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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту веб додатків від DDoS-атак на основі AWS WAF»

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

_____ Ярослав КРАВЧЕНКО
(підпис)

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

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

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

WAAP – Web Application and API protection

SOC – Security Operations Center

OWASP – Open Web Application Security Project

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. У сучасному швидкозмінному цифровому середовищі безпека онлайн-додатків є пріоритетом для будь-якої організації. Кіберзагрози продовжують зростати як за частотою, так і за складністю. Серед цих небезпек розподілені атаки типу «відмова в обслуговуванні» (DDoS) залишаються поширеною та руйнівною силою.

Захист корпоративних веб додатків від розподілених DDoS-атак передбачає багаторівневу стратегію, яка поєднує безпеку інфраструктури, управління трафіком та спеціалізовані служби пом’якшення наслідків. Ефективний захист вимагає проактивного моніторингу та чітко визначеного плану реагування для забезпечення безперервності бізнесу.

Для захисту корпоративних веб додатків використовують брандмауер веб-додатків (WAF). WAF працює на рівні застосунків (рівень 7) між публічним Інтернетом та корпоративним веб додатком та перевіряє HTTP/S-трафік, блокуючи шкідливі запити, що є симптомами DDoS-атак на рівні застосунків, таких як HTTP-флуд та атаки «низького та повільного» типу (наприклад, Slowloris).

Сучасні WAF включають поведінкову аналітику, обмеження швидкості, управління ботами та можливість оскаржувати підозрілі запити за допомогою CAPTCHA. WAF можна розгортати локально, у хмарі або як послугу, що забезпечує гнучкість для різних інфраструктур. WAF додає життєво важливий рівень захисту на рівні додатків (рівень 7), захищаючи від більш складних, цілеспрямованих атак.

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

Об’єкт дослідження – захист веб додатків від DDoS-атак.

Предмет дослідження – технологія захисту веб додатків від DDoS-атак на основі AWS WAF.

Мета роботи – розробити порядок застосування технології захисту веб додатків від DDoS-атак на основі AWS WAF та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту веб додатків від DDoS-атак;

проаналізувати підходи до захисту веб додатків від DDoS-атак;

проаналізувати існуючі рішення для захисту веб додатків від DDoS-атак;

проаналізувати методи та засоби захисту веб додатків від DDoS-атак на основі AWS WAF;

розкрити порядок реалізації технології захисту веб додатків від DDoS-атак на основі AWS WAF.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту веб додатків від DDoS-атак на основі AWS WAF, 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 ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД DDOS-АТАК

1.1. Дослідження проблеми захисту веб додатків від DDoS-атак

У 2025 році основними загрозами для хмарних сервісів є зростання масштабів DDoS-атак, ускладнення атак за допомогою AI, а також загрози, повязані з неправильною конфігурацією хмарних сервісів та недостатньою безпекою доступу. Ці загрози призводять до операційних збоїв, фінансових втрат та компрометації даних, що вимагає активного впровадження заходів безпеки.

Останні ринкові прогнози демонструють підвищену зацікавленість бізнесу до хмарних сервісів. За даними Gartner, світові витрати на публічні хмарні сервіси досягнуть 723,4 мільярда доларів у 2025 році – що на понад 20 відс. більше, ніж у 2024 році. 90 відс. організацій перейдуть на гібридну хмарну стратегію до 2027 року. Markets and Markets очікує, що світові витрати на хмарні сервіси перевищать 1,25 мільярда доларів до 2028 року. У світі, де масштабованість, гнучкість та економічна ефективність є першочерговими, майбутнє явно за хмарою [1].

Хмарні обчислення стали невід'ємною частиною сучасних бізнес-процесів, оскільки вони пропонують гнучкість, масштабованість та перевагу у скороченні витрат. Однак, це супроводжуються величезними ризиками безпеки, пов'язаними з хмарними обчисленнями. У процесі переходу до хмари багато організацій не враховують основні вимоги безпеки, які можуть поставити під загрозу їхні хмарні системи. Повідомляється, що близько 45% інцидентів безпеки виникли в хмарних середовищах, що вимагає посилених заходів безпеки. Тому цей зсув вимагає від організацій вжиття проактивних заходів безпеки, включаючи аудити безпеки, підвищення обізнаності співробітників про безпеку та вдосконалені системи виявлення загроз [2].

Крім того, фінансовий вплив низької безпеки хмарних сервісів – це проблема, яку бізнес не повинен ігнорувати. Середня вартість витоку даних зросла до 4,88

мільйона доларів у 2024 році, що включає не лише прямі збитки, пов’язані з викраденими записами, але й довгострокові втрати репутації та штрафи за невідповідність. Організаціям давно час звернути належну увагу на активне інвестування в рішення для хмарної безпеки, щоб мінімізувати цей ризик. Це включає впровадження політик управління доступом, таких як багатофакторна автентифікація, відповідне налаштування хмарних сервісів та глибокі оцінки вразливостей.

Однак, ширше впровадження хмарних технологій означає більше проблем безпеки на основі хмарних технологій, від зростання складності до вразливостей, що виникають через нові технології. А прискорення темпів змін лише загострює проблеми безпеки хмарних технологій. Ось лише кілька прикладів тенденцій, за якими уважно стежать керівники інформаційних систем [1]:

збільшення впровадження хмарних технологій. Чим більше хмарних сервісів розгортається, тим складнішим і взаємопов’язанішим стає корпоративне середовище. Це створює дедалі більшу та важчу для захисту поверхню для атак, яку можуть використати зловмисники;

інтеграція штучного інтелекту та машинного навчання. Оскільки постачальники хмарних послуг (CSP) інтегрують нові можливості штучного інтелекту та машинного навчання у свої платформи та послуги, клієнти отримують нові способи підвищення операційної ефективності, а зловмисники – нові способи здійснення атак;

хмарні додатки. DevOps та контейнеризація дозволяють зробити квантові стрибки у швидкості розгортання та гнучкості бізнесу, але в більшості організацій заходи безпеки, що захищають ці нові архітектури, ще перебувають у процесі розробки;

поширення API. API є основою сучасних IT-середовищ. Але недостатньо захищені API можуть дати зловмисникам шлях до найчутливіших зон гібридного середовища.

Оскільки зловмисники постійно адаптують свої інструменти та тактики до мінливого середовища, їхні потенційні жертви намагаються бути на крок попереду.

Це означає бути обізнаним з останніми загрозами безпеці хмарних технологій у міру їх виникнення, а також з постійними проблемами безпеки хмарних технологій, які продовжують створювати труднощі. Освіта та підготовка є ключами до мінімізації загроз безпеці в хмарних обчисленнях та забезпечення безперервного ведення бізнесу у 2025 році та надалі [1].

Найбільш поширені проблеми у хмарній безпеці наведено у таблиці 1.1.

Таблиця 1.1

Найбільш поширені проблеми у хмарній безпеці [3]

Виклики	Деталі	Вплив
Витоки даних	Хмарні сервіси зберігають багато конфіденційних даних. Це робить їх головними цілями для хакерів.	Крадіжка даних, втрата довіри клієнтів, юридичні проблеми та фінансові втрати.
Внутрішні загрози	Працівники, які мають доступ до інструментів, можуть навмисно чи ненавмисно завдати шкоди.	Витік даних, несанкціонований доступ та інші порушення безпеки.
Неправильні конфігурації	Неправильно налаштовані хмарні інструменти можуть розкривати конфіденційні дані для неавторизованих користувачів.	Випадкове витікання даних, порушення безпеки та проблеми безпеки, спричинені людською помилкою.
Питання відповідності та нормативно-правового регулювання	Хмарні хости працюють у багатьох регіонах. Дотримання всіх нормативних вимог є складним завданням.	Штрафи, юридичні проблеми та шкода репутації через недотримання вимог.
Відсутність видимості та контролю	Обмежена видимість хмарних систем ускладнює моніторинг та забезпечення дотримання правил безпеки.	Прогалини в захисті та проблеми з відстеженням безпеки послаблюють підхід до хмарної безпеки.
Атаки типу «відмова в обслуговуванні» (DoS)	DDoS-атаки можуть перевантажувати хмарні інструменти та спричиняти перебої в роботі сервісів.	Збій у роботі сервісу, втрата довіри клієнтів та перебої в роботі.
Незахищені API	Хакери можуть використовувати незахищені API для отримання несанкціонованого доступу до хмарних ресурсів.	Несанкціонований доступ до інструментів призводить до втрати даних або збоїв у роботі.

Хоча все більше компаній переносять свою діяльність у хмарні середовища, зростає потреба в безпеці цих інфраструктур. Перехід до хмарних обчислень

збільшує площу атаки завдяки новим вразливостям, які супроводжуються додатковою складністю. Цей зростаючий виклик вимагатиме від компаній пріоритезації стратегії безпеки для хмари, яка охоплює всі сфери, де бізнес вразливий.

Розширення поверхні атаки. Перехід до хмарних середовищ розширює поверхню атаки організації. Оскільки компанії зберігають більше даних і запускають програми в хмарі, вони відкривають більше потенційних точок входу для кібератак. Кожен хмарний сервіс, програма та інтеграція збільшують кількість потенційних вразливостей, які можуть використовувати зловмисники. Без надійних заходів безпеки ця ширша поверхня атаки збільшує ймовірність несанкціонованого доступу, витоків даних та компрометації системи [2].

Модель спільної відповідальності. Хмарні обчислення працюють за моделлю спільної відповідальності, де безпека покладається на CSP та сам бізнес. Постачальник хмарних послуг бере на себе відповідальність за захист фізичної інфраструктури, всіх мереж та рівнів віртуалізації. Однак усі бізнес-дані, конфігурації та засоби контролю доступу повинні бути захищені самим бізнесом. Відсутність належного розуміння спільної відповідальності в хмарі або її неправильне управління може призвести до серйозних прогалин у хмарній безпеці, через які може бути розкрита конфіденційна інформація [2].

Більший ризик витоку даних. Витоки даних створюють значні ризики для безпеки в хмарних обчисленнях. Неправильні конфігурації хмарних налаштувань, включаючи погано захищені сховища та слабкі політики IAM, можуть розкрити конфіденційні дані для неавторизованих користувачів. Такі відкриті вразливості можуть бути використані зловмисниками для крадіжки конфіденційних даних, що завдасть значної фінансової шкоди та завдасть репутаційної шкоди. Правильне налаштування хмарних ресурсів та постійний моніторинг потенційних загроз можуть лише запобігти витокам даних [2].

Проблеми дотримання нормативних вимог. Більшість галузей, таких як охорона здоров’я, фінанси та електронна комерція, обмежені дуже суворими правилами щодо безпеки даних та конфіденційності. Кожна організація повинна

забезпечити відповідність своїх хмарних конфігурацій галузевим стандартам, таким як GDPR, HIPAA або PCI DSS, під час впровадження хмарного середовища. Недотримання хмарної безпеки призводить до великих штрафів, дорогих юридичних санкцій та втрати довіри клієнтів через недотримання вимог. Тому ці регуляторні проблеми завжди повинні бути пріоритетними на самому початковому етапі впровадження хмари [2].

Відсутність видимості хмари. Хмарні середовища є динамічними та розширюваними, що перетворюється на сліпі зони для всіх хмарних ресурсів. Тому може бути важко виявити потенційну загрозу безпеці, неправильну конфігурацію або несанкціонований доступ. Неадекватні інструменти для моніторингу хмарної інфраструктури можуть означати, що підприємства не можуть розпізнати критичні прогалини в безпеці. Видимість та контроль над хмарними активами для швидкої ідентифікації та реагування на потенційні загрози підтримуються за допомогою власних інструментів та рішень для управління безпекою хмари для постійного моніторингу [2].

DDoS-атаки були основою кіберзлочинності протягом десятиліть, але вони можуть бути особливо проблематичними в контексті хмарної безпеки. Хоча хмарні платформи можуть забезпечити динамічну масштабованість для поглинання надзвичайно великих обсягів трафіку DDoS-атаки, ця ж функція може призвести до різкого зростання операційних витрат на хмарні ресурси на вимогу [1].

Ширша поверхня атаки та багата на API інфраструктура хмарних систем ускладнюють ефективний захист, а неправильні конфігурації клієнтів можуть ще більше посилити вразливість. Спільна роль хмарних середовищ в обробці стрибків попиту може ускладнити розрізнення звичайного пікового використання та шкідливого трафіку [1].

Масштаб DDoS-загрози хмарній безпеці зростає у 2025 році разом із впровадженням хмарних технологій. Зростаюча залежність від хмарних сервісів та додатків реального часу робить організації більш вразливими до цих атак та поширених операційних збоїв, які вони можуть спричинити.

Зловмисники використовують штучний інтелект та машинне навчання для

створення складніших та важчих для виявлення схем атак, включаючи атаки, які можуть адаптуватися в режимі реального часу до захисту жертви.

У Звіті ENISA [4] зазначається, що у розподілі типів інцидентів домінують DDoS-атаки, які складають близько 76,7 відс. зареєстрованих випадків (рисунок 1.1). Ця категорія переважно належить хактивістським групам, на які припадає більшість зібраних DDoS-інцидентів, тоді як кіберзлочинні групи складають незначну частку, часто пов’язану з вимаганням (наприклад, DDoS з метою вимагання викупу). Далі йдуть вторгнення з 17,8 відс., переважно кіберзлочинною діяльністю, далі йдуть групи вторгнень, узгоджені з державою, які зазвичай прагнуть стійкості. Хактивісти з’являються лише незначно у випадках вторгнень. Дефейси майже виключно пов’язувалися з хактивістами, що підкреслювало їхню роль як символічної тактики для видимості та протесту, а не як методу тривалого вторгнення [4].

