ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Богдан КОВАЛЬСЬКИЙ
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
КОВАЛЬСЬКИЙ Богдан
(прізвище, ім'я)

Керівник д.ф. СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 9

ВСТУП ……..…… 10

1 **ДОСЛІДЖЕННЯ ПРОБЛЕМИ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК** … 12

1.1 Дослідження проблеми керованого захисту хмарних корпоративних додатків від DDoS-атак ……...…….…. 12
1.2 Аналіз підходів до керованого захисту хмарних корпоративних додатків від DDoS-атак ……..……... 17
1.3 Аналіз існуючих рішень для керованого захисту хмарних корпоративних додатків від DDoS-атак ……..... 24

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS SHIELD** ……..……..... 34

2.1 Призначення та основні функції рішення AWS Shield ……..….. 34
2.2 Архітектура рішення AWS Shield ……..……..…..… 37
2.3 Порядок функціонування рішення AWS Shield ……..……. 40

3 **ТЕХНОЛОГІЯ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS SHIELD** …….. 45

3.1 Порядок застосування рішення AWS Shield ……... 45
3.2 Технологія керованого захисту хмарних корпоративних додатків від DDoS-атак ……..…… 47
3.3 Рекомендації щодо керованого захисту хмарних корпоративних додатків від DDoS-атак …….……...……. 57

ВИСНОВКИ …….. 63

ПЕРЕЛІК ПОСИЛАНЬ 65

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACLs – Access Control Lists

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CIPS – Cloud Infrastructure and Platform Service

CNAPP – Cloud-Native Application Protection Platform

DAST – Dynamic Application Security Testing

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

MSSP – Managed Security Service Provider

SOC – Security Operations Center

OWASP – Open Web Application Security Project

VPC – Virtual Private Cloud

WAAP – Web Application and API protection

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Керований захист хмарних корпоративних застосунків від розподілених атак типу «відмова в обслуговуванні» (DDoS) має вирішальне значення через серйозні операційні збої, фінансові втрати та репутаційну шкоду, які ці атаки можуть завдати. Оскільки підприємства все більше покладаються на хмарну інфраструктуру, їхня вразливість до цих складних кіберзагроз зростає, що робить проактивний захист під керівництвом експертів необхідністю.

DDoS-атака – це зловмисна спроба порушити нормальний трафік цільового сервера, служби або мережі шляхом перевантаження цільової атаки або навколишньої інфраструктури потоком інтернет-трафіку. Ці атаки є «розподіленими», оскільки вони походять з численних, часто скомпрометованих джерел, що ускладнює їх зупинку. Існує кілька типів DDoS-атак, кожна з яких спрямована на різні компоненти мережевого з'єднання: об'ємні атаки, протокольні атаки, атаки на рівні додатків. Для корпоративних додатків, розміщених у хмарі, успішна DDoS-атака може мати далекосяжні наслідки.

Хоча хмарні постачальники пропонують певний рівень захисту від DDoS-атак, зростаюча складність і масштаб атак часто вимагають більш спеціалізованого та керованого підходу. Складність та потенційний вплив DDoS-атак на хмарні корпоративні додатки вимагають надійної та керованої системи безпеки. Покладатися виключно на базові засоби захисту більше не достатньо перед обличчям постійно мінливих кіберзагроз.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield.

Об'єкт дослідження – керований захист хмарних корпоративних додатків від DDoS-атак.

Предмет дослідження – технологія керованого захисту хмарних

корпоративних додатків від DDoS-атак на основі AWS Shield.

Мета роботи – розробити порядок застосування технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми керованого захисту хмарних корпоративних додатків від DDoS-атак;

проаналізувати підходи до керованого захисту хмарних корпоративних додатків від DDoS-атак;

проаналізувати існуючі рішення для керованого захисту хмарних корпоративних додатків від DDoS-атак;

проаналізувати методи та засоби керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield;

розкрити порядок реалізації технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК

1.1. Дослідження проблеми керованого захисту хмарних корпоративних додатків від DDoS-атак

DDoS (distributed-denial-of-service) атака намагається перервати роботу сервера або мережі шляхом затоплення її фальшивим інтернет-трафіком, запобігаючи доступу користувачів та порушуючи роботу. Мета DDoS-атаки полягає в тому, щоб порушити здатність організації обслуговувати своїх користувачів.

Ботнет – це мережа комп'ютерів, заражених шкідливим програмним забезпеченням, яке дозволяє зловмисникам керувати комп'ютерами віддалено. Ці ботнети є «розподіленими», оскільки вони можуть бути розташовані будь-де та належати будь-кому. Невинні власники заражених комп'ютерів можуть ніколи не знати, що їхні системи є частиною ботнету.

Після створення масивної ботнету з мільйонів скомпрометованих пристроїв, DDoS-зловмисник віддалено спрямовує кожного бота на надсилання запитів на IP-адресу цілі. Мета полягає в тому, щоб перевищити ліміти пропускної здатності веб-ресурсів жертви величезною кількістю запитів на підключення або даних, щоб зрештою зупинити їхню роботу.

DDoS-атаки можна класифікувати по-різному, але зазвичай їх групують на три типи [4, 5]:

об'ємна атака. Ботнети надсилають величезні обсяги фальшивого трафіку до ресурсу. Цей тип атаки може використовувати ping-флуд, флуд підроблених пакетів або UDP-флуд. Атака на основі об'єму вимірюється в бітах за секунду (BPS).

атаки мережевого рівня або атаки на протокол, надсилають велику кількість пакетів до цілі. Атака мережевого рівня не вимагає відкритого з'єднання

TCP та не спрямована на певний порт. Атака мережевого рівня вимірюється в пакетах за секунду (PPS). Приклади атаки мережевого рівня включають:

атака Smurf – спроба перевантажити сервер на мережевому рівні за допомогою пакетів протоколу ICMP (Internet Control Message Protocol) та експлуатуючи вразливості IP-адрес;

SYN Flood – ініціює з'єднання із сервером без його розірвання, що призводить до перевантаження серверів. Цей тип атаки використовує величезну кількість TCP-запитів на встановлення зв'язку зі підробленими IP-адресами.

атаки на рівні додатків використовують поширені запити, такі як HTTP GET та HTTP POST. Ці атаки впливають як на серверні, так і на мережеві ресурси, тому такого ж руйнівного ефекту, як у інших типів DDoS-атак, можна досягти з меншою пропускною здатністю. Розрізнити легітимний та шкідливий трафік на цьому рівні складно, оскільки трафік не підробляється, тому він виглядає нормальним. Атака на рівні додатків вимірюється в запитах за секунду (RPS).

Хоча більшість атак базуються на об'ємі, існують також DDoS-атаки типу «низький та повільний», які залишаються невиявленими, надсилаючи невеликі, постійні потоки запитів, які можуть непомітно знижувати продуктивність протягом тривалого часу. Атаки типу «низький та повільний» спрямовані на веб-сервери на основі потоків і призводять до дуже повільної передачі даних легітимним користувачам, але не настільки повільної, щоб спричинити помилку тайм-ауту. Деякі інструменти, що використовуються в атаках типу «низький та повільний», включають Slowloris, RUDY та Sockstress.

Кількість DDoS-атак стрімко зростає. Незважаючи на спад у 2018 році, коли ФБР закрило найбільші сайти DDoS-атак на замовлення в даркнеті, кількість DDoS-атак зросла на 151% у першій половині 2020 року. У деяких країнах DDoS-атаки можуть становити до 25% від загального інтернет-трафіку під час атаки. Рушійною силою цієї ескалації є впровадження Інтернету речей (IoT). Більшість пристроїв IoT не мають вбудованої прошивки або засобів контролю безпеки. Оскільки пристроїв IoT багато, і вони часто впроваджуються без тестування та контролю безпеки, вони вразливі до захоплення в ботнети IoT.

Ще однією слабкою стороною є API, або інтерфейси прикладного програмування. API – це невеликі фрагменти коду, які дозволяють різним системам обмінюватися даними. Наприклад, туристичний сайт, який публікує розклади авіарейсів, використовує API для отримання цих даних із сайтів авіакомпаній на веб-сторінки туристичного сайту. «Публічні» API, доступні для використання будь-ким, можуть бути погано захищені. Типові вразливості включають слабкі перевірки автентифікації, недостатній захист кінцевих точок, відсутність надійного шифрування та недосконалу бізнес-логіку.

Друга за величиною та одна з найпопулярніших DDoS-атак сталася з одним із клієнтів хмарних сервісів Google. У певний момент клієнт Google зазнавав бомбардування 46 мільйонами RPS (запитів за секунду). Google попередив свого клієнта про атаку та зміг заблокувати її протягом години.

У жовтні 2022 року веб-сайти кількох великих аеропортів США вийшли з ладу в результаті DDoS-атаки. Атаку організувала російська група під назвою KillNet. На щастя, робота аеропорту не була порушена, окрім того, що мандрівникам та членам їхніх сімей було заважено шукати інформацію про рейси. Ця атака сталася через кілька днів після того, як кілька веб-сайтів урядів штатів США, таких як веб-портал штату Колорадо, постраждали від атаки. Жодна з цих атак не закінчилася довгостроковими негативними наслідками, і сайти зараз працюють належним чином.

Коли йдеться про DDoS-атаки, розмір не має значення. Жодна компанія не є повністю безпечною. На сьогоднішній день найбільша DDoS-атака сталася в лютому 2023 року на CloudFlare з показником 71 мільйон RPS (запитів за секунду), що на 35% перевищує показник Google Cloud з червня 2022 року. Це була найбільша з десятків DDoS-атак, які вони виявили та пом’якшили протягом вихідних 11 лютого, кожна з яких в середньому становила від 50 до 70 мільйонів RPS.

Жертви DDoS-атак зазвичай помічають, що їхня мережа, веб-сайт чи пристрій працює повільно або не надає послуг. Однак ці симптоми не є унікальними для DDoS-атак – вони можуть бути спричинені багатьма факторами,

такими як несправність сервера, сплеск легітимного трафіку або навіть обрив кабелю. Ось чому не можна просто покладатися на ручні спостереження, а натомість слід використовувати інструмент аналізу трафіку для виявлення розподілених атак типу «відмова в обслуговуванні».

Захист від DDoS-атак та їх пом’якшення вимагає багатогранного підходу – жоден окремий інструмент не може гарантувати повний захист від усіх типів DDoS-атак.

Компанії повинні використовувати проактивний підхід до захисту від DDoS-атак. Перший крок – усвідомити всі вразливості та сильні сторони вашої компанії. Проведіть оцінку ризиків для всіх корпоративних цифрових активів (тобто мереж, серверів, пристроїв, програмного забезпечення), щоб бути готовими до найкращого плану пом’якшення наслідків, коли настане час.

WAF подібний до контрольної точки для веб-застосунків, оскільки він використовується для моніторингу вхідних HTTP-запитів та фільтрації шкідливого трафіку. Коли виявляється DDoS-атака на рівні застосунку, політики WAF можна швидко змінити, щоб обмежити кількість запитів та заблокувати шкідливий трафік, оновивши список контролю доступу (ACL).

SIEM – це інструмент, який збирає дані з кожного куточка середовища та агрегує їх в єдиному централізованому інтерфейсі, забезпечуючи видимість шкідливої активності, яку можна використовувати для кваліфікації сповіщень, створення звітів та підтримки реагування на інциденти.

CDN та балансувальники навантаження можна використовувати для зменшення ризику перевантаження сервера та подальших проблем із продуктивністю/доступністю шляхом автоматичного розподілу потоку трафіку між кількома серверами.

Під час маршрутизації через чорну діру адміністратор мережі пропускає весь трафік, хороший чи поганий, через маршрут через чорну діру. Мета полягає в тому, щоб відкинути весь трафік з мережі, що має негативний вплив на втрату легітимного трафіку та потенційно частини бізнесу.

Обмеження кількості запитів на обслуговування, які корпоративна мережа

отримує та приймає протягом певного періоду часу. Зазвичай цього недостатньо для боротьби з більш складними DDoS-атаками, тому це слід використовувати разом з іншими стратегіями пом’якшення наслідків.

ETL 2025 [2] підкреслює зрілість середовища загроз, що характеризується швидким використанням вразливостей та зростаючою складністю відстеження противників.

Активність вторгнень залишається значною, в її основі лежить програма-вимагач. Кіберзлочинці, зокрема, реагували на дії правоохоронних органів, децентралізуючи операції, застосовуючи агресивну тактику вимагання та використовуючи побоювання щодо дотримання нормативних вимог. Постійне поширення моделей «програм-вимагач як послуга», витоків інформації від розробників та послуг брокерів доступу ще більше знизило бар’єри для входу та диверсифікувало сімейства програм-вимагачів, що сприяло професійній та стійкій злочинній екосистемі.

Паралельно, пов’язані з державою групи загроз активізували свої довгострокові кібершпигунські кампанії проти телекомунікаційних, логістичних мереж та виробничого секторів ЄС, демонструючи передові методи, такі як компрометація ланцюгів поставок, приховані системи шкідливого програмного забезпечення та зловживання підписаними драйверами.

Активність хактивістів продовжує домінувати у звітах, складаючи майже 80% зареєстрованих інцидентів та зумовлена переважно низькорівневими розподіленими операціями відмови в обслуговуванні. Хоча загалом ці кампанії мають дуже низький вплив, вони демонструють, як недорогі інструменти масштабуються для ідеологічно керованих операцій.

Галузеві моделі таргетування посилюють системний вплив ЄС. Мережі державного управління залишаються основним фокусом (38%), особливо для хактивістів та систем вторгнення у зв'язки з державами, тоді як транспорт став високоцінним сектором, особливо морський та логістичний. Авіаційні та вантажні перевезення зіткнулися з перебоями, спричиненими програмами-вимагачами, тоді як цифрова інфраструктура та послуги залишаються стратегічними цілями як для

операторів кібершпигунства, так і для операторів програм-вимагачів.

Фішинг залишається домінуючим вектором вторгнення (60%) і розвивається завдяки методам, що використовуються у масштабних кампаніях. Доступність платформ фішинг як послуга демонструє індустріалізацію фішингових операцій, що дозволяє зловмисникам будь-якого рівня кваліфікації запускати складні кампанії. Зловживання кіберзалежностями також посилилися, про що свідчать компрометації у репозиторіях з відкритим кодом, шкідливі розширення браузерів та порушення безпеки постачальників послуг, що посилює ризик у взаємопов'язаних цифрових екосистемах.

У всіх кампаніях зловмисники продовжують покладатися на узгоджений набір тактик, методів та процедур.

Експлуатація вразливостей залишається наріжним каменем початкового доступу (21,3%), причому широко поширені кампанії швидко перетворюють їх на зброю протягом кількох днів після їх розкриття, що підкреслює необхідність забезпечення доступності патчів та впровадження та забезпечення дотримання основних заходів кібергігієни.

Штучний інтелект став визначальним елементом ландшафту загроз. Повідомляється, що на початок 2025 року фішингові кампанії, що підтримуються штучним інтелектом, становили понад 80 відсотків спостережуваної діяльності соціальної інженерії у всьому світі, причому зловмисники використовували моделі з джейлбрейком, синтетичні носії та методи отруєння моделей для підвищення своєї операційної ефективності.

1.2. Аналіз підходів до керованого захисту хмарних корпоративних додатків від DDoS-атак

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це скоординована спроба зробити веб-сайт, мобільний додаток або API недоступним шляхом перевантаження його трафіком з кількох джерел. На відміну від простих кібератак, які відбуваються з одного комп’ютера, DDoS-атаки використовують

мережі скомпрометованих комп’ютерів, щоб завалити свої цілі запитами, роблячи їх недоступними для реальних користувачів [6].

Останні дані яскраво демонструють зростання загрози DDoS-атак. Згідно з останнім звітом Zayo Group про аналітику DDoS-атак, середня DDoS-атака у 2023 році тривала 68 хвилин і коштувала незахищеним підприємствам у середньому 6000 доларів за хвилину, що загалом становить понад 408 000 доларів за атаку [6].

Керований захист від DDoS-атак включає використання хмарних сервісів захисту, впровадження аналізу та фільтрації трафіку, а також зменшення поверхні атаки за допомогою конфігурацій мережі та додатків. Ключові підходи включають використання брандмауерів веб-застосунків (WAF) та мереж доставки контенту (CDN), безперервний моніторинг трафіку та виявлення аномалій, а також масштабування інфраструктури для обробки пікових значень трафіку.

