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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія захисту корпоративних веб-додатків і API на базі Imperva Web Application Firewall»

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

_____ Олена КУБРАК
(підпис)

Виконав: здобувачка вищої освіти групи БСДМ-63
КУБРАК Олена
(прізвище, ім'я)

Керівник к.держ.упр. СКИБУН Олександр
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2024

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API** ……..…….. 12

1.1 Дослідження загроз корпоративним веб-додаткам і API …..…….. 12
1.2 Аналіз підходів до захисту корпоративних веб-додатків і API ….. 21
1.3 Аналіз існуючих рішень для захисту корпоративних веб-додатків і API ……..... 30

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API НА БАЗІ IMPERVA WAF** ……..…. 37

2.1 Призначення та основні функції рішення Imperva WAF ……..… 37
2.2 Архітектура рішення Imperva WAF ……... 41
2.3 Призначення та функції рішення Imperva Cloud WAF ……..... 45
2.4 Призначення та функції рішення Imperva WAF Gateway …… 49

3 **ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API НА БАЗІ IMPERVA WAF** …….. 53

3.1 Варіанти розгортання системи захисту веб-додатків та API на базі Imperva WAF ……...…… 53
3.2 Реалізація функцій моніторингу рішенням Imperva WAF ……..… 58
3.3 Рекомендації щодо захисту корпоративних веб-додатків і API …. 65

ВИСНОВКИ …….. 71

ПЕРЕЛІК ПОСИЛАНЬ 73

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 75

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

APT – Advanced Persistent Threat

ASM – Attack Surface Management

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

PoLP – Principle of Least Privilege

SASE – Secure Access Service Edge

SAST – Static Application Security Testing

SOA – Start of Authority

SOC – Security Operations Center

OWASP – Open Web Application Security Project

WAF – Web Application Firewall

WAAP – Web App and API Protection

ZT – Zero Trust

ВСТУП

Актуальність дослідження. Сучасні веб-додатки стали невід'ємною частиною нашого життя, але вони також є привабливою мішенню для зловмисників.

WAF (Web Application Firewall) або міжмережевий екран веб-застосунків – це система безпеки, яка фільтрує вхідний і вихідний трафік до корпоративного веб-додатку. Він діє як захисний щит, відбиваючи атаки, спрямовані на вразливості корпоративних веб-додатків та API. WAF допомагає захистити корпоративні веб-додатки від різних типів атак, таких як втілення шкідливих команд в SQL-запити для отримання доступу до бази даних, впровадження шкідливого коду на веб-сторінку для виконання його в браузері користувача, використання авторизованого користувача для виконання небажаних дій, проведення масованих атак на веб-сервер з метою зробити його недоступним, сканування вразливостей, створення та застосування ботнетів тощо.

WAF можуть бути на основі хоста, мережі або хмари і зазвичай розгортаються через зворотні проксі та розміщуються перед додатком чи веб-сайтом (або кількома додатками та сайтами). WAF можуть працювати як мережеві пристрої, серверні плагіни або хмарні служби, перевіряючи кожен пакет і аналізуючи логіку прикладного рівня відповідно до правил, щоб відфільтрувати підозрілий або небезпечний трафік. WAF аналізує весь вхідний трафік на наявність ознак атаки. Він використовує різні методи для виявлення загроз, включаючи аналіз сигнатур, аналіз поведінки та глибоку інспекцію пакетів.

WAF є важливим елементом безпеки корпоративних веб-додатків та API. Він допомагає захистити корпоративні дані, забезпечити безперебійну роботу сервісів і підвищити довіру клієнтів. Тому, в загальному процесі забезпечення безпеки інформаційних ресурсів організацій, захист корпоративних веб-додатків і API займає відповідальне місце.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи,

основний зміст якої становлять дослідження технології захисту корпоративних веб-додатків і API на базі Imperva WAF.

Об'єкт дослідження – захист корпоративних веб-додатків і API.

Предмет дослідження – технологія захисту корпоративних веб-додатків і API на базі Imperva WAF.

Мета роботи – розробити порядок застосування технології захисту корпоративних веб-додатків і API та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту корпоративних веб-додатків і API;

проаналізувати підходи до захисту корпоративних веб-додатків і API;

проаналізувати існуючі рішення для захисту корпоративних веб-додатків і API;

проаналізувати методи та засоби захисту корпоративних веб-додатків і API на базі Imperva WAF;

розкрити порядок реалізації технології захисту корпоративних веб-додатків і API на базі Imperva 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 корпоративних веб-додатків і API на базі Imperva WAF, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API

1.1. Дослідження загроз корпоративним веб-додаткам і API

У Звіті Imperva [1] зазначається, що за останній рік автоматизовані загрози викликали 30% атак API. Серед них 17% атак було здійснено поганими ботами, які використовували вразливості бізнес-логіки, 13% атак було здійснено іншими видами автоматичних загроз. Атаки на бізнес-логіку використовують недоліки в дизайні та реалізації додатків, що дозволяє зловмисникам маніпулювати законними функціями та потенційно отримати доступ до конфіденційних даних або облікових записів користувачів.

Погані боти взаємодіють із додатками таким чином, щоб імітувати дії законних користувачів, що ускладнює їх виявлення та блокування. Вони використовують бізнес-логіку, використовуючи призначені функції та процеси додатків, а не її технічні вразливості. Погані боти сприяють високошвидкісному зловживанню, неправильному використанню та атакам на веб-сайти, мобільні додатки та API. Вони дозволяють операторам ботів, зловмисникам, недобросовісним конкурентам і шахраям брати участь у зловмисних діях. Такі дії, як сканування веб-сайтів, конкурентоспроможний аналіз даних, збір особистих і фінансових даних, спроби входу грубою силою, скальпінг, шахрайство з цифровою рекламою, атаки на відмову в обслуговуванні, спам, шахрайство з транзакціями та інші подібні дії можуть завдати шкоди бізнесу. Ці дії споживають пропускну здатність, уповільнюють роботу серверів і викрадають конфіденційні дані, що призводить до фінансових втрат і шкоди репутації компанії [1].

Також відмічається, що рівень трафіку поганих ботів зростає п’ятий рік поспіль, що вказує на тривожну тенденцію. Це збільшення частково зумовлене зростанням популярності штучного інтелекту (AI) і великих моделей навчання (LLM). У 2023 році довелося на поганих ботів 32% всього інтернет-трафіку – на

1,8% збільшення порівняно з 2022 р. Частка хорошого бот-трафіку також зросла, хоч і трохи менш значно: 17,3% усього трафіку у 2022 році до 17,6% у 2023 р. Разом 49,6% усього інтернет-трафіку у 2023 році не був людський, оскільки рівень людського трафіку знизився до 50,4% всього трафіку (рисунок 1.1) [1].

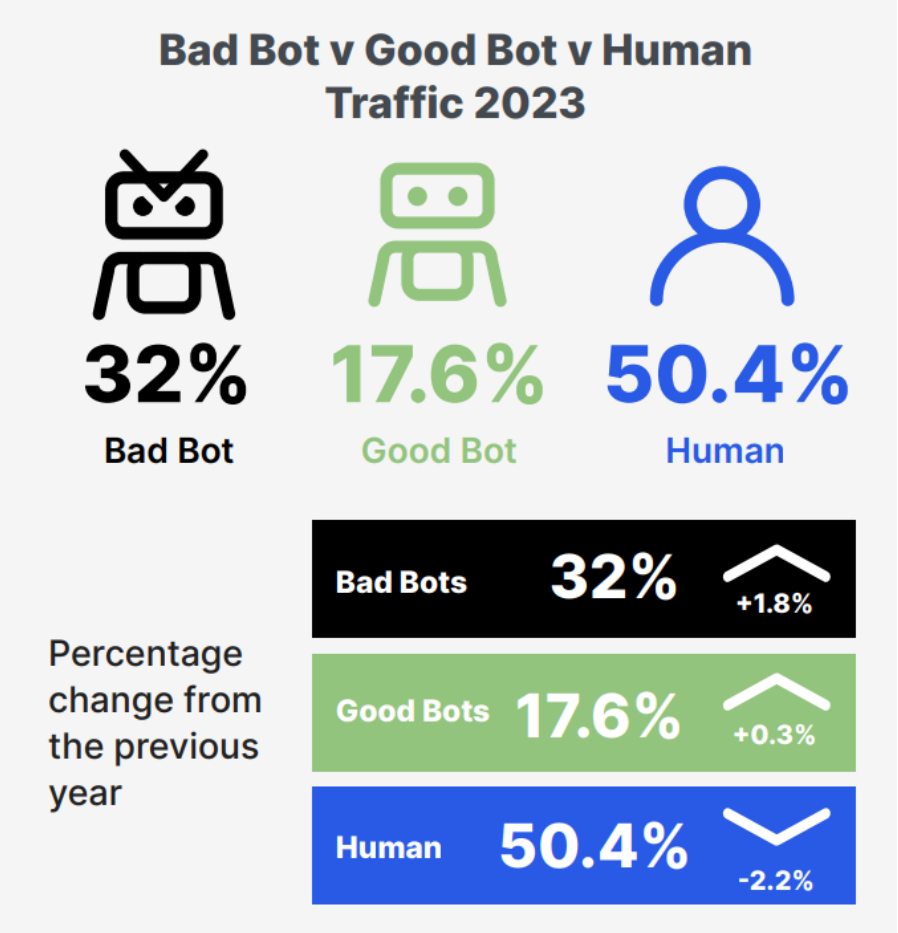

Рис. 1.1. Порівняння об’ємів інтернет-трафіку [1]

З усіх атак, зафіксованих і пом’якшених Imperva за минулий рік, 31,7% були автоматизованими загрозами, як визначено OWASP. Деталізація типів атак показує це 25% атак складних поганих ботів, які намагалися зловживати бізнес-логікою, було пом’якшено (рисунок 1.2) [1].

Погані боти становлять серйозну загрозу для різних галузей промисловості та організаційних функцій. Вони можуть здійснювати зловмисну діяльність із швидкістю та масштабом, що перевищує людські можливості, що робить їх улюбленим інструментом для зловживань, неправильного використання та атак. У

той час як деякі випадки використання шкідливих ботів, як-от сканування вмісту та захоплення облікового запису, поширені в різних галузях, інші, як-от скальпування, зазвичай впливають на певні сектори, як-от онлайн-торгівлю та розваги (продаж квитків) [1].

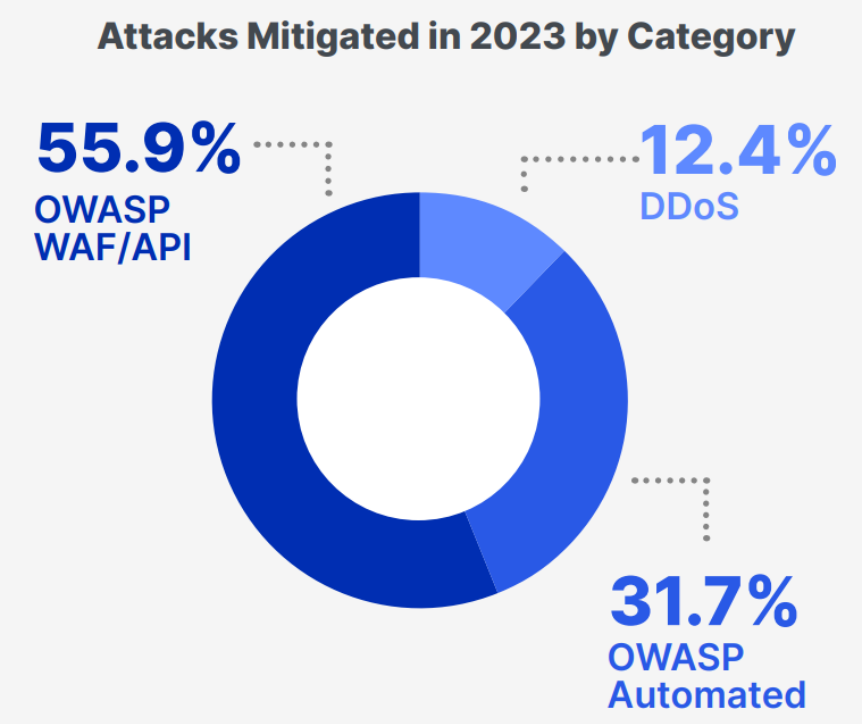

Рис. 1.2. Розподіл атак, зафіксованих і пом’якшених Imperva [1]

Атаки захоплення облікового запису є одними з найпоширеніших автоматизованих загроз. Вони передбачають використання ботів для спроб несанкціонованого доступу та захоплення облікових записів користувачів за допомогою методів підміни облікових даних і злому, що призводить до крадіжки цифрових даних і значних збитків для організацій. Згідно з даними Aite Group, у 2023 році збитки від крадіжки особистих даних сягнуть 635,4 млрд доларів [1].