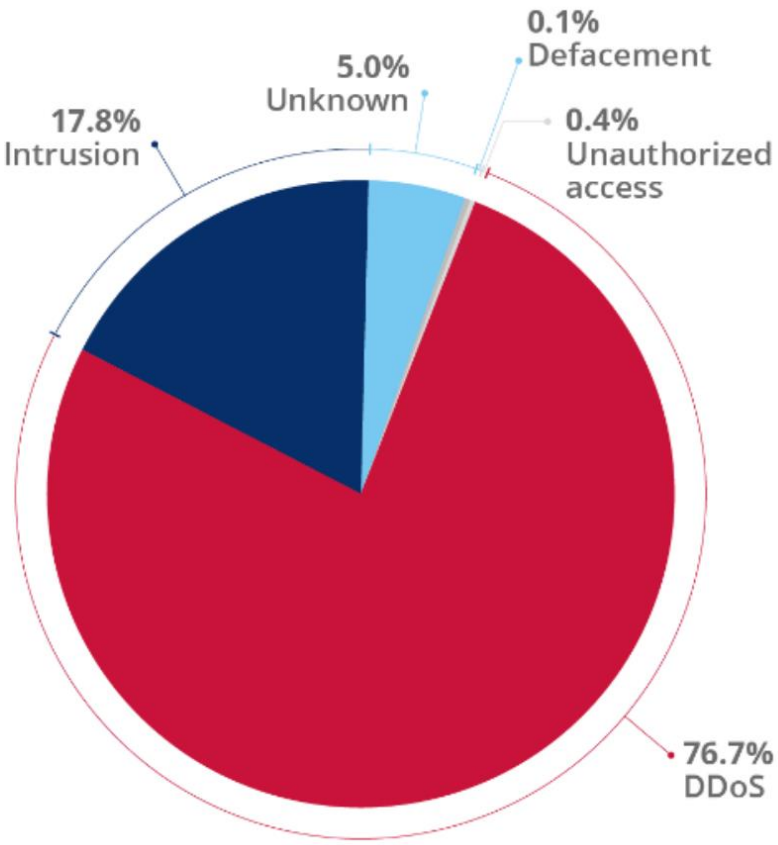

Рис. 1.1. Розподіл типів інцидентів за даними ENISA [4]

Інструменти та методи, доступні для захисту хмарних ресурсів від DDoS-атак

останнього покоління, включають [1]:

послуги захисту від DDoS-атак від хмарних провайдерів, розроблені для поглинання та пом’якшення масштабних атак;

обмеження швидкості для обмеження кількості запитів від одного користувача або програми;

механізми геоблокування та фільтрації IP-адрес для обмеження трафіку з відомих шкідливих джерел або регіонів;

масштабовані архітектурні шаблони для ефективного розподілу навантаження між незалежними компонентами, а не для досягнення єдиної точки відмови;

безперервний моніторинг та аналіз трафіку для виявлення незвичайних закономірностей, які можуть свідчити про майбутню атаку;

регулярні стрес-тести, що імітують умови DDoS-атак, для оцінки ефективності стратегій пом’якшення та виявлення вузьких місць або вразливостей.

Отже, масштаб і складність DDoS-атак зростатимуть із зростанням використання хмарних сервісів. Атакуючі використовують штучний інтелект (AI) та машинне навчання (ML) для створення більш складних, адаптивних до захисту патернів атак, що призводить до операційних збоїв у роботі організацій.

Неправильна конфігурація хмарних сервісів, помилки в налаштуваннях хмарних середовищ створюють вразливості, які можуть призвести до витоку даних. Цей ризик залишається актуальним, попри наявність інструментів безпеки.

Недостатній контроль доступу до хмарних ресурсів, зокрема, відсутність багатофакторної аутентифікації (MFA), створює ризик несанкціонованого доступу та крадіжки даних.

1.2. Аналіз підходів до захисту веб додатків від DDoS-атак

Сучасні веб-сайти – це складні багатокомпонентні додатки, які обслуговують різноманітних користувачів та пристроїв – браузери від різних розробників, мобільні додатки та інші онлайн-сервіси, що взаємодіють через HTTP-запити та

API. На відміну від десятирічної давності, сучасні веб-додатки покладаються на передові технології, такі як AJAX, API та BFF (Backend-for-Frontend), для забезпечення безперебійного взаємодії [19].

Однак, ця архітектурна складність має й зворотний бік: більшу вразливість до кіберзагроз, включаючи DDoS-атаки. Веб-сайти мають бути захищені на кількох рівнях моделі OSI, включаючи мережевий (L3), транспортний (L4) та прикладний (L7) рівні [19].

В останні роки «розумні» атаки на рівні додатків стають дедалі поширенішими. На відміну від традиційних DDoS-атак, вони спрямовані не лише на протоколи HTTP/HTTPs, а й на те, як серверні компоненти взаємодіють з клієнтськими модулями та іншими системами, такими як бази даних (СУБД) або шини даних. Зловмисники використовують слабкі місця в цих взаємодіях, щоб порушувати роботу таким чином, що стандартні засоби захисту можуть не виявити їх [19].

Захист веб додатків від DDoS-атак (розподілена відмова в обслуговуванні) вимагає багатошарової стратегії, спрямованої на поглинання та фільтрацію шкідливого трафіку до того, як він вплине на корпоративні сервіси. Основна мета – відрізнити легітимних користувачів від трафіку атаки.

Розглянемо ключові підходи, розподілені за техніками та стратегіями.

Основними інструментами та сервісами, що використовуються для створення захисту від DDoS є [4-6]:

очищення трафіку (Scrubbing). Це найефективніший метод проти великомасштабних атак. Увесь вхідний трафік перенаправляється через мережу провайдера захисту від DDoS («центр очищення»). Ці центри мають величезну пропускну здатність і використовують спеціалізоване обладнання для аналізу трафіку, відфільтровування шкідливих пакетів («поганого» трафіку) і передачі лише «чистого» трафіку на корпоративний сервер:

брандмауер для веб додатків (WAF). WAF працює на рівні застосунків (Layer 7) і є критично важливим для зупинки складних атак, що імітують поведінку реальних користувачів. Він може перевіряти окремі HTTP-запити та блокувати їх

на основі правил, поведінкового аналізу або репутації. Наприклад, він може зупинити бота, який постійно намагається увійти в систему або виконати запит до бази даних;

мережа доставки контенту (CDN). CDN розподіляє контент корпоративного додатка по глобальній мережі серверів. Для захисту від DDoS це надає дві основні переваги:

розподілене поглинання: атака поглинається всією мережею CDN, а не спрямовується на єдиний сервер;

кешування: кешуючи статичний контент (зображення, CSS тощо), CDN зменшує кількість запитів до корпоративного сервера, що знижує вплив атаки;

обмеження частоти запитів (Rate Limiting). Ця техніка контролює кількість трафіку, яку сервер приймає з однієї IP-адреси за певний проміжок часу. Якщо користувач або бот перевищує ліміт (наприклад, понад 100 запитів на хвилину), його наступні запити тимчасово блокуються або сповільнюються. Це проста, але ефективна перша лінія захисту;

списки репутації IP-адрес. Цей метод використовує заздалегідь складені списки IP-адрес, які відомі як джерела спаму, шкідливого ПЗ або DDoS-атак. Трафік із цих IP-адрес можна проактивно блокувати ще до того, як він досягне корпоративного веб додатка.

Різні атаки спрямовані на різні рівні мережевого стека, що вимагає специфічних методів захисту.

Об’ємні атаки (рівні 3/4) мають на меті перевантажити пропускну здатність мережі величезним потоком трафіку (наприклад, UDP-флуд). Основним захистом від них є застосування сервісів очищення трафіку та CDN. Ці сервіси поглинають флуд і пропускають лише легітимний трафік [4-6].

Нульова маршрутизація (або blackholing) – це крайній захід, коли провайдер відкидає весь трафік на корпоративну IP-адресу. Це виводить вас з мережі, але захищає мережу провайдера.

Протокольні атаки (рівні 3/4) використовують слабкості в мережевих протоколах для вичерпання ресурсів серверів, брандмауерів або балансувальників

навантаження (наприклад, SYN-флуд). Основним захистом є спеціалізоване обладнання в центрах очищення та сучасні брандмауери, які ефективно керують з’єднаннями та виявляючи некоректні пакети. Звичайні сервери легко перевантажуються.

Атаки на рівні застосунку (рівень 7) є найскладнішими, оскільки вони імітують поведінку реальних користувачів для вичерпання ресурсів сервера, таких як CPU та пам’ять (наприклад, HTTP-флуд). Вони часто є повільними й менш помітними («low and slow»). Основним захистом від них є застосування WAF. Він використовує передові техніки для виявлення шкідливої поведінки [4-6]:

поведінковий аналіз. Виявляє нелюдські патерни (наприклад, запити сторінок швидше, ніж людина могла б їх прочитати);

перевірки CAPTCHA. Пропонує підозрілим ботам пройти тести, щоб довести, що вони не роботи;

інспекція запитів. Блокує некоректні або шкідливі HTTP-запити.

1.3. Аналіз існуючих рішень для захисту веб додатків від DDoS-атак

Розподілені атаки типу «відмова в обслуговуванні» (DDoS) еволюціонували від простих флуд-атак до складних, багатовекторних кампаній, здатних паралізувати інфраструктуру будь-якого масштабу. У сучасному цифровому ландшафті, де доступність веб додатків є синонімом безперервності бізнесу, ефективний захист від DDoS-атак перестав бути опцією і став критичною необхідністю.

Зловмисники все частіше фокусуються на L7, оскільки такі атаки потребують менше ресурсів, їх важче виявити, і вони можуть бути дуже ефективними. Особливою ціллю стають API, які є основою сучасних веб додатків. Як зловмисники використовують ШІ для автоматизації та ускладнення атак, так і захисні платформи впроваджують ML для проактивного виявлення аномалій та автоматичної адаптації захисних політик у реальному часі.

Спостерігається тенденція проведення короткотривалих, але потужних

атаки. Проведення так званих «burst-атак» – коротких (кілька хвилин), але надзвичайно інтенсивних атак, спрямованих на те, щоб вивести систему з ладу до того, як спрацює захист «за запитом». Це підвищує цінність «always-on» моделей.

DDoS-атаки все частіше використовуються для відволікання уваги команди безпеки під час проведення інших, більш цілеспрямованих атак, таких як злам систем чи крадіжка даних.

Сучасні атаки часто є багатовекторними, поєднуючи методи L3/L4 та L7 для максимального ефекту. Це вимагає від захисних рішень комплексності та гнучкості.

Існує три основні моделі розгортання систем захисту від DDoS-атак, кожна з яких має свої переваги та недоліки.

Локальні рішення (On-Premise). Цей підхід передбачає встановлення спеціалізованого апаратного або програмного забезпечення безпосередньо в дата-центрі компанії.

Принцип роботи: пристрій (DDoS mitigation appliance) встановлюється «в розріз» інтернет-каналу і аналізує весь вхідний трафік. У разі виявлення аномалій воно починає фільтрацію, відсіюючи шкідливі пакети. Провідні вендори: NETSCOUT (Arbor), Radware, Fortinet [7-9].

Переваги:

мінімальна затримка (latency). Оскільки трафік обробляється локально, затримки для легітимних користувачів у мирний час є мінімальними;

повний контроль. Компанія повністю контролює обладнання, конфігурації та політики безпеки;

захист від L7-атак. Ефективно справляється з атаками на рівні додатків, оскільки має повний контекст роботи внутрішніх сервісів.

Недоліки:

обмежена масштабованість. Рішення обмежене пропускною здатністю інтернет-каналу. Якщо потужність волюметричної атаки перевищує ширину каналу, він буде перевантажений ще до того, як трафік дійде до захисного пристрою;

висока вартість. Значні капітальні витрати (CapEx) на закупівлю обладнання та подальші операційні витрати (OpEx) на обслуговування, оновлення та персонал;

вимоги до кваліфікації. Потребує наявності висококваліфікованих інженерів для налаштування та підтримки.

Хмарні рішення (Cloud-Based). Це найпопулярніша модель, що передбачає використання послуг стороннього провайдера, який фільтрує трафік у своїй глобальній мережі.

Принцип роботи – весь трафік до веб додатку спрямовується через мережу провайдера захисту. Це досягається зміною DNS-записів (для L7-захисту) або анонсуванням IP-адрес через BGP (для L3/L4-захисту). Провайдер аналізує трафік у своїх центрах очищення (scrubbing centers) і доставляє до сервера клієнта лише легітимні запити.

Типи хмарних рішень:

CDN-based (на основі мережі доставки контенту). Завжди активний («always-on») захист, де DDoS-фільтрація є частиною глобальної мережі, що також прискорює доставку контенту;

On-Demand (за запитом). Трафік перенаправляється до центрів очищення лише після виявлення атаки.

Провідні провайдери: Cloudflare, Akamai, Imperva, AWS Shield, Google Cloud Armor [10-14].

Переваги:

практично необмежена масштабованість. Глобальні провайдери мають мережі з пропускною здатністю в десятки та сотні терабіт на секунду, що дозволяє витримувати найпотужніші волюметричні атаки;

відсутність капітальних витрат. Модель оплати за підпискою (OpEx), що робить її доступною для бізнесу будь-якого розміру;

простота впровадження. Зазвичай вимагає лише зміни DNS-записів, що займає кілька хвилин;

експертиза провайдера. Клієнт отримує доступ до досвіду та знань команди безпеки світового рівня.

Недоліки:

можливе збільшення затримки. Перенаправлення трафіку через третю сторону може додати мілісекунди до часу відповіді. Втім, сучасні CDN-провайдери часто навіть зменшують затримку завдяки кешуванню;

менший контроль. Конфігурація та політики залежать від можливостей, що надає провайдер;

ризики, пов'язані з третіми сторонами. Залежність від стабільності та безпеки самого провайдера.

Гібридні рішення (Hybrid). Ця модель поєднує найкращі аспекти локального та хмарного підходів.

Принцип роботи – локальний пристрій (On-Premise) обробляє постійний трафік і відбиває невеликі та середні атаки, зокрема на рівні додатків (L7). У разі виявлення потужної волюметричної атаки, яка загрожує перевантажити інтернет-канал, локальний пристрій автоматично сигналізує хмарному провайдеру про необхідність перенаправити трафік на глобальні центри очищення. Провідні вендори: Radware, F5 Networks [8, 15].

Переваги:

найкраща ефективність. Мінімальна затримка в мирний час та практично необмежена масштабованість під час потужних атак;

комплексний захист. Ефективний проти всіх типів атак, від низькорівневих флудів до складних атак на логіку додатків.

Недоліки:

найвища складність та вартість. Потребує інтеграції двох різних систем та є найдорожчим варіантом, що поєднує CapEx та OpEx;

складність управління. Вимагає злагодженої роботи локальної команди та хмарного провайдера.

Оскільки хмарні рішення є домінуючими на ринку, розглянемо ключових гравців. Результати їхнього порівняльного аналізу наведено в таблиці 1.2.

В контексті захисту від DDoS-атак, WAF є ключовим компонентом для протидії атакам на рівні додатків (L7). На відміну від мережевих фільтрів, WAF

аналізує HTTP/S запити, розуміючи їхню логіку.