Розглянемо основні методи запобігання DDoS-атак.

Зменшення поверхні атаки. Обмеження впливу поверхні атаки може допомогти мінімізувати вплив DDoS-атаки. Кілька методів зменшення цього впливу включають обмеження трафіку певними місцями, впровадження балансувальника навантаження та блокування зв’язку із застарілими або невикористаними портами, протоколами та додатками.

Розповсюдження мережі Anycast. Мережа Anycast допомагає збільшити площу поверхні мережі організації, щоб вона могла легше поглинати об’ємні сплески трафіку (і запобігати збоям) шляхом розподілу трафіку між кількома розподіленими серверами.

Адаптивний моніторинг загроз у режимі реального часу. Моніторинг журналів може допомогти точно визначити потенційні загрози, аналізуючи закономірності мережевого трафіку, відстежуючи піки трафіку або іншу незвичайну активність, а також адаптуючись для захисту від аномальних або шкідливих запитів, протоколів і блоків IP-адрес.

Кешування. Кеш зберігає копії запитуваного контенту, щоб сервери походження обслуговували менше запитів. Використання мережі доставки контенту (CDN) для кешування ресурсів може зменшити навантаження на сервери

організації та ускладнити їх перевантаження як легітимними, так і шкідливими запитами.

Обмеження швидкості. Обмеження швидкості обмежує обсяг мережевого трафіку протягом певного періоду часу, по суті запобігаючи перевантаженню веб-серверів запитами з певних IP-адрес. Обмеження швидкості може бути використане для запобігання DDoS-атакам, які використовують ботнети для спаму кінцевої точки аномальною кількістю запитів одночасно.

Розглянемо основні інструменти запобігання DDoS-атак.

Брандмауер веб-застосунків (WAF). WAF допомагає блокувати атаки, використовуючи налаштовувані політики для фільтрації, перевірки та блокування шкідливого HTTP-трафіку між веб-застосунками та Інтернетом. За допомогою WAF організації можуть запровадити позитивну та негативну модель безпеки, яка контролює вхідний трафік з певних місць розташування та IP-адрес.

Постійне пом'якшення DDoS-атак. Постачальник послуг із пом'якшення DDoS-атак може допомогти запобігти DDoS-атакам, постійно аналізуючи мережевий трафік, впроваджуючи зміни політик у відповідь на нові моделі атак та надаючи розгалужену та надійну мережу центрів обробки даних. Оцінюючи хмарні послуги з пом'якшення DDoS-атак, шукайте постачальника, який пропонує адаптивний, масштабований та постійно активний захист від складних та об'ємних атак.

Ефективна стратегія захисту від DDoS-атак включає кілька ключових елементів (рисунок 1.1) [7]:

виявлення: виявлення та розрізнення легітимного трафіку від шкідливого DDoS-трафіку;

пом'якшення: фільтрація та блокування шкідливого трафіку з одночасним пропусканням легітимного трафіку;

масштабованість: забезпечення того, щоб механізм захисту міг обробляти масштабні атаки без погіршення продуктивності;

стійкість: впровадження механізмів резервування та відновлення після збоїв для підтримки доступності послуг під час атаки.

Рис. 1.1. Ефективна стратегія захисту від DDoS-атак [7]

Сімейство рішень Radware для захисту від DDoS-атак та систем запобігання вторгненням забезпечує інтегровану безпеку додатків і мережі, а також управління інструментами безпеки для створення найкращої багаторівневої архітектури безпеки та запобігання DDoS-атакам. Radware пропонує *системи пом'якшення атак* (AMS) – це перше в галузі повністю інтегроване рішення IT-безпеки, яке захищає інфраструктуру додатків у режимі реального часу від простоїв мережі та додатків, використання вразливостей додатків, поширення шкідливого програмного забезпечення, крадіжки інформації, атак веб-сервісів та пошкодження веб-сторінок [8].

Мережа пом'якшення наслідків атак (AMN) – це цілісна архітектура безпеки, розроблена для вирішення нових проблем безпеки DDoS. AMN поєднує розподілені елементи виявлення та пом'якшення наслідків, які синхронізовані з легітимними базовими показниками трафіку та інформацією про атаки в режимі реального часу. AMN розширює охоплення виявлення на всі ресурси підприємства та автоматизує пом'якшення наслідків, вибираючи найефективніші інструменти та місця розташування – у центрі обробки даних, на периметрі або в хмарі. В

результаті AMN пропонує безпрецедентний захист від сьогоднішніх та майбутніх DDoS-загроз, пов’язаних з доступністю, на всіх фронтах [8].

Оскільки методи DDoS-атак зростають за частотою, складністю та серйозністю, рішення для додатків та безпеки повинні відповідати цим загрозам та перевершувати їх. Рішення Radware [8] для запобігання DDoS-атакам у режимі реального часу забезпечує необхідний рівень захисту для сучасних потреб безпеки додатків та мережі, а також готове до викликів майбутнього. Засновані на адаптивних технологіях, заснованих на поведінці та сигнатурах, системи та рішення для запобігання вторгненням забезпечують організації інтегрованими системами виявлення та запобігання вторгненням, а також захистом від DoS-атак (DoS) та розподілених DoS-атак (DDoS). Рішення Radware для запобігання DoS/DDoS-атак захищає від атак як на мережевому, так і на рівні додатків, забезпечуючи цілісний підхід до загроз на рівні додатків та мережі, одночасно підвищуючи загальну ефективність безпеки в організації.

Radware DefensePro – це мережевий пристрій у режимі реального часу, який забезпечує надійне запобігання DDoS/DoS-атакам, безпеку та захист як для мереж, так і для додатків.

DDoS-атаки з перевантаженням навмисно використовують ресурси пропускної здатності, щоб вивести з ладу корпоратвині сайти, мережі та додатки. Ці типи DDoS-атак можуть бути розпочаті будь-коли, і багато з них використовують автоматизовані програми, які дозволяють тисячам користувачів атакувати мережу або додаток. DefensePro захищає від цих загроз, аналізуючи поведінку та запити користувачів і зіставляючи їх з розпізнаними шаблонами та сигнатурами атак у своїй пам’яті. Коли виявляється DDoS/DoS-атака, DefensePro, що є частиною систем пом’якшення наслідків атак (AMS) від Radware, запобігає атакам, не блокуючи легітимних користувачів у корпоративній мережі чи програмах. Рішення може запобігти вторгненням і перевантаженням, не перешкоджаючи реальним користувачам отримати доступ до необхідної їм інформації.

DefensePro швидко та точно розрізняє три широкі категорії поведінки:

легітимний звичайний трафік, атакуючий трафік та незвичайні моделі, створені легітимною активністю. Цей модуль має дві функції для забезпечення такого захисту.

Функція поведінкового виявлення DoS-атак, яка швидко пом’якшує DDoS/DoS-атаки «нулевого дня», автоматично генеруючи сигнатури в режимі реального часу для запобігання DDoS-атаці без необхідності втручання людини.

Захист корпоративних ресурсів від DDoS-атак вимагає багаторівневого підходу. Жоден окремий метод не є панацеєю, тому ефективна стратегія базується на принципі «глибокого захисту» (Defense in Depth).

Розглянемо основні методи запобігання та пом’якшення наслідків DDoS-атак на корпоративні інформаційні ресурси, розподілені за рівнями захисту.

Архітектурні рішення (Infrastructure Level). Це фундамент захисту, який дозволяє системі витримувати великі навантаження ще до того, як атака досягне критичної точки.

Розподіл навантаження (Load Balancing). Використання балансувальників навантаження дозволяє розподіляти вхідний трафік між декількома серверами. Якщо один сервер перевантажений, трафік автоматично перенаправляється на інші.

Використання CDN (Content Delivery Network). CDN кешує статичний контент (зображення, CSS, JS) на серверах по всьому світу. Це дозволяє поглинати величезні об’єми трафіку на кордоні мережі, не пропускаючи його до корпоративного основного сервера (Origin).

Визначається, що CDN є одним з найефективніших методів проти volumetric attacks (атак на переповнення каналу).

Надлишковість ресурсів (Overprovisioning). Забезпечення більшої пропускної здатності каналу та обчислювальної потужності, ніж потрібно у звичайному режимі, щоб витримати раптові сплески трафіку.

Хмарні сервіси захисту (Cloud Scrubbing). Для більшості корпорацій це найнадійніший метод захисту від масштабних атак.

Центри очищення трафіку (Scrubbing Centers). Весь вхідний трафік перенаправляється через спеціалізованого провайдера (наприклад, Cloudflare, AWS

Shield, Akamai). Там шкідливий трафік відфільтровується, а до корпоративних серверів доходить лише «чистий» трафік.

Приховування реальної IP-адреси. Корпоративні сервери не повинні бути доступні напряму з Інтернету. Вони мають приймати з'єднання тільки від IP-адрес провайдера захисту.

Мережевий захист та конфігурація (Network & Transport Layer). Ці методи працюють на рівнях L3/L4 моделі OSI (IP та TCP/UDP).

Брандмауери (Firewalls) та ACL. Налаштування списків контролю доступу (ACL) для блокування трафіку з підозрілих підмереж або портів, які не використовуються.

Обмеження швидкості (Rate Limiting). Обмеження кількості запитів, які сервер приймає від однієї IP-адреси за певний проміжок часу. Це допомагає проти атак типу «brute force» та повільних DDoS-атак.

Geo-blocking. Якщо бізнес працює лише в Україні, ми можемо заблокувати або обмежити трафік з регіонів, звідки часто йдуть атаки (наприклад, Китай, рф тощо).

Blackholing / Sinkholing. У разі критичної атаки весь трафік (і хороший, і поганий) на певну IP-адресу перенаправляється в «нікуди» (null route), щоб врятувати решту мережі.

Захист на рівні додатків (Application Layer – L7). Найскладніші атаки імітують поведінку реальних користувачів (наприклад, HTTP floods).

WAF (Web Application Firewall). Інтелектуальний фаєрвол, який аналізує HTTP-запити. Він може відрізнити бота від людини за допомогою перевірки User-Agent, аналізу поведінки та використання CAPTCHA.

Механізми перевірки (Challenge-Response). Перед тим як обробити важкий запит (наприклад, пошук у базі даних), система вимагає від клієнта виконати просту задачу (JavaScript challenge або CAPTCHA), яку боти часто не можуть пройти.

Організаційні заходи. Технології не працюють без процесів.

Моніторинг та аналітика. Впровадження систем SIEM та аналізу трафіку

(NetFlow) для виявлення аномалій у реальному часі. Ми маємо знати, як виглядає наш «нормальний» трафік.

DDoS Response Plan. Чіткий план дій: кому дзвонити провайдеру, хто приймає рішення про відключення сервісів, як комунікувати з клієнтами.

Таблиця 1.1

Результати порівняльного аналізу методів захисту хмарних корпоративних додатків від DDoS-атак

Метод	**Рівень захисту (OSI)**	**Ефективність проти**	**Складність впровадження**
CDN	L3, L4, L7	Volumetric attacks (об'ємні)	Низька/Середня
WAF	L7	HTTP floods, SQLi, XSS	Середня
Rate Limiting	L4, L7	Brute force, Slowloris	Низька
Scrubbing Center	Всі рівні	Масштабні атаки всіх типів	Висока (або дорого)

1.3. Аналіз існуючих рішень для керованого захисту хмарних корпоративних додатків від DDoS-атак

Впровадження хмарних технологій прискорюється на кожному архітектурному рівні, особливо на гібридному, мультихмарному та периферійному, але стратегії безпеки не встигають за цим. 62% організацій розширили хмарні технології на периферії (такі як SASE), 57% розширили гібридну хмару, а 51% перейшли на багатохмарні, фрагментуючі середовища та переважні традиційні засоби захисту на основі периметра. Незважаючи на багаторічні інвестиції в інструменти та стратегії хмарної безпеки, рівень інцидентів зростає, що свідчить про невідповідність між сучасними хмарними середовищами та засобами захисту, призначеними для їх захисту [10].

Керований захист хмарних корпоративних додатків від DDoS-атак передбачає використання спеціалізованих послуг від хмарних постачальників або сторонніх розробників, які використовують багаторівневий захист, постійний моніторинг трафіку та автоматизоване пом’якшення наслідків для захисту корпоративних додатків від об’ємних, протокольних та прикладних атак. Ключові функції включають автоматичне реагування, очищення трафіку, брандмауери веб додатків (WAF), обмеження швидкості та екстрену підтримку для забезпечення безперервності бізнесу.

Великі хмарні постачальники, такі як AWS, Azure та Google Cloud, пропонують власні керовані сервіси захисту від DDoS-атак для захисту корпоративних додатків, розгорнутих на їхній інфраструктурі.

Сервіси захисту хмарних корпоративних додатків від DDoS-атак автоматично виявляють та блокують шкідливий трафік у режимі реального часу, часто протягом кількох секунд, щоб запобігти перебоям у роботі сервісу. Захист включає кілька стратегій захисту для обробки різних типів атак. Масштабні атаки, спрямовані на перевантаження пропускної здатності мережі, обробляються шляхом перенаправлення трафіку до центрів очищення, які фільтрують шкідливий трафік. Складні потоки, такі як HTTP-потоки, пом’якшуються за допомогою таких методів, як JavaScript challenges та обмеження швидкості, часто через WAF. Безперервний моніторинг трафіку допомагає швидко виявляти атаки. Деякі сервіси пропонують доступ до команди екстреного реагування для більш складних ситуацій. Функції обмеження швидкості та дроселювання контролюють кількість запитів, які клієнт може зробити протягом певного періоду часу, щоб запобігти зловживанням.

Керований захист хмарних корпоративних застосунків від DDoS-атак передбачає використання спеціалізованих сервісів для фільтрації шкідливого трафіку, перш ніж він досягне корпоративних застосунків. Ці сервіси, що пропонуються хмарними постачальниками, такими як AWS, Azure та Google Cloud, а також сторонніми постачальниками, забезпечують безперервний моніторинг, автоматичне очищення трафіку та пом'якшення наслідків у режимі реального часу, щоб забезпечити безперервність бізнесу та запобігти перебоям у роботі сервісів.

Ключові компоненти включають постійний моніторинг трафіку, автоматичне реагування на загрози та часто можливість масштабування захисту за потреби.

Ключові компоненти керованого захисту від DDoS-атак:

постійний моніторинг трафіку. Сервіси постійно відстежують трафік вашої програми на наявність незвичайних закономірностей, які можуть свідчити про DDoS-атаку;

автоматизоване реагування. Коли виявляється атака, система автоматично вживає заходів, таких як перенаправлення та очищення шкідливого трафіку, щоб нейтралізувати загрозу, перш ніж вона зможе вплинути на корпоративний додаток;

глобальні центри очищення. Хмарні рішення використовують мережу глобальних центрів для фільтрації шкідливого трафіку, перш ніж він досягне корпоративних серверів, процес, відомий як очищення трафіку;

масштабованість. Керовані сервіси розроблені для автоматичного масштабування для обробки масштабних атак, гарантуючи, що корпоративний додаток залишається доступною навіть під час пікового навантаження;

захист на рівні додатків. Окрім атак на мережевому рівні, ці сервіси також можуть захищати від атак на рівні додатків, таких як HTTP-флуд, часто шляхом інтеграції з брандмауерами веб-додатків (WAF).

Приклади керованих сервісів:

Amazon Web Services (AWS) Shield пропонує як автоматичний вбудований захист (стандартний), так і платний сервіс (розширений) з розширеними можливостями, такими як експертні рекомендації та автоматичне пом’якшення складних атак.

Azure DDoS Protection захищає сервіси, розгорнуті у віртуальній мережі, за допомогою цілодобового моніторингу та автоматизованих відповідей.

Google Cloud Armor допомагає захистити додатки в Google Cloud, локально або в інших хмарах від DDoS-атак та інших веб-загроз.

Cloudflare, Akamai та Netscout, пропонують спеціалізований керований захист від DDoS-атак для підприємств.

Розподілені атаки типу «відмова в обслуговуванні» (DDoS) є одними з

найбільших проблем доступності та безпеки, з якими стикаються клієнти, що переносять свої програми в хмару. DDoS-атака намагається вичерпати ресурси програми, роблячи її недоступною для законних користувачів. DDoS-атаки можуть бути спрямовані на будь-яку кінцеву точку, яка є загальнодоступною через Інтернет [3].