Атаки захоплення облікових записів, націлені на API, становлять 44% усіх атак захоплення облікових записів, зафіксованих Imperva, порівняно з 35% минулого року. Широке впровадження API завдяки поширенню мобільних і веб-додатків зробило їх привабливою точкою входу для зловмисників, які прагнуть скомпрометувати облікові записи користувачів. Ці API обробляють найважливіші

процеси перевірки особи, що робить їх ідеальною ціллю [1].

Однак впровадження заходів безпеки є складним завданням через складність сучасних IT середовищ і взаємопов’язаний характер онлайн-платформ. У результаті кіберзлочинці використовують уразливості в API автентифікації, щоб отримати несанкціонований доступ до облікових записів користувачів. Вони використовують такі методи, як введення облікових даних, атаки грубою силою або зловживання API. Зростаюча частота атак на захоплення облікових записів, націлених на API автентифікації, підкреслює потребу організацій посилити заходи безпеки API та захистити їх від найскладніших сучасних автоматизованих атак [1].

Вразливості веб-додатків – це недоліки безпеки, які зловмисники використовують для маніпулювання вихідним кодом, отримання несанкціонованого доступу, викрадення даних або порушення функціональності додатка. Список OWASP Top 10 визначає найбільш критичні ризики для безпеки веб-додатків. Ось короткий огляд кожного з них [6]:

порушений контроль доступу – коли контроль доступу реалізований погано, неавторизовані користувачі можуть отримати доступ до конфіденційних даних або систем, що призведе до витоку даних або підвищення привілеїв;

криптографічні збої – слабкі методи шифрування можуть розкрити конфіденційні дані. Це включає використання застарілих алгоритмів або неправильне керування ключами, що може призвести до витоку даних;

ін’єкція – зловмисники вводять шкідливий код, наприклад SQL, для маніпулювання базами даних, вилучення даних або отримання неавторизованого адміністративного доступу;

незахищений дизайн – недоліки в дизайні програми, які призводять до вразливості, наражаючи систему на різні загрози з самого початку;

неправильна конфігурація безпеки – належним чином налаштовані параметри безпеки, як-от залишення ввімкненими непотрібних функцій, можуть дозволити зловмисникам використовувати систему;

вразливі та застарілі компоненти – використання застарілих або незахищених сторонніх бібліотек і фреймворків може створити вразливості, якими можуть

скористатися зловмисники;

помилки ідентифікації та автентифікації – неефективні механізми автентифікації, як-от недостатня політика паролів, можуть призвести до неавторизованого доступу;

порушення цілісності програмного забезпечення та даних – це відбувається, коли оновлення програмного забезпечення, критичні дані або конвеєри CI/CD змінюються, що призводить до скомпрометованих систем;

збої в журналі безпеки та моніторингу – недостатнє журналювання та моніторинг ускладнюють виявлення та реагування на порушення, дозволяючи зловмисникам використовувати системи непоміченими;

підробка запитів на стороні сервера (SSRF) – зловмисники маніпулюють сервером, щоб надсилати неавторизовані запити, потенційно викриваючи внутрішні системи або призводячи до викрадання даних.

Рис. 1.3. Загальні загрози безпеці веб-додатків [11]

Щоб пом’якшити ці ризики, вкрай важливо застосувати методи безпечного кодування, дезінфікувати вхідні та вихідні дані та проводити регулярне тестування

безпеки протягом життєвого циклу розробки веб-додатків . Крім того, постійний моніторинг і сканування сторонніх компонентів необхідні для швидкого виявлення та усунення вразливостей [6].

Imperva [1] надає наступні рекомендації щодо безпеки для виявлення поганого бота:

1. Ідентифікація ризиків.

Ініціативи з маркетингу та електронної комерції часто приваблюють підвищену присутність ботів, особливо під час запуску обмеженої кількості продуктів, які користуються високим попитом. Незалежно від того, чи це найновіші кросівки, ігрові консолі нового покоління чи ексклюзивні предмети колекціонування, вказівка дати запуску цих бажаних продуктів є маяком для ботів.

Ці автоматизовані організації прагнуть захистити товар до того, як це зроблять справжні клієнти, потенційно монополізуючи доступ і підриваючи ваші продажі. Дуже важливо зміцнити захист вашого веб-сайту, щоб ефективно керувати різким зростанням трафіку, гарантуючи, що ви зможете відрізнити законних споживачів від ухильних ботів, які мають намір перехопити запуск продукту. Впровадження розширеного аналізу трафіку, механізмів виявлення ботів у режимі реального часу та надійних заходів автентифікації можуть допомогти захистити вашу платформу, забезпечуючи справедливий доступ для фактичних клієнтів.

Розпізнавання потенційних вразливостей на вашому сайті є важливим елементом ефективної стратегії керування ботом. Деякі функції веб-сайту особливо сприйнятливі до зловмисних ботів. Наприклад, використання можливостей входу в систему може призвести до атак із заповнення обліковими даними та злому облікових даних, коли зловмисники використовують викрадені облікові дані для отримання несанкціонованого доступу. Так само наявність касової форми може підвищити ризик шахрайства з кредитними картками, відомого як кардинг або злом карток. Крім того, впровадження функцій подарункових карток може залучити ботів, які мають намір вчинити шахрайство. Щоб зменшити такі ризики, важливо застосувати посилені заходи безпеки та суворіші правила на цих сторінках.

Впровадження багатофакторної автентифікації, CAPTCHA та постійного моніторингу підозрілих дій може значно посилити захист вашого сайту від цих автоматизованих загроз.

2. Зменшення вразливості.

Захист відкритих API і мобільних додатків є таким же важливим, як і захист корпоративного веб-сайту, підкреслюючи необхідність цілісної стратегії кібербезпеки, яка охоплює всі цифрові точки дотику.

Потрібно більше, ніж просто зосередитися на безпеці веб-сайту. API і мобільні програми часто служать шлюзами для корпоративних веб-програм і конфіденційних даних, представляючи додаткові вектори для кіберзагроз. Впровадження надійних заходів безпеки на цих платформах і блокування між системами має важливе значення для зменшення вразливості. Цей інтегрований підхід забезпечує уніфікований механізм захисту від потенційних атак, мінімізуючи ризик неавторизованого доступу до ваших веб-додатків і важливих даних через будь-яку цифрову точку входу.

3. Зменшення загрози: агенти користувача.

Багато інструментів і скриптів ботів містять рядки агента користувача із застарілими версіями браузера. Навпаки, люди змушені автоматично оновлювати свої браузери до нових версій. Виконайте дії для блокування застарілих версій браузера.

4. Зменшення загрози: проксі.

Використання проксі-служб зловмисними ботами для приховування своєї діяльності зростає, оскільки зловмисники використовують ці служби для імітації законної поведінки користувачів. Використовуючи ротацію IP-адрес від групових IP-сервісів, вони можуть маскувати своє справжнє походження, ускладнюючи зусилля з виявлення. Стратегічний підхід до пом’якшення цієї загрози передбачає обмеження доступу з відомих масових IP-центрів обробки даних, що значно зменшує ймовірність проникнення трафіку ботнету у вашу мережу. Відомими джерелами таких атак на основі проксі є центри обробки даних і постачальники хмарних послуг, такі як Host Europe GmbH, Dedibox SAS, Digital Ocean, OVH SAS

і Choopa, LLC. Впровадження засобів контролю доступу та моніторингу трафіку, що надходить від цих об’єктів, може підвищити вашу безпеку шляхом завчасного виявлення та блокування створеного роботами трафіку, таким чином мінімізуючи ризик, пов’язаний з цими атаками з підтримкою проксі.

5. Зменшення загроз: автоматизація.

Зловмисники часто зловживають такими сучасними інструментами, як Puppeteer, Selenium і WebDriver, щоб імітувати людські дії в Інтернеті, що дозволяє їм виконувати шкідливі дії, такі як масова реєстрація облікових записів і крадіжка даних. Щоб відрізнити ці зловмисні дії від законного трафіку, потрібно застосувати стратегії виявлення ознак автоматизації, таких як неприродно швидкі взаємодії або ненормальні шаблони перегляду. Відточуючи цю поведінку, організації можуть ефективно виявляти та зупиняти автоматизовані атаки, захищаючи справжню взаємодію користувачів.

6. Оцінка трафіку.

Ідентифікація трафіку ботів без явних індикаторів викликає труднощі, але конкретні шаблони часто вказують на їхню присутність. Високі показники відмов і низькі коефіцієнти конверсії можуть бути ознаками нелюдського трафіку. Крім того, раптові незрозумілі сплески трафіку або надзвичайно велика кількість запитів, націлених на конкретну URL-адресу, часто свідчать про активність бота. Моніторинг цих аномалій дозволяє організаціям позначати потенційний трафік ботів, сприяючи подальшому розслідуванню та відповідним реагуванням для пом’якшення небажаного втручання.

Раптовий сплеск трафіку до певної кінцевої точки може вказувати на те, що боти націлені на певну подію чи операцію. Щоб оцінити, чи цей сплеск викликаний роботом, проаналізуйте джерело цього збільшення трафіку. Шукайте шаблони, такі як одна IP-адреса, Інтернет-провайдер або певна URL-адреса, які генерують рівень трафіку, значно вищий за норму. Виявлення цих джерел може надати чіткі докази активності бота, що дозволить вам здійснювати цілеспрямовані дії. Наприклад, якщо трафік переважно походить з однієї IP-адреси або вузького діапазону IP-адрес, це вагомий показник автоматизованих спроб доступу. Така інформація має

вирішальне значення для впровадження ефективних заходів протидії атакам ботів, гарантуючи захист ваших цифрових активів.

7. Контролюйте трафік.

Визначте базовий рівень невдалих спроб входу на сторінках входу, а потім спостерігайте за аномаліями чи сплесками. Налаштуйте сповіщення, щоб ви отримували автоматичне сповіщення, якщо вони трапляються. Розширені «низькі та повільні» атаки не викликають попередження на рівні користувача чи сеансу, тому обов’язково встановіть глобальні порогові значення.

На сторінках оформлення замовлення та перевірки подарункових карток збільшення кількості збоїв або навіть трафіку може свідчити про кардінг-атаки або те, що такі боти, як GiftGhostBot, намагаються викрасти баланси подарункових карток.

8. Обізнаність.

Необхідно стежити за глобальними порушеннями та витоками даних. Простота, з якою зловмисники можуть придбати дамп облікових даних у цих зламах або орендувати інфраструктуру ботів для автоматизації атак, підвищує загрозу до відчутного ризику. Боти часто використовують нещодавно скомпрометовані облікові дані для здійснення атак із заповненням і захоплення облікових записів (ATO), оскільки ці облікові дані, швидше за все, залишаться активними. Ця тактика значно підвищує ймовірність успішного зламу облікових записів користувачів на вашій платформі. Поінформованість про такі порушення та розуміння їх наслідків може допомогти вам завчасно посилити захист, зменшивши ймовірність того, що ваш сайт стане мішенню для цих автоматизованих загроз.

9. Оцінка рішення для захисту від ботів.

Оцінка рішень захисту від ботів є надзвичайно важливою, оскільки ландшафт атак ботів значно змінився. Для захисту від зловмисних ботів достатньо спрощених заходів зараз неефективний. Складність і адаптивність сучасних ботів перевершують попередні рівні, а простота використання та ефективність роблять їх улюбленим інструментом серед кіберзлочинців. Ці боти швидко розвиваються,

роблячи традиційні методи виявлення застарілими, але вони також імітують людську поведінку більш точно, ніж будь-коли, тому важко відрізнити їх від законних користувачів у цьому середовищі, де зловмисники використовують ботів для отримання високої винагороди та вигод з низьким ризиком, спроба самостійно протистояти цим загрозам майже неможлива.

Потреба в стратегії динамічного захисту є гострою, ніж будь-коли. Йдеться не лише про виявлення шкідливих ботів; мова йде про те, щоб відрізнити їх від корисних серед їхньої зростаючої складності.

Комплексне рішення для запобігання роботів має включати багаторівневий підхід захисту, включаючи аналіз поведінки користувачів, профілювання та відбитки пальців. Ця стратегія не тільки зберігає переваги законних ботів, але й ефективно відфільтровує зловмисну діяльність. Такий тонкий підхід вимагає досвіду спеціальної команди, здатної розвивати ваш захист відповідно до темпів появи загроз.

1.2. Аналіз підходів до захисту корпоративних веб-додатків і API

Брандмауери веб-додатків (Web Application Firewall, WAF) є критично важливим захистом для веб-сайтів, мобільних додатків і API. Вони відстежують, фільтрують і блокують пакети даних до та з веб-додатків, захищаючи їх від загроз. WAF розроблено (навчено) для виявлення та захисту від небезпечних недоліків безпеки, які найчастіше зустрічаються в веб-трафіку. Це робить їх необхідними для онлайн-бізнесу, як-от роздрібна торгівля, банки, охорона здоров’я та соціальні мережі, яким необхідно захищати конфіденційні дані від несанкціонованого доступу. WAF можна розгортати як мережеві, хостові або хмарні рішення, забезпечуючи видимість даних додатків на прикладному рівні HTTP [2].