Таблиця 1.2

Порівняльний аналіз провідних хмарних провайдерів

Критерій	**Cloudflare**	**Akamai (Prolexic)**	**AWS Shield Advanced**
Модель роботи	CDN-based, always-on.	CDN-based (Kona Site Defender) та Cloud Scrubbing (Prolexic).	Інтегрований сервіс для ресурсів AWS.
Масштабованість	Дуже висока (мережа >200 Tbps).	Дуже висока (мережа >200 Tbps).	Висока, інтегрована з глобальною інфраструктурою AWS.
Захист L7	Потужний WAF, захист API, управління ботами.	Потужний WAF, захист API, управління ботами.	Інтеграція з AWS WAF, гнучкі правила.
Простота використання	Дуже висока. Інтуїтивно зрозумілий інтерфейс, швидке налаштування.	Середня. Вимагає більше технічної експертизи.	Середня. Призначений для користувачів екосистеми AWS.
Час реакції (TTM)	Миттєвий (завдяки always-on моделі).	Миттєвий для always-on, хвилини для on-demand.	Дуже низький для ресурсів AWS (секунди).
Цінова політика	Прозора, є безкоштовний тариф. Передбачувана вартість.	Висока. Орієнтована на великі ентерпрайз-компанії.	Фіксована місячна плата + плата за трафік. Може бути дорого.
Додаткові переваги	CDN, оптимізація продуктивності, Serverless (Workers).	Глибока експертиза в безпеці, широке портфоліо рішень.	Глибока інтеграція з AWS, захист від сплат за трафік під час атак.
Ідеально для	SMB, стартапів, великих компаній, які шукають універсальне рішення.	Великих корпорацій, фінансового сектору, де потрібен	Компаній, що повністю або переважно працюють в

Критерій	Cloudflare	Akamai (Prolexic)	AWS Shield Advanced
		максимальний рівень захисту.	інфраструктурі AWS.

WAF захищає від L7 DDoS завдяки реалізації таких функцій:

рейт-лімітинг – обмежує кількість запитів з однієї IP-адреси;

блокування за сигнатурами – виявляє відомі вектори атак (наприклад, Slowloris);

аналіз поведінки – використовує машинне навчання для виявлення аномальної активності, що схожа на дії бота;

перевірка «людяності» – використовує CAPTCHA або JavaScript-челенджі для відсіювання автоматизованого трафіку.

Отже, сучасний захист від DDoS-атак неможливий без інтегрованого та інтелектуального WAF. Більшість провідних хмарних провайдерів пропонують WAF як частину свого комплексного рішення.

Вибір правильного рішення – це не пошук «найкращого», а пошук «найбільш відповідного» для конкретних завдань.

Необхідно проводити оцінку ризиків. Які активи є критичними? Якими будуть фінансові та репутаційні втрати від простою протягом години, дня?

Треба враховувати тип корпоративної інфраструктури. Чи розташовані корпоративні додатки в одному дата-центрі, чи вони розподілені по хмарних провайдерах (multi-cloud)? Для інфраструктури в AWS логічним вибором може стати AWS Shield, тоді як для multi-cloud краще підійде агностичне рішення, як Cloudflare або Akamai [16].

Необхідно враховувати пропускну здатність та трафік. Який звичайний обсяг корпоративного трафіку? Це допоможе розрахувати вартість послуг, особливо у провайдерів, що тарифікують за обсягом.

Треба проводити технічну експертизу. Чи є у вас команда, яка здатна керувати складними локальними або гібридними системами? Якщо ні, кероване

хмарне рішення буде кращим вибором.

Необхідно враховувати наявний бюджет. Визначте, що є прийнятним: високі капітальні витрати (On-Premise) чи регулярні операційні (Cloud).

Треба ретельно вивчати пропоновану SLA (Угода про рівень обслуговування). Уважно вивчіть, що гарантує провайдер. Який гарантований час реакції на атаку? Які компенсації передбачені за недотримання SLA?

Найкращим вибором для малого та середнього бізнесу (SMB)є хмарні CDN-based рішення (наприклад, Cloudflare Pro/Business). Вони пропонують відмінний баланс ціни, простоти управління та ефективності, забезпечуючи надійний захист «з коробки».

Для великих підприємств та E-commerce варто розглядати просунуті хмарні рішення від лідерів ринку (Cloudflare Enterprise, Akamai) або, за наявності специфічних вимог до затримок, гібридні моделі.

Для фінансового сектора та державних організацій тощо, де вимоги до безпеки та надійності максимальні, часто обирають преміальні хмарні сервіси (Akamai Prolexic) або складні гібридні архітектури.

Як висновок, у 2025 році питання захисту від DDoS-атак остаточно перейшло з технічної площини у стратегічну. Домінування хмарних рішень є беззаперечним завдяки їхній масштабованості, гнучкості та економічній доступності. Локальні системи залишаються нішевим рішенням для специфічних завдань, тоді як гібридні моделі пропонують найвищий рівень захисту ціною високої складності.

Ключовим фактором успіху є не лише вибір технології, але й побудова комплексної стратегії безпеки, що включає захист на всіх рівнях, моніторинг у реальному часі та регулярне тестування стійкості інфраструктури. Правильно обране рішення дозволить не просто «пережити» атаку, а й гарантувати безперебійну роботу бізнесу в умовах постійно зростаючих кіберзагроз.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS WAF

2.1. Призначення та основні функції рішення AWS WAF

AWS WAF – це брандмауер веб-застосунків, який дозволяє контролювати HTTP(S)-запити, що пересилаються до ресурсів корпоративного захищеного веб-застосунку. Ми можемо захистити такі типи ресурсів [17]:

розповсюдження Amazon CloudFront;

API шлюзу Amazon REST;

балансувальник навантаження застосунків;

API GraphQL AWS AppSync;

пул користувачів Amazon Cognito;

сервіс AWS App Runner;

екземпляр перевіреного доступу AWS;

AWS Amplify.

AWS WAF дозволяє нам контролювати доступ до корпоративного контенту. На основі вказаних нами критеріїв, таких як IP-адреси, з яких надходять запити, або значення рядків запиту, служба, пов’язана з корпоративним захищеним ресурсом, відповідає на запити або запитуваним контентом, або кодом стану HTTP 403 (Заборонено), або власною відповіддю.

Ми також можемо використовувати AWS WAF для захисту корпоративних додатків, розміщених у контейнерах Amazon Elastic Container Service (Amazon ECS). Amazon ECS – це високомасштабована, швидка служба керування контейнерами, яка спрощує запуск, зупинку та керування контейнерами Docker у кластері. Щоб скористатися цією опцією, потрібно налаштувати Amazon ECS на використання балансувальника навантаження додатків, увімкненого для AWS WAF, для маршрутизації та захисту трафіку HTTP(S) рівня 7 між завданнями у відповідній службі.

AWS WAF (Web Application Firewall) – це фаєрвол рівня додатків, який допомагає захистити ваші веб-додатки та API від поширених веб-експлойтів та ботів, що можуть вплинути на доступність, порушити безпеку або споживати надмірну кількість ресурсів.

Він працює на 7-му рівні (Application Layer) моделі OSI, аналізуючи вміст HTTP/HTTPS запитів.

Головна мета AWS WAF – фільтрація вхідного трафіку перед тим, як він досягне корпоративних серверів. Він вирішує три критичні завдання [20]:

захист від зламу. Блокування атак типу SQL Injection (SQLi), Cross-Site Scripting (XSS) та інших вразливостей з переліку OWASP Top 10;

захист від ботів. Запобігання скрапінгу контенту, спаму та DDoS-атакам рівня додатків (HTTP floods);

контроль доступу. Дозвіл або заборона доступу на основі географії, IP-адрес або характеристик запиту.

Розглянемо основні функції та можливості AWS WAF.

1. Гнучкі правила фільтрації (Web ACLs)

Основою роботи WAF є списки контролю доступу (Web ACL), які містять правила. Правила можуть діяти за логікою: Block (блокувати), Allow (дозволити) або Count (тільки рахувати для аналітики). Ми можемо фільтрувати трафік за:

IP-адресами (або діапазонами CIDR);

країною походження (Geo-blocking);

заголовками запитів (Headers), тілом запиту (Body) або URI;

довжиною запиту (щоб уникнути переповнення буфера).

2. AWS Managed Rules (Керовані правила)

Щоб не писати кожне правило вручну, AWS надає готові набори правил (Managed Rulesets), які автоматично оновлюються при появі нових загроз.

Core rule set (CRS) – захист від найпоширеніших загроз.

Admin protection – блокування доступу до адмін-панелей із зовнішніх мереж.

IP reputation lists – блокування IP-адрес, відомих як джерела спаму або ботнетів (на базі даних Amazon Threat Intelligence).

3. Захист від ботів (Bot Control)

Це просунута функція, яка дозволяє розрізняти «хороших» ботів (наприклад, Googlebot) від «поганих» (скрапери, сканери вразливостей). Вона може використовувати CAPTCHA або JavaScript challenge для перевірки, чи є клієнт реальною людиною.

4. Інтеграція з сервісами AWS

AWS WAF не встановлюється на сам сервер (EC2). Він прикріплюється до точок входу трафіку в інфраструктуру:

Amazon CloudFront (CDN);

Application Load Balancer (ALB);

Amazon API Gateway (для захисту REST та WebSocket API);

AWS AppSync (для GraphQL API).

5. Моніторинг та логування у реальному часі

WAF інтегрується з Amazon CloudWatch, надаючи графіки заблокованих та дозволених запитів. Також можна налаштувати повне логування (Full Logging) через Amazon Kinesis Firehose для подальшого аналізу в SIEM-системах (наприклад, Splunk або ElasticSearch).

Розглянемо, як це працює на практиці (приклад сценарію). Уявіть, що ми виявили атаку, де зловмисники намагаються підібрати паролі до нашого API. Ми можемо швидко налаштувати AWS WAF таким чином:

увімкнути Rate-based rule: «Якщо одна IP-адреса робить більше 100 запитів на хвилину до /login, заблокувати цю IP на 5 хвилин».

Це правило працюватиме автоматично, відсікаючи атакувальників, при цьому звичайні користувачі не помітять змін.

Враховуючи наш інтерес до автоматизації захисту, варто зазначити, що AWS WAF має повний API. Це дозволяє створювати автоматичні сценарії реагування. Наприклад: Lambda-функція аналізує логи, знаходить підозрілі IP і автоматично додає їх у чорний список WAF.

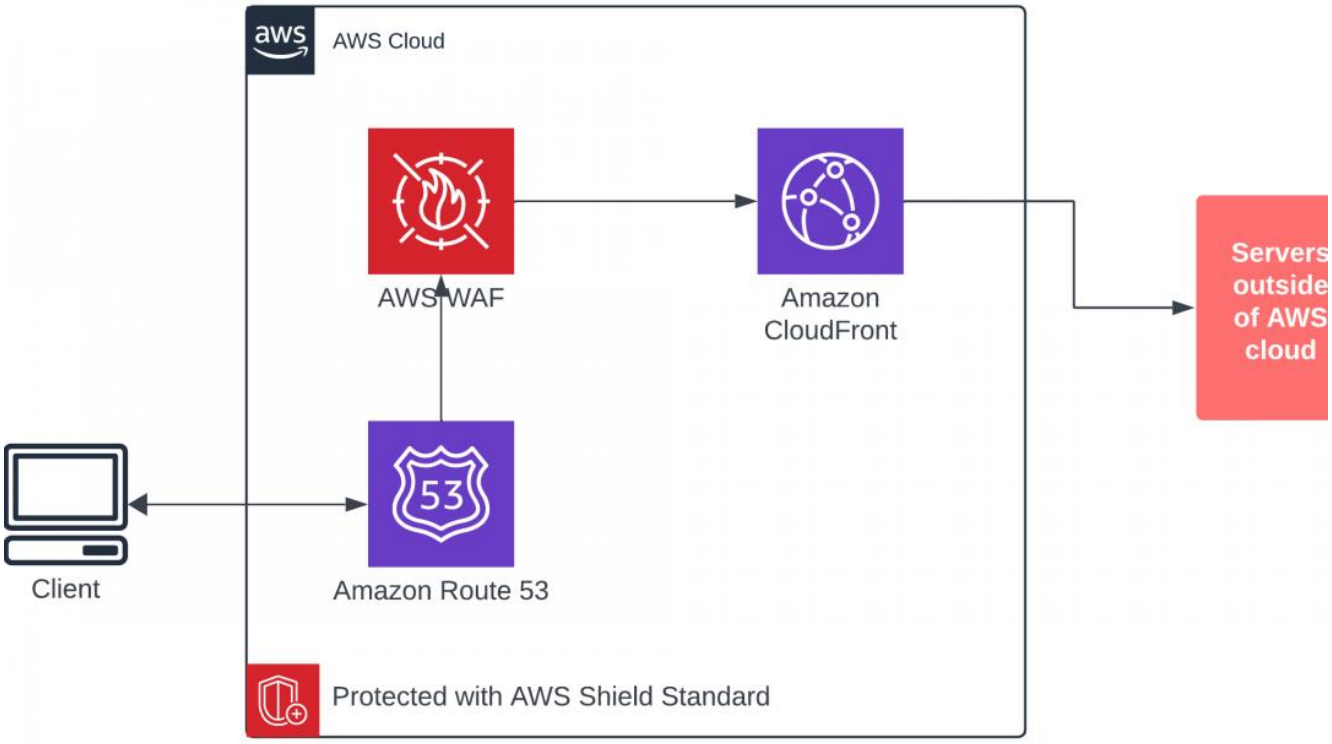

Рис. 2.1. Місце AWS WAF в архітектурі безпеки AWS [20]

До основних компонентів AWS WAF відносяться наступні [20]:

правила: AWS WAF дозволяє створювати правила, які визначають типи трафіку, які ви хочете дозволити або заблокувати доступ до ваших веб-додатків. Ви можете створювати правила на основі різних умов, таких як IP-адреси, заголовки HTTP, рядки URI та вміст тіла HTTP;

керовані групи правил: AWS WAF надає попередньо створені керовані групи правил, які пропонують захист від поширених веб-атак, таких як SQL-ін'єкція, міжсайтовий сценарій (XSS) тощо. Ці групи правил створюються та підтримуються AWS і регулярно оновлюються, щоб забезпечити сучасний захист від останніх загроз;

веб-ACL: AWS WAF використовує веб-ACL (списки контролю доступу до Інтернету) для групування правил, які потім можна застосувати до одного або кількох веб-додатків. Веб-ACL дозволяють застосовувати набір правил у кількох веб-додатках, що полегшує керування та послідовне застосування політик безпеки.