Azure DDoS Protection у поєднанні з найкращими практиками проектування додатків забезпечує розширені функції пом'якшення DDoS-атак для захисту від DDoS-атак. Він автоматично налаштовується для захисту конкретних ресурсів Azure у віртуальній мережі. Захист легко ввімкнути в будь-якій новій або існуючій віртуальній мережі, і він не вимагає змін у додатках чи ресурсах [3].

Azure DDoS Protection забезпечує захист на мережевих рівнях 3 та 4. Для захисту веб-застосунків на рівні 7 потрібно додати захист на рівні застосунку за допомогою пропозиції WAF.

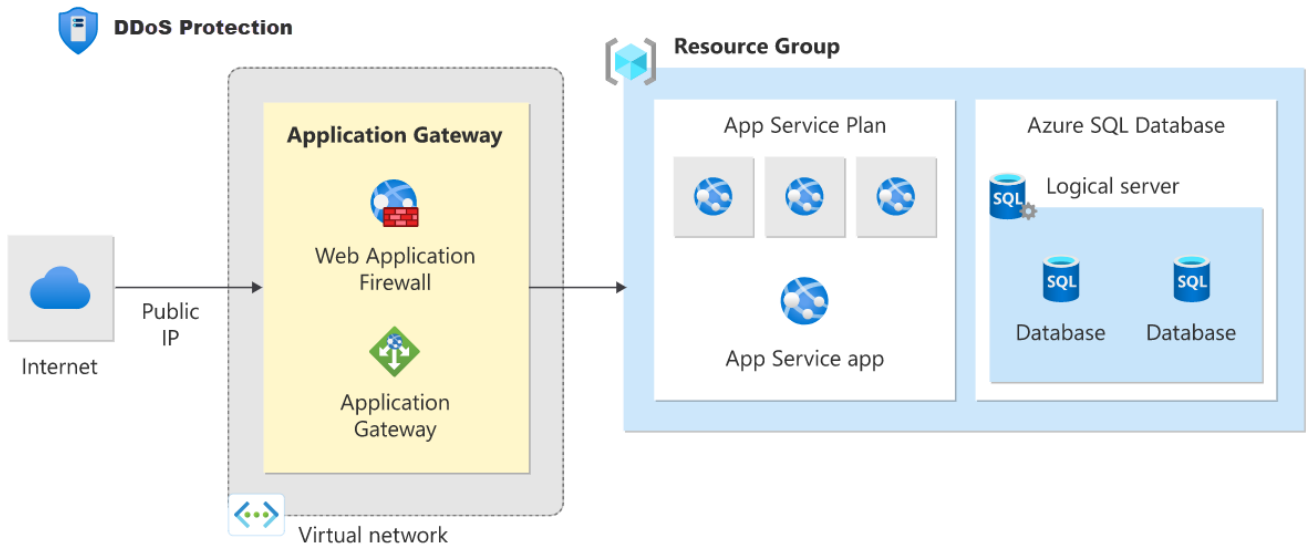

Рис. 1.2. Архітектура Azure DDoS Protection [3]

Azure DDoS Protection це один із сервісів, що входять до категорії «Мережева безпека» в Azure. Інші сервіси цієї категорії включають Azure Firewall та Azure Web Application Firewall. Кожен сервіс має свої унікальні функції та варіанти використання.

Захист мережі Azure DDoS у поєднанні з найкращими практиками проектування застосунків забезпечує розширені функції пом’якшення наслідків DDoS-атак. Він автоматично налаштовується для захисту конкретних ресурсів Azure у віртуальній мережі.

Захист DDoS IP – це модель оплати за захищений IP. Захист DDoS IP містить ті ж основні інженерні функції, що й захист мережі DDoS, але відрізнятиметься такими додатковими послугами: підтримка швидкого реагування на DDoS, захист витрат і знижки на WAF.

Основні характеристики Azure DDoS Protection [3]:

постійний моніторинг трафіку. Трафік корпоратинвих додатків контролюється 24 години на добу, 7 днів на тиждень, шукаючи ознаки DDoS-атак. Azure DDoS Protection миттєво та автоматично пом’якшує атаку після її виявлення;

адаптивне налаштування в режимі реального часу. Інтелектуальне профілювання трафіку вивчає трафік корпоративного додатка з часом, а також вибирає та оновлює профіль, який найкраще підходить для нього. Профіль коригується відповідно до змін трафіку з часом;

аналітика, метрики та сповіщення захисту від DDoS-атак. Azure DDoS Protection застосовує три автоматично налаштовані політики пом’якшення наслідків (TCP SYN, TCP та UDP) для кожної публічної IP-адреси захищеного ресурсу у віртуальній мережі, в якій увімкнено DDoS-атаки. Порогові значення політик налаштовуються автоматично за допомогою профілювання мережевого трафіку на основі машинного навчання. Пом’якшення наслідків DDoS-атак відбувається для IP-адреси, що піддається атаці, лише коли перевищено поріг політики;

аналітика атак. Надання детальних звітів з інтервалом у п’ять хвилин під час атаки та повний зведений звіт після завершення атаки. Передавання журналів процесу пом’якшення наслідків до Microsoft Sentinel або автономній системі керування інформацією та подіями безпеки (SIEM) для моніторингу майже в режимі реального часу під час атаки;

метрики атаки. Зведені метрики кожної атаки доступні через Azure Monitor;

сповіщення про атаки. Сповіщення можна налаштувати на початку та в кінці атаки, а також протягом її тривалості, використовуючи вбудовані метрики атаки. Сповіщення інтегруються у корпоративне операційне програмне забезпечення, таке як журнали Microsoft Azure Monitor, Splunk, Azure Storage, електронна пошта та портал Azure;

швидке реагування на DDoS-атаки Azure. Під час активної атаки клієнти з увімкненим захистом мережі Azure DDoS мають доступ до команди швидкого реагування на DDoS-атаки (DRR), яка може допомогти з розслідуванням атаки під час атаки та аналізом після атаки;

інтеграція з власною платформою. Включає налаштування через портал Azure. Azure DDoS Protection розуміє ваші ресурси та їх конфігурацію;

захист «під ключ». Спрощена конфігурація миттєво захищає всі ресурси віртуальної мережі, щойно ввімкнено захист мережі від DDoS. Не потрібно втручання чи визначення користувача. Аналогічно, спрощена конфігурація миттєво захищає публічний IP-ресурс, коли для нього ввімкнено захист IP-адрес від DDoS;

багаторівневий захист. Коли розгортається разом із брандмауером веб-застосунків (WAF), Azure DDoS Protection захищає як на мережевому рівні (рівні 3 та 4, що пропонуються Azure DDoS Protection), так і на рівні застосунків (рівень 7, що пропонується WAF). Пропозиції WAF включають Azure Application Gateway WAF SKU та пропозиції брандмауерів веб-застосунків сторонніх розробників, доступні на Azure Marketplace;

широкий масштаб пом’якшення наслідків. Усі вектори атак L3/L4 можна пом’якшити за допомогою глобальних можливостей для захисту від найбільших відомих DDoS-атак.

Cloud Armor допомагає захистити ваші розгортання Google Cloud від різних типів загроз, включаючи розподілені атаки типу «відмова в обслуговуванні» (DDoS) та атаки на програми, такі як міжсайтовий скриптинг (XSS) та SQL-інєкції (SQLi). Cloud Armor має деякі автоматичні засоби захисту, а також деякі, які потрібно налаштувати вручну. Цей документ містить загальний огляд цих функцій,

деякі з яких доступні лише для глобальних зовнішніх балансувальників навантаження програм та класичних балансувальників навантаження програм.

У Cloud Armor використовуються політики безпеки для захисту програм, що працюють за балансувальником навантаження, від розподілених атак типу «відмова в обслуговуванні» (DDoS) та інших веб-атак, незалежно від того, чи розгорнуті програми в Google Cloud, у гібридному розгортанні чи в багатохмарній архітектурі. Політики безпеки можна налаштувати вручну, з налаштовуваними умовами відповідності та діями в політиці безпеки. Cloud Armor також має попередньо налаштовані політики безпеки, які охоплюють різноманітні випадки використання. Для отримання додаткової інформації див. огляд політики безпеки Cloud Armor [11].

Cloud Armor дозволяє визначати пріоритетні правила з налаштовуваними умовами збігу та діями в політиці безпеки. Правило набуває чинності, тобто застосовується налаштована дія, якщо це правило має найвищий пріоритет, атрибути якого відповідають атрибутам вхідного запиту.

Попередньо налаштовані правила WAF від Cloud Armor – це складні правила брандмауера веб-застосунків (WAF) з десятками сигнатур , складених з галузевих стандартів з відкритим кодом. Кожна сигнатура відповідає правилу виявлення атаки в наборі правил. Ці правила пропонуються «як є». Правила дозволяють Cloud Armor оцінювати десятки різних сигнатур трафіку, звертаючись до зручно названих правил, а не вимагати від вас визначення кожної сигнатури вручну [11].

Попередньо налаштовані правила Cloud Armor допомагають захистити корпоративні веб-програми та сервіси від поширених атак з Інтернету та зменшити ризики, що входять до топ-10 OWASP.

Cloud Armor забезпечує постійний захист від DDoS-атак у мережевих або протокольних волюметричних DDoS-атак. Цей захист призначений для програм або служб, що знаходяться за балансувальниками навантаження. Він здатний виявляти та пом’якшувати мережеві атаки, щоб пропускати лише правильно сформовані запити через проксі-сервери балансування навантаження. Політики безпеки застосовують користувацькі політики фільтрації рівня 7, включаючи

попередньо налаштовані правила WAF, які зменшують ризики вразливості веб-застосунків, що входять до топ-10 OWASP. Ми можемо додати політики безпеки до серверних служб таких балансувальників навантаження [11]:

усі зовнішні балансувальники навантаження додатків, включаючи класичні балансувальники навантаження додатків;

регіональний внутрішній балансувальник навантаження додатків;

глобальний зовнішній проксі-сервер балансування мережевого навантаження (TCP/SSL);

класичний проксі-балансер мережевого навантаження (TCP/SSL);

зовнішній розподільник мережевого навантаження (TCP/UDP).

Політики безпеки Cloud Armor дозволяють або забороняють доступ до корпоративного розгортання на периферії Google Cloud, якомога ближче до джерела вхідного трафіку. Це запобігає споживанню ресурсів небажаним трафіком або потраплянню його до корпоративних мереж віртуальної приватної хмари (VPC).

Рисунок 1.3 ілюструє розташування глобальних зовнішніх балансувальників навантаження додатків, класичних балансувальників навантаження додатків, мережі Google та центрів обробки даних Google.

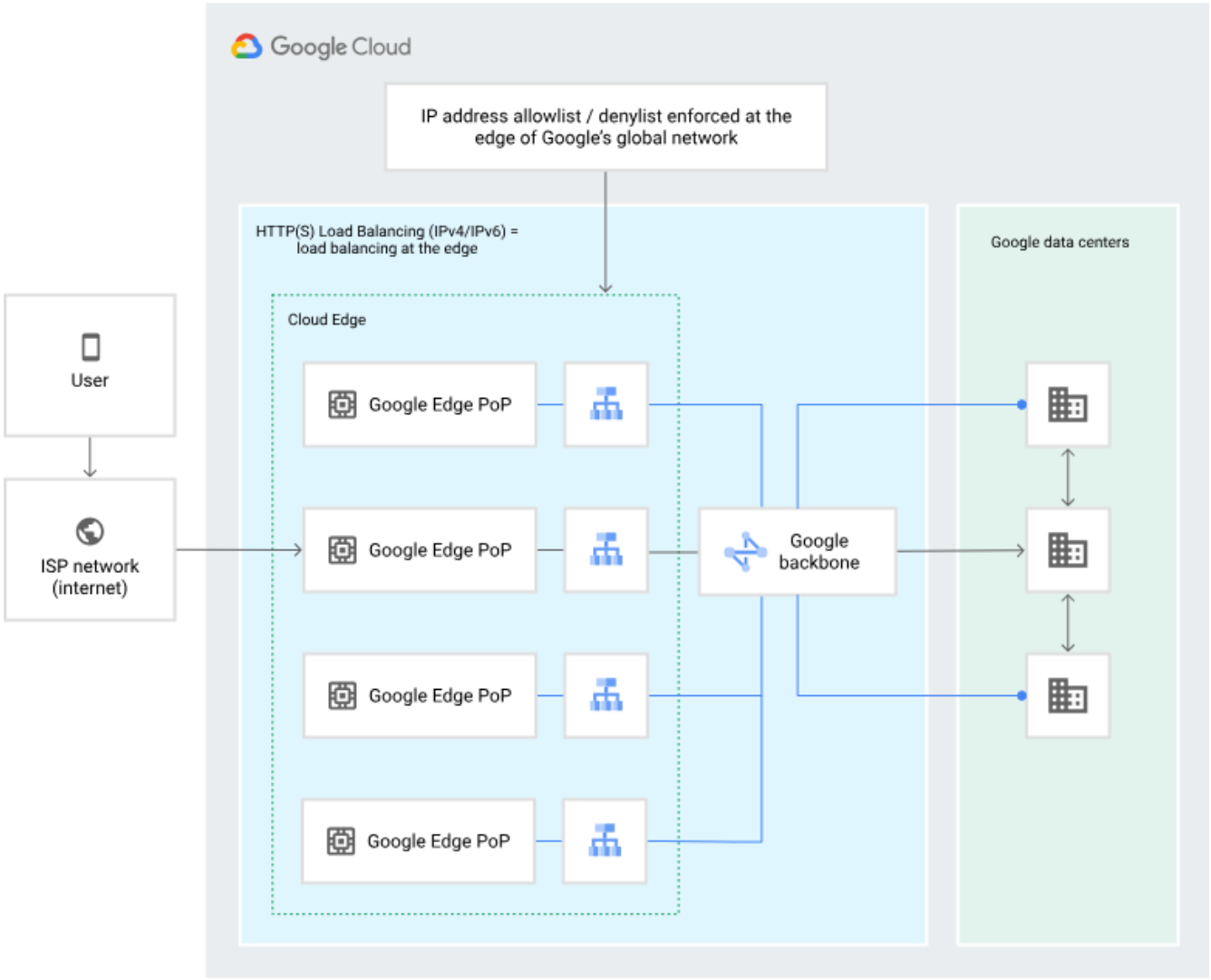

Рис. 1.3. Схема балансувальників навантаження додатків мережі Google та центрів обробки даних Google [11]

Типовий випадок використання для додавання IP-адрес користувачів до білого списку – це коли до корпоративного глобального зовнішнього балансувальника навантаження програм або класичного балансувальника навантаження програм доступ має лише певна група користувачів. На рисунку 1.4 наведено приклад, де лише користувачі з організації мають доступ до служб, що знаходяться за корпоративними балансувальником навантаження.