Оскільки веб- і мобільні додатки та API схильні до ризиків безпеки, які можуть порушити роботу або виснажити ресурси, брандмауери веб-додатки призначені для протидії поширеним веб-експлойтам, таким як шкідливі роботи. WAF захищають від загроз, які можуть впливати на доступність, безпеку або

ресурси, включаючи експлойти нульового дня, ботів і шкідливе програмне забезпечення [2].

WAF може бути програмним забезпеченням, пристроєм або послугою. Він аналізує HTTP-запити та застосовує набір правил для визначення, які частини цієї розмови є доброякісними, а які – шкідливими [3].

Основними частинами HTTP-розмов, які аналізує WAF, є запити GET і POST. Запити GET використовуються для отримання даних із сервера, а запити POST використовуються для надсилання даних на сервер для зміни його стану.

Безпека веб-додатків полягає не лише в безпеці самої програми. Це також стосується захисту даних, до яких він отримує доступ, мережевих з'єднань, на які він покладається, серверів, з якими він взаємодіє, і навіть кінцевих користувачів, які з ним взаємодіють. Це комплексний підхід до того, щоб веб-програми були надійними, стійкими та надійними [7].

Безпека веб-додатків часто ігнорується в процесі розробки, але це важливий компонент будь-якого успішного веб-проекту. Ризики, пов'язані з поганою безпекою веб-додатків, можуть бути серйозними, включаючи втрату даних, шкоду репутації, фінансові збитки та порушення відповідності. Тому дуже важливо враховувати безпеку веб-додатків із самих ранніх етапів розробки та підтримувати послідовні методи безпеки протягом усього життєвого циклу додатка.

Є кілька причин, чому організації повинні надавати пріоритет безпеці веб-додатків [7]:

зростаючі загрози: кіберзлочинці шукають уразливості у веб-додатках, щоб використовувати їх у зловмисних цілях. Ці атаки можуть призвести до значних фінансових втрат, шкоди репутації бренду та втрати довіри клієнтів;

вимоги до відповідності. Багато урядів і галузей мають суворі правила щодо безпеки та конфіденційності даних. Невиконання цих правил може призвести до великих штрафів, судових позовів і втрати бізнесу;

технічна складність: складність веб-додатків зростає. З розвитком мобільних додатків, хмарних обчислень і архітектур мікросервісів розширюється зона атаки для веб-додатків. Ця складність ускладнює захист веб-додатків.

Розглянемо типи рішень та інструментів, які застосовуються для безпеки веб-додатків [7]/

Брандмауери веб-додатків (WAF) – це рішення безпеки, призначені для моніторингу та потенційного блокування трафіку HTTP до та з веб-програми. WAF працює як воротар для всього вхідного трафіку, аналізуючи вміст кожного HTTP-запиту та відповіді, щоб визначити та відфільтрувати потенційно шкідливий трафік. Це включає захист від поширених атак, таких як впровадження SQL, міжсайтовий сценарій (XSS) і включення файлів.

WAF можуть бути дуже ефективними для запобігання використанню відомих уразливостей і можуть бути оновлені для відповіді на нові загрози. Однак вони не є окремим рішенням і повинні бути частиною комплексної стратегії безпеки. WAF іноді можуть блокувати законний трафік (помилкові спрацьовування) або не виявляти складні чи цілеспрямовані атаки. Таким чином, важливо правильно налаштувати та регулярно оновлювати WAF, щоб адаптуватися до мінливого середовища безпеки.

Рішення Web App and API Protection (WAAP) створені для захисту як традиційних веб-програм, так і сучасних API. WAAP виходить за рамки традиційних можливостей WAF, пропонуючи покращений захист від більш складних і витончених атак, таких як зловживання API та просунуті боти. Ці рішення часто інтегруються з іншими інструментами безпеки, забезпечуючи більш цілісну стратегію захисту.

Рішення WAAP зазвичай пропонують такі функції, як автоматичне виявлення загроз, аналітика поведінки та можливості машинного навчання для виявлення аномалій і реагування на них. Вони особливо цінні в середовищах, де широко використовуються API, оскільки забезпечують спеціалізований захист, який вирішує унікальні проблеми безпеки, з якими стикаються API, наприклад уразливість кінцевих точок і неавторизований доступ до даних.

Хмарні послуги пом’якшення розподіленої відмови в обслуговуванні (DDoS) забезпечують масштабований і гнучкий захист від широкомасштабних атак DDoS. Ці служби використовують величезні ресурси хмарної інфраструктури для

поглинання та пом’якшення потоку інтернет-трафіку, характерного для DDoS-атак.

Будучи хмарними, ці служби можуть швидко адаптуватися до різних розмірів атак, пропонуючи економічно ефективне рішення, яке масштабується відповідно до загрози. Вони також дозволяють організаціям звільнити від внутрішньої інфраструктури захист від DDoS-атак, забезпечуючи безперервність роботи та захищаючи від збоїв у роботі служби. Однак залежність від зовнішніх служб вимагає ретельного розгляду угод про рівень обслуговування та наслідків конфіденційності даних.

Керування поверхнею атаки (ASM) включає ідентифікацію, категоризацію та керування всіма різними точками («поверхнею атаки»), де неавторизований користувач може спробувати ввести дані в середовище або отримати дані з нього. У безпеці веб-додатків ASM передбачає ідентифікацію всіх веб-додатків, API та пов’язаних кінцевих точок, а потім оцінку та керування ризиками безпеки, які представляє кожна з них.

Ефективний ASM вимагає постійного моніторингу та оцінки, оскільки нові вразливості можуть з’явитися в будь-який момент. Це також передбачає визначення пріоритетів ризиків і впровадження заходів безпеки, щоб спочатку пом’якшити найбільш критичні вразливості. Цей проактивний підхід не лише допомагає захистити веб-додатки, але й підтримує відповідність різноманітним нормативним стандартам. Інструменти ASM часто інтегруються з іншими рішеннями безпеки, щоб забезпечити комплексне уявлення про стан безпеки організації.

Безпека веб-додатків – це процес захисту веб-сайтів і онлайн-сервісів від різних загроз безпеці, які використовують вразливі місця в коді додатка. Загальними цілями атак веб-додатків є системи керування вмістом (наприклад, WordPress), інструменти адміністрування баз даних (наприклад, phpMyAdmin) і програми SaaS [8].

В [11] зазначається, що безпека веб-додатків – широке та динамічне поле. Отже, у міру виявлення нових атак і слабких місць найкращі практики для дисципліни оновлюються. Незважаючи на це, сучасний ландшафт Інтернет-загроз

є досить динамічним, тому жодна організація не зможе вижити без кількох послуг безпеки, які відповідають їхнім конкретним бізнес-потребам.

Рис. 1.4. Технології захисту веб-додатків [11]

Для запобігання DDOS можна використовувати різні доступні служби запобігання DDOS і розміщувати їх між сервером і публічним Інтернетом. Цей засіб пом'якшення має мати спеціальну фільтрацію та надзвичайно високу пропускну здатність, щоб запобігти стрибкам зловмисного трафіку, який переповнює сервер. Ці служби важливі, щоб запобігти стрибкам зловмисного трафіку від перевантаження сервера. Ці служби важливі, оскільки багато сучасних DDoS-атак забезпечують достатню кількість шкідливого трафіку, щоб перевантажити навіть найстійкіші сервери [11].

Брандмауер веб-додатків, також відомий як WAF, може блокувати трафік, який, як відомо, використовує вразливості веб-додатка або підозрюється, що це робить. Швидка та непомітна поява нових уразливостей робить WAF критично важливими, оскільки майже жодна організація не може виявити їх самостійно.

Шлюзи API – обмежуючи трафік, який, як відомо або ймовірно, спрямований на вразливості API, це обхідне рішення допомагає виявити ігноровані тіньові API. Крім того, вони допомагають керувати та відстежувати трафік API.

Керування сертифікатами шифрування – це обхідне рішення працює, коли третя сторона керує ключовими елементами процесу шифрування SSL/TLS, такими

як генерація закритих ключів, оновлення сертифікатів і відкликання сертифікатів через уразливості. Це усуває ризик того, що ці елементи залишаться непоміченими та виявлятимуть приватний трафік.

DNSSEC – щоб додати рівень безпеки для DNS, DNSSEC це протокол, який гарантує, що DNS-трафік веб-додатку безпечно спрямовується на правильні сервери, тому зловмисник на шляху не перехоплює користувачів. Управління ботом Ви також можете включити систему керування ботом, щоб розрізнити людей-користувачів і автоматизований трафік. Можливість запобігти переповненню корпоративного веб-додатка автоматизованим трафіком також допоможе вам вжити заходів.

Безпеку корпоративного веб-сайту можна підвищити, дотримуючись деяких основних найкращих практик (рисунок 1.5).

Рис. 1.5. Найкращі практики безпеки веб-додатків [11]

Усі аспекти моніторингу стану безпеки корпоративного онлайн-додатка в режимі реального часу охоплені брандмауером веб- додатка (WAF). Використовуючи WAF, ми можемо миттєво припинити будь-яку діяльність, яка здається небезпечною на корпоративному веб-сайті чи веб-додатку, включаючи XSS, впровадження SQL або зловмисних ботів, які намагаються отримати

інформацію з корпоративного веб-сайту або провести DDoS-атаки.

Тим не менш, можуть бути випадки, коли WAF повідомляють про помилкові спрацьовування, пропускаючи попереджувальні індикатори про порушення безпеки. У результаті ми також можемо використовувати WAF у поєднанні з платформою керування безпекою додатків (ASMP), такою як Sqreen, або рішенням самозахисту додатків під час виконання (RASP). Моніторинг загроз і захист у реальному часі є функціями цих рішень, які адаптуються до корпоративних вимог безпеки.

Брандмауери веб-додатків (WAF) – це апаратні та програмні рішення, які використовуються для захисту від загроз безпеці програм. Ці рішення призначені для перевірки вхідного трафіку для блокування спроб атак, таким чином компенсуючи будь-які недоліки дезінфекції коду [8].

Захищаючи дані від крадіжки та маніпуляцій, розгортання WAF відповідає ключовим критеріям для сертифікації PCI DSS. Вимога 6.6 стверджує, що всі дані власників кредитних і дебетових карток, які зберігаються в базі даних, повинні бути захищені.

Як правило, для розгортання WAF не потрібно вносити жодних змін у програму, оскільки вона розміщується попереду своєї DMZ на межі мережі. Звідти він діє як шлюз для всього вхідного трафіку, блокуючи зловмисні запити до того, як вони зможуть взаємодіяти з програмою.

WAF використовують кілька різних евристик, щоб визначити, який трафік має доступ до програми, а який потрібно відсіяти. Постійно оновлюваний пул сигнатур дозволяє їм миттєво ідентифікувати зловмисників і відомі вектори атак.

Майже всі WAF можна налаштувати для конкретних випадків використання та політик безпеки, а також для боротьби з новими загрозами (також відомими як «нульовий день»). Нарешті, більшість сучасних рішень використовують дані про репутацію та поведінку, щоб отримати додаткову інформацію про вхідний трафік.

WAF зазвичай інтегруються з іншими рішеннями безпеки для формування периметра безпеки. Вони можуть включати служби захисту від розподіленої відмови в обслуговуванні (DDoS), які забезпечують додаткову масштабованість,

необхідну для блокування атак великого обсягу [8].

Існує кілька фреймворків безпеки веб-додатків, які містять вказівки та найкращі методи створення безпечних веб-додатків. Ось деякі з найпопулярніших фреймворків кібербезпеки для веб-додатків [9]:

ISO 27001: ISO 27001 – це набір міжнародних стандартів, які містять рекомендації щодо систем управління інформаційною безпекою. Він охоплює всі аспекти інформаційної безпеки, включаючи управління ризиками, політику безпеки, процедури та засоби контролю;

NIST Cybersecurity Framework: Національний інститут стандартів і технологій (NIST) Cybersecurity Framework забезпечує структуру для управління та зменшення ризиків кібербезпеки. Він містить набір інструкцій, найкращих практик і стандартів, які організації можуть використовувати для створення комплексної програми кібербезпеки;

PCI DSS (Стандарт безпеки даних індустрії платіжних карток): PCI DSS – це набір стандартів, який застосовується до організацій, які обробляють транзакції кредитних карток. Він містить вказівки та вимоги щодо захисту даних кредитних карток і запобігання витоку даних;

CIS Controls: Center for Internet Security (CIS) Controls – це набір інструкцій і найкращих практик, які забезпечують пріоритетний підхід до кібербезпеки. Елементи керування розроблено, щоб допомогти організаціям захистити себе від найпоширеніших кібератак шляхом впровадження спеціальних заходів безпеки;

CSA Security, Trust & Assurance Registry (STAR): Cloud Security Alliance (CSA) STAR – це реєстр, який дозволяє постачальникам хмарних послуг демонструвати клієнтам відповідність вимогам безпеки та прозорість. Реєстр містить анкету для самооцінки, яку постачальники послуг можуть заповнити, щоб продемонструвати свої засоби контролю безпеки.

