережа Qrator спроектована і побудована для роботи під постійним впливом великої кількості DDoS-атак. Вузли фільтрації Qrator Labs підключені до каналів найбільших магістральних інтернет-провайдерів США, Західної та Східної Європи,

Південно-Східної Азії. Таким чином, на відміну від мереж операторів хостингу (особливо, віртуального) мережа Qrator Labs спроектована для екстремальних навантажень, і атака на ресурс одного з клієнтів ніяк не впливає на працездатність сайтів інших клієнтів.

Досліджено технічний алгоритм підключення клієнтів, що включає перенаправлення трафіку користувача на вузли фільтрації Qrator, де аналізується, і вже «чистий» трафік перенаправляється на сайт, що захищається.

Перераховано додаткові можливості вендора, а також виокремлено покроковий алгоритм виконання превентивного тестування конфігурації послуг у Qrator Labs. Приведено особливості налаштування TTL A-запису DNS, фаєрволів, фільтрування HTTPS (в тому числі з розкриттям та без розкриття ключів (PCI-DSS ready)).

Досліджено особливості блокування IP-адрес з використанням методів Qrator API та налаштування двоетапної автентифікації (з використанням Google Authenticator). Розроблено рекомендацій щодо протидії DDoS атакам для користувачів та клієнтів.

ВИСНОВКИ

В магістерській роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено методи, призначені для захисту від DDoS атак та виведено таксономію атак на відмову в обслуговуванні.

2. Виокремлено рішення та механізми, які необхідні для виявлення та реагування на DDoS атаки. Зазначено, що одним з недоліків цих механізмів є те, що клієнти повинні знати про захист і встановлювати спеціальне програмне забезпечення. Це означає, що система повинна бути встановлена в кінцевій мережі.Іншим недоліком є те, що за останні роки відбулося прогресивне зростання кількості DDoS атак.

3. Досліджено найкращих постачальників послуг захисту від DDoS (за версією звіту Quadrant Knowledge Solutions DDoS). До них відносять: Akamai, Verisign, Radware DefensePro, Cloudflare DDoS, Arbor Networks APS, Nexusguard, DOSarrest, F5 Захист від DDoS, Neustar SiteProtect NG, FortiDDoS, Qrator Labs та ін.

4. Підкреслено, що перелічені вендори окрім обробки традиційних DDoS-атак, включають хмарні, мобільні та IoT-функції, та проводять детальний аналіз цільових ринків, варіантів використання, функцій, показників, використання агентів та сертифікати безпеки.

5. Проведено детальний аналіз технологій функціонування та особливостей налаштування сервісу захисту сайтів та доменів від DDoS атак від вендора Qrator Labs. Мережа Qrator спроектована і побудована для роботи під постійним впливом великої кількості DDoS-атак. Вузли фільтрації Qrator Labs підключені до каналів найбільших магістральних інтернет-провайдерів США, Західної та Східної Європи, Південно-Східної Азії. Таким чином, на відміну від мереж операторів хостингу (особливо, віртуального) мережа Qrator Labs спроектована для екстремальних навантажень, і атака на ресурс одного з клієнтів ніяк не впливає на працездатність сайтів інших клієнтів.

6. Досліджено технічний алгоритм підключення клієнтів, що включає перенаправлення трафіку користувача на вузли фільтрації Qrator, де аналізується, і вже «чистий» трафік перенаправляється на сайт, що захищається.

7. Перераховано додаткові можливості вендора, а також виокремлено покроковий алгоритм виконання превентивного тестування конфігурації послуг у Qrator Labs. Приведено особливості налаштування TTL A-запису DNS, фаєрволів, фільтрування HTTPS (в тому числі з розкриттям та без розкриття ключів (PCI-DSS ready)).

8. Досліджено особливості блокування IP-адрес з використанням методів Qrator API та налаштування двоетапної автентифікації (з використанням Google Authenticator). Розроблено рекомендацій щодо протидії DDoS атакам для користувачів та клієнтів.