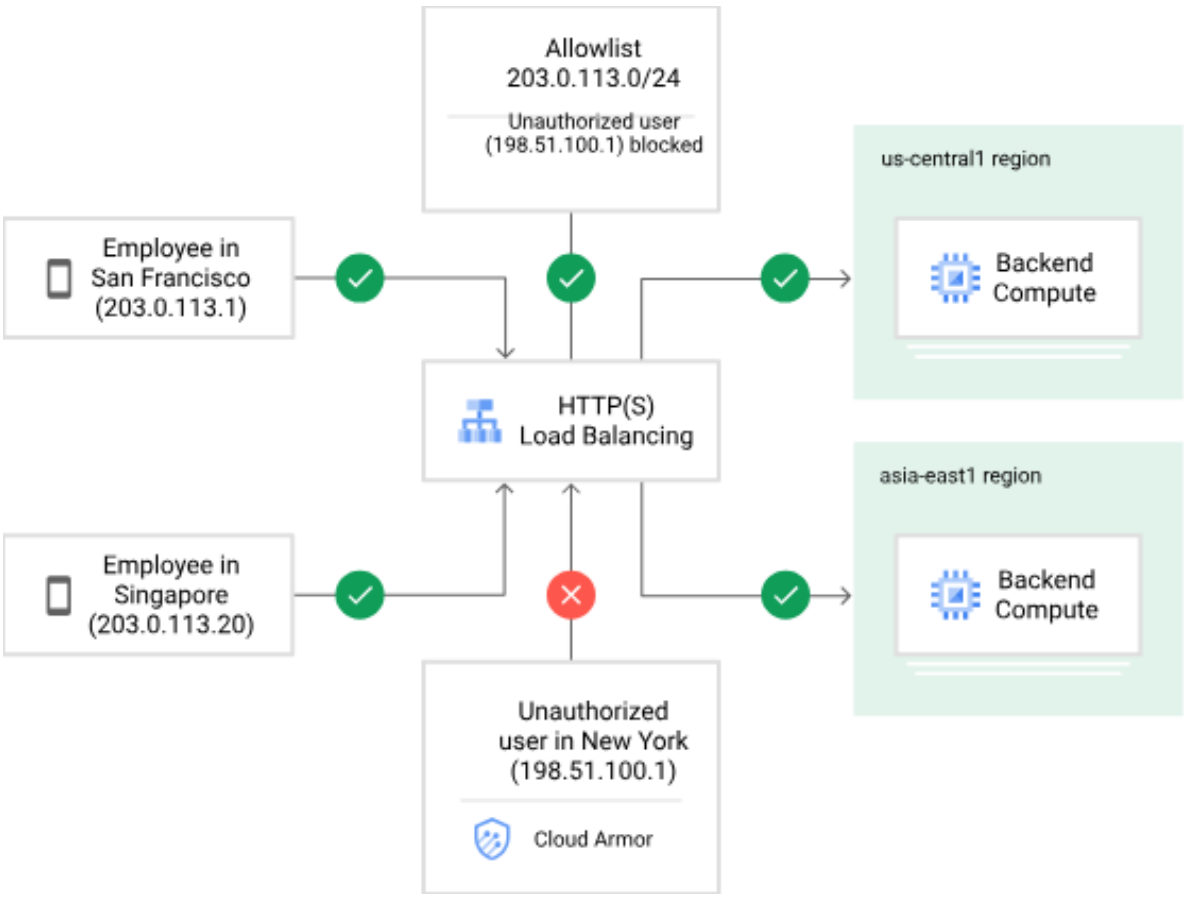

Рис. 1.4. Типовий випадок використання [11]

Цим користувачам призначені IP-адреси або блоки адрес організацією. Ми можете додавати ці IP-адреси або діапазони CIDR до білого списку, щоб лише ці користувачі мали доступ до балансувальника навантаження.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS SHIELD

2.1. Призначення та основні функції рішення AWS Shield

AWS Shield Standard та AWS Shield Advanced забезпечують захист від розподілених атак типу «відмова в обслуговуванні» (DDoS) для ресурсів AWS на мережевому та транспортному рівнях (рівень 3 та 4) і прикладному рівні (рівень 7). DDoS-атака – це атака, під час якої кілька скомпрометованих систем намагаються перевантажити ціль трафіком. DDoS-атака може перешкодити законним кінцевим користувачам отримати доступ до цільових служб і призвести до збою цільової системи через надмірний обсяг трафіку [9].

AWS Shield забезпечує захист від широкого спектру відомих векторів DDoS-атак та векторів атак «нульового дня». Виявлення та пом’якшення загроз Shield розроблено для забезпечення захисту від загроз, навіть якщо вони явно не відомі сервісу на момент виявлення.

Класи атак, які виявляє Shield, включають наступне [9]:

мережеві волюметричні атаки (рівень 3) – це підкатегорія векторів атак на рівні інфраструктури. Ці вектори намагаються перевантажити потужність цільової мережі або ресурсу, щоб відмовити в обслуговуванні легітимним користувачам;

атаки мережевого протоколу (рівень 4) – це підкатегорія векторів атак інфраструктурного рівня. Ці вектори зловживають протоколом, щоб відмовити в обслуговуванні цільового ресурсу. Поширеним прикладом атаки мережевого протоколу є перевантаження TCP SYN, яке може виснажити стан з’єднання на таких ресурсах, як сервери, балансувальники навантаження або брандмауери. Атака мережевого протоколу також може бути об’ємною. Наприклад, більша перевантаження TCP SYN може мати на меті перевантажити пропускну здатність мережі, одночасно виснажуючи стан цільового ресурсу або проміжних ресурсів;

атаки на рівні додатків (рівень 7) – ця категорія векторів атаки намагається відмовити в обслуговуванні легітимним користувачам шляхом перевантаження додатка запитами, які є дійсними для цілі, наприклад, перевантаженням веб-запитів.

AWS Shield – це керована служба захисту від загроз, яка захищає периметр корпоративного додатка. Периметр – це перша точка входу для трафіку додатка, що надходить з-за меж мережі AWS. Щоб визначити, де знаходиться периметр корпоративного додатка, треба подивитися, як користувачі отримують доступ до корпоративного додатка з Інтернету. Якщо перша точка входу знаходиться в регіоні AWS, то периметр додатка – це корпоративна віртуальна приватна хмара Amazon (VPC). Якщо користувачі перенаправляються до корпоративного додатка через Amazon Route 53 і спочатку отримують доступ до додатка за допомогою Amazon CloudFront або AWS Global Accelerator, то периметр додатка починається на межі мережі AWS [9].

Shield забезпечує переваги виявлення та пом’якшення DDoS-атак для всіх додатків, що працюють на AWS, але рішення, які приймаються під час проектування архітектури корпоративного додатка, впливатимуть на рівень стійкості до DDoS. Стійкість до DDoS – це здатність корпоративного додатка продовжувати працювати в межах очікуваних параметрів під час атаки.

Усі клієнти AWS отримують переваги автоматичного захисту Shield Standard без додаткової плати. Shield Standard захищає від найпоширеніших, найчастіших DDoS-атак мережевого та транспортного рівня, спрямованих на ваш веб-сайт або програми. Хоча Shield Standard допомагає захистити всіх клієнтів AWS, ми отримуємо особливі переваги завдяки розміщеним зонам Amazon Route 53, дистрибутивам Amazon CloudFront та стандартним акселераторам AWS Global Accelerator. Ці ресурси отримують комплексний захист доступності від усіх відомих атак мережевого та транспортного рівня [9].

Shield Advanced забезпечує розширений захист від DDoS-атак для корпоративних екземплярів Amazon EC2, балансувальників навантаження Elastic Load Balancing, дистрибутивів CloudFront, розміщених зон Route 53 та стандартних

акселераторів AWS Global Accelerator. Опції та функції Shield Advanced включають автоматичне пом’якшення DDoS-атак на рівні додатків, розширену видимість подій та спеціальну підтримку від команди реагування Shield (SRT) [9].

AWS Shield Advanced забезпечує розширений захист від багатьох типів атак. У наступному списку описано деякі поширені типи атак [9]:

атаки відбиття протоколу користувацьких дейтаграм (UDP). Під час атак на основі відбиття UDP зловмисник може підробити джерело запиту та використовувати UDP для отримання великої кількості даних від сервера. Додатковий мережевий трафік, спрямований на підроблену атаковану IP-адресу, може уповільнити роботу цільового сервера та перешкодити законним кінцевим користувачам отримати доступ до необхідних ресурсів;

TCP SYN-флуд. Метою атаки TCP SYN flood є виснаження доступних ресурсів системи, залишаючи з’єднання у напіввідкритому стані. Коли користувач підключається до TCP-сервісу, такого як веб-сервер, клієнт надсилає пакет TCP SYN. Сервер повертає підтвердження, а клієнт повертає своє власне підтвердження, завершуючи тристороннє рукостискання. Під час атаки TCP SYN flood третє підтвердження ніколи не повертається, і сервер залишається в очікуванні відповіді. Це може перешкодити іншим користувачам підключитися до сервера;

потоки DNS-запитів. Під час перевантаження DNS-запитами зловмисник використовує кілька DNS-запитів, щоб вичерпати ресурси DNS-сервера. AWS Shield Advanced може допомогти забезпечити захист від атак перевантаження DNS-запитами на DNS-сервери Route 53;

атаки HTTP-флуд/вимкнення кешу (рівень 7). Під час HTTP-флуду, включаючи GET та POST, зловмисник надсилає кілька HTTP-запитів, які виглядають як від реального користувача веб-застосунку. Атаки з використанням кеш-бустингу – це тип HTTP-флуду, який використовує варіації в рядку запиту HTTP, що запобігають використанню кешованого контенту, розташованого на периферії, та змушує контент обслуговуватися з веб-сервера джерела, що створює додаткове та потенційно шкідливе навантаження на веб-сервер джерела.

2.2. Архітектура рішення AWS Shield

AWS Shield Standard та AWS Shield Advanced забезпечують захист від розподілених DDoS-атак для ресурсів AWS на мережевому та транспортному рівнях (рівень 3 та 4) і прикладному рівні (рівень 7) [9].

AWS Shield забезпечує захист від широкого спектру відомих векторів DDoS-атак та векторів атак «нульового дня». Виявлення та пом'якшення загроз AWS Shield розроблено для забезпечення захисту від загроз, навіть якщо вони явно не відомі сервісу на момент виявлення. Класи атак, які виявляє AWS Shield, включають [9]:

мережеві об'ємні атаки (рівень 3) – це підкатегорія векторів атак на рівні інфраструктури. Ці вектори намагаються перевантажити потужність цільової мережі або ресурсу, щоб відмовити в обслуговуванні легітимним користувачам;

атаки мережевого протоколу (рівень 4) – це підкатегорія векторів атак інфраструктурного рівня. Ці вектори зловживають протоколом, щоб відмовити в обслуговуванні цільового ресурсу. Поширеним прикладом атаки мережевого протоколу є перевантаження TCP SYN, яке може виснажити стан з'єднання на таких ресурсах, як сервери, балансувальники навантаження або брандмауери. Атака мережевого протоколу також може бути об'ємною. Наприклад, більша перевантаження TCP SYN може мати на меті перевантажити пропускну здатність мережі, одночасно виснажуючи стан цільового ресурсу або проміжних ресурсів;

атаки на рівні додатків (рівень 7) – ця категорія векторів атаки намагається відмовити в обслуговуванні легітимним користувачам шляхом перевантаження додатка запитами, які є дійсними для цілі, наприклад, перевантаженням веб-запитів.

Розглянемо приклад архітектури, яка забезпечує максимальну стійкість до DDoS-атак за допомогою веб-застосунків AWS.

Ми можемо створити веб-застосунок у будь-якому регіоні AWS та отримати автоматичний захист від DDoS-атак завдяки можливостям виявлення та пом'якшення наслідків, які AWS надає в цьому регіоні [9].

Цей приклад стосується архітектур, які спрямовують користувачів до веб-застосунку за допомогою таких ресурсів, як класичні балансувальники навантаження, балансувальники навантаження застосунків, балансувальники мережевого навантаження, рішення AWS Marketplace або корпоративний власний проксі-рівень. Ми можемо покращити стійкість до DDoS-атак, вставивши зони розміщення Amazon Route 53, дистрибутиви Amazon CloudFront та веб-списки ACL AWS WAF між цими ресурсами веб-застосунків та корпоративними користувачами. Ці вставки можуть приховати походження застосунку, обслуговувати запити ближче до корпоративних кінцевих користувачів, а також виявляти та пом’якшувати перевантаження запитів на рівні застосунків. Застосунки, які надають статичний або динамічний контент користувачам за допомогою CloudFront та Route 53, захищені інтегрованою, повністю вбудованою системою пом’якшення DDoS-атак, яка пом’якшує атаки на рівні інфраструктури в режимі реального часу [9].

Завдяки цим архітектурним покращенням ми можемо захистити свої зони, розміщені на Route 53, та дистрибутиви CloudFront за допомогою Shield Advanced. Під час захисту дистрибутивів CloudFront Shield Advanced пропонує пов’язати веб-списки ACL AWS WAF та створити для них правила на основі тарифів, а також надає нам можливість увімкнути автоматичне пом’якшення DDoS-атак на рівні додатків або проактивну взаємодію. Проактивна взаємодія та автоматичне пом’якшення DDoS-атак на рівні додатків використовують перевірки справності Route 53, які пов’язуються з ресурсом [9].

На рисунку 2.1 зображено стійку до DDoS-атак архітектуру для веб-застосунку.

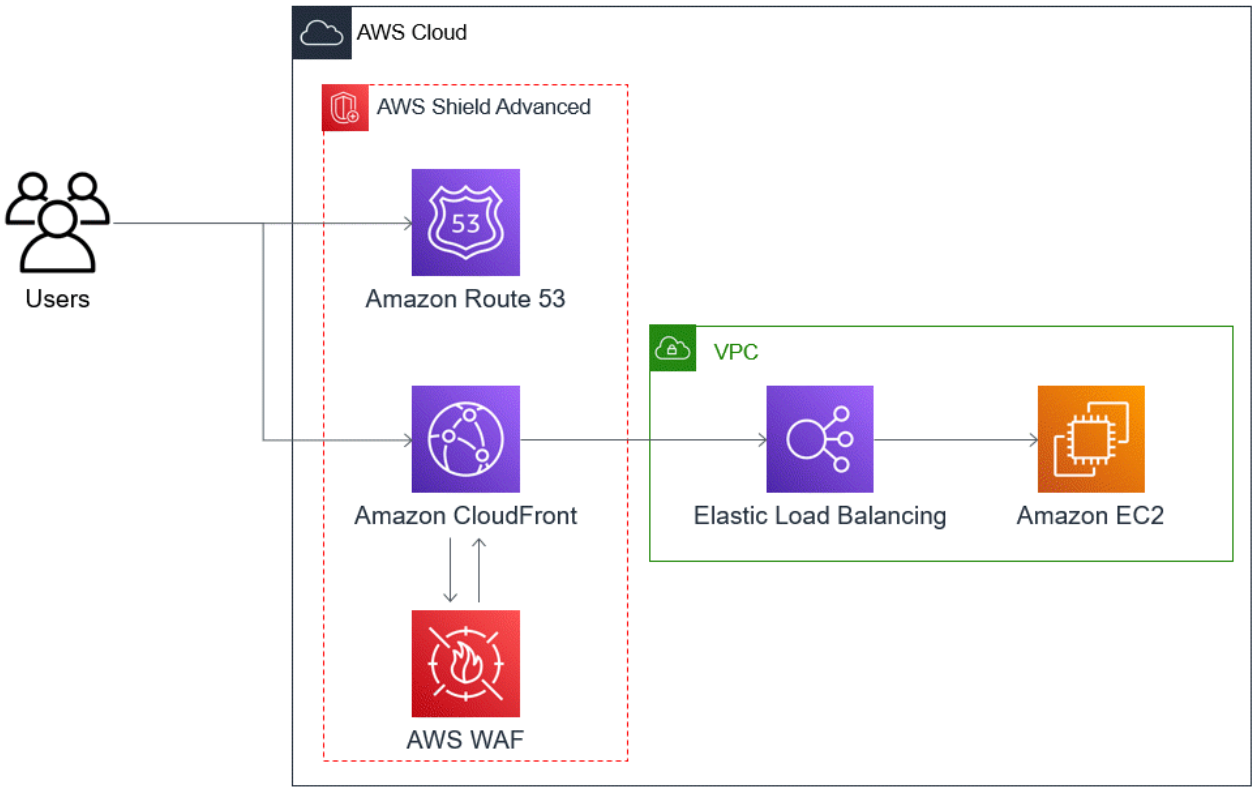

Рис. 2.1. Стійка до DDoS-атак архітектура для веб-застосунку [9]

Переваги, які цей підхід надає корпоративному веб-застосунку, включають наступне [9]:

захист від DDoS-атак, що часто використовуються на рівні інфраструктури (рівень 3 та рівень 4), без затримки виявлення. Крім того, якщо ресурс часто є мішенню, Shield Advanced застосовує заходи захисту на триваліші періоди часу. Shield Advanced також використовує контекст додатка, отриманий з мережевих ACL (NACL), для блокування небажаного трафіку далі по черзі. Це ізолює збої ближче до їх джерела, мінімізуючи вплив на законних користувачів;

захист від перевантажень TCP SYN. Системи пом'якшення DDoS-атак, інтегровані з CloudFront, Route 53 та AWS Global Accelerator, забезпечують можливість проксі-сервера TCP SYN, яка перевіряє нові спроби підключення та обслуговує лише легітимних користувачів;

захист від атак на рівні додатків DNS, оскільки Route 53 відповідає за обслуговування авторитетних відповідей DNS;

захист від перевантаження запитами на рівні веб-застосунків. Правило на

основі тарифу, яке ви налаштовуєте у своєму веб-списку контролю доступу AWS WAF, блокує вихідні IP-адреси, коли вони надсилають більше запитів, ніж дозволяє правило;

автоматичне пом'якшення DDoS-атак на рівні додатків для корпоративних дистрибутивів CloudFront, якщо ви ввімкнете цю опцію. Завдяки автоматичному пом'якшенню DDoS-атак Shield Advanced підтримує правило на основі частоти у пов'язаному з дистрибутивом веб-списку контролю доступу AWS WAF, яке обмежує обсяг запитів від відомих джерел DDoS. Крім того, коли Shield Advanced виявляє подію, яка впливає на справність корпоративного додатка, він автоматично створює, тестує та керує правилами пом'якшення у веб-списку контролю доступу;

проактивна взаємодія з командою реагування Shield (SRT), якщо ми вмикаємо цю опцію. Коли Shield Advanced виявляє подію, яка впливає на працездатність корпоративного додатка, SRT реагує та проактивно взаємодіє з командами безпеки або операцій, використовуючи надану контактну інформацію. SRT аналізує закономірності у корпоративному трафіку та може оновлювати правила AWS WAF, щоб блокувати атаку.