В [10] зазначається, що *безпека веб-додатків* – це практика захисту веб-додатків від різних загроз і вразливостей. Це передбачає захист даних і функцій веб-додатків від несанкціонованого доступу та зловмисних атак.

Процес захисту веб-додатку включає такі кроки [10]:

1. Оцінка ризику: визначення потенційних загроз і вразливостей.

2. Практики безпечного кодування: написання безпечного та вільного коду.

3. Перевірка вхідних даних: забезпечення належної перевірки вхідних даних для запобігання атакам.

4. Автентифікація та авторизація: забезпечення доступу до конфіденційної інформації лише авторизованим користувачам.

5. Безпека зв’язку: шифрування даних під час передачі для запобігання несанкціонованому доступу.

6. Брандмауер веб-додатка (WAF): захист веб-додатка від атак.

7. Управління вразливостями: регулярна оцінка та пом’якшення вразливостей.

8. Реагування на інциденти: наявність плану реагування на інциденти безпеки.

WAF – це рішення безпеки, яке знаходиться між веб-додатком та Інтернетом, захищаючи веб-додаток від зловмисного трафіку. Він аналізує вхідний трафік і блокує зловмисні запити до того, як вони досягнуть веб-додатка, допомагаючи запобігти загрозам безпеці, таким як XSS, впровадження SQL і CSRF [10].

Існує два основних типи WAF [10]:

Мережеві WAF розгортаються на мережевому рівні та працюють на мережевому рівні моделі OSI.

WAF на основі програми розгортаються у веб-додатку та працюють на прикладному рівні моделі OSI.

WAF пропонують різноманітні функції, зокрема [10]:

1. Фільтрація на основі правил: WAF використовують фільтрацію на основі правил для блокування шкідливого трафіку на основі певних критеріїв.

2. Виявлення на основі сигнатур: WAF використовують виявлення на основі сигнатур, щоб ідентифікувати та блокувати відомі атаки, такі як впровадження SQL і XSS.

3. Виявлення на основі поведінки: WAF використовують виявлення на основі поведінки, щоб ідентифікувати та блокувати нові, невідомі атаки або атаки

нульового дня.

Щоб налаштувати та розгорнути WAF, слід виконати такі дії [10]:

1. Виберіть відповідний тип WAF і постачальника на основі конкретних потреб веб-додатка.

2. Налаштуйте WAF на основі конкретних вимог безпеки веб-додатка, включаючи вибір відповідних правил і сигнатур.

3. Розгорніть WAF перед веб-додатком і налаштуйте його для блокування шкідливого трафіку.

4. Регулярно відстежуйте та оновлюйте WAF, щоб переконатися, що він залишається ефективним у захисті веб-додатка від загроз безпеці.

Підсумовуючи, для організацій життєво важливо регулярно переглядати та оновлювати методи безпеки своїх веб-додатків, щоб забезпечити захист конфіденційної інформації та підтримувати цілісність своїх додатків.

Цього можна досягти за допомогою регулярних оцінок безпеки, впровадження найкращих практик для автентифікації та авторизації, безпечного зв’язку, WAF, управління вразливістю та реагування на інциденти.

1.3. Аналіз існуючих рішень для захисту корпоративних веб-додатків і API

Брандмауери веб-додатків (WAF) можуть відстежувати, фільтрувати та блокувати підозрілий або небажаний трафік HTTP до та з веб-служби чи додатка. Він спеціально аналізує трафік між Інтернетом і веб-додатком. Використовуючи модель OSI, рішення WAF забезпечуватимуть захист на прикладному рівні (також відомий як рівень 7). У той час як проксі-сервери можуть захистити ідентичність кінцевої точки користувача за допомогою посередника, WAF працює інакше. Вони діють як зворотні проксі-сервери, захищаючи сервер від впливу та вимагаючи від користувачів навігації WAF перед доступом до сервера чи додатка [12].

Брандмауери веб-додатків важливі для середовищ із кількома веб-додатками та багатьма користувачами, які регулярно намагаються отримати доступ до цих

програм. WAF забезпечують адаптивний і комплексний захист веб-додатків і будь-яких даних компанії, які можуть зберігатися в цих додатках. Рішення брандмауера для веб-додатків можуть бути хмарними, хостовими або мережевими [12].

Radware є постачальником рішень безпеки та доставки для локальних, хмарних і гібридних середовищ. Їхній брандмауер веб-додатків поєднує позитивні та негативні (на основі сигнатур) моделі безпеки, щоб забезпечити доставку критично важливих веб-додатків та API у мережах компанії та в хмарі. Cloud WAF від Radware є частиною Cloud Application Protection Service від Radware, яка включає WAF, захист API, керування ботами, захист L7 DDoS і захист на стороні клієнта [13].

Служба аналізує веб-додатки, щоб виявити потенційні загрози, а потім автоматично генерує детальні правила захисту для пом’якшення цих загроз. Він також пропонує відбитки пальців пристрою, щоб допомогти ідентифікувати атаки ботів, виявлення та захист API на основі штучного інтелекту для запобігання зловживанням API, повне охоплення топ-10 вразливостей OWASP і запобігання витоку даних, що запобігає передачі конфіденційних даних. Нарешті, Radware Cloud WAF рекомендовано NSS, сертифіковано ICSE Labs і відповідає PCI-DSS.

Radware Cloud WAF доступний як хмарний сервіс або інтегрований у пакет Radware Application Delivery Controller (ADC); on-prem і в хмарі; вбудований або позасмуговий; або як видання Kubernetes. Платформа також пропонує тісну інтеграцію з рішеннями DAST, які дозволяють їй пропонувати виправлення безпеки в реальному часі для додатків у середовищах безперервного розгортання. Завдяки такій гнучкості та потужному набору функцій безпеки Radware Cloud WAF рекомендують як надійне рішення для будь-якої організації чи команди розробників, які прагнуть покращити доставку своїх веб-додатків і API, захищаючи їх від атак, таких як порушення доступу, маніпуляції API, груба сила та розширені HTTP-атаки.

Cloud WAF Service від Radware забезпечує безперервний адаптивний захист безпеки веб-додатків корпоративного рівня. Заснований на сертифікованому ICSA Labs, провідному на ринку брандмауері для веб-додатків, він забезпечує повне

охоплення 10 найпопулярніших загроз OWASP і автоматично адаптує захист до нових загроз і захищених активів. Служба реалізує як негативну, так і позитивну моделі безпеки, використовуючи свою унікальну здатність автоматично адаптуватися до постійно мінливого ландшафту загроз і доступних для захисту онлайн-активів [14].

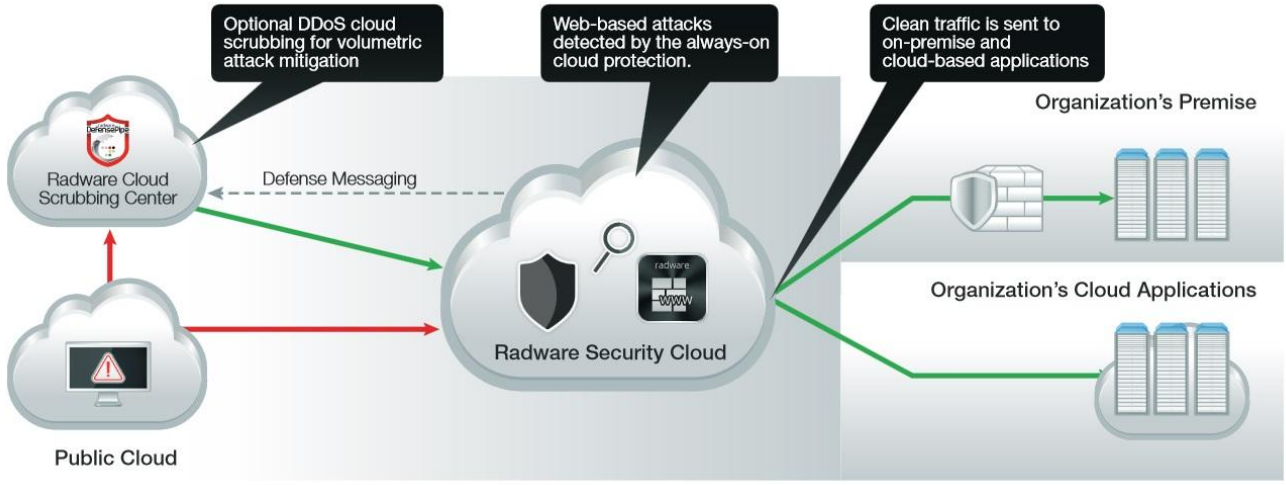

Рис. 1.6. Схема роботи рішення Radware Cloud WAF [14]

Створена з використанням найсучасніших технологій машинного навчання, Cloud WAF Service від Radware автоматично виявляє домени програм, аналізує потенційні вразливості та призначає оптимальні політики захисту. Сервіс постійно відстежує та аналізує шаблони використання додатків і генерує точні базові показники для законного трафіку. Це дозволяє швидко виявляти та пом'якшувати атаки нульового дня, а також безперервно налаштовувати політику безпеки завдяки мінливим моделям використання програм. Технологія Device Fingerprinting від Radware дозволяє автоматично відстежувати IP-незалежність шкідливих джерел, які намагаються приховати себе за динамічними змінами IP. Веб-ресурси завжди захищені, навіть якщо програми постійно змінюються, а загрози швидко розвиваються, що гарантує безпеку в Інтернеті в майбутньому [14].

Активована простою зміною DNS без встановлення додаткового апаратного чи програмного забезпечення, Cloud WAF Service від Radware легко розгортається,

щоб швидко забезпечити охоплення веб-безпеки за короткий час до розгортання. Портал сервісу забезпечує неперевершену простоту використання та детальне бачення сповіщень про атаки та статистики в реальному часі для підтримки планування на майбутнє. Сповіщення про атаки в реальному часі надають вам інформацію про атаки, активи під загрозою та те, як Cloud WAF Service реагує. Команда екстреного реагування Radware, група експертів із веб-безпеки, надає додаткову підтримку для пом'якшення атак, криміналістичного аналізу та майбутнього планування [14].

Компанія Akamai Technologies, розташована в Кембриджі, штат Массачусетс, розробила інтегрований брандмауер для веб-додатків із захистом від ботів, безпекою API та захистом від DDoS 7 рівня. Рішення забезпечує високу продуктивність для кінцевих користувачів із широким спектром можливостей налаштування. Адміністратори отримують автоматичні оновлення стану мережі в рамках спрощеного процесу виправлення. Інтерфейсом також легко керувати завдяки зрозумілому інтерфейсу, який забезпечує широку видимість усього трафіку та атак. Akamai пропонує низку моделей ціноутворення, кожна з яких має різні функції та можливості для різних випадків використання [12].

Рішення має розширену функцію виявлення API, яка дозволяє адміністраторам керувати ризиками за допомогою нових або раніше невідомих API. Він також підтримує інтеграцію DevOps через простий графічний інтерфейс. Захист від DDoS надається через прикладний рівень. Akamai App & API Protector можна швидко розгорнути та легко керувати ним. Рішення надає посібники на порталі, налаштування майстра та робочі процеси конфігурації, які допомагають у початковій адаптації та налаштуваннях. Інші важливі функції включають виявлення ботів і додаткові інструменти, такі як розширені засоби керування AppSec, керовані служби та професійні послуги. Akamai надає корисну підтримку під час адаптації та може допомогти вам повністю налаштувати рішення відповідно до ваших потреб [12].