Основні характеристики AWS WAF [20]:

1. Користувацькі правила безпеки. AWS WAF надає організаціям можливість створювати спеціальні правила безпеки, адаптовані до їхніх конкретних потреб безпеки. Це включає в себе керування трафіком ботів і перешкоджання поширеним векторам веб-атак, таким як SQL-ін'єкція та міжсайтовий сценарій.

2. Списки контролю доступу до Інтернету (веб-ACL). Веб-ACL є основною функцією AWS WAF, що дозволяє налаштовувати правила, відомі як списки керування веб-доступом. Ці правила можуть бути встановлені для дозволу, блокування або підрахунку веб-запитів на основі різних умов, забезпечуючи детальний рівень контролю над веб-трафіком.

3. Інтеграція з AWS Services. AWS WAF розроблено для бездоганної інтеграції з безліччю служб AWS, включаючи Amazon CloudFront, Application Load Balancer і Amazon API Gateway. Ця інтеграція зміцнює веб-додатки, забезпечуючи цілісний периметр безпеки.

2.2. Архітектура рішення AWS WAF

AWS WAF – це брандмауер веб-застосунків, який дозволяє фахівцям контролювати та керувати веб-запитами, що пересилаються до захищених ресурсів AWS. За допомогою AWS WAF ми можемо захистити такі ресурси, як дистрибутиви Amazon CloudFront, REST API Amazon API Gateway, балансувальники навантаження додатків та API AWS AppSync GraphQL. Ми можемо використовувати AWS WAF для перевірки веб-запитів на відповідність заданим умовам, таким як IP-адреса, з якої надходять запити, значення певного компонента запиту або швидкість надсилання запитів. AWS WAF може керувати запитами на відповідність різними способами, включаючи їх підрахунок, блокування або дозвіл, а також надсилання завдань, таких як головоломки CAPTCHA, користувачеві клієнта або браузеру [13].

Місце рішення AWS WAF в загальній архітектурі AWS та основний функціонал показано на рисунку 2.2:

AWS WAF – розгортає веб-список контролю доступу AWS WAF, групи

правил керованих правил AWS, користувацькі правила та набори IP-адрес. Здійснює виклики API AWS WAF для блокування поширених атак та захисту веб-застосунків.

Amazon Data Firehose – доставляє журнали AWS WAF до корзин Amazon S3.

Амазон S3 – зберігає журнали AWS WAF, CloudFront та ALB.

AWS Lambda – розгортає кілька лямбда-функцій для підтримки користувацьких правил.

Amazon EventBridge – створює правила подій для виклику Lambda.

Amazon Athena – створює запити Athena та робочі групи для підтримки парсера журналів Athena.

AWS Glue – створює бази даних і таблиці для підтримки парсера журналів Athena.

Amazon SNS – надсилає сповіщення електронною поштою Amazon Simple Notification Service (Amazon SNS) для підтримки збереження IP-адрес у списках дозволених та заборонених.

AWS Systems Manager – забезпечує моніторинг ресурсів на рівні додатка та візуалізацію операцій з ресурсами та даних про витрати.

Архітектура розгортання рішення AWS WAF в корпоративному хмарному середовищі з параметрами за замовчуванням вкорпоративному обліковому записі AWS показано на рисунку 2.1. Шаблон CloudFormation розгортає AWS WAF та інші ресурси AWS для захисту корпоративних веб-додатків від поширених атак.

В основі дизайну AWS WAF лежить веб-список контролю доступу (ACL), який діє як центральна точка перевірки та прийняття рішень для всіх вхідних запитів до веб-застосунку. Під час початкового налаштування стеку CloudFormation користувач визначає, які захисні компоненти активувати. Кожен компонент працює незалежно та додає різні правила до веб-списку контролю доступу.

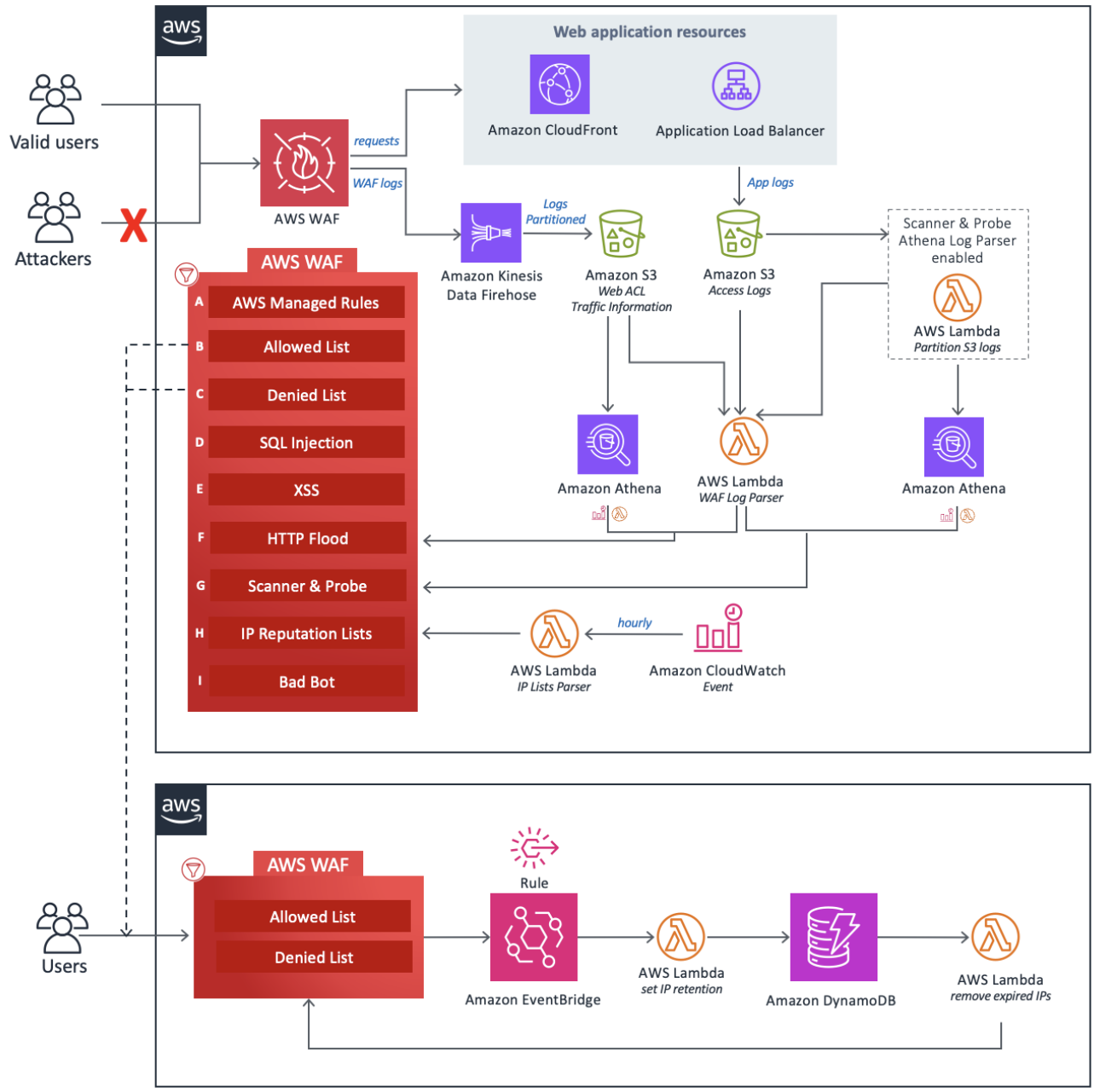

Рис. 2.2. Місце в архітектурі корпоративного хмарного середовища та функції безпеки AWS WAF [18]

Компоненти рішення AWS WAF можна згрупувати в такі області захисту [18]:

керовані правила AWS (A) – цей компонент містить групи правил репутації IP-адрес керованих правил AWS, групи базових правил та групи правил для конкретних випадків використання. Ці групи правил захищають від експлуатації поширених вразливостей програм або іншого небажаного трафіку, включаючи ті,

що описані в публікації OWASP, без необхідності писати власні правила;

ручні списки IP-адрес (B та C) – ці компоненти створюють два правила AWS WAF. За допомогою цих правил ми можемо вручну вставляти IP-адреси, які потрібно дозволити або заборонити. Ми можемо налаштувати збереження IP-адрес та видалити прострочені IP-адреси з дозволених або заборонених наборів IP-адрес за допомогою правил Amazon EventBridge та Amazon DynamoDB;

SQL-ін'єкція (D) та XSS (E) – ці компоненти налаштовують два правила AWS WAF, призначені для захисту від поширених шаблонів SQL-ін'єкцій або міжсайтового скриптингу (XSS) в URI, рядку запиту або тілі запиту;

HTTP Flood (F) – цей компонент захищає від атак, що складаються з великої кількості запитів з певної IP-адреси, таких як DDoS-атака на веб-рівні або спроба входу методом грубої сили. За допомогою цього правила ми встановлюємо квоту, яка визначає максимальну кількість вхідних запитів, дозволених з однієї IP-адреси протягом стандартного п'ятихвилинного періоду (налаштовується за допомогою параметра «Розклад часу виконання запиту Athena»). Після порушення цього порогу додаткові запити з IP-адреси тимчасово блокуються. Ми можемо реалізувати це правило, використовуючи правило AWS WAF на основі швидкості або обробляючи журнали AWS WAF за допомогою функції Lambda або запиту Athena;

сканер і зонд (G) – цей компонент аналізує журнали доступу до додатків, шукаючи підозрілу поведінку, таку як аномальна кількість помилок, згенерованих джерелом. Потім він блокує ці підозрілі IP-адреси джерел на визначений клієнтом період часу. Ми можемо реалізувати це правило за допомогою виразу функції Lambda або запиту Athena;

списки репутації IP-адрес (H) – цей компонент є IP Lists Parser функцією Lambda, яка щогодини перевіряє списки репутації IP-адрес третіх сторін на наявність нових діапазонів для блокування. Ці списки включають списки Spamhaus Don't Route Or Peer (DROP) та Extended DROP (EDROP), список IP-адрес Proofpoint Emerging Threats та список вихідних вузлів Tor;

поганий бот (I) – цей компонент покращує виявлення шкідливих ботів,

моніторячи прямі підключення до балансувальника навантаження програм (ALB) або Amazon CloudFront, на додаток до механізму honeypot. Якщо бот обходить honeypot і намагається взаємодіяти з ALB або CloudFront, система аналізує шаблони запитів і журнали, щоб виявити шкідливу активність. Коли виявляється шкідливий бот, його IP-адреса витягується та додається до списку блокування AWS WAF, щоб запобігти подальшому доступу. Виявлення шкідливих ботів працює через структурований логічний ланцюжок, що забезпечує комплексне охоплення загроз:

захист від HTTP Flood Lambda Log Parser – збирає погані IP-адреси ботів із записів журналу під час аналізу флуду;

захист сканера та зонда Lambda Log Parser – Виявляє погані IP-адреси ботів із записів журналу, пов’язаних зі сканером;

захист від HTTP-флуду. Парсер журналів Athena – витягує погані IP-адреси ботів із журналів Athena, використовуючи розділи під час виконання запиту;

захист сканера та зонда. Аналізатор журналів Athena – отримує погані IP-адреси ботів із журналів Athena, пов’язаних зі сканером, використовуючи ту саму стратегію розділення;

виявлення резервного доступу – якщо вимкнено захист від HTTP-перевантаження та захист від сканера та зонда, система покладається на парсер Log Lambda, який реєструє активність бота на основі фільтрів міток WAF.

Кожна з трьох користувацьких функцій Lambda у цьому рішенні публікує показники виконання до CloudWatch.

Таблиця 2.1

Перелік сервісів AWS

Сервіс AWS	**Опис**
AWS WAF	**Core**. Розгортає веб-список контролю доступу AWS WAF, групи правил керованих правил AWS, користувацькі правила та набори IP-адрес. Здійснює виклики API AWS WAF для блокування поширених атак та захисту веб-застосунків.
Amazon Data Firehose	**Core**. Доставляє журнали AWS WAF до корзин Amazon S3.

Сервіс AWS	Опис
Amazon S3	**Core**. Зберігає журнали AWS WAF, CloudFront та ALB.
AWS Лямбда	**Core**. Розгортає кілька функцій Lambda для підтримки користувацьких правил.
Amazon EventBridge	**Core**. Створює правила подій для виклику Lambda.
Amazon Athena	**Підтримка**. Створює запити Athena та робочі групи для підтримки парсера журналів Athena.
AWS Glue	**Підтримка**. Створює бази даних і таблиці для підтримки парсера журналів Athena.
Amazon SNS	**Підтримка**. Надсилає сповіщення електронною поштою Amazon Simple Notification Service (Amazon SNS) для підтримки збереження IP-адрес у списках дозволених та заборонених.
AWS Systems Manager	**Підтримка**. Забезпечує моніторинг ресурсів на рівні програми та візуалізацію операцій з ресурсами та даних про витрати.

2.3. Порядок функціонування рішення AWS WAF

Рішення AWS WAF застосовується, щоб контролювати, як корпоративні захищені ресурси відповідають на веб-запити HTTP(s). Це можна зробити, визначивши список керування доступом до Інтернету (web ACL), а потім пов’язавши його з одним або кількома веб-сайтами ресурси додатків, які ми хочемо захистити. Пов’язані ресурси пересилають вхідні запити до AWS WAF для перевірки веб-ACL.

Консоль спрощує процес конфігурації веб ACL. Вона представляє пакети захисту для оптимізації налаштування, зберігаючи при цьому повну контроль над своїми правилами безпеки.

Пакети захисту є новим місцем для веб-ACL і спрощують керування веб-ACL у консолі, але вони не змінюють базову функціональність веб-ACL. При використанні стандарту консолі або API, нам все одно потрібно працювати безпосередньо з веб-ACL.

У нашому пакеті захисту (веб-ACL) ми створюємо правила для визначення шаблонів трафіку, які потрібно шукати в запитах, і для визначення дій, які потрібно

виконати для відповідних запитів. Вибір дій включає наступне:

дозволити запитам перейти до захищеного ресурсу для обробки та відповіді;

блокувати запити;

підрахувати запити;

запустити CAPTCHA або викликати перевірки запитів на перевірку користувачів і стандартне використання браузера.