2.3. Порядок функціонування рішення AWS Shield

Розглянемо логіку виявлення загроз на рівні інфраструктури (рівень 3 та рівень 4) за допомогою AWS Shield.

Логіка виявлення, що використовується для захисту цільових ресурсів AWS від DDoS-атак на рівнях інфраструктури (рівень 3 та рівень 4), залежить від типу ресурсу та від того, чи захищений ресурс за допомогою AWS Shield Advanced.

Виявлення для Amazon CloudFront та Amazon Route 53

Коли ми обслуговуємо свій веб-застосунок за допомогою CloudFront та Route 53, усі пакети, що надходять до застосунку, перевіряються повністю вбудованою системою запобігання DDoS-атакам, яка не створює жодної помітної затримки. DDoS-атаки на дистрибутиви CloudFront та зони, розміщені на Route 53, запобігаються в режимі реального часу. Ці засоби захисту застосовуються

незалежно від того, чи використовуєте ви AWS Shield Advanced [9].

Необхідно дотримуватися найкращих практик використання CloudFront та Route 53 як точки входу корпоративного веб-застосунку, де це можливо, для найшвидшого виявлення та усунення наслідків DDoS-подій.

Виявлення для AWS Global Accelerator та регіональних сервісів

Виявлення на рівні ресурсів захищає стандартні акселератори та ресурси AWS Global Accelerator, запущені в регіонах AWS, такі як класичні балансувальники навантаження, балансувальники навантаження додатків та еластичні IP-адреси (EIP). Ці типи ресурсів відстежуються на наявність підвищеного трафіку, який може свідчити про наявність DDoS-атаки, що потребує заходів щодо зменшення наслідків. Щохвилини оцінюється трафік до кожного ресурсу AWS. Якщо трафік до ресурсу підвищено, виконуються додаткові перевірки для вимірювання його пропускної здатності.

Shield виконує такі стандартні перевірки [9]:

екземпляри Amazon Elastic Compute Cloud (Amazon EC2), EIP, підключені до екземплярів Amazon EC2 – Shield отримує ємність із захищеного ресурсу. Ємність залежить від типу екземпляра цільового об’єкта, розміру екземпляра та інших факторів, таких як те, чи використовує екземпляр розширену мережу;

класичні балансувальники навантаження та балансувальники навантаження додатків – Shield отримує потужність з цільового вузла балансувальника навантаження;

EIP, підключені до балансувальників мережевого навантаження – Shield отримує ємність від цільового балансувальника навантаження. Ємність не залежить від конфігурації групи цільового балансувальника навантаження;

стандартні прискорювачі AWS Global Accelerator – Shield отримує ємність, яка залежить від конфігурації кінцевої точки.

Ці оцінки відбуваються за кількома вимірами мережевого трафіку, такими як порт і протокол. Якщо пропускна здатність цільового ресурсу перевищено, Shield встановлює пом’якшувальні заходи DDoS. Заходи, встановлені Shield, зменшать DDoS-трафік, але можуть не повністю його усунути. Shield також може

встановлювати пом’якшувальні заходи, якщо перевищено частину пропускної здатності ресурсу за виміром трафіку, що відповідає відомим векторам DDoS-атак. Shield встановлює для цих пом’якшувальних заходів обмежений час дії (TTL), який продовжується до тих пір, поки триває атака.

Розглянемо логіку виявлення Shield Advanced для загроз прикладного рівня (рівень 7).

AWS Shield Advanced забезпечує виявлення рівня веб-застосунків для захищених дистрибутивів Amazon CloudFront та балансувальників навантаження застосунків. Захищаючи ці типи ресурсів за допомогою Shield Advanced, ви можете пов’язати веб-список контролю доступу (ACL) AWS WAF зі своїм захистом, щоб увімкнути виявлення рівня веб-застосунків. Shield Advanced використовує дані запитів для пов’язаного веб-списку контролю доступу (ACL) та створює базову лінію трафіку для корпоративного застосунку. Виявлення рівня веб-застосунків залежить від власної інтеграції між Shield Advanced та AWS WAF [9].

Для виявлення на рівні веб-застосунків Shield Advanced відстежує трафік застосунків і порівнює його з історичними базовими показниками, шукаючи аномалії. Цей моніторинг охоплює загальний обсяг і склад трафіку. Під час DDoS-атаки ми очікуємо зміни як обсягу, так і складу трафіку, і Shield Advanced вимагає статистично значущого відхилення в обох показниках, щоб оголосити подію.

Shield Advanced виконує свої вимірювання з урахуванням історичних часових вікон. Такий підхід зменшує кількість хибнопозитивних сповіщень про законні зміни обсягу трафіку або про зміни трафіку, які відповідають очікуваній закономірності, наприклад, про розпродаж, що пропонується щодня в один і той самий час.

Час, який потрібен Shield Advanced для виявлення події, залежить від того, наскільки сильно змінюється обсяг трафіку. Для менших змін обсягу Shield Advanced спостерігає за трафіком протягом тривалішого періоду, щоб переконатися, що подія відбувається. Для більших змін обсягу Shield Advanced виявляє та повідомляє про подію швидше.

Правило на основі частоти атак у веб-списку контролю доступу (ACL),

додане нами чи функцією автоматичного пом’якшення на рівні додатків Shield Advanced, може пом’якшити атаку до того, як вона досягне рівня виявлення.

Розглянемо логіку виявлення Shield Advanced для кількох ресурсів у додатку.

Ми можемо використовувати групи захисту AWS Shield Advanced для створення колекцій захищених ресурсів, що є частиною одного додатка. Ми можемо вибрати, які захищені ресурси розмістити в групі, або вказати, що всі ресурси одного типу повинні розглядатися як одна група. Наприклад, ми можемо створити групу всіх балансувальників навантаження додатків. Під час створення групи захисту функція виявлення Shield Advanced агрегує весь трафік для захищених ресурсів у групі. Це корисно, якщо у нас багато ресурсів, кожен з яких має невеликий обсяг трафіку, але великий сукупний обсяг. Ми також можемо використовувати групи захисту для збереження базових станів додатків, у випадку розгортань, де трафік передається між захищеними ресурсами.

Ми можемо агрегувати трафік у нашій групі захисту одним із наведених нижче способів.

Sum – ця агрегація об’єднує весь трафік між ресурсами в групі захисту. Ми можете використовувати цю агрегацію, щоб переконатися, що новостворені ресурси мають існуючий базовий рівень, і зменшити чутливість виявлення, що може допомогти запобігти хибним спрацьовуванням.

Mean – ця агрегація використовує середнє значення всього трафіку в групі захисту. Цю агрегацію можна використовувати для додатків, де трафік між ресурсами є рівномірним, наприклад, для балансувальників навантаження.

Max – ця агрегація використовує найбільший трафік серед усіх ресурсів у групі захисту. Ми можемо використовувати цю агрегацію, коли в групі захисту є кілька рівнів додатка. Наприклад, у нас може бути група захисту, яка включає дистрибутив CloudFront, його джерело Application Load Balancer та цільові екземпляри Amazon EC2 Application Load Balancer.

Ми також можемо використовувати групи захисту, щоб покращити швидкість, з якою Shield Advanced розміщує засоби пом’якшення, для атак, спрямованих на кілька еластичних IP-адрес, вихідних в Інтернет, або стандартні

прискорювачі AWS Global Accelerator. Коли один ресурс у групі захисту є ціллю, Shield Advanced встановлює довіру для інших ресурсів у групі. Це ставить виявлення Shield Advanced у стан тривоги та може скоротити час, необхідний для створення додаткових засобів пом’якшення.

3 ТЕХНОЛОГІЯ КЕРОВАНОГО ЗАХИСТУ ХМАРНИХ КОРПОРАТИВНИХ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS SHIELD

3.1. Порядок застосування рішення AWS Shield

Важливо розуміти: AWS Shield Standard активується автоматично для всіх клієнтів AWS без додаткової плати. Тому важливим моментом є побудова правильної архітектури, яка дозволить цьому безкоштовному захисту працювати ефективно. Shield Standard захищає лише від атак на рівні мережі та транспорту (L3/L4), тому захист додатку (L7) потребує додаткових зусиль.

Розглянимо порядок побудови ешелонованого захисту на базі AWS Shield Standard.

Етап 1: Архітектурна підготовка (Зменшення поверхні атаки).

Оскільки Shield Standard найкраще працює на глобальній інфраструктурі AWS, необхідно винести точку входу в додаток якомога далі від корпоративних серверів.

Необхідно впровадити Amazon CloudFront. CloudFront використовується як CDN перед корпоративним Application Load Balancer (ALB) або S3.

Shield Standard автоматично розсіює атаки (SYN/UDP floods) на краях мережі (Edge Locations) AWS, не пропускаючи їх до нашого регіону тому, що ємність мережі CloudFront значно перевищує будь-яку атаку.

Необхідно провести приховування Origin-ресурсів. Для цього налаштовуємо Security Groups (мережеві екрани) наших балансувальників та серверів так, щоб вони приймали трафік тільки з діапазонів IP-адрес CloudFront (використовуються AWS Managed Prefix List). Це призведе до того, що зловмисники не зможуть обійти CDN і атакувати IP-адресу сервера напряму.

Використання Route 53. Для DNS використовуємо Amazon Route 53. Shield Standard має вбудований захист для зон Route 53 від найпоширеніших DNS-атак.

Етап 2: Ручний захист L7 (Заміна функцій Advanced).

Shield Standard не захищає від атак рівня додатків (наприклад, HTTP Flood або SQL Injection). Ми повинні закрити цю прогалину самостійно за допомогою AWS WAF.

Розгортання AWS WAF. Підключаємо Web Application Firewall до нашого CloudFront distribution (рекомендовано) або ALB.

Налаштування Rate-Limiting. Створюємо правила, що блокують IP-адреси, які надсилають аномальну кількість запитів (наприклад, понад 1000 за 5 хвилин). Це головний захист від HTTP-флуду, який у версії Advanced робиться автоматично, а тут – вручну.

Геоблокування (за потреби). Якщо наш корпоративний додаток працює лише в Україні/Європі, необхідно заблокувати трафік з інших регіонів через WAF.

Етап 3: Моніторинг та сповіщення.

Shield Standard не надає детальної аналітики про атаки та не має виділеної команди підтримки. Ми повинні налаштувати аналітику самостійно.

CloudWatch Alarms. Налаштовуємо тривоги на метрики CloudFront та ALB:

requests (різкий сплеск запитів)$

4xxErrorRate та *5xxErrorRate* (зростання помилок може свідчити про сканування вразливостей або перевантаження).

Аналіз логів. Вмикаємо логування запитів WAF (WAF Access Logs) та зберігаємо їх у S3 або CloudWatch Logs Insights для розслідування інцидентів постфактум.

Етап 4: Управління масштабуванням та витратами.

Оскільки Shield Standard не компенсує фінансові втрати від масштабування ресурсів під час атаки (на відміну від Advanced), ми маємо контролювати витрати.

AWS Auto Scaling. Налаштовуємо групи автомасштабування (Auto Scaling Groups) для корпоративних EC2 інстансів. Це дозволить додатку «роздутися» і поглинути сплеск трафіку, який пройшов крізь фільтри.

AWS Budgets Alerts. Встановлюємо жорсткі сповіщення про бюджет. DDoS-атака може викликати «Economic Denial of Service» (EDoS) – коли ми платимо за обробку сміттєвого трафіку. Ми повинні дізнатися про це миттєво.

Ліміти масштабування. Встановлюємо розумний максимум (Maximum capacity) для Auto Scaling, щоб атака не призвела до нескінченного створення серверів і гігантського рахунку.

3.2. Технологія вторгнень до хмарних корпоративних ресурсів

Порядок із захисту корпоративних додатків від DDoS-атак з використанням AWS Shield.

Важливо розуміти, що в AWS є два рівні захисту:

AWS Shield Standard: увімкнено автоматично для всіх клієнтів AWS. Захищає від найпоширеніших атак на інфраструктурному рівні (рівні 3 та 4 OSI);

AWS Shield Advanced: платна послуга (підписка ~$3000/міс), яка надає розширений захист, доступ до команди реагування (DRT), фінансові гарантії та безкоштовний AWS WAF.

Оскільки AWS Shield Standard активується автоматично та безкоштовно, «налаштування» захисту насправді означає побудову правильної архітектури, яка дозволяє Shield Standard ефективно працювати. Shield Standard захищає лише на рівнях 3 (мережа) та 4 (транспорт), тому для корпоративних додатків критично важливо вручну додати захист рівня 7 (додаток) за допомогою AWS WAF та правильної маршрутизації.

Розглянемо порядок дій для захисту корпоративного додатку на базі AWS Shield Standard.

Етап 1: Перенесення точки входу на «Edge» (CloudFront)

AWS Shield Standard працює найефективніше, коли трафік проходить через глобальну мережу AWS (Global Edge Network). Не треба виставляти ALB (Application Load Balancer) або EC2 безпосередньо в Інтернет.

Створюємо CloudFront Distribution:

у консолі AWS перейдіть до CloudFront;

натискаємо *Create Distribution*;

вказуємо наш ALB як «*Origin Domain*».

Це потрібно для того, що CloudFront приймає удар DDoS-атаки (наприклад, SYN Flood) на себе, розподіляючи його по сотнях точок присутності (PoP) по всьому світу. Shield Standard на рівні CloudFront має набагато більшу пропускну здатність для фільтрації, ніж на рівні регіонального ALB.