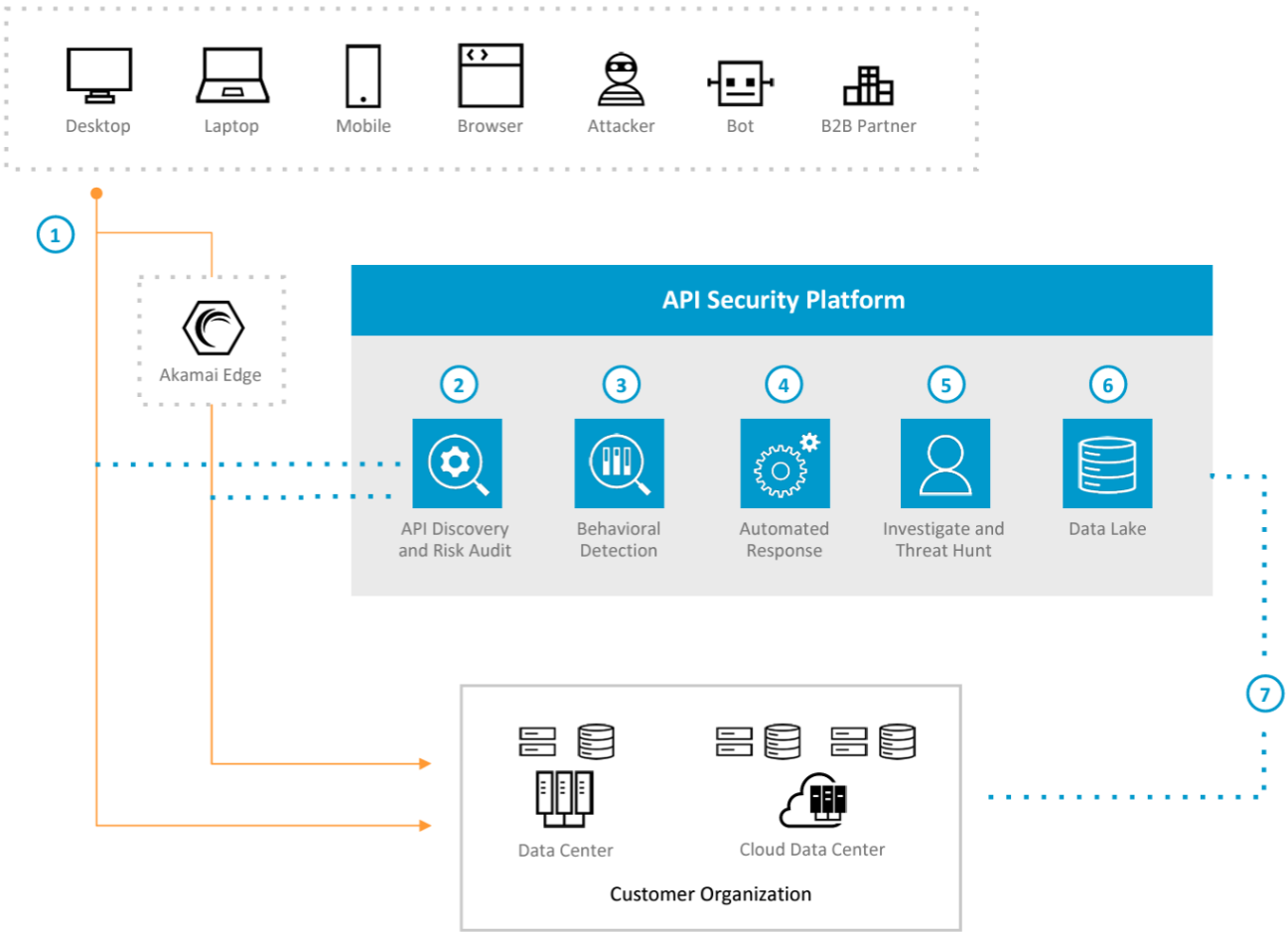

Рис. 1.7. Схема розгортання рішення Akamai App & API Protector [12]

AWS WAF – це потужний брандмауер для веб-додатків, який забезпечує надійний захист від поширених загроз, таких як веб-експлойти та боти, за допомогою ретельного моніторингу, фільтрації та можливостей обмеження швидкості. Керування рішенням здійснюється через AWS Firewall Manager, що надає адміністраторам централізований уніфікований доступ до даних і елементів керування. Широко настроюване рішення дозволяє командам розробляти власні правила та політику відповідно до процедур компанії або вимог дотримання. Це досягається за допомогою вбудованого інструменту, візуального конструктора правил або коду JSON.

Можливості фільтрації інструментів особливо надійні; адміністратори можуть успішно фільтрувати атаки, такі як SOLi та XXS, а також фільтрувати небажаний трафік на основі IP-адрес або поведінки. AWS WAF можна повністю керувати через API, що дозволяє командам автоматично створювати та

підтримувати правила. Рішення забезпечує широку видимість, забезпечуючи показники в реальному часі та може отримувати необроблені метадані запиту щодо географічного розташування, URL-адрес та IP-адрес. Це рішення підійде середнім і великим компаніям, які використовують веб-додатки AWS.

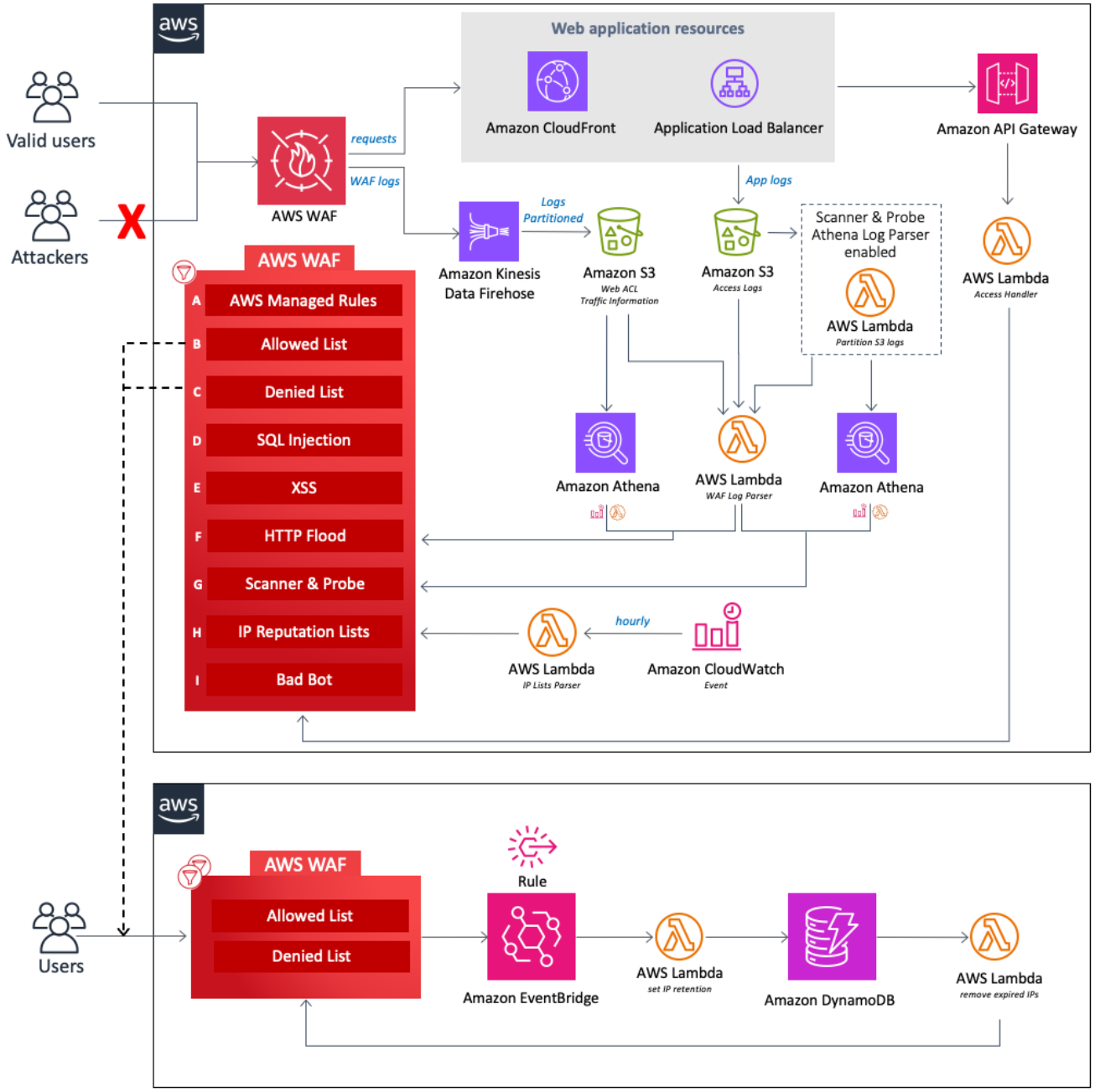

Рис. 1.8. Схема розгортання рішення AWS WAF [15]

Рішення, AWS WAF, допомагає захистити веб-додатки від методів атак, які можуть вплинути на доступність додатка, поставити під загрозу безпеку або

споживати надмірні ресурси. Ми можемо використовувати AWS WAF для визначення настроюваних правил веб-безпеки.

Підсумовуючи, безпека веб-додатків є важливою складовою загальної безпеки будь-якої організації, яка залежить від веб-додатків для надання послуг своїм користувачам. Щоб захистити конфіденційні дані та підтримати довіру клієнтів, підприємства повинні надавати пріоритет посиленню безпеки веб-додатків у світлі зростання кількості кіберзагроз і атак.

Загалом посилення безпеки веб-додатків вимагає поєднання технічних і нетехнічних дій, які передбачають співпрацю та координацію між багатьма зацікавленими сторонами організації. Організації можуть знизити ризик подій безпеки, захистити свою репутацію та бренд, а також захистити особисті дані своїх клієнтів, використовуючи проактивний підхід до безпеки веб-додатків.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API НА БАЗІ IMPERVA WAF

2.1. Призначення та основні функції рішення Imperva WAF

WAF можуть бути на основі хоста, мережі або хмари і зазвичай розгортаються через зворотні проксі та розміщуються перед додатком чи веб-сайтом (або кількома додатками та сайтами) (рисунок 2.1) [4].

WAF можуть працювати як мережеві пристрої, серверні плагіни або хмарні служби, перевіряючи кожен пакет і аналізуючи логіку прикладного рівня (рівень 7) відповідно до правил, щоб відфільтрувати підозрілий або небезпечний трафік [4].

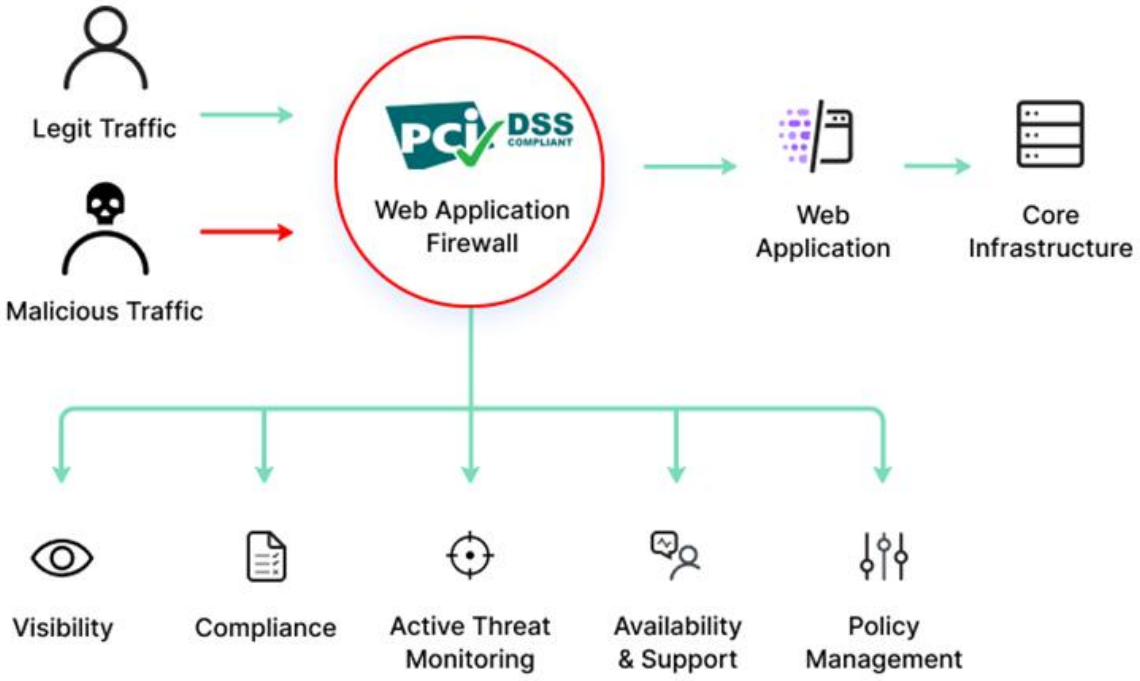

Рис. 2.1. Місце WAF в архітектурі веб-додатків [4]

WAF зазвичай пропонують такі функції та можливості [4]:

виявлення атак на основі бази даних сигнатур. Сигнатури атак – це шаблони, які можуть вказувати на зловмисний трафік, включаючи типи запитів, аномальні

відповіді сервера та відомі шкідливі IP-адреси. Раніше WAF покладалися переважно на бази даних шаблонів атак, які були менш ефективними проти нових або невідомих атак;

аналіз трафіку за допомогою штучного інтелекту. Алгоритми штучного інтелекту дозволяють аналізувати поведінку моделей трафіку, використовуючи базові показники поведінки для різних типів трафіку для виявлення аномалій, які вказують на атаку. Це дозволяє виявляти атаки, які не відповідають відомим шаблонам шкідливих дій;

профілювання додатка. Це передбачає аналіз структури додатка, включаючи типові запити, URL-адреси, значення та дозволені типи даних. Це дозволяє WAF ідентифікувати та блокувати потенційно шкідливі запити;

налаштування WAF. Адміністратори можуть визначати правила безпеки, що застосовуються до трафіку додатка. Це дозволяє організаціям налаштовувати поведінку WAF відповідно до своїх потреб і запобігати блокуванню законного трафіку;

механізми кореляції. Вони аналізують вхідний трафік і сортують його за відомими сигнатурами атак, профілюванням додатків, аналізом ШІ та спеціальними правилами, щоб визначити, чи слід його блокувати;

платформа захисту від DDoS. Є можливість інтегрувати хмарну платформу, яка захищає від розподіленої атаки відмови в обслуговуванні (DDoS). Якщо WAF виявляє DDoS-атаку, він може передати трафік на платформу захисту від DDoS, яка може впоратися з великою кількістю атак;

забезпечення мережі доставки контенту (CDN). WAF розгортаються на межі мережі, тому WAF, розміщений у хмарі, може забезпечити CDN для кешування веб-сайту та скорочення часу його завантаження. WAF розгортає CDN у кількох точках присутності (PoP), які розподілені по всьому світу, тому користувачі обслуговуються з найближчої точки присутності.