Розглянемо основні компоненти AWS WAF:

веб ACL – ми використовуємо список контролю доступу до Інтернету (web ACL) для захисту набору ресурсів AWS. Ми створюємо веб-ACL і визначаємо його стратегію захисту шляхом додавання правил. Правила визначають критерії перевірки веб-запити, і вони визначають дії, які необхідно виконати щодо запитів, які відповідають їх критерії. Ми також встановлюємо дію за замовчуванням для веб-ACL, яка вказує чи блокувати чи дозволяти будь-які запити, яких немає в правилах вже заблоковані або дозволені;

пакет захисту (Web ACL) – у новому консолі, пакети захисту є новим місцем для корпоративних веб-ACL. Під час налаштування ми надаємо інформацію про корпоративні додатки та ресурси. AWS WAF рекомендує захисний пакет, адаптований до наш сценарій, а потім створює веб-ACL, який містить правила, групи правил і дії визначається пакетом захисту (веб ACL), який ми вибираємо;

правила – кожне правило містить твердження, що визначає критерії перевірки та дії, які необхідно вжити, якщо веб-запит відповідає критеріям. Коли веб-запит відповідає критеріям, це збігається. Ми можемо налаштувати правила для блокування відповідних запитів, дозволити їх через, порахуйте їх або запустіть проти них елементи керування ботами, які використовують головоломки CAPTCHA або тихі виклики браузера клієнта. Правило не є ресурсом AWS WAF. Він існує лише в контексті пакета захисту (веб-ACL) або групи правил;

групи правил – ви можете визначити правила безпосередньо всередині пакет захисту (веб-ACL) або в групах правил багаторазового використання. Керовані правила AWS і продавці AWS Marketplace надають керовані групи правил для нашого використання. Ми також можемо визначити власні групи правил. Група

правил - це ресурс AWS WAF;

веб-одиниці ємності ACL (WCU) – AWS WAF використовує WCU для розрахунку та контролю операційних ресурсів, необхідних для запуску наших правил, груп правил, пакетів захисту (веб-ACL) або веб-ACL. WCU не є ресурсом AWS WAF. Він існує лише в контексті захисного пакета (веб-ACL), правила або групи правил.

Початок роботи з AWS WAF залежить від того, який інтерфейс консолі ми використовуємо. Обидва інтерфейси надають доступ до однакових основних функцій AWS WAF, але відрізняються способом налаштування та керування захистом веб-застосунків.

AWS WAF пропонує два варіанти використання консолі [17]:

нова консоль має на меті спростити процес налаштування веб-списків контролю доступу (ACL), який вимагається стандартними робочими процесами консолі. Ми можемо використовувати керовані робочі процеси для спрощення процесу створення та керування веб-списками контролю доступу (ACL) за допомогою пакета захисту. Пакет захисту спрощує використання та керування веб-списками контролю доступу (ACL) у консолі, але функціонально не відрізняється від веб-списків контролю доступу (ACL). Окрім покращеного процесу налаштування захисту, нова консоль пропонує покращену видимість корпоративних засобів захисту через панелі інструментів безпеки, що спрощує моніторинг стану безпеки в консолі AWS WAF;

стандартна консоль AWS WAF пропонує традиційний підхід до налаштування захисту брандмауера веб-застосунків за допомогою веб-списків контролю доступу (ACL). Вона пропонує детальний контроль над окремими правилами та групами правил і знайома існуючим користувачам AWS WAF. За допомогою цієї консолі ми маємо детальний контроль над конфігураціями захисту, що дозволяє точно налаштовувати параметри безпеки.

Ми використовуємо AWS WAF для керування тим, як корпоративні захищені ресурси реагують на веб-запити HTTP(S). Ми робимо це, визначаючи список керування веб-доступом (веб-ACL), а потім пов’язуючи його з одним або кількома

ресурсами веб-застосунку, які ми хочемо захистити. Пов’язані ресурси пересилають вхідні запити до AWS WAF для перевірки веб-ACL.

Нова консоль спрощує процес налаштування веб-списку контролю доступу (ACL). Вона пропонує пакети захисту для оптимізації налаштування, зберігаючи при цьому повний контроль над правилами безпеки.

Пакети захисту – це нове місце для веб-списків контролю доступу (ACL) і спрощують керування веб-списками контролю доступу в консолі, але вони не змінюють базову функціональність веб-списків контролю доступу (ACL). Під час використання стандартної консолі або API ми все ще працюватимо безпосередньо з веб-списками контролю доступу.

У нашому пакеті захисту (веб-списку контролю доступу) ми створюємо правила для визначення шаблонів трафіку, які слід шукати в запитах, і для визначення дій, які потрібно виконувати для відповідних запитів. Варіанти дій включають наступне [17]:

дозволяємо запитам надсилати їх до захищеного ресурсу для обробки та отримання відповіді;

блокуємо запити;

підрахуємо запити.

Виконуємо CAPTCHA або перевірки на відповідність запитам, щоб підтвердити, що користувачі-люди та стандартне використання браузера використовуються користувачами.

Розглянемо компоненти AWS WAF. Основними компонентами AWS WAF є [17]:

веб-списки контролю доступу (ACL). Ми використовуємо список контролю доступу до веб-сайтів (веб-список контролю доступу) для захисту набору ресурсів AWS. Ми створюємо веб-список контролю доступу (ACL) та визначаємо його стратегію захисту, додаючи правила. Правила визначають критерії для перевірки веб-запитів і вказують дію, яку потрібно виконати щодо запитів, що відповідають їхнім критеріям. Ми також встановлюємо дію за замовчуванням для веб-списку контролю доступу (ACL), яка вказує, чи блокувати, чи дозволяти будь-які запити,

які правила ще не заблокували або не дозволили;

веб-список контролю доступу (ACL) – це ресурс AWS WAF;

пакети захисту (веб-ACL) – у новій консолі пакети захисту – це нове розташування для корпоративних веб-ACL. Під час налаштування ви надаєте інформацію про свої програми та ресурси. AWS WAF рекомендує пакет захисту, адаптований до корпоративного сценарію, а потім створює веб-ACL, який містить правила, групи правил та дії, визначені вибраним вами пакетом захисту (веб-ACL). Пакет захисту (веб-ACL) – це ресурс AWS WAF;

правила – кожне правило містить оператор, який визначає критерії перевірки, та дію, яку потрібно виконати, якщо веб-запит відповідає критеріям. Коли веб-запит відповідає критеріям, це вважається збігом. Ми можемо налаштувати правила для блокування відповідних запитів, пропускання їх, підрахунку або запуску ботів-керувань, які використовують головоломки CAPTCHA або тихі перевірки браузера клієнта. Правило не є ресурсом AWS WAF. Воно існує лише в контексті пакета захисту (веб-ACL) або групи правил;

групи правил – ми можемо визначати правила безпосередньо всередині пакета захисту (веб-ACL) або в групах правил повторного використання. Керовані правила AWS та продавці AWS Marketplace надають керовані групи правил для корпоративного використання. Ми також можемо визначати власні групи правил. Група правил – це ресурс AWS WAF;

одиниці потужності веб-ACL (WCU) – AWS WAF використовує WCU для розрахунку та контролю операційних ресурсів, необхідних для виконання корпоративних правил, груп правил, пакетів захисту (веб-ACL) або веб-ACL. WCU не є ресурсом AWS WAF. Він існує лише в контексті пакета захисту (веб-ACL), правила або групи правил.

Розглянемо, що таке пакети захисту (веб-списки ACL) і як вони працюють.

Пакет захисту (веб-ACL) надає нам детальний контроль над усіма веб-запитами HTTP(S), на які відповідає корпоративний захищений ресурс. Ми можемо захистити ресурси Amazon CloudFront, Amazon API Gateway, Application Load Balancer, AWS AppSync, Amazon Cognito, AWS App Runner, AWS Amplify, Amazon

CloudWatch та AWS Verified Access.

Ми можемо використовувати такі критерії, як наведено нижче, щоб дозволити або заблокувати запити [17]:

IP-адреса джерела запиту;

країна походження запиту;

збіг рядка або регулярного виразу (regex) у частині запиту;

розмір певної частини запиту;

виявлення шкідливого SQL-коду або скриптів.

Ми також можемо перевірити будь-яку комбінацію цих умов. Ми можемо блокувати або підраховувати веб-запити, які не лише відповідають заданим умовам, але й перевищують певну кількість запитів за одну хвилину. Ми можемо комбінувати умови за допомогою логічних операторів. Ми також можемо запускати головоломки CAPTCHA та тести тихих сеансів клієнта для запитів.

Ми вказуємо критерії відповідності та дії, які потрібно виконати щодо збігів, в інструкціях із правилами AWS WAF. Ми можемо визначати інструкції із правилами безпосередньо всередині корпоративного пакета захисту (веб-ACL) та в групах правил повторного використання, які ми використовуємо в своєму пакеті захисту (веб-ACL).

Під час створення пакета захисту (веб-ACL) ми вказуємо типи ресурсів, з якими його потрібно використовувати. Після визначення пакета захисту (веб-ACL) ми можемо пов’язати його зі своїми ресурсами, щоб розпочати забезпечення їх захисту.

3 ТЕХНОЛОГІЯ ЗАХИСТУ ВЕБ ДОДАТКІВ ВІД DDOS-АТАК НА ОСНОВІ AWS WAF

3.1. Порядок застосування рішення AWS WAF

Захист веб додатків від DDoS-атак за допомогою AWS WAF – це багаторівневий процес, який поєднує автоматичні засоби захисту та власні правила для фільтрації шкідливого трафіку. Розглянемо основні дії для реалізації ефективного захисту.

Крок 1: Створення архітектури та інтеграція AWS WAF.

Перш за все, важливо правильно побудувати архітектуру. AWS WAF працює разом з іншими сервісами AWS, тому ключовим є розміщення додатків за ресурсами, що підтримують WAF.

Необхідно використовувати AWS Edge сервіси: необхідно розмістити корпоративний додаток за Amazon CloudFront (для глобального контенту) або Application Load Balancer (ALB) (для регіонального). Це створює перший рубіж оборони та дозволяє WAF аналізувати трафік ще до того, як він досягне сервера.

Необхідно створити Web ACL (Access Control List): Web ACL – це контейнер для правил, які застосовуються до трафіку. Ми створюємо один Web ACL і пов’язуємо його з відповідним ресурсом (CloudFront або ALB).

Крок 2: Налаштування Керованих Правил (AWS Managed Rules).

Це найпростіший і найшвидший спосіб отримати базовий захист. AWS надає готові набори правил, розроблені для захисту від поширених загроз.

Amazon IP reputation list: необхідно увімкнути групу правил AmazonIpReputationList. Вона автоматично блокує запити з IP-адрес, які відомі як джерела ботів або іншої шкідливої активності.

Core rule set (CRS): необхідно додати групу правил AWSManagedRulesCommonRuleSet. Вона захищає від широкого спектра вразливостей, таких як SQL-ін’єкції та міжсайтовий скриптинг (XSS), які часто є

частиною DDoS-атак на рівні додатку.

Anonymous IP list: необхідно розглянути можливість увімкнення AWSManagedRulesAnonymousIpList для блокування трафіку з анонімних проксі, VPN та Tor, які часто використовуються для атак.

Bot Control: необхідно увімкнути групу правил для контролю ботів, щоб ідентифікувати та блокувати шкідливий автоматизований трафік.

Крок 3: Створення Власних Правил (Custom Rules).

Для більш специфічного захисту, адаптованого до конкретного додатку, необхідно створити власні правила. Правила на основі частоти запитів (Rate-Based Rules) – це найважливіший інструмент протидії HTTP-флуду (найпоширеніший тип DDoS-атак на рівні додатку).

Необхідно створити загальне правило: необхідно налаштувати правило, яке блокує будь-яку IP-адресу, що надсилає надмірну кількість запитів. Наприклад, заблокувати IP, якщо кількість запитів перевищує 1000 за 5 хвилин.

Необхідно створити специфічні правила: необхідно визначити «важкі» для корпоративного сервера запити (наприклад, сторінка входу, пошук, API-ендпоїнти) і встановіть для них більш жорсткі ліміти. Наприклад, не більше 100 запитів за 5 хвилин на сторінку /login.

Необхідно застосовувати географічне блокування (Geographic Match Rules). Якщо бізнес орієнтований на певні країни, можна заблокувати трафік з регіонів, звідки ми не очікуємо легітимних користувачів. Це може значно зменшити поверхню атаки.

Необхідно здійснювати блокування за IP-адресами (IP Set Match Rules). Під час атаки ми можемо аналізувати лог-файли, ідентифікувати IP-адреси зловмисників і додавати їх до списку блокування (IP set) вручну або автоматично.

Правила на основі сигнатур (String and Regex Match Rules). Необхідно створити правила, які перевіряють частини запиту (наприклад, User-Agent, URI, query string) на наявність певних патернів, характерних для атаки, і блокують їх.

Крок 4: Моніторинг, Логування та Автоматизація.

Захист – це безперервний процес, а не одноразове налаштування. Необхідно

ввімкнути логування. Обов’язково активуйте логування для корпоративного Web ACL. Логи можна надсилати в Amazon S3 через Kinesis Data Firehose для подальшого аналізу.

Необхідно налаштувати сповіщення. Використовується Amazon CloudWatch для моніторингу метрик WAF (наприклад, кількість заблокованих запитів). Необхідно налаштувати сповіщення (Alarms), які повідомлятимуть про аномальні сплески трафіку.

Здійснюється автоматизація реагування. Для цього використовується AWS Lambda для автоматизації реагування на загрози. Наприклад, можна створити функцію, яка автоматично аналізує логи, виявляє IP-адреси атакуючих і додає їх до списку блокування в WAF.

Крок 5: Інтеграція з AWS Shield Advanced.

Для критично важливих додатків рекомендується використовувати AWS Shield Advanced. AWS Shield Standard надається безкоштовно і захищає від поширених DDoS-атак на мережевому та транспортному рівнях (L3/L4). AWS Shield Advanced – це платний сервіс, що пропонує:

розширений захист від атак на рівні додатку (L7);

цілодобовий доступ до команди реагування на DDoS-атаки (DDoS Response Team);

захист від фінансових втрат, пов’язаних зі сплесками трафіку під час атаки;

автоматичне пом’якшення атак на рівні додатку.

Таким чином, поєднання AWS WAF з правильно налаштованими керованими та власними правилами, а також інтеграція з AWS Shield Advanced створює надійний та ешелонований захист від більшості видів DDoS-атак.