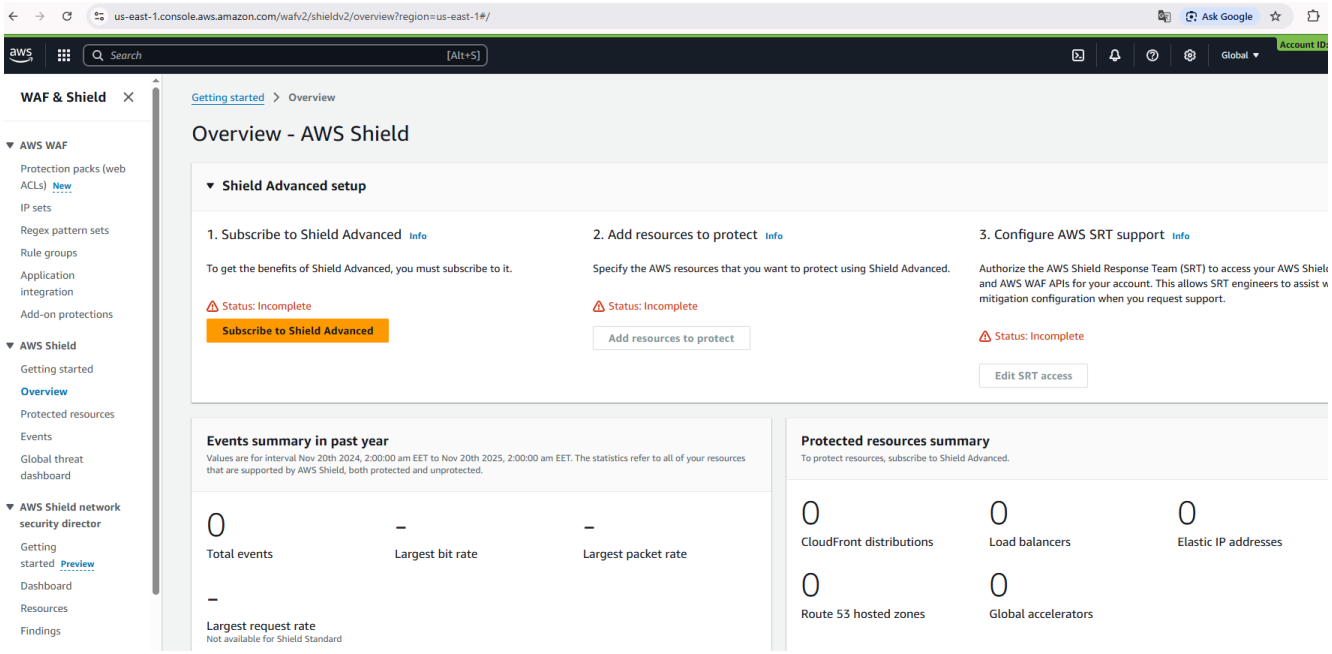

Рис. 3.1. Вкладка Overview – AWS Shield

Етап 2: Блокування прямого доступу (Security Groups)

Якщо зловмисник дізнається IP-адресу нашого балансувальника (ALB), він може атакувати його напряму, обходячи CloudFront і захист Shield:

переходимо у *VPC -> Security Groups*;

знаходимо групу безпеки нашого ALB;

редагуємо *Inbound rules*, для цього:

видаляємо правило, що дозволяє трафік з 0.0.0.0/0 (весь Інтернет);

додаємо правило, що дозволяє трафік тільки від префікс-листа CloudFront (Managed prefix list);

шукаємо в списку Source: *com.amazonaws.global.cloudfront.origin-facing*.

Як результат: тепер наш додаток приймає трафік лише через захищений периметр CloudFront.

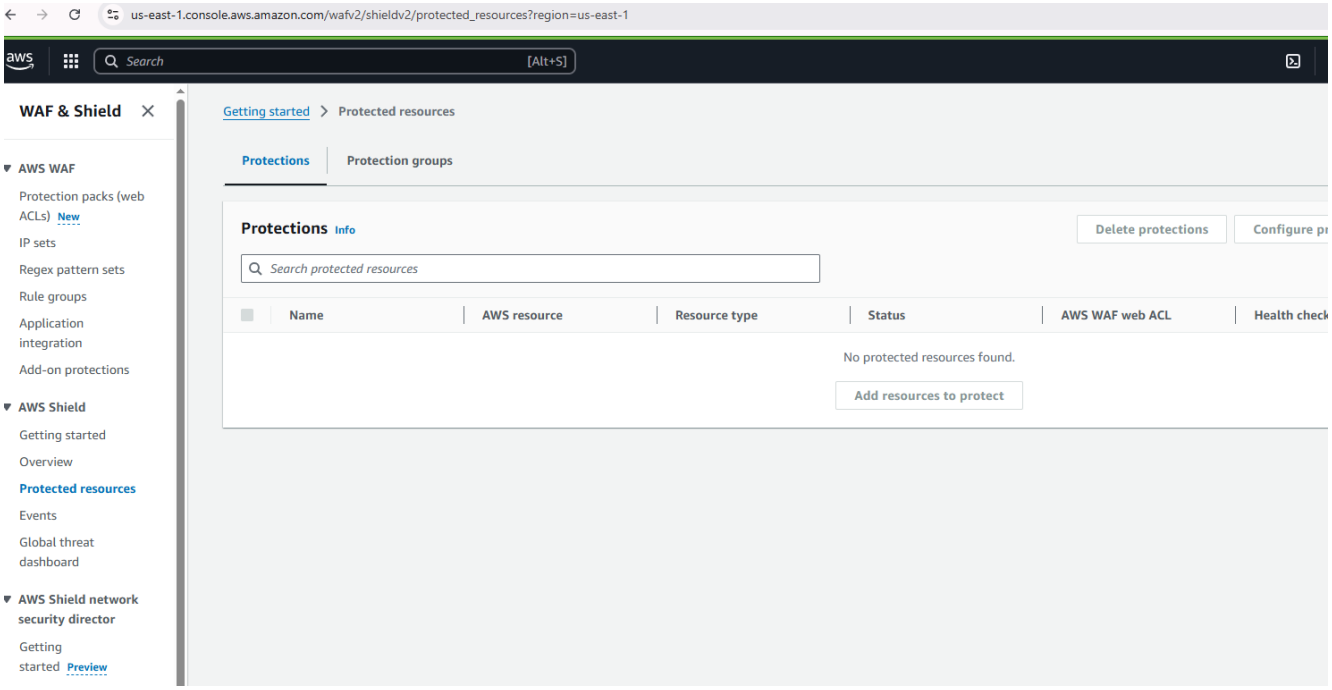

Рис. 3.2. Вкладка Protected resources

Етап 3: Налаштування AWS WAF (Захист рівня 7)

Shield Standard не захищає від HTTP-флуду (коли боти роблять тисячі легітимних запитів, перевантажуючи базу даних). Для цього потрібен AWS WAF (оплачується окремо, але необхідний для Standard).

переходимо у консоль WAF & Shield;

натискаємо *Create Web ACL*;

Resource type: вибераємо *CloudFront distribution* (оскільки ми закрили прямий доступ до ALB).

Add rules, для цього:

вибираємо *Add my own rules and rule groups -> Rule builder*;

Type: Rate-based rule;

Rate limit: встановлюємо ліміт, наприклад, 1000 запитів за 5 хвилин;

Action: Block.

Це приведе до того, що, якщо одна IP-адреса надсилає понад 1000 запитів, WAF автоматично блокує її. Це компенсує відсутність інтелектуального захисту Shield Advanced.

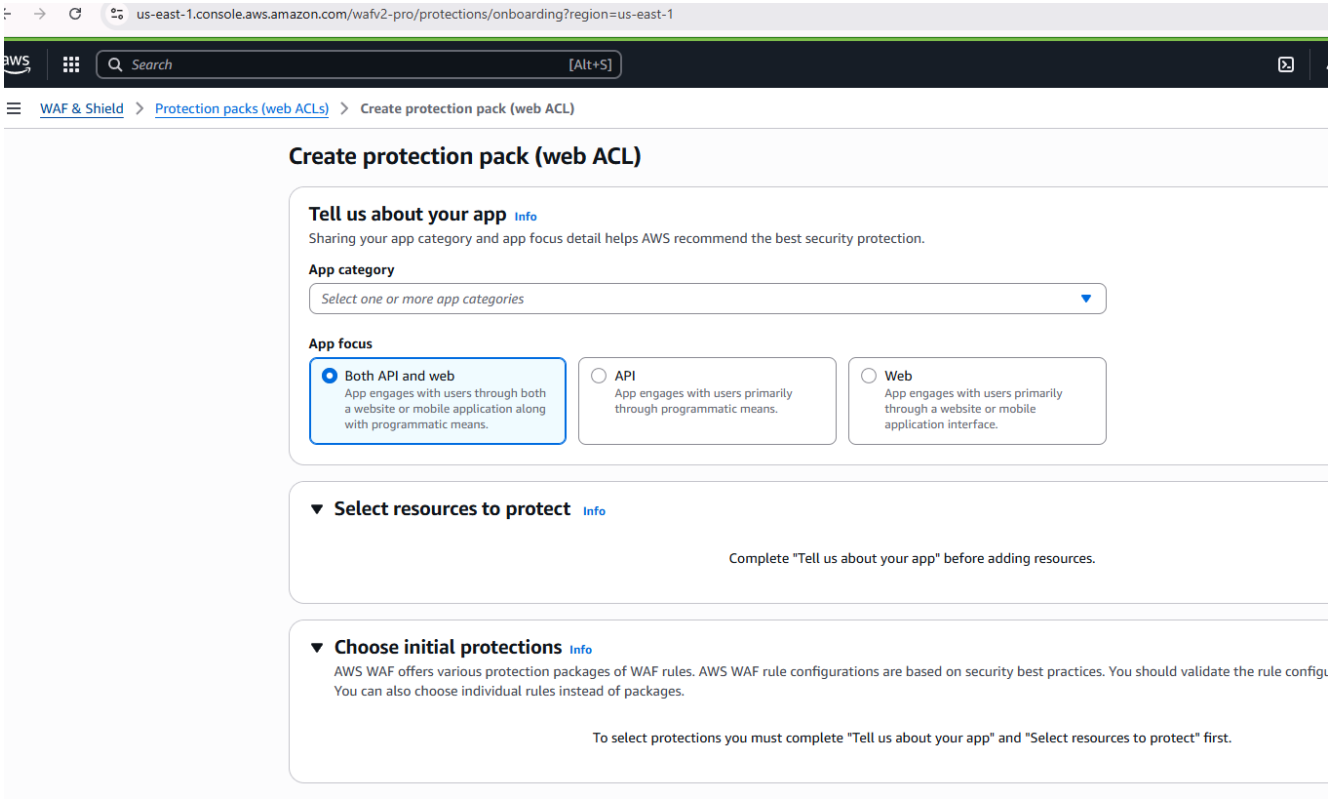

Рис. 3.3. Вкладка Create protection pack (web ACL)

Етап 4: Використання керованих правил (Managed Rules)

Щоб не писати правила вручну для відомих бот-мереж необхідно:

у тому ж меню створення Web ACL натисніть *Add managed rule groups*;

розгортаємо *AWS managed rule groups*;

вмикаємо:

Amazon IP reputation list: блокує відомі IP ботнетів, проксі та тор-вузлів;

Core rule set (CRS): захищає від загальних веб-вразливостей (OWASP Top 10), які часто використовуються паралельно з DDoS.

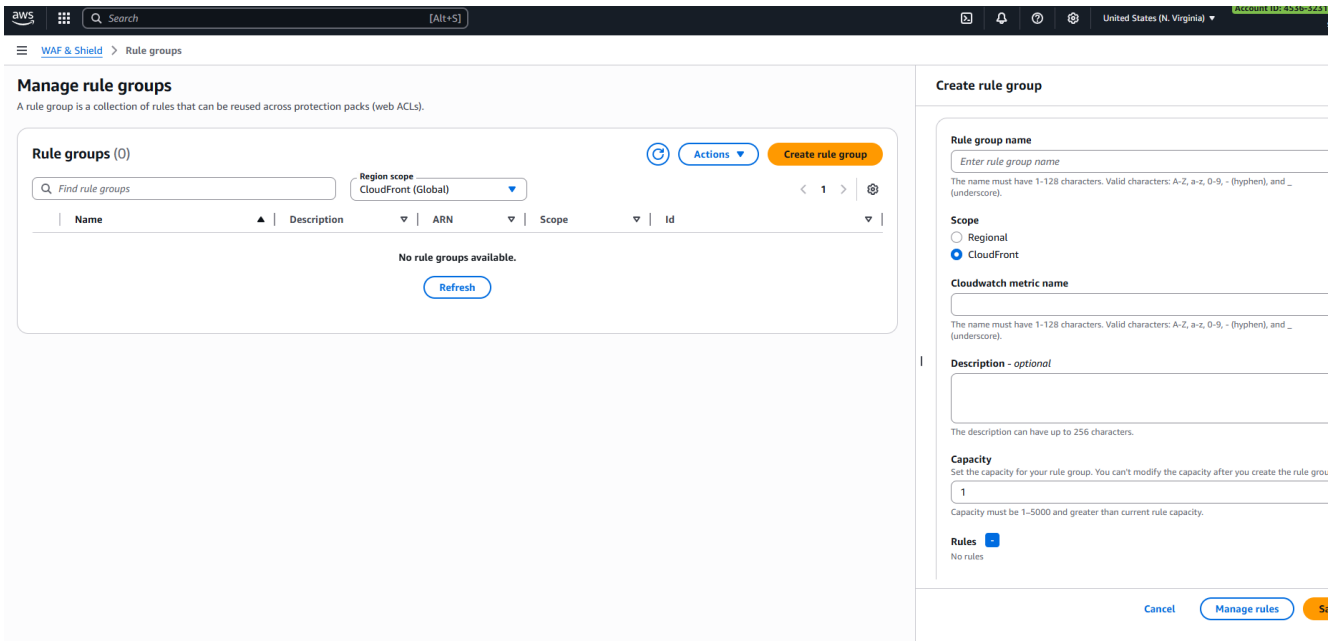

Рис. 3.4. Create rule group

Етап 5: Моніторинг через CloudWatch

Оскільки у версії Standard немає доступу до детальної аналітики DDoS, ми повинні налаштувати власні сповіщення на основі WAF. Для цього:

переходимо у *CloudWatch -> Alarms*;

створюємо сповіщення на метрику *AllowedRequests* та *BlockedRequests* з простору імен *AWS/WAFV2*;

встановлюємо поріг (Threshold). Наприклад, якщо кількість заблокованих запитів різко зростає, то це ознака атаки;

налаштовуємо *SNS Topic* для відправки email-сповіщення адміністратору.

Етап 6: Валідація захисту (Checklist)

Перевіряємо нашу конфігурацію за таблицею 3.1.

Таблиця 3.1

Перелік налаштувань

Компонент	Налаштування	Функція захисту
Route 53	Використовується як DNS	Shield Standard захищає DNS-запити (Layer 3)
CloudFront	Є єдиною точкою входу	Поглинає об'ємні атаки (Syn/UDP Flood)
Security Group	Дозволяє тільки CloudFront IP	Запобігає обходу захисту
AWS WAF	Rate-based Rules + IP Reputation	Блокує HTTP Flood (Layer 7)
Autoscaling	Увімкнено для Backend	Дозволяє пережити сплеск трафіку, що пройшов через фільтри