WAF можуть використовувати позитивну або негативну модель безпеки або комбінацію двох [4]:

Позитивна модель безпеки WAF передбачає білий список, який фільтрує

трафік відповідно до списку дозволених елементів і дій. Все, що не входить до списку, блокується. Перевагою цієї моделі є те, що вона може блокувати нові або невідомі атаки, яких розробник не передбачав.

Негативна модель безпеки WAF передбачає чорний список (або список заборони), який блокує лише певні елементи – дозволено все, що не входить до списку. Цю модель легше реалізувати, але вона не може гарантувати, що всі загрози будуть усунені. Це також вимагає ведення потенційно довгого списку шкідливих сигнатур. Рівень безпеки залежить від кількості реалізованих обмежень.

Рішення SecureSphere Web Application Security захищають веб-додатки від кібератак. SecureSphere постійно адаптується до загроз, що розвиваються, і дає змогу фахівцям із безпеки, адміністраторам мережі та розробникам додатків зменшити ризик злому даних та відповідати ключовим вимогам відповідності, таким як PCI DSS [5].

Захист системи SecureSphere працює на рівнях, які відповідають 7-рівневій моделі OSI. Брандмауер відповідає рівням OSI з 2 по 4. Перевірка протоколу та сигнатури прикладного рівня відповідають шару 7 моделі OSI, як показано нижче.

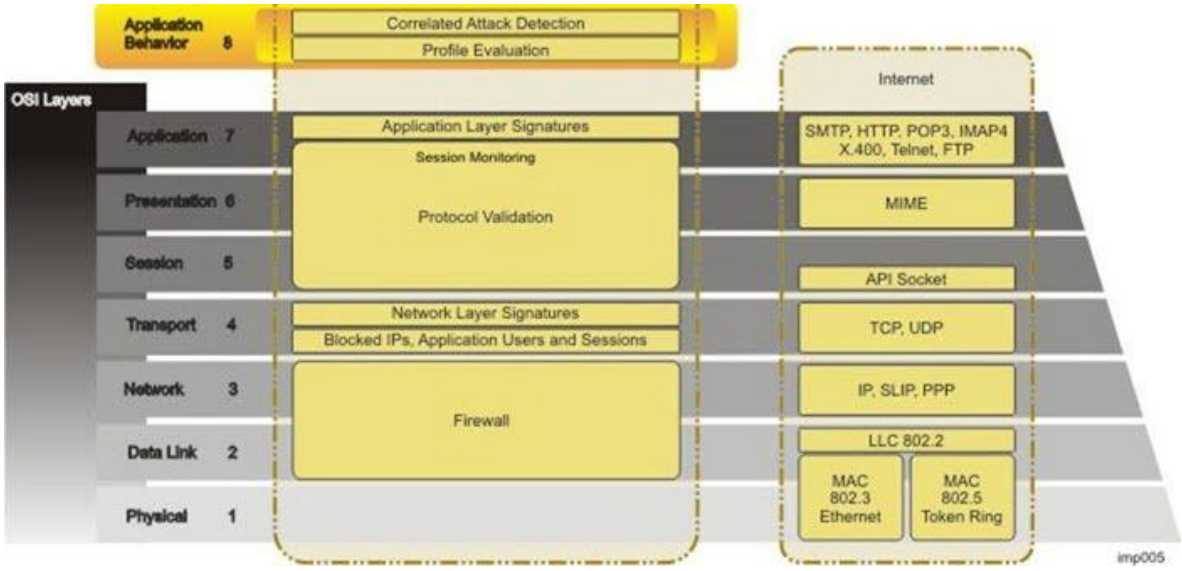

Рис. 2.2. Рівні моделі OSI, де представлені функції захисту рішення SecureSphere Web Application Security [5]

Декілька вдосконалених процесів захисту SecureSphere, таких як оцінка

профілю, кореляція Web/DB та кореляційне виявлення атак, працюють на рівні програми і, таким чином, забезпечують захист на рівні 8, не визначеному в моделі OSI (рисунок 2.2) [5].

Рішення SecureSphere WAF компанії Imperva захищає веб-додатки, забезпечуючи захист і контроль над критично важливими даними.

Рис. 2.3. Модель захисту, яка реалізується SecureSphere WAF [5]

Модель захисту, яка реалізується SecureSphere WAF, показано на рисунку 2.3, містить наступні рівні захисту [5]:

перевірка протоколу – фільтрує порушення протоколу HTTP та атаки, які використовують переваги протоколу HTTP. Наприклад, спроба зробити переповнення буфера за допомогою аномально великого заголовка HTTP-запиту;

сигнатури атак – ідентифікує відомі додатки, платформи та мережеві атаки. SecureSphere має базу даних із понад 6500 сигнатурами, яка регулярно оновлюється експертами Центру захисту додатків;

запобігання витоку даних – виявляє конфіденційні дані, такі як дані кредитних карток або особисту інформацію, коли вони виходять із веб-сайту. Часто це законно, але іноді це означає витік даних. SecureSphere може спостерігати, як конфіденційні дані виходять із додптка, а адміністратори можуть переконатися, що

ці дані використовуються законно;

профіль додатка – SecureSphere порівнює фактичне використання додатка з очікуваним використанням у моделі, щоб визначити підозрілі випадки або підозрілу поведінку користувача;

виявлення веб-хробаків – SecureSphere використовує розширені алгоритми для зупинки атак веб-додатків Zero-day;

кореляційний механізм – кореляція подій і автоматизована базова лінія забезпечують SecureSphere WAF потужною вертикальною інтеграцією та аналізом даних за допомогою механізму перевірки кореляційних атак.

Отже, WAF мають вирішальне значення для безпеки онлайн-бізнесу. Вони захищають конфіденційні дані, запобігають витоку та впровадженню шкідливого коду на сервер і відповідають вимогам, таким як Стандарт безпеки даних платіжних карток (PCI DSS). Оскільки організації все більше використовують веб-додатки та пристрої IoT, зловмисники намагаються націлитися на їхні вразливості. Інтеграція WAF з іншими інструментами безпеки має створювати надійну стратегію захисту інформаційних ресурсів організацій.

2.2. Архітектура рішення Imperva WAF

На рисунку 2.4 показано схему SecureSphereWAF в IT інфраструктурі.

Архітектура SecureSphere дозволяє налаштувати сайти, які відображають архітектуру корпоративної мережі, профілює поведінку трафіку на цих сайтах, а потім дає змогу налаштувати політики для визначення очікуваної поведінки трафіку на цих сайтах. На рисунок 2.6 показано, як концепція безпеки даних програми застосовується SecureSphere.

Домен, захищений SecureSphere, містить такі основні елементи [5]:

сайти: фізичний сайт, де встановлено групи серверів (наприклад, центри обробки даних);

групи серверів: містять фізичні сервери, служби та фактичні програми;

сервіси: HTTP. Сервіс характеризується використовуваним портом, набором

відповідних плагінів, наборами символів, шифруванням і включає набір програм;

програми: веб-додатки.

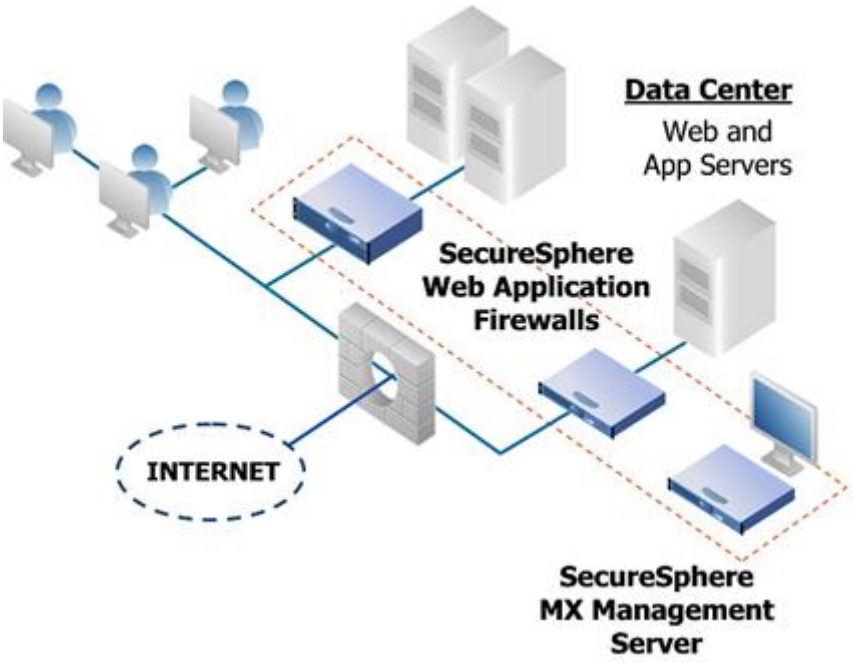

Рис. 2.4. Місце SecureSphereWAF в інфраструктурі [5]

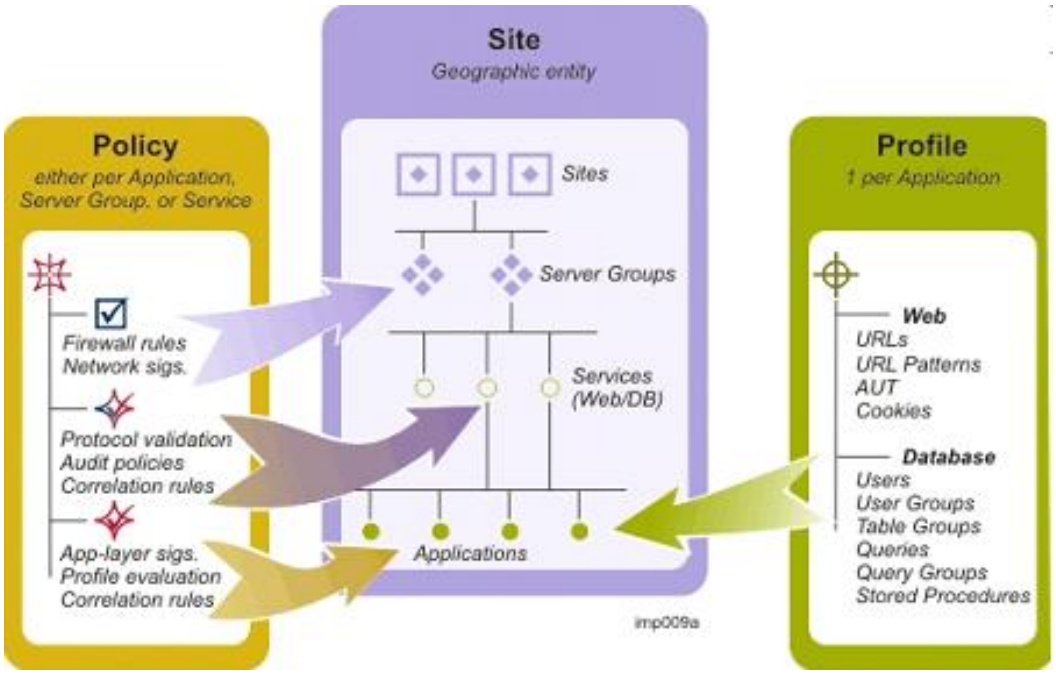

Рис. 2.5. Принцип роботи SecureSphereWAF [5]

Окрім фізичного представлення захищеного домену (використання сайтів, груп серверів, служб, програм), SecureSphere забезпечує логічне представлення

захищеного домену. Логічне представлення зосереджено на рівні програми та забезпечує необмежену ієрархічну групу програм [5].

Основна мета базової конфігурації – визначити трафік, який потрібно захистити. Це досягається шляхом визначення основних будівельних блоків, які складають домен SecureSphere, за допомогою ряду параметрів, включаючи IP-адреси, порти, протоколи тощо. Знімок екрана (рисунок 2.6) ілюструє основну конфігурацію цих компонентів.

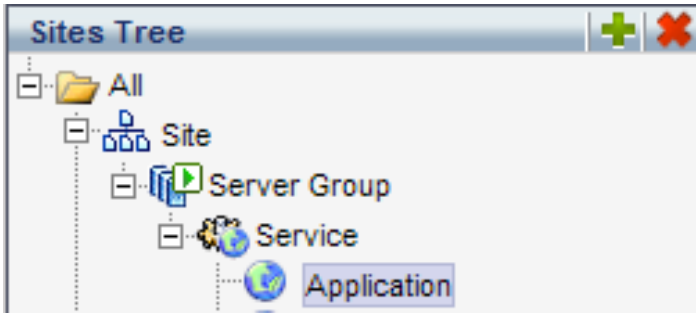

Рис. 2.6. Основна конфігурація компонентів SecureSphere

Основні компоненти налаштовуються в такому порядку [5]:

сайти: визначає основний контейнер для всіх інших об'єктів;

групи серверів: визначає один або кілька серверів у певному місці на основі IP-адрес;

служби: визначає типи послуг, розміщені групою серверів на основі портів;

програми: фактична програма, яка працює у мережі.