3.2. Технологія захисту веб додатків від DDoS-атак на основі AWS WAF

Технологія захисту веб-додатків від DDoS-атак на основі AWS WAF зосереджена на рівні додатків (рівень 7) моделі OSI, доповнюючи автоматичний захист на мережевому та транспортному рівнях, який надає AWS Shield Standard,

який доступний усім клієнтам AWS безкоштовно.

Нижче наведено покрокову технологію реалізації захисту веб додатків від DDoS-атак на основі AWS WAF:

1. Попередня підготовка та інтеграція

використання AWS-сервісів. Необхідно переконатися, що корпоративний веб-додаток розміщено за сумісними сервісами AWS, такими як Amazon CloudFront (рекомендовано для використання глобальної мережі AWS Edge locations та ізоляції від атак ближче до джерела трафіку), Application Load Balancer (ALB), Amazon API Gateway або AWS AppSync;

створення Web ACL. В консолі AWS WAF необхідно створити новий список контролю доступу до Інтернету (Web ACL). Цей Web ACL буде пов’язаний із вибраним ресурсом AWS (наприклад, CloudFront distribution або ALB);

дія за замовчуванням. Необхідно встановити дію за замовчуванням для Web ACL на *Allow* (Дозволити), а правила використовуватимуться для блокування шкідливого трафіку.

2. Впровадження правил AWS WAF для захисту від DDoS

Основна стратегія захисту полягає у використанні комбінації керованих (managed) та власних правил.

А. Керовані правила AWS (AWS Managed Rules)

Необхідно підписатися на відповідні керовані групи правил, які регулярно оновлюються AWS Threat Research Team:

AWSManagedRulesCommonRuleSet (CRS): забезпечує захист від поширених загроз, включно з OWASP Top 10, що може допомогти у виявленні аномальної активності, пов'язаної з DDoS;

AWSManagedRulesAnonymousIpList: блокує запити від анонімних проксі-серверів та вихідних вузлів Tor, які часто використовуються в DDoS-атаках;

AWSManagedRulesAmazonIpReputationList: автоматично блокує трафік із відомих шкідливих IP-адрес на основі даних AWS про загрози;

AWSManagedRulesBotControl: (оплачувана послуга) допомагає блокувати «поганих» ботів, одночасно дозволяючи «хорошим» ботам (наприклад, пошуковим

ботам).

B. Власні правила (Custom Rules)

Необхідно створити специфічні правила для додаткового захисту:

правила на основі ліміту запитів (Rate-based rules): це критично важливий елемент захисту від HTTP-флуд атак (Layer 7 DDoS);

Необхідно встановити порогове значення (наприклад, 2000 запитів за 5-хвилинний період) для окремої IP-адреси. Якщо кількість запитів перевищує ліміт, AWS WAF автоматично заблокує цю IP-адресу на певний час.

Також можна налаштувати агрегацію правил на основі різних параметрів, наприклад, IP-адреси та User-Agent, щоб точніше ідентифікувати аномальну поведінку.

правила блокування за географічною ознакою (Geo-match rules): якщо корпоративний додаток не обслуговує користувачів з певних країн, ми можемо заблокувати трафік з цих регіонів;

правила на основі сигнатур (String/Regex match rules): необхідно блокувати запити, що містять специфічні заголовки, URL-рядки або тіла запитів, характерні для відомих атак.

3. Моніторинг та автоматизація

логування (Logging): необхідно увімкнути детальне логування трафіку Web ACL до Amazon S3, Amazon CloudWatch Logs або Amazon Kinesis Data Firehose для аналізу та відстеження заблокованих запитів;

сповіщення (Alarms): необхідно налаштувати сповіщення через Amazon CloudWatch, щоб отримувати повідомлення про значне зростання трафіку, спрацьовування правил WAF або перевищення лімітів запитів;

AWS Shield Advanced: для критично важливих додатків необхідно розглянути підписку на AWS Shield Advanced. Він пропонує розширені можливості, включаючи автоматичне пом’якшення атак на рівні додатків (L7 automatic mitigation), виявлення на основі стану ресурсу та доступ до команди реагування на інциденти DDoS (SRT).

Рекомендований порядок правил (пріоритет)

Ефективний порядок правил допомагає оптимізувати витрати та швидкість реагування:

Allow (Дозволити) відомі надійні IP-адреси (адреси корпоративного офісу, систем моніторингу тощо);

блокувати відомі шкідливі IP-адреси (наприклад, через AmazonIpReputationList);

Bot Control (ідентифікація та маркування ботів);

Rate-based rules для обмеження аномального трафіку;

Інші керовані та власні правила (Geo-match, XSS, SQLi тощо).

Поєднання AWS WAF та AWS Shield забезпечує комплексний, багаторівневий захист від DDoS-атак.

3.3. Порядок дій для налаштування захисту веб-додатків від DDoS-атак за допомогою AWS WAF.

Розглянемо порядок дій для налаштування захисту веб-додатків від DDoS-атак (зокрема атак прикладного рівня L7) за допомогою AWS WAF.

Для ефективного захисту ми будемо використовувати комбінацію Managed Rules (керованих правил) та Rate-based Rules (обмеження частоти запитів).

Етап 1: Архітектурна підготовка (Best Practice)

Найкращий спосіб захиститися від DDoS – зупинити атаку ще до того, як вона досягне корпоративного серверу.

Використовуємо Amazon CloudFront для налаштування WAF не напряму на Load Balancer (ALB), а на CloudFront Distribution. CloudFront має величезну пропускну здатність і автоматично поглинає атаки рівня L3/L4 (через AWS Shield Standard).

AWS WAF буде фільтрувати HTTP/HTTPS трафік (L7).

Етап 2: Створення Web ACL (Access Control List)

Web ACL – це контейнер для правил захисту. Заходимо у консоль AWS та знаходимо сервіс *WAF & Shield*.

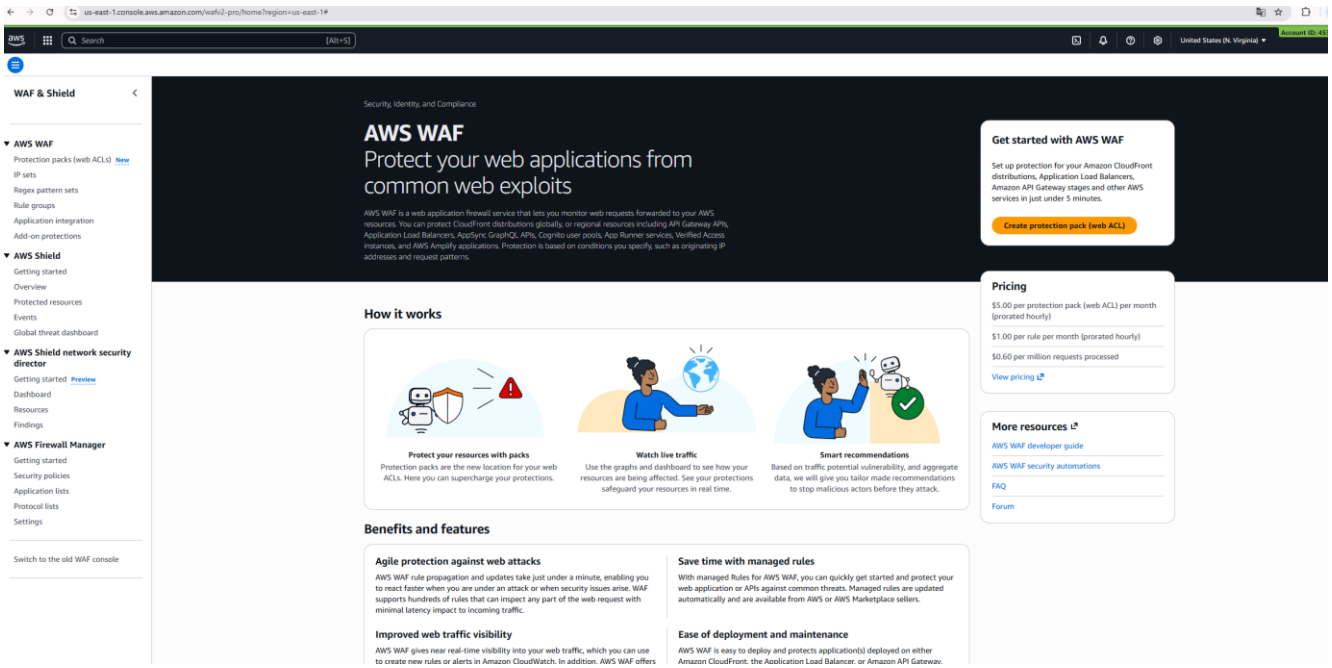

Рис. 3.1. Консоль AWS

У меню зліва виберіть *Web ACLs* та натискаємо помаранчеву кнопку *Create web ACL*.

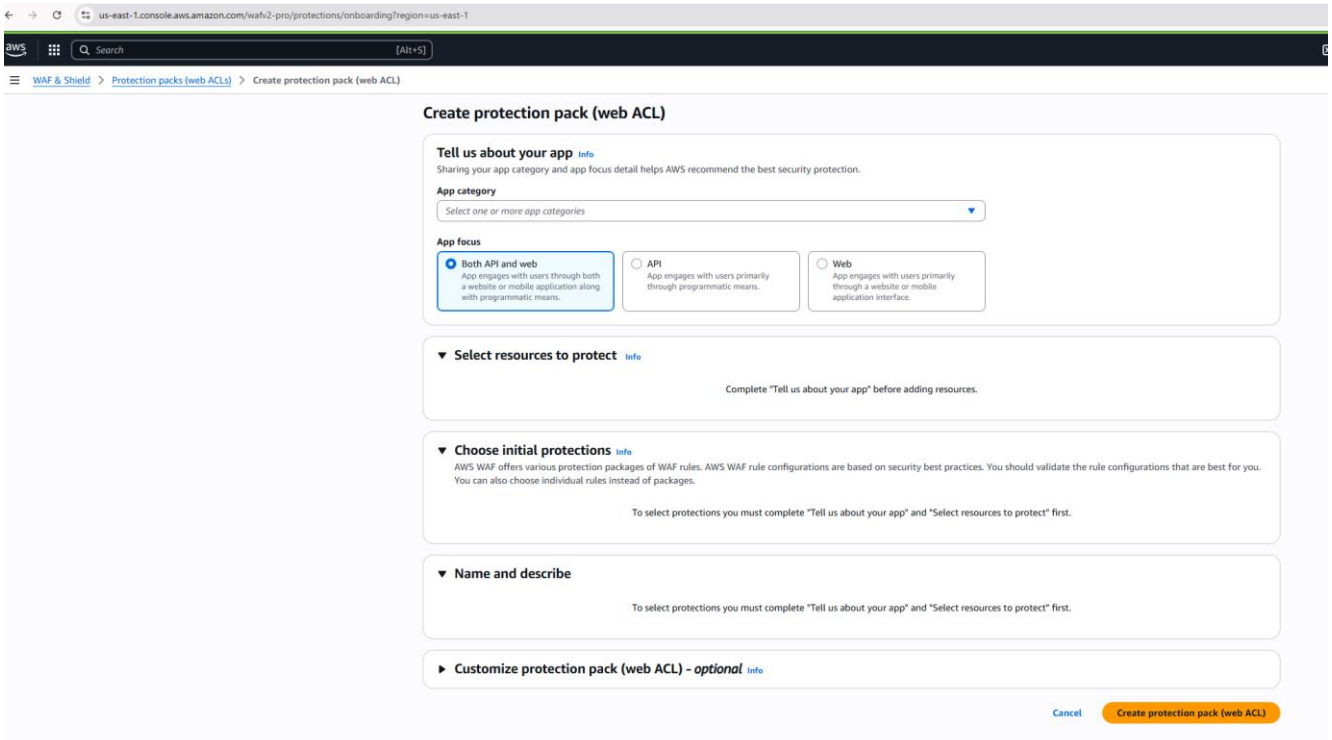

Рис. 3.2. Вкладка web ACL

Налаштування:

Name: вводимо зрозумілу назву (наприклад, *Main-App-Protection*).

Resource type: вибираємо *CloudFront distribution*, якщо ми використовуємо *CloudFront* (рекомендовано для DDoS), вибираємо *Regional resources*, якщо ми підключаємо WAF напряму до ALB або API Gateway.

Етап 3: Налаштування базового захисту (Managed Rules)

AWS надає готові набори правил, які оновлюються автоматично. Це «фундамент».

У розділі *Rules* натисніть *Add rules -> Add managed rule groups*.

Розгортаємо секцію *AWS managed rule groups*.

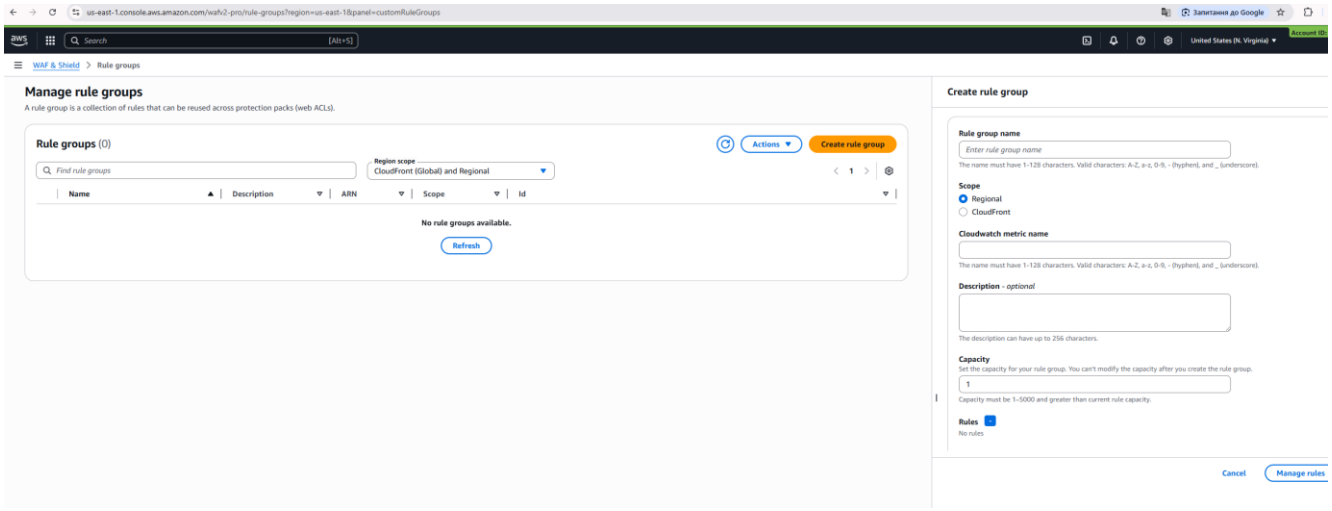

Рис. 3.3. Вкладка Manage rule group

Рекомендовані групи для включення:

Amazon IP reputation list: блокує IP-адреси, відомі як джерела ботнетів та DDoS-атак (обов'язково для DDoS);

Core rule set: захищає від загальних загроз (OWASP Top 10);

Known bad inputs: блокує запити з неправильними заголовками або підозрілими URL, які часто використовують DDoS-тулзи.