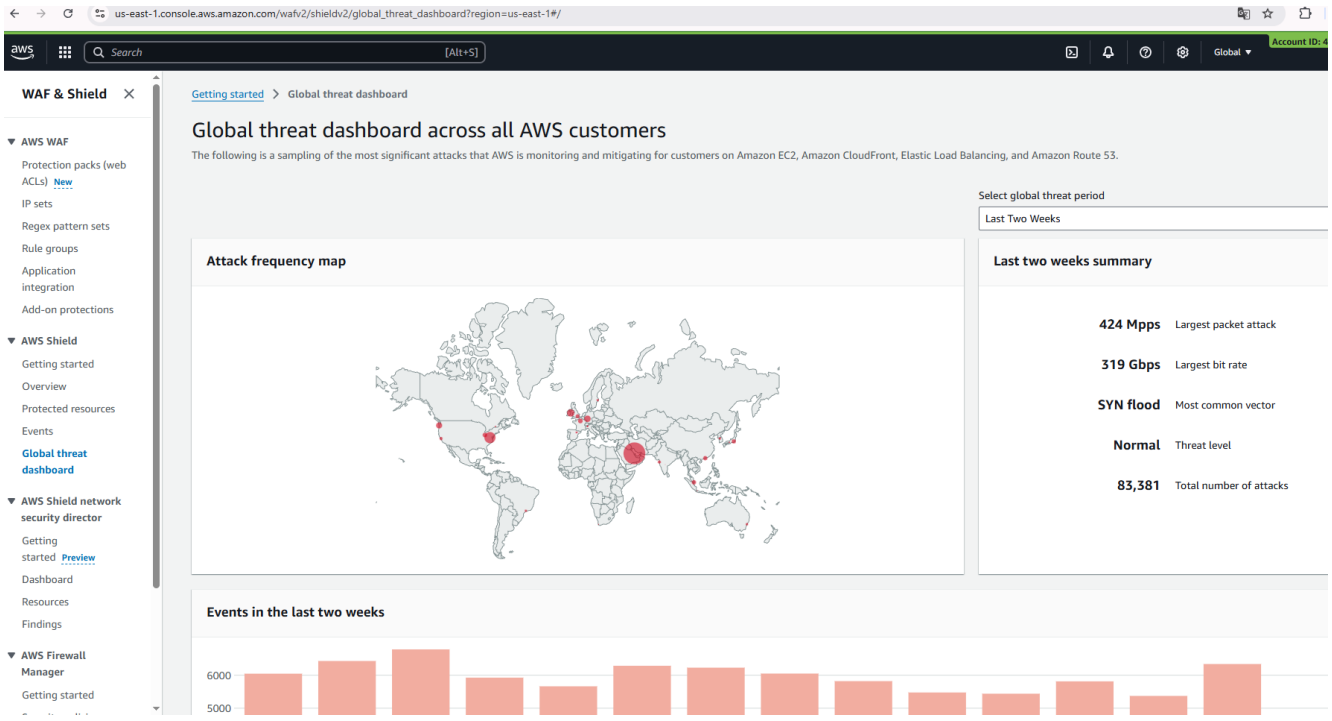

Рис. 3.5. Global threat dashboard across all AWS customers

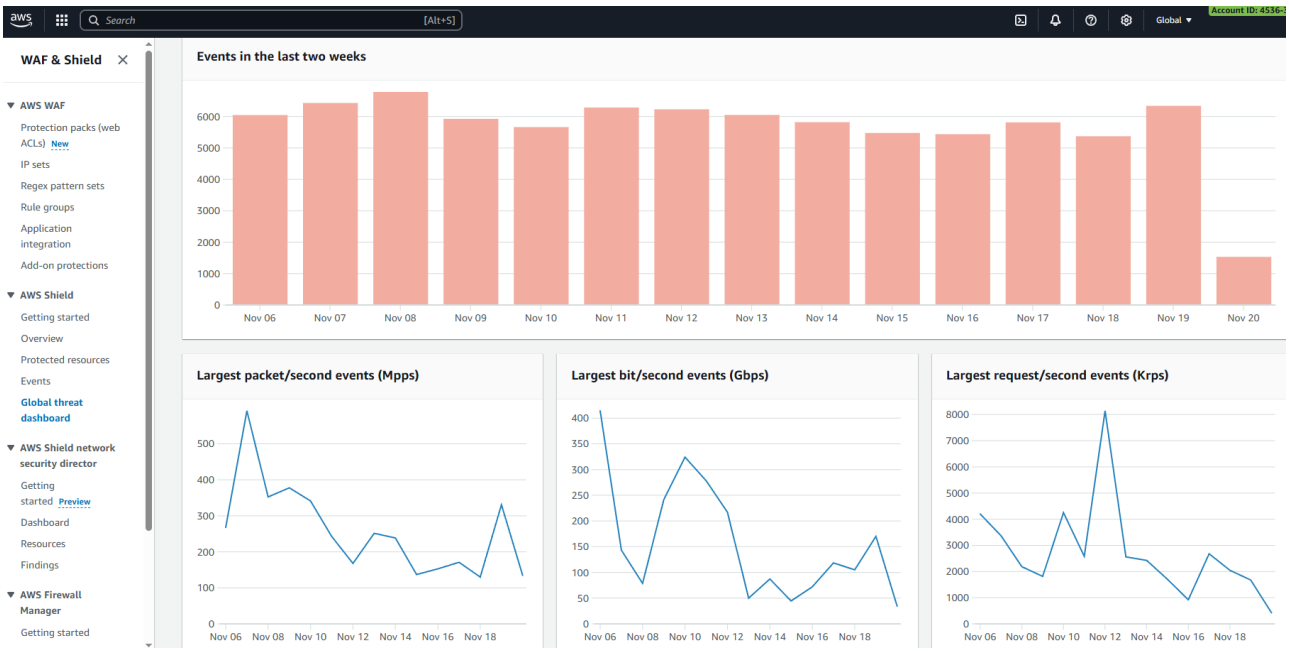

Рис. 3.6. Global threat dashboard across all AWS customers

Важливе обмеження Shield Standard. Використовуючи Standard для корпоративних цілей, необхідно пам’ятати про фінансовий ризик. Якщо атака буде настільки масивною, що CloudFront або WAF почнуть обробляти мільйони запитів, ми заплатимо за обробку цього трафіку. AWS Shield Standard (на відміну від Advanced) не компенсує витрати, що виникли внаслідок DDoS-атаки (Cost Protection відсутній).

Розглянемо порядок налаштування правил у Security Group для дозволу трафіку виключно від CloudFront, щоб уникнути помилок блокування легітимних користувачів.

Це налаштування часто називають «Origin Lock» (блокування джерела). Це критично важливий крок: якщо ми не зробимо цього, зловмисники можуть знайти пряму IP-адресу нашого сервера і атакувати її, повністю ігноруючи CloudFront і наш захист.

Замість того щоб вручну вводити сотні IP-адрес серверів CloudFront, ми використаємо *AWS Managed Prefix List*. Це динамічний список IP-адрес, який AWS оновлює автоматично.

Розглянемо порядок дій:

Крок 1: Визначення Security Group нашого балансувальника

1. Відкриваємо EC2 Console (або VPC Console).
2. У лівому меню переходимо у розділ Load Balancers.
3. Вибираємо свій балансувальник (ALB), який знаходиться за CloudFront.
4. У вкладці Security дивимося ID групи безпеки (наприклад, sg-01234abcd...). Натискаємо на цей ID.

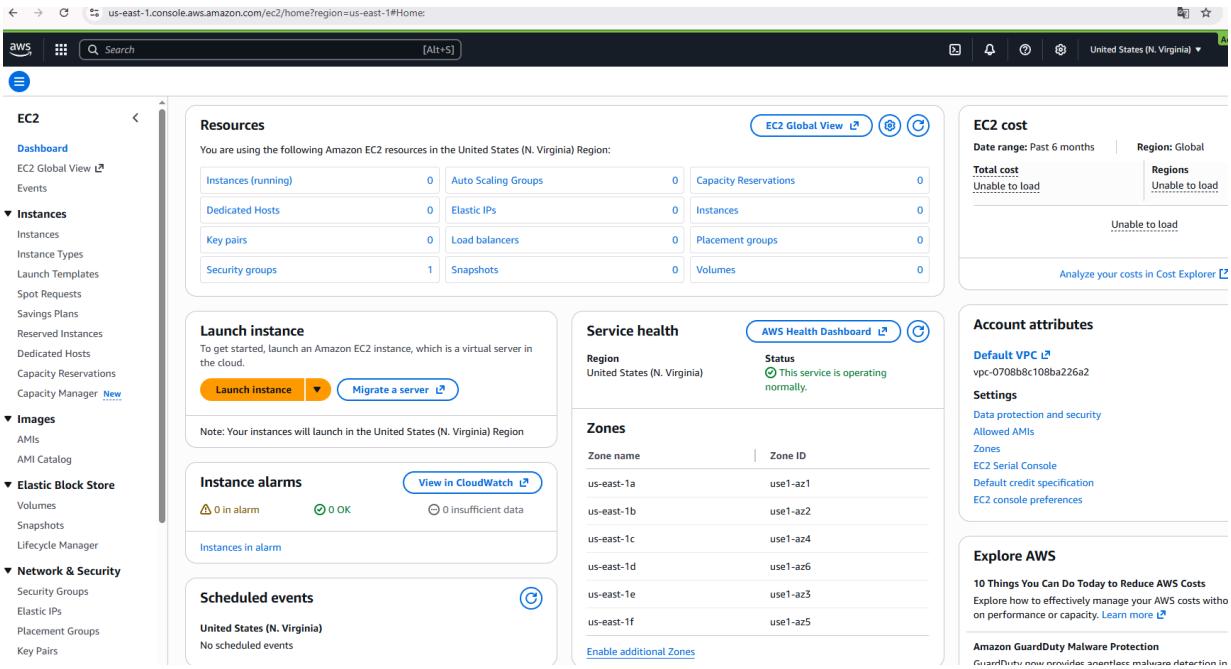

Рис. 3.7. Консоль EC2

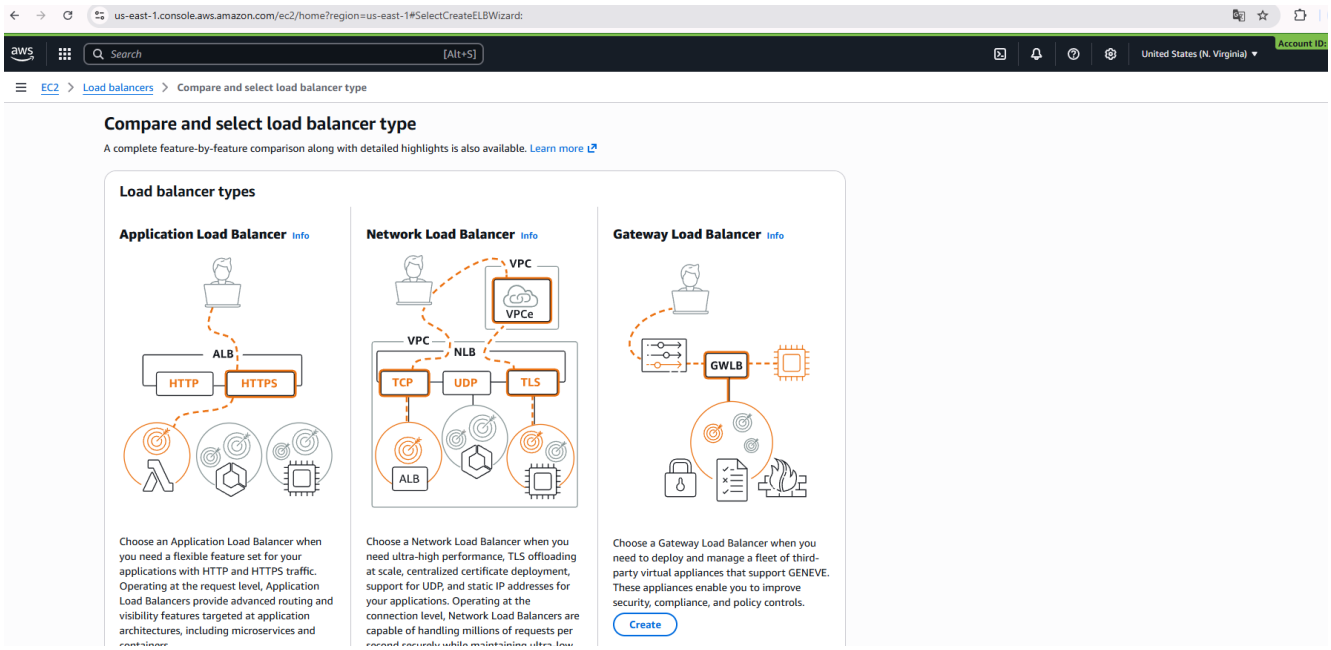

Рис. 3.8. Compare and select load balancer type

Крок 2: Редагування вхідних правил (Inbound Rules)

1. Ми переходимо на сторінку налаштувань конкретної Security Group.
2. Вибираємо вкладку Inbound rules (Вхідні правила).
3. Натискаємо кнопку Edit inbound rules.

Крок 3: Додавання правила для CloudFront (Managed Prefix List)

Це найважливіший момент.

1. Натискаємо Add rule.
2. Type (Тип): вибираємо HTTPS (порт 443) або HTTP (порт 80), залежно від того, як налаштований ваш CloudFront Origin Protocol Policy. *Рекомендовано використовувати HTTPS.*
3. Source (Джерело):
    - натискаємо у поле пошуку поруч із Custom.
    - замість введення цифр, починаємо вводити слово CloudFront.
    - ми побачимо список. Вибираємо саме цей пункт:

com.amazonaws.global.cloudfront.origin-facing

Це «магічний» список, який містить усі поточні IP-адреси серверів CloudFront.

Крок 4: Видалення старого правила (Відкритий Інтернет)

Щоб захист спрацював, потрібно заборонити все інше.

1. Знаходимо старе правило, яке дозволяло трафік з 0.0.0.0/0 (Anywhere) або ::/0.
2. Натискаємо кнопку Delete (сміттєвий бак) праворуч від цього правила.

Треба звернути увагу на те, що після натискання Save прямий доступ до нашого сайту за IP-адресою або DNS-іменем ALB зникне. Сайт буде доступний тільки через домен CloudFront.

3. Натискаємо Save rules внизу сторінки.

Крок 5: Як перевірити, що це працює?

Ми повинні переконатися, що «чорний хід» зачинено, а «парадний вхід» працює.

1. Перевірка «чорного ходу» (Прямий доступ):
    - знаходимо DNS-ім’я нашого Load Balancer (наприклад, my-alb-123.us-

east-1.elb.amazonaws.com).

- вставляємо його в браузер.
- очікуваний результат: браузер буде довго вантажитися і видасть помилку Connection Timed Out. Це означає, що Firewall відхиляє прямі пакети.

2. Перевірка «парадного входу» (Через CloudFront):
   - відкриваємо домен нашого дистрибутиву CloudFront (наприклад, d12345.cloudfront.net або наш кастомний домен).
   - очікуваний результат: сайт завантажується нормально.

Схема роботи трафіку після налаштування. Тепер шлях атаки виглядає так:

1. хакер (DDoS) $\rightarrow$ пряма IP адреса сервера $\rightarrow$ Security Group (BLOCK).
2. легітимний клієнт $\rightarrow$ CloudFront (Shield Standard + WAF) $\rightarrow$ Security Group (ALLOW) $\rightarrow$ наш додаток.