Сайти є основним контейнером, в якому знаходяться всі інші об'єкти мережі. Створення нових сайтів дає змогу розробити топологію вашої архітектури SecureSphere, щоб вона відображала вашу реальну фізичну топологію. Наприклад, якщо сайт призначений для відображення вашого фінансового відділу, він буде налаштований з усіма серверами, службами та програмами, які використовуються цим відділом. Основна мета сайту – допомогти логічно організувати вашу мережеву структуру в SecureSphere, роблячи великі системи більш керованими. Невеликі мережі можуть включати лише один або два сайти, тоді як великі мережі включають десяток або більше сайтів.

Групи серверів – це представлення одного або кількох серверів, розташованих на певному сайті. Сервер у SecureSphere – це набір служб або програм, що належать одній IP-адресі. Групи серверів дозволяють SecureSphere визначати конкретні об’єкти на сайті, які потрібно захистити, і чиї операції необхідно відстежувати та перевіряти. Вони також дозволяють вибирати трафік, яким необхідно керувати, використовуючи такі функції: ігнорувати IP-адреси, обмежувати моніторинг певними IP-адресами, керувати застосовуваними політиками на рівні групи серверів і встановлювати статус групи серверів (активний, симуляційний або вимкнений). Можливо, необхідно створити нову групу серверів (рисунок 2.7), щоб забезпечити окремий контроль над певним набором служб, що дозволить перемістити їх з режиму активного моніторингу в режим симуляції, не впливаючи на захист інших служб у мережі.

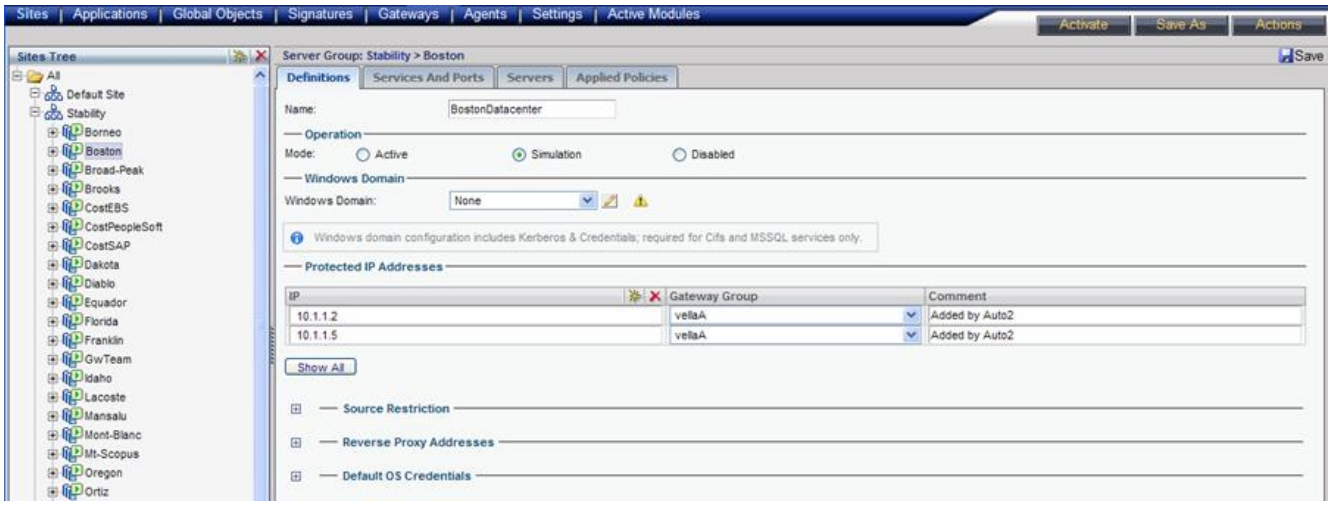

Рис. 2.7. Інтерфейс керування групами серверів

Веб-служби в SecureSphere – це веб-служби, встановлені та запущені на серверах у групі серверів, трафік яких відстежує SecureSphere. Додавання веб-служби визначає послуги, які відстежуються для IP-адрес, визначених у групі серверів. Це необхідний крок для базової конфігурації, залежно від типу служби, що відстежується.

Веб-програми в SecureSphere представляють реальні веб-додатки, що працюють у мережі, і дозволяють відстежувати трафік для кожної програми.

Визначаючи програми, ви дозволяєте SecureSphere відстежувати трафік і звітувати про нього для кожної програми, забезпечуючи додаткову деталізацію під час моніторингу та звітування.

2.3. Призначення та функції рішення Imperva Cloud WAF

Веб-додатки є легкодоступними та часто служать точкою входу до цінних даних. Вони завжди будуть основною мішенню для атак [19].

Дійсно, хакерські атаки, які знищують корпоративні та урядові сайти, DDoS-атаки на великі фінансові установи та масові веб-зломи, що призводять до зламаних мільйонів номерів кредитних карток і особистих даних.

Щоб прискорити швидкість технічних веб-атак, зловмисники стали «індустріалізованими». Вони використовують комбінацію готових інструментів для атак, інфікованих «ботів» і пошукових систем, щоб швидко знаходити та використовувати вразливості веб-додатків [19].

Хакери не зупиняються на традиційних веб-атаках. Атаки на бізнес-логіку та шахрайство також стають все більш популярними методами. Сьогодні хакери використовують недоліки бізнес-логіки, щоб розміщувати рекламу на онлайн-форумах. Вони шукають на веб-сайтах цінну інтелектуальну власність. Вони здійснюють повторні атаки грубою силою. Вони використовують символи підстановки в пошукових полях, щоб призупинити додатки. Ці атаки залишили багато організацій у стані розуму, оскільки сканери додатків не можуть виявити недоліки бізнес-логіки, а безпечні процеси розробки не завжди можуть їх усунути [19].

Сучасні веб-додатки стали критично важливими для великих організацій зі списку Fortune 500, які покладаються на свої додатки для збільшення прибутку, розвитку бажаного іміджу бренду та розвитку відносин із клієнтами. Проте вони стикаються з глобальними загрозами з усіх частин світу. Кіберзлочинці прагнуть використати цифрову присутність організації, щоб закріпитися в її ІТсередовищі та отримати доступ до цінних корпоративних даних. Крім того, перехід програмного

забезпечення веб-додатків до практики гнучкої розробки часто означає, що програмне забезпечення не було ретельно перевірено та може бути випущене з критичними вразливими місцями, якими може скористатися кіберзлочинець. Організації шукають рішення для веб-безпеки, які не лише забезпечують комплексний захист безпеки, але й гнучкість масштабування для користувачів у всьому світі [20].

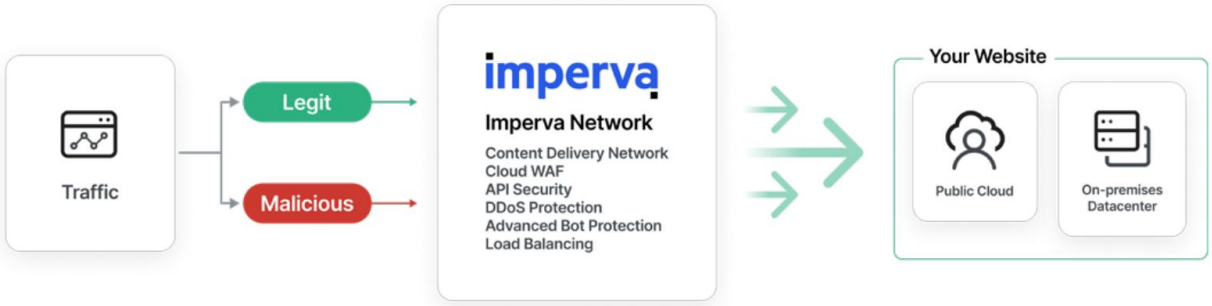

Рис. 2.8. Cloud WAF перевіряє кожен запит, фільтруючи зловмисну активність

Imperva Cloud WAF пропонує провідний у галузі брандмауер безпеки веб-додатків, який забезпечує захист корпоративного рівня від найскладніших загроз безпеки. Незалежно від того, чи розміщені ваші веб-сайти та програми у загальнодоступній хмарі чи локально, Cloud WAF гарантує, що ваші критично важливі активи завжди захищені від будь-яких спроб злому на прикладному рівні.

Цілодобова служба безпеки та підтримка Cloud WAF є частиною інтегрованого комплексу служб безпеки та доставки додатків із глибоким захистом, включаючи CDN, захист від DDoS, розширений захист від ботів, Безпека API і балансування навантаження в кожній нашій глобальній точці присутності. Усі компоненти спільно використовують інтелектуальні дані, щоб логіку безпеки та доставки можна було застосувати прямо з краю, щойно запит потрапляє в нашу мережу. Рішення інтегрується з провідними SIEM, а Imperva Attack Analytics використовує штучний інтелект (ШІ), щоб розділити тисячі подій Cloud WAF на окремі наративи, значно покращуючи ефективність операційного центру безпеки (SOC) і знижуючи ризики [20].

Розширений механізм ідентифікації профілює весь вхідний трафік на межі в

режимі реального часу, точно розрізняючи легітимних і зловмисних клієнтів задовго до того, як вони досягнуть веб-додатка. Цей автоматизований процес безпеки означає не тільки підвищену безпеку в Інтернеті, меншу завантаженість веб-сервера та зменшення споживання пропускної здатності, але й меншу залежність від внутрішніх експертів із безпеки та зниження точності, яка виникає завдяки ручному контролю. Не дивно, що переважна більшість клієнтів Imperva Cloud WAF одразу розгортають режим блокування, оскільки це рішення забезпечує легальний трафік із майже нульовою кількістю помилкових спрацьовувань.

Imperva Cloud WAF захищає від 10 найпопулярніших загроз безпеці OWASP, таких як міжсайтовий сценарій, незаконний доступ до ресурсів і віддалене включення файлів, блокуючи атаки в режимі реального часу. Рішення працює в поєднанні зі стеком рішень Imperva Application Security, використовуючи різні можливості пом’якшення, які вимагають різні атаки – будь то атака DDoS або бот, який використовує ін’єкцію SQL для атаки на ваш API. Більше того, команда дослідницьких лабораторій Imperva активно виявляє нові загрози, щоб забезпечити сучасний захист безпеки, необхідний у сучасному середовищі атак, що швидко змінюється. Експерти з безпеки відстежують зовнішні джерела, як-от нові розкриття вразливостей, і допомагають вам зменшити ризик коду сторонніх розробників. Команда аналізує весь трафік, що проходить через Imperva, за допомогою краудсорсингу, автоматично перевіряючи та поширюючи нові правила пом’якшення для всіх наших клієнтів. Щодня додаються нові сигнатури безпеки, які захищають від нещодавно виявлених загроз.

Imperva Cloud WAF налаштовується через простий у використанні веб-інтерфейс, захищений за допомогою двофакторної автентифікації. Простий графічний інтерфейс дозволяє конфігурувати власні правила безпеки для оптимального застосування політик безпеки в унікальних середовищах. Завдяки автоматизації DevOps через постачальника Terraform, поширення політики десятків тисяч правил може відбуватися за лічені секунди. Панель інструментів Cloud WAF високого рівня надає короткий огляд загального ландшафту загроз для організації, а керування централізоване разом із іншими функціями, такими як

безпека API, захист від DDoSатак тощо.