Після вибору натисніть *Add rules*.

Етап 4: Налаштування захисту від HTTP Flood (Rate-based Rules)

Це найважливіший крок для захисту від DDoS на рівні додатку. Ми створимо правило, яке автоматично блокує IP, якщо з нього надходить забагато запитів.

Натисніть *Add rules -> Add my own rules and rule groups*.

Rule type: вибираємо *Rate-based rule*.

Rate limit: Встановіть ліміт.

Приклад: 1000 або 2000. Це означає, що якщо одна IP-адреса зробить більше 1000 запитів за 5 хвилин, вона буде заблокована.

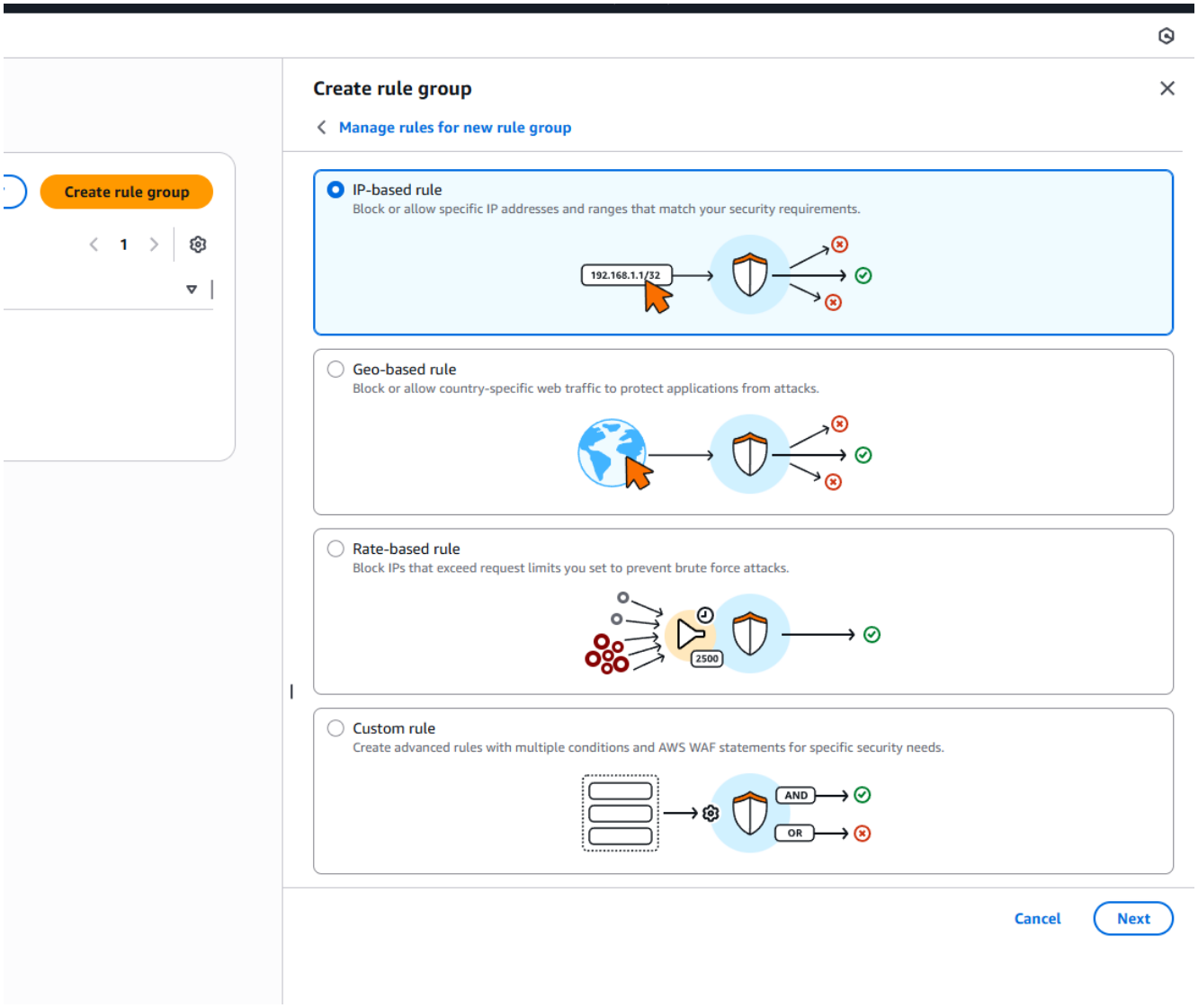

Рис. 3.4. Вкладка Create rule group

Необхідно подивитися свої логи, щоб зрозуміти нормальну активність користувача, і поставити ліміт трохи вище.

IP detection: вибираємо *Source IP address*.

Action: вибираємо *Block*.

Ми можемо створити кілька правил *Rate-based*. Наприклад:

загальне: 2000 запитів/5 хв на весь сайт;

логін: 100 запитів/5 хв на шлях /login (більш суворе правило для чутливих зон).

Етап 5: Гео-блокування (Geo-blocking)

Якщо наш бізнес працює лише в Україні та Європі, немає сенсу приймати трафік з інших континентів, звідки часто йдуть атаки. Для цього:

створюємо нове правило (*Add my own rules*);

Rule type: Regular rule;

If a request: Matches the statement.

Statement:

Inspect: Originates from a country in;

вибираємо країни, які ми хочемо дозволити або заблокувати.

Action: Block (для небажаних країн).

Етап 6: Моніторинг та реагування

Після налаштування правил важливо слідкувати за тим, що відбувається.

У консолі WAF переходимо на вкладку *Overview* корпоративного *Web ACL*.

Ми побачимо графік *Allowed vs Blocked requests*.

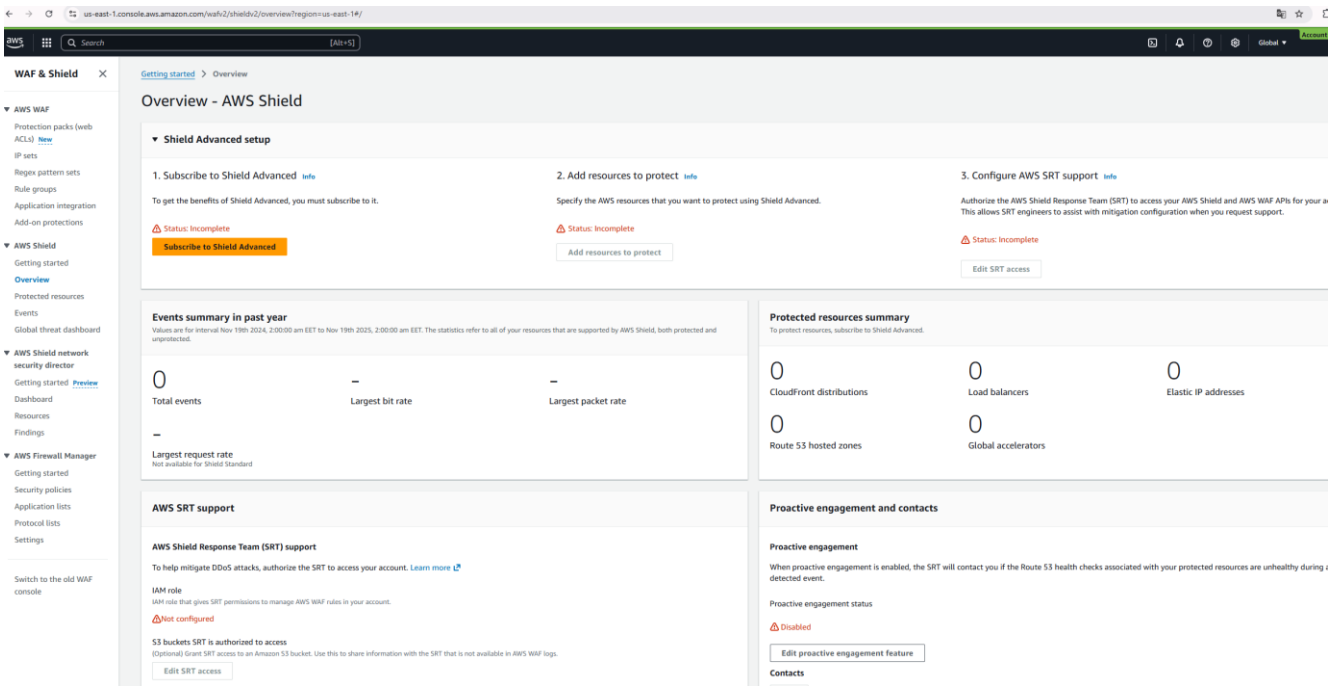

Рис. 3.5. Вкладка Overview

Внизу є секція *Sampled requests*. Там можна побачити конкретні IP-адреси та URI, які були заблоковані. Це допоможе зрозуміти, чи не блокуються легітимні користувачі.

Підсумкова таблиця пріоритетів правил (Processing Order)

У WAF важливий порядок виконання правил. Рекомендований порядок:

Пріоритет	**Тип правила**	**Дія**	**Чому?**
1	**AWS IP Reputation**	Block	Відсікаємо відомі ботнети одразу (найдешевше).
2	**Rate-based Rule**	Block	Блокуємо тих, хто спамить запитами (Flood).
3	**Geo Block**	Block	Відсікаємо зайві країни.
4	**Core Rule Set**	Block/Count	Перевіряємо на вразливості (SQLi, XSS).

JSON-код для конкретного Rate-based правила (наприклад, для захисту сторінки логіну), який можна просто вставити в консоль AWS.

Це правило налаштовано спеціально для захисту сторінки входу (наприклад, */login*). Воно набагато суворіше за загальне правило, оскільки звичайна людина не повинна відправляти 100 запитів на логін за 5 хвилин.

JSON-код правила (Rate-based Login Protection)

Це правило блокує IP-адресу на 5 хвилин, якщо з неї надійде понад 100 запитів саме на сторінку, що починається з */login*.

```
{
  "Name": "Protect-Login-Page-Flood",
  "Priority": 10,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "SearchString": "/login",
          "FieldToMatch": {
            "UriPath": {}
          },
          "TextTransformations": [
            {
              "Priority": 0,
              "Type": "LOWERCASE"
            }
          ],
          "PositionalConstraint": "STARTS_WITH"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "Protect-Login-Page-Flood"
  }
}
```

Додаємо це правило у консоль AWS:

1. Відкриваємо наш *Web ACL*.

2. Переходимо у вкладку *Rules*.

3. Натискаємо *Add rules -> Add my own rules and rule groups*.

4. У верхній частині вікна перемикаємо тип редактора з *Rule builder* на *Rule JSON editor*.

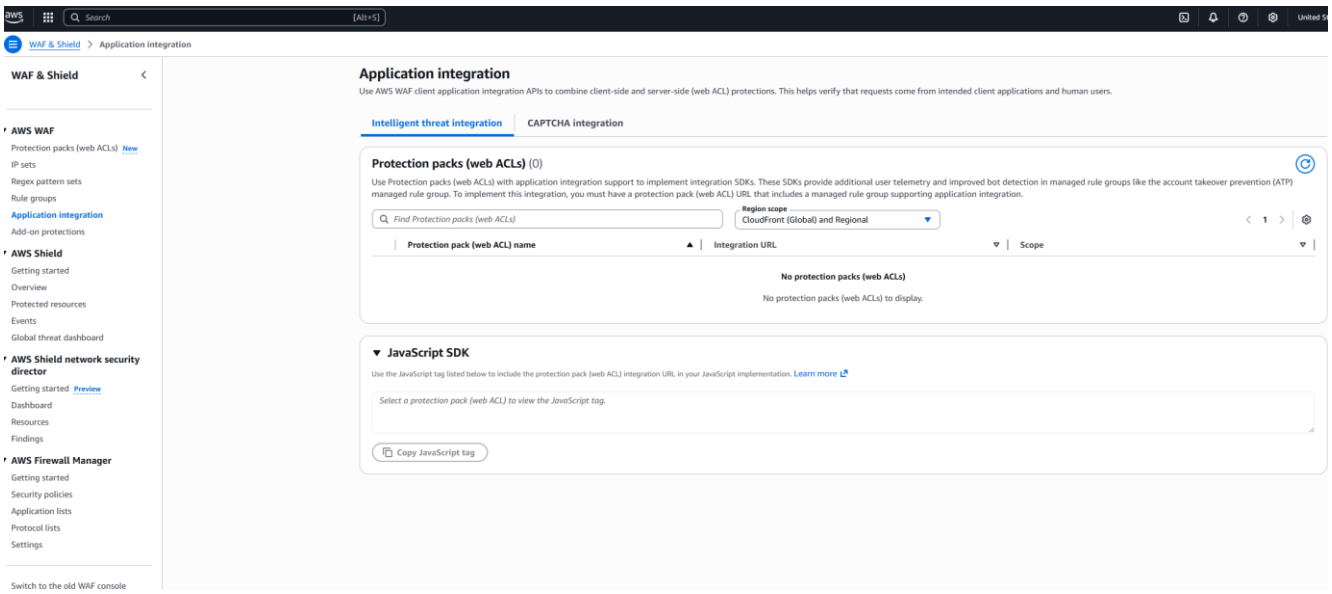

Рис. 3.6. Вкладка Application integration

5. Видаляємо все з поля редагування та вставдяємо код, наведений вище.

6. Натискаємо *Add rule*.

Якщо сторінка входу має іншу адресу (наприклад, */admin*, */wp-login.php* або */signin*), замініть рядок «SearchString»: «*/login*» у коді на нашу адресу.

Наступний крок: замість повного блокування (*Block*), AWS WAF дозволяє показувати користувачеві CAPTCHA, якщо він перевищив ліміт. Це корисно, щоб випадково не заблокувати реальних людей за NAT-ом. Ми можемо написати код так, щоб замість блокування показувалась CAPTCHA.

3.4. Рекомендації щодо захисту веб додатків від DDoS-атак

Рекомендації щодо захисту корпоративних веб-додатків від DDoS-атак охоплюють багаторівневий підхід, що поєднує технологічні рішення, архітектурні практики та процедури реагування.