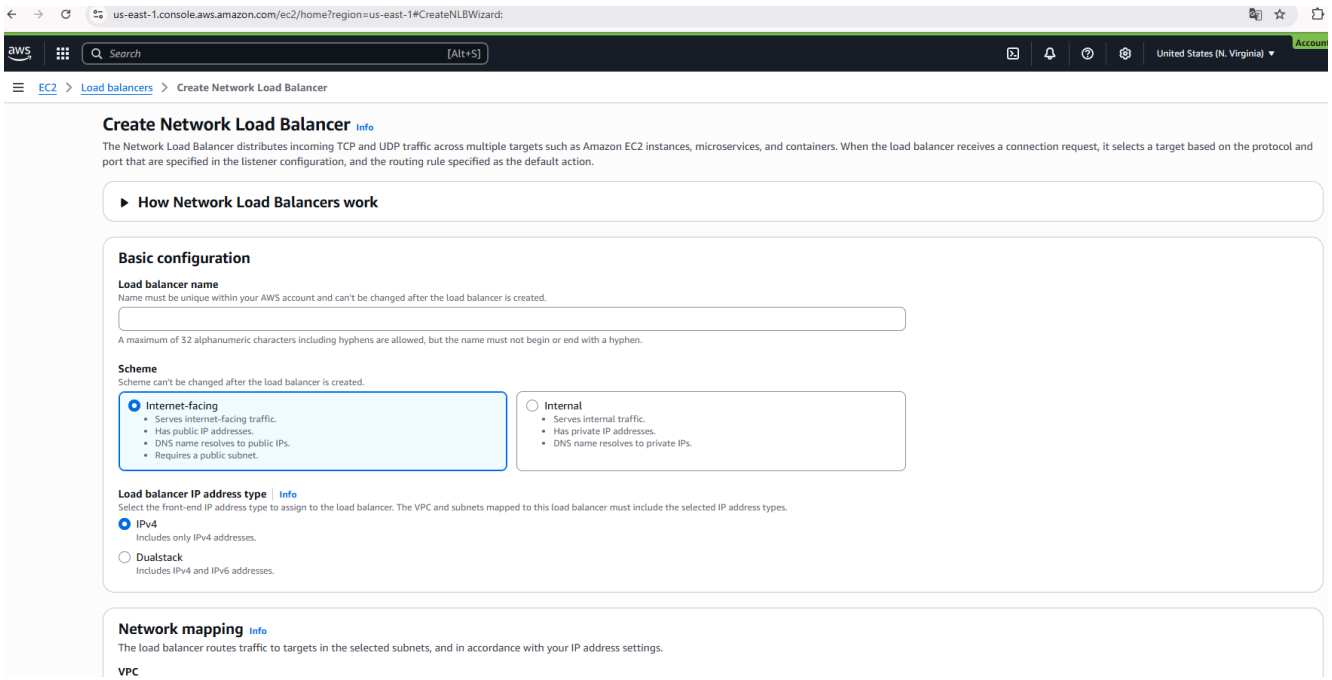

Рис. 3.9. Create Network Load Balancer

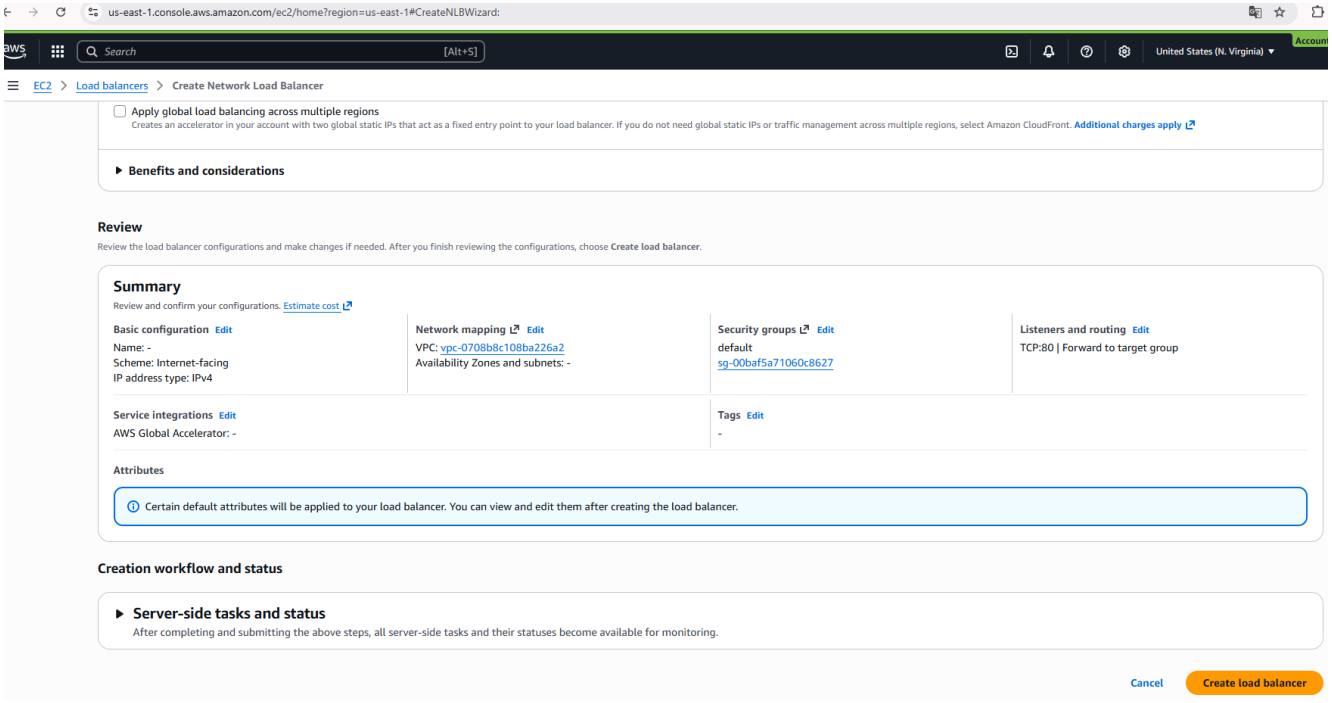

Рис. 3.10. Вкладка Review

Переглядаємо конфігурації балансувальника навантаження та вносимо зміни за потреби. Після завершення перевірки конфігурацій вибираємо «Створити балансувальник навантаження».

3.3. Рекомендації щодо керованого захисту хмарних корпоративних додатків від DDoS-атак

Захист хмарних корпоративних додатків від DDoS-атак – це не одноразове завдання. Це безперервний процес, який вимагає ретельного планування, регулярного тестування та постійного вдосконалення.

Для забезпечення ефективного керованого захисту хмарних корпоративних додатків від DDoS-атак необхідно:

Постійно досліджувати трафік корпоративної мережі. Необхідно встановлювати базові показники для звичайних моделей трафіку, включаючи типові показники запитів, розміри корисного навантаження та географічні джерела. Контролюйте використання системних ресурсів, включаючи використання процесора, пам’яті та мережі. Розуміючи типові моделі, можна швидко виявити

незвичайну активність, яка може свідчити про атаку.

Постійно підвищувати стійкість мережі. Розподіліть корпоративну інфраструктуру по різних мережах та центрах обробки даних. Розмістить веб-сервери в різних місцях, переконайтеся, що немає вузьких місць у трафіку, та підтримуйте резервні ресурси. Такий підхід допомагає поглинати трафік атак та підтримувати сервіс, навіть якщо деякі компоненти скомпрометовані.

Необхідно впроваджувати багаторівневий захист. Різні типи DDoS-атак спрямовані на різні рівні OSI корпоративної інфраструктури. Впроваджуйте захист на кількох рівнях:

на мережевому рівні – для атак на основі об’єму;

на протокольному рівні – для обробки SYN-потоків та подібних загроз;

на рівні додатків – для захисту від складних HTTP-флудів;

на рівні DNS – для підтримки служб розв’язання імен.

Ефективно використовувати обмеження швидкості. Налаштуйте інтелектуальне обмеження швидкості, щоб обмежити кількість запитів з одного джерела. Це допомагає запобігти вичерпанню ресурсів, не впливаючи на законних користувачів. Встановіть різні пороги для різних типів запитів та налаштуйте їх на основі історичних закономірностей.

Постійно моніторити та аналізувати трафік та журнали подій. Налаштуйте комплексний моніторинг на всіх мережевих рівнях. Встановіть сповіщення про раптові зміни в моделях трафіку. Ведіть детальні журнали всіх подій безпеки для аналізу після інцидентів. Використовуйте ці дані для покращення вашої стратегії захисту з часом.

Підтримувати актуальність Планів реагування. Створіть детальні методичні посібники для різних типів атак. Визначте чіткі ролі та обов'язки вашої команди реагування. Включіть контактну інформацію всіх відповідних співробітників та постачальників послуг. Задокументуйте процедури спілкування з клієнтами під час атаки.

Масштабувати корпоративну інфраструктуру. Переконайтеся, що корпоративна інфраструктура може обробляти піки трафіку, що значно

перевищують звичайний обсяг. Розгляньте можливість використання хмарних сервісів, які можуть автоматично масштабуватися під час атак. Побудуйте відносини з кількома постачальниками послуг вище рівня, щоб підтримувати зв'язок під час масштабних атак.

Впроваджувати системи викликів. Використовуйте системи, які можуть перевіряти підозрілий трафік, такі як:

CAPTCHA для перевірки людиною;

проблеми JavaScript для перевірки браузера;

перевірка легітимних клієнтів за допомогою файлів *cookie*;

користувацькі механізми запиту-відповіді.

Дотримуватися належної гігієни мережі. Оновлюйте всі системи останніми оновленнями безпеки. Видаляйте непотрібні служби та закривайте невикористовувані порти. Регулярно перевіряйте свою мережу на наявність потенційних вразливостей. Це зменшує площу атаки, доступну для потенційних зловмисників.

Створювати та застосовувати системи раннього попередження. Налаштуйте сповіщення для поширених індикаторів атак:

незвичайні сплески трафіку;

високий рівень невдалих запитів;

аномальні географічні моделі трафіку;

раптове збільшення кількості певних типів запитів.

Отже, DDoS-атаки є серйозною загрозою для всіх організацій, великих чи малих. Захист від них має вирішальне значення для підтримки роботи веб-сайтів та запобігання збоям у бізнесі. Заходи з пом'якшення наслідків DDoS захищають доходи, зберігають репутацію бренду та запобігають дороговартісним простоям. Завдяки ефективному пом'якшенню наслідків DDoS-атак, конфіденційні дані користувачів захищаються від зловмисників. Надійні стратегії пом'якшення наслідків зміцнюють довіру клієнтів, демонструючи відданість кібербезпеці та захисту даних, навіть під час зіткнення зі складними атаками.

Розглянемо основні рекомендації щодо застосування рішення AWS Shield для

керованого захисту хмарних корпоративних додатків від DDoS-атак.

Рекомендації щодо застосування AWS Shield для корпоративних додатків можна розділити на три рівні: архітектурний (як будувати), операційний (як діяти) та фінансовий (як оптимізувати).

1. Архітектурні рекомендації (Зменшення поверхні атаки).

Це фундамент захисту. AWS Shield працює найефективніше, коли корпоративна інфраструктура побудована правильно.

Використовуйте CloudFront для всього трафіку (навіть динамічного). Не відкривайте Application Load Balancer (ALB) або EC2 безпосередньо в Інтернет. CloudFront діє як гігантський щит, поглинаючи атаки на рівні L3/L4 (SYN Flood, UDP Reflection) ще до того, як вони досягнуть корпоративних серверів.

Приховуйте Origin-ресурси (Security Groups chaining). Налаштуйте Security Groups корпоративного ALB так, щоб вони приймали вхідний трафік виключно від діапазонів IP-адрес CloudFront (використовуйте AWS Managed Prefix List pl-xxxx). Якщо зловмисник дізнається реальну IP-адресу корпоративного сервера, він зможе обійти Shield/WAF і «покласти» сервер напряму.

Розділяйте статичний та динамічний контент. Статику (зображення, JS, CSS) винесіть на Amazon S3 + CloudFront. Це робить цю частину додатку практично невразливою до DDoS, оскільки S3 масштабується автоматично і не має серверів, які можна перевантажити CPU-атаками.

2. Рекомендації щодо налаштування WAF (L7 захист)

Для захисту від «розумних» атак (HTTP Flood, повільні запити), які імітують реальних користувачів необхідно:

впровадити правила в режимі Count перед Block. Ніколи не вмикайте нові правила WAF одразу в режим блокування. Спочатку запустіть їх у режимі підрахунку (Count) на 24-48 годин, проаналізуйте метрики, щоб не заблокувати реальних клієнтів (False Positives), і лише потім вмикайте блокування;

використовувати Rate-Limiting (обмеження швидкості). Для сторінок авторизації (/login) встановіть жорсткі ліміти (наприклад, 5 запитів на хвилину з IP). Для API – ліміти, що відповідають нормальному профілю навантаження;

здійснити гео-блокування. Якщо ваш бізнес працює тільки в Україні, заблокуйте або поставте в режим Challenge (CAPTCHA) трафік з країн з високим ризиком бот-мереж (Китай, РФ, Бразилія тощо).

3. *Операційні рекомендації (Підготовка до інциденту)*

Найгірший час розбиратися, як працює захист – це під час атаки. Необхідно розробити DDoS Runbook – документ, у якому чітко прописано наступне:

Як ідентифікувати атаку (які метрики дивитися).

Хто приймає рішення про ескалацію.

Шаблони звернення в підтримку AWS.

Процедура перемикання на статичну заглушку (Failover page).

Проводьте Game Days (Симуляції). Регулярно тестуйте реакцію команди. Використовуйте партнерів AWS для проведення санкціонованих пентестів/DDoS-симуляцій, щоб перевірити, чи спрацюють ваші WAF правила та чи витримає автомасштабування.

Треба мати на увазі, що будь-яка симуляція DDoS вимагає попереднього дозволу від AWS, інакше вони можуть заблокувати ваш акаунт за підозрілу активність.

4. Рекомендації щодо вибору рівня Shield (Standard vs Advanced)

Для корпоративного сектору вибір часто зводиться до вартості простою (Cost of Downtime) (таблиця 3.2).

5. Моніторинг і видимість

Треба мати на увазі, що ви не можете захистити те, чого не бачите.

Використовуйте Global Threat Environment. Використовуйте дашборд Shield, щоб бачити загальний фон загроз у мережі AWS. Якщо AWS зараз під масованою атакою глобально, це може вплинути на латентність.

Таблиця 3.2

Врахування вартості простою для вибору рішення

Критерій	**Залишайтесь на Shield Standard**	**Переходьте на Shield Advanced ($3000/міс)**
Команда	У вас є сильні DevOps/SecOps, готові реагувати 24/7	Команда мала, потрібна допомога експертів AWS (SRT)
Бюджет	Обмежений, ризики простою прийнятні	Вартість години простою > $3000
Тип білінгу	Платите за фактичні ресурси	Потрібна страховка від сплесків рахунків (Cost Protection)
Звітність	Достатньо базових метрик	Потрібні детальні звіти для комплаєнсу/аудиту

Використовуйте метрики реального часу. Створіть окремий дашборд CloudWatch «DDoS Status», вивівши туди:

WAFBlockedRequests;

CloudFrontBytesDownloaded;

ALB 5xx Errors;

SurgeQueueLength (для балансувальників).

ВИСНОВКИ

В роботі досліджено проблему керованого захисту хмарних корпоративних додатків від DDoS-атак, визначено його мету та завдання.

Визначено існуючі підходи до керованого захисту хмарних корпоративних додатків від DDoS-атак. Керований захист хмарних корпоративних додатків від DDoS-атак передбачає використання спеціалізованих послуг від хмарних постачальників або сторонніх розробників, які використовують багаторівневий захист, постійний моніторинг трафіку та автоматизоване пом'якшення наслідків для захисту корпоративних додатків від об'ємних, протокольних та прикладних атак. Ключові функції включають автоматичне реагування, очищення трафіку, WAF, обмеження швидкості та екстрену підтримку для забезпечення безперервності бізнесу.

Великі хмарні постачальники, такі як AWS, Azure та Google Cloud, пропонують власні керовані сервіси захисту від DDoS-атак для захисту корпоративних додатків, розгорнутих на їхній інфраструктурі.

Проаналізовано методи та засоби керованого захисту хмарних корпоративних додатків від DDoS-атак на базі AWS Shield. Відмічено, що AWS Shield Standard та AWS Shield Advanced забезпечують захист від розподілених DDoS-атак для ресурсів AWS на мережевому та транспортному рівнях (рівень 3 та 4) і прикладному рівні (рівень 7).

Визначено призначення, основні функції та склад рішення AWS Shield. Зміст технології керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield включає захист від DDoS-атак, що часто використовуються на рівні інфраструктури (рівень 3 та рівень 4), без затримки виявлення, захист від перевантажень TCP SYN, захист від атак на рівні додатків DNS, захист від перевантаження запитами на рівні веб додатків, автоматичне пом'якшення DDoS-атак на рівні додатків для корпоративних дистрибутивів CloudFront, проактивна взаємодія з командою реагування Shield (SRT).

На основі досліджень проведених в роботі запропоновано порядок застосування технології керованого захисту хмарних корпоративних додатків від DDoS-атак. Розроблено рекомендації фахівцям з кібербезпеки щодо керованого захисту хмарних корпоративних додатків від DDoS-атак.

Таким чином, керований захист хмарних корпоративних додатків від DDoS-атак забезпечує доступність критично важливих сервісів під час атаки, запобігає дороговартісним перебоям у наданні послуг, потенційним юридичним санкціям та втраті доходу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bart Lenaerts-Bergmans. Distributed Denial-of-Service (DDoS) Attacks. CrowdStrike, April 21, 2023. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/ddos-attack/

2. ENISA THREAT LANDSCAPE 2025. October 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf

3. What is Azure DDoS Protection? 07/08/2025. URL: https://learn.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview

4. Protecting Against Distributed Denial of Service (DDoS) Attack. November 6, 2024. URL: https://www.alibabacloud.com/blog/protecting-against-distributed-denial-of-service-ddos-attack_601733

5. Nigel Douglas. How to Prevent a DDoS Attack. URL: https://www.sysdig.com/blog/how-to-prevent-ddos-attack-cloud

6. Paige Tester.10 Best Practices for Protecting Your Business Against Devastating DDoS Attacks with Anti-DDoS Protection. 16 Jan, 2025. URL: https://datadome.co/bot-management-protection/anti-ddos/

7. Manoj Mehra. DDoS Protection: The Comprehensive Guide to Safeguarding Your Digital Assets. Oct 4, 2024. URL: https://buzzclan.com/managed-it/ddos-protection/

8. The Industry’s Most Advanced DDoS Protection. Data Sheet. Radware. URL: https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-cloud-ddos-2024.pdf

9. AWS WAF, AWS Firewall Manager, AWS Shield Advanced, and AWS Shield network security director. Developer Guide. URL: https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html

10. 2025 Cloud Security Report. Check Point. URL: https://www.checkpoint.com/resources/items/report-cloud-security-report-2025

11. Google Cloud Armor. URL: https://cloud.google.com/security/products/armor?hl=en

12. Ковальський Богдан Андрійович. Технологія керованого захисту хмарних корпоративних додатків від DDoS-атак на основі AWS Shield. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». 29 жовтня 2025 року. Державний університет інформаційно-комунікаційних технологій, м. Київ. Тези доповідей. С. 116-118. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)