Необхідно реалізовувати багаторівневу стратегію захисту (Defense-in-Depth).

DDoS-атаки можуть відбуватися на різних рівнях (мережевому, транспортному та прикладному). Ефективний захист вимагає застосування рішень на кожному з них.

На рівні 3/4 (мережевий та транспортний) необхідно використовувати сервіси, які автоматично поглинають і фільтрують великі обсяги трафіку поблизу джерела атаки (наприклад, AWS Shield, Azure DDoS Protection, Google Cloud Armor).

На рівні 7 (прикладний) необхідно використовувати WAF (Web Application Firewall) для аналізу вмісту запитів та блокування аномальної поведінки (наприклад, AWS WAF, Cloudflare WAF, Akamai Kona Site Defender).

Необхідно реалізовувати архітектурні практики та масштабованість.

Для досягнення горизонтальної масштабованості необхідно розробляти додатки, які можуть легко масштабуватися горизонтально (додавання нових інстансів серверів) для поглинання збільшеного легітимного трафіку та зменшення впливу атаки на кожен окремий інстанс.

Необхідно використовувати CDN (Content Delivery Network). Розміщення статичного контенту (зображення, CSS, JavaScript) на CDN зменшує навантаження на основні сервери додатків. CDN також діють як перша лінія оборони, фільтруючи частину шкідливого трафіку.

Необхідно реалізовувати розподілену інфраструктуру. Розгортання додатків у кількох регіонах або зонах доступності хмарного провайдера необхідно для підвищення стійкості.

Необхідно постійно займатися зменшенням поверхні атаки. Використання приватних підмереж (Private Subnets) та груп безпеки (Security Groups) необхідно для обмеження доступу до серверів баз даних та внутрішніх сервісів лише з необхідних джерел (наприклад, Load Balancer).

Необхідно впроваджувати та застосовувати WAF (Web Application Firewall).

Налаштування правил обмеження швидкості (Rate Limiting) необхідно для автоматичного блокування IP-адрес, які генерують надмірну кількість запитів за короткий проміжок часу.

Використання керованих наборів правил від провайдерів (наприклад, AWS Managed Rules) необхідно для захисту від поширених загроз.

Необхідно блокувати трафік з географічних регіонів, які не мають легітимних

користувачів корпоративним додатком.

Необхідно використовувати можливості провайдерів DNS, які пропонують захист від атак на DNS-сервери (DNS amplification attacks).

Необхідно реалізовувати захист API. Необхідне застосування спеціальних політик WAF та лімітування запитів для ендпоінтів API, які часто стають мішенню ботів.

Необхідно здійснювати постійний моніторинг та реагування на інциденти.

Здійснення проактивного моніторингу шляхом налаштування сповіщень (alerts) у системах моніторингу (наприклад, Amazon CloudWatch, Datadog) про аномалії в трафіку, високе використання CPU або мережевої пропускної здатності.

Необхідно розробити План реагування на інциденти (IRP). Необхідно розробити та регулярно оновлювати чіткий план дій у разі DDoS-атаки. Необхідно визначити відповідальних осіб та їхні ролі (технічна команда, PR-відділ, керівництво).

Необхідно включити кроки з активації додаткових засобів захисту (наприклад, перемикання в «режим підтвердження» WAF, залучення команди реагування хмарного провайдера).

Необхідно проводити регулярне тестування шляхом проведення симуляцій DDoS-атак (з дозволу хмарного провайдера) для перевірки ефективності Плану реагування та налаштувань захисту.

Дотримуючись цих рекомендацій, корпоративні веб-додатки можуть значно підвищити свою стійкість до DDoS-атак.

Захист веб-додатків від DDoS-атак є важливим завданням, оскільки AWS WAF є першою лінією оборони саме на 7-му рівні моделі OSI (рівень додатків). Він захищає від атак типу HTTP Floods, повільних запитів та спроб виснаження ресурсів сервера.

Розглянемо рекомендації щодо налаштування AWS WAF для ефективної протидії DDoS-атакам.

1. Стратегія Rate-Based Rules (Обмеження частоти)

Це найефективніший інструмент проти HTTP-флуду. Замість того, щоб

блокувати IP назавжди, обмежується кількість запитів, які одна IP-адреса може зробити за 5-хвилинне вікно.

Необхідно створити «ковдру» (Blanket Rule). Встановіть загальне обмеження для всього додатку. Наприклад, якщо нормальний користувач робить 20 запитів на хвилину, встановіть ліміт на рівні 1000-2000 запитів за 5 хвилин.

Необхідно застосовувати дію Block або CAPTCHA.

Використовуйте захист критичних URL (URI Specific). Сторінки логіну (/login), пошуку або важких обчислень вимагають суворіших правил, оскільки вони споживають більше ресурсів бекенду. Для цього необхідно встановлювати ліміт 100-300 запитів за 5 хвилин для специфічних шляхів URI.

Необхідно застосовувати захист від сканування (Status Code Tracking). Якщо одна IP-адреса отримує багато помилок 404 або 403, це може бути сканер вразливостей або бот. Для цього необхідно налаштувати блокування IP, якщо кількість відповідей 404/403 перевищує певний поріг.

2. Використання AWS Managed Rules (Керовані правила)

AWS надає готові набори правил, які постійно оновлюються на основі глобальної аналітики загроз Amazon.

Необхідно використовувати Amazon IP Reputation List. Обов’язково увімкніть цей набір. Він автоматично блокує IP-адреси, пов’язані з ботнетами, проксі-серверами та іншими відомими джерелами загроз.

Необхідно використовувати Anonymous IP List. Це блокує трафік з VPN, Tor-хостів та хостинг-провайдерів (хмари, з яких часто запускають атаки). Будьте обережні з блокуванням VPN, якщо корпоративні легітимні користувачі часто їх використовують. У такому разі краще використовувати дію Challenge замість Block.

3. Географічні обмеження (Geo-blocking)

Зменшення поверхні атаки – це половина успіху.

Необхідно застосовувати білий список (Allowlist). Якщо бізнес працює тільки в Україні, дозвольте трафік тільки з UA і блокуйте все інше.

Необхідно застосовувати чорний список (Blocklist). Якщо організація працює

глобально, але бачимо аномальний трафік з регіонів, де у нас немає клієнтів, необхідно заблокувати ці країни або застосувати до них CAPTCHA.

4. Challenge та CAPTCHA

AWS WAF дозволяє не просто блокувати, а «перевіряти» клієнта. Це критично для захисту від розумних DDoS-ботів, які імітують браузери.

Необхідно застосовувати Silent Challenge (JS Challenge). WAF надсилає невидимий JavaScript-запит. Якщо клієнт (браузер) його виконує, трафік пропускається. Прості DDoS-скрипти (наприклад, на Python) зазвичай не вміють виконувати JS.

Необхідно застосовувати CAPTCHA. Використовуйте для підозрілого трафіку, який не перевищує ліміт блокування, але виглядає аномально.

5. Архітектурні рекомендації (CloudFront + WAF)

Розгортання WAF безпосередньо на Application Load Balancer (ALB) є можливим, але для захисту від DDoS краще використовувати Amazon CloudFront.

Необхідно застосовувати поглинання на Edge. CloudFront має величезну пропускну здатність і приймає удар на себе ще до того, як трафік дійде до корпоративного дата-центру (VPC).

Використовуйте кешування. Налаштуйте кешування статичного контенту. Якщо боти запитують закешовані сторінки, ваш бекенд не навантажується.

Застосовуйте WAF Scope. Прикріпіть WebACL до дистрибуції CloudFront (Global scope).

Зверніть увагу на Зведену таблиця пріоритетів правил (Rule Priority). Порядок правил у WAF критичний. WAF оцінює їх зверху вниз.

Таблиця 3.1. Зведена таблиця пріоритетів правил (Rule Priority)

Пріоритет	**Тип правила**	**Дія**	**Опис**
1 (Найвищий)	IP Allowlist	Allow	Дозволити трафік офісу/розробників.
2	AWS IP Reputation	Block	Блокування відомих ботнетів.

Пріоритет	Тип правила	Дія	Опис
3	Rate Limit (High Risk)	Block	Суворий ліміт для /login, /api.
4	Geo-blocking	Block/Count	Блокування країн-агресорів або нецільових регіонів.
5	Rate Limit (Blanket)	Block	Загальний ліміт для всього сайту.
6 (Найнижчий)	AWS Core Rule Set	Block	Захист від OWASP Top 10 (SQLi, XSS).

ВИСНОВКИ

В роботі досліджено проблему захисту веб додатків від DDoS-атак, визначено його мету та завдання. Архітектурна складність сучасних корпоративних веб додатків має більшу вразливість до кіберзагроз, включаючи DDoS-атаки. Веб-сайти мають бути захищені на кількох рівнях моделі OSI, включаючи мережевий (L3), транспортний (L4) та прикладний (L7) рівні.

В останні роки «розумні» атаки на рівні додатків стають дедалі поширенішими. На відміну від традиційних DDoS-атак, вони спрямовані не лише на протоколи HTTP/HTTPs, а й на те, як серверні компоненти взаємодіють з клієнтськими модулями та іншими системами, такими як бази даних (СУБД) або шини даних. Зловмисники використовують вразливості в цих взаємодіях, щоб порушувати роботу таким чином, що стандартні засоби захисту можуть не виявити їх.

Визначено існуючі підходи до захисту веб додатків від DDoS-атак. Захист веб додатків від DDoS-атак вимагає багатошарової стратегії, спрямованої на поглинання та фільтрацію шкідливого трафіку до того, як він вплине на корпоративні сервіси. Основна мета – відрізнити легітимних користувачів від трафіку атаки. Розглянуто ключові підходи, розподілені за техніками та стратегіями.

Проаналізовано методи та засоби захисту веб додатків від DDoS-атак Відмічено, що основним захистом від DDoS-атак є застосування WAF. Він використовує передові техніки для виявлення шкідливої поведінки, а саме поведінковий аналіз, перевірки CAPTCHA та інспекцію запитів.

Визначено призначення, основні функції та склад рішення AWS WAF. Рішення AWS WAF – це брандмауер веб-застосунків, який дозволяє фахівцям контролювати та керувати веб-запитами, що пересилаються до захищених ресурсів AWS. За допомогою AWS WAF ми можемо захистити такі ресурси, як дистрибутиви Amazon CloudFront, REST API Amazon API Gateway,

балансувальники навантаження додатків та API AWS AppSync GraphQL. Ми можемо використовувати AWS WAF для перевірки веб-запитів на відповідність заданим умовам, таким як IP-адреса, з якої надходять запити, значення певного компонента запиту або швидкість надсилання запитів. AWS WAF може керувати запитами на відповідність різними способами, включаючи їх підрахунок, блокування або дозвіл, а також надсилання завдань, таких як головоломки CAPTCHA, користувачеві клієнта або браузеру [2].

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

Таким чином, правильна реалізація технології захисту веб додатків від DDoS-атак має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cloud Security: New Threats on the Horizon. Commvault. URL: https://www.commvault.com/explore/top-cloud-security-threats (дата звернення 20.10.2025).

2. 17 Security Risks of Cloud Computing in 2025. SentinelOne, Updated: August 8, 2025. URL: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/ (дата звернення 20.10.2025).

3. Cloud Security Trends 2025: Top 6 Innovations Shaping the Future. CloudPanel. URL: https://www.cloudpanel.io/blog/cloud-security-trends/ (дата звернення 20.10.2025).

4. How Does a WAF Protect Against DDoS? Prophaze. URL: https://www.prophaze.com/learn/ddos/how-does-a-waf-protect-against-ddos/ (дата звернення 20.10.2025).

5. Як запобігти DDoS-атакам: інструменти та найкращі практики. Check Point. URL: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-a-ddos-attack/how-to-prevent-ddos-attacks-tools-and-best-practices/ (дата звернення 20.10.2025).

6. Sergey Volynets. 3 Strategies to Prevent DDoS Attacks on Web Content Purchase Systems. Lightpoint Global, 19 Dec 2023. URL: https://lightpointglobal.com/blog/3-strategies-to-prevent-ddos-attacks-on-web-content-purchase-systems (дата звернення 20.10.2025).

7. Arbor DDoS Detection & Defense. URL: https://www.netscout.com/arbor (дата звернення 20.10.2025).

8. What Does AppWall Do? URL: https://www.radware.com/products/appwall/ (дата звернення 20.10.2025).

9. Web Application Firewall. URL: https://www.fortinet.com/products/web-application-firewall/fortiweb (дата звернення 20.10.2025).

10. Connect, protect, and build everywhere. URL: https://www.cloudflare.com/

(дата звернення 20.10.2025).

11. App & API Protector. One-stop, zero-compromise security for websites, applications, and APIs. URL: https://www.akamai.com/products/app-and-api-protector (дата звернення 20.10.2025).

12. Web Application Firewall (WAF). URL: https://www.imperva.com/products/web-application-firewall-waf/ (дата звернення 20.10.2025).

13. How AWS Shield and Shield Advanced work. 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/ddos-overview.html (дата звернення 20.10.2025).

14. Google Cloud Armor. URL: https://cloud.google.com/security/products/armor?hl=en (дата звернення 20.10.2025).

15. Web Application and API Protection. URL: https://www.f5.com/solutions/web-app-and-api-protection (дата звернення 20.10.2025).

16. Prolexic – Comprehensive DDoS Attack Protection. Akamai Product Brief. URL: https://www.akamai.com/resources/product-brief/prolexic (дата звернення 20.10.2025).

17. AWS WAF, AWS Firewall Manager, AWS Shield Advanced, and AWS Shield network security director. Developer Guide. https://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html (дата звернення 20.10.2025).

18. Security Automations for AWS WAF. Implementation Guide. URL: https://docs.aws.amazon.com/solutions/latest/security-automations-for-aws-waf/architecture-overview.html (дата звернення 20.10.2025).

19. How to Protect Websites and Web Applications from DDoS Attacks. StormWall. URL: https://stormwall.network/resources/blog/how-to-prevent-ddos-attacks-on-websites (дата звернення: 08.10.2025).

20. Exploring AWS WAF Features and Benefits. URL:

https://www.genesesolution.com/blog/waf-features-and-benefits/

21. Кравченко Ярослав Ігорович. Технологія захисту веб додатків від DDoS-атак на основі AWS WAF. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». 29 жовтня 2025 року. Державний університет інформаційно-комунікаційних технологій, м. Київ. Тези доповідей. С. 100-103. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)