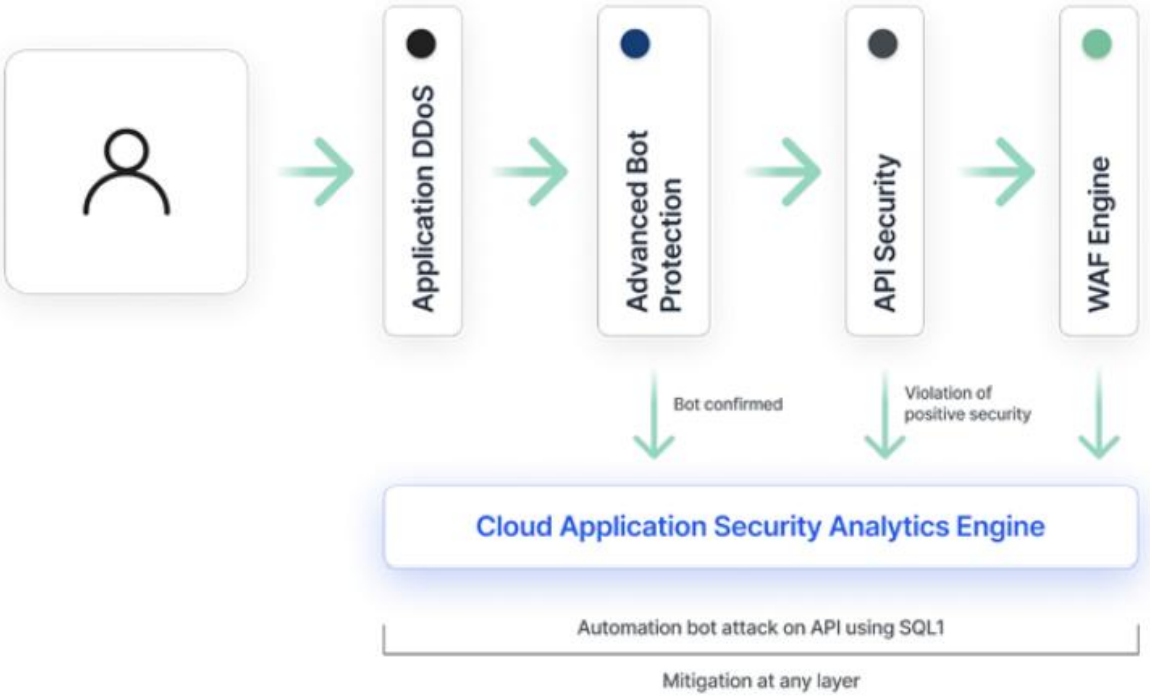

Рис. 2.9. Схема реалізації основних функцій Imperva Cloud WAF [20]

Основними перевагами рішення Imperva Cloud WAF є [20]:

найкращий у своєму класі WAF, сертифікований PCI;

з коробки, автоматизований захист;

розгортається в режимі блокування з майже нульовим помилковим спрацьовуванням;

інтеграція Terraform забезпечує автоматичне надання DevOps;

підтримується експертами з безпеки в Imperva Research Labs, які знижують ризик використання коду сторонніх розробників;

спеціальні правила самообслуговування;

цілодобова служба безпеки та підтримка;

частина комплексної безпеки та доставки хмарних додатків;

надає інформацію про загрози для ефективної статистики в Attack Analytics.

Imperva Cloud WAF є ключовим компонентом Imperva Application Security, який знижує ризик, забезпечуючи оптимальну взаємодію з користувачем. Рішення

захищає додатки локально та в хмарі за допомогою реалізації таких функцій [20]:

надання корисної інформації про безпеку;

забезпечення захисту WAF;

захист від DDoS-атак;

пом'якшення атак ботнетів;

блокування кібератак, спрямованих на API;

включення захисту від RASP;

забезпечення оптимальної доставки контенту.

2.4. Призначення та функції рішення Imperva WAF Gateway

Веб-додатки є основною мішенню для кібератак, оскільки вони легкодоступні та пропонують просту точку входу до цінних даних. Організаціям необхідно захищати веб-додатки від існуючих і нових кіберзагроз, не впливаючи на продуктивність або час безвідмовної роботи. Швидкий темп змін додатків може ускладнити командам безпеки не відставати від правил оновлення, які належним чином захищають вебресурси. Це може створити прогалини в безпеці та вразливості, якими можуть скористатися кіберзлочинці, що призведе до дорогого витоку даних. Крім того, організації прагнуть розгорнути рішення безпеки, які можна масштабувати з їхніми програмами, щоб відповідати зростанню попиту користувачів, забезпечуючи належну безпеку веб-активів, зберігаючи взаємодію з кінцевим користувачем [21].

Провідний на ринку шлюз Imperva WAF дає змогу організаціям захищати корпоративні додатки за допомогою автоматизованої веб-безпеки та гнучкого розгортання. Шлюз WAF забезпечує комплексний захист і деталізовані можливості, що робить його ідеальним рішенням для захисту цінних веб-ресурсів, досягнення відповідності PCI та забезпечення надійного захисту від атак безпеки OWASP Top 10 [21].

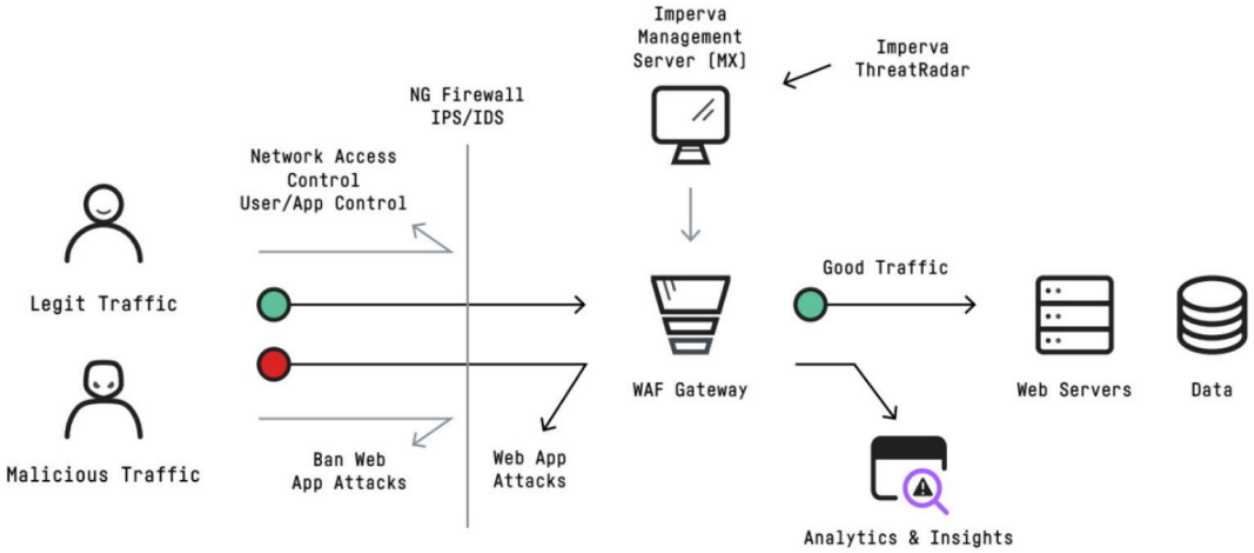

Рис. 2.10. Шлюз Imperva WAF захищає додатки від веб-атак, використовуючи дослідницькі дані [21]

Ключові можливості рішення Imperva WAF Gateway [21]:

динамічне профілювання вивчає захищені програми та поведінку користувачів, автоматично застосовуючи позитивну модель безпеки;

гнучке розгортання для підтримки гібридних і хмарних середовищ;

може бути розгорнуто в діапазоні та як слухач із підтримкою Envoy та Nginx;

оновлює веб-захист за допомогою дослідницької інформації про поточні загрози;

співвідносить порушення безпеки для виявлення складних багатоетапних атак;

автоматизоване віртуальне виправлення висока продуктивність; прозоре розгортання.

Шлюз Imperva WAF може ідентифікувати та реагувати на небезпеки, зловмисно вплетені в, здавалося б, нешкідливий трафік веб-сайту – трафік, який прослизає через інші рівні захисту – запобігаючи атакам уразливості додатків, таким як ін’єкції SQL, міжсайтові сценарії та віддалене включення файлів або атаки на бізнес-логіку, такі як сайт копіювання або спам у коментарях.

Автоматизоване навчання додатків

WAF Gateway використовує запатентовану технологію Dynamic Profiling для

автоматизації процесу профілювання додатків і створення базового або «білого списку» прийнятної поведінки користувачів. Перевага цього підходу до позитивної моделі безпеки полягає в автоматичному внесенні дійсних змін у профіль програми з часом. Динамічне профілювання позбавляє від необхідності вручну налаштовувати та оновлювати незліченну кількість URL-адрес програм, параметрів, файлів cookie та методів у ваших правилах безпеки.

Надійний набір API дозволяє командам DevOps і Security інтегрувати розгортання шлюзу WAF і повсякденне налаштування в існуючі процеси DevOps.

Шлюз WAF можна розгорнути як фізичний пристрій, віртуальний пристрій або в хмарі через Amazon Web Services або Azure Marketplace. Крім того, WAF Gateway можна розгортати прозоро, не вимагаючи практично жодних змін у мережі. Деталізована політика контролю забезпечує виняткову точність і неперевершений контроль відповідно до конкретних вимог захисту кожної організації.

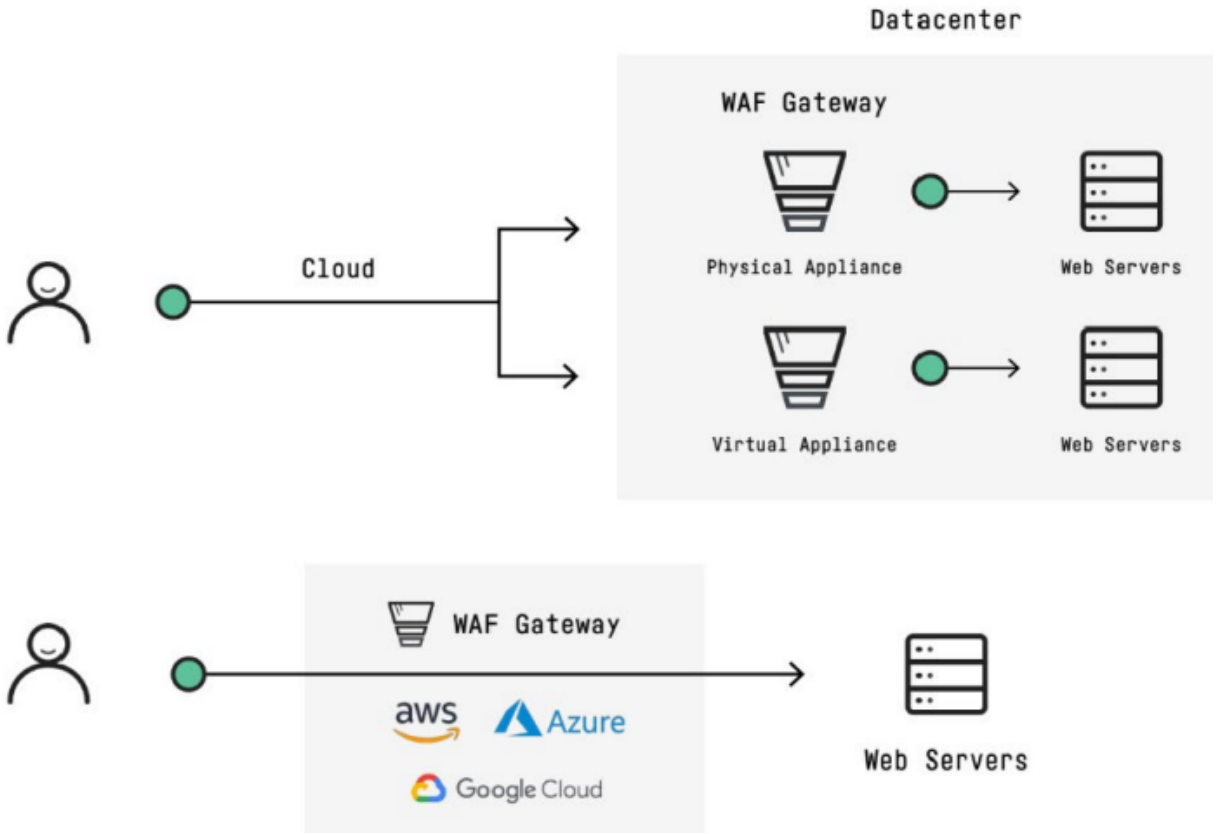

Рис. 2.11. Шлюз Imperva WAF можна розгорнути як фізичний пристрій, віртуальний пристрій або в хмарі [21]

Шлюз WAF є ключовим компонентом Imperva Application Security, який знижує ризик, забезпечуючи оптимальну взаємодію з користувачем. Рішення Imperva захищають додатки локально та в хмарі за допомогою [21]:

брандмауера веб-додатків (WAF);

розподіленого захисту від відмови в обслуговуванні (DDoS);

пом'якшенню атак ботнету;

самозахисту програми під час виконання (RASP);

дійсні відомості про безпеку;

захищена доставка програм.

3 ТЕХНОЛОГІЯ ЗАХИСТУ КОРПОРАТИВНИХ ВЕБ-ДОДАТКІВ І API НА БАЗІ IMPERVA WAF

3.1. Варіанти розгортання системи захисту веб-додатків та API на базі Imperva WAF

Розглянемо варіанти розгортання Imperva SecureSphere.

Шлюз SecureSphere можна розгорнути або як вбудований, коли трафік проходить через шлюз SecureSphere, або як шлюз, що перевіряє, де трафік не проходить через шлюз, а копіюється до нього для аналізу. Найважливіші відмінності між цими розгортаннями [16]:

Вбудований шлюз може блокувати шкідливий трафік, щоб він ніколи не досягав захищеної мережі, але, з іншого боку, він вносить певну затримку.

Переглядаючий шлюз не створює затримки, і він може запобігти потраплянню шкідливого трафіку в захищену мережу, видаляючи скидання TCP на сервер на його інтерфейсі блокування.

Вбудовані шлюзи можуть бути розгорнуті в кількох конфігураціях [16]:

Bridge STP: шлюз SecureSphere розгортається в режимі моста в існуючих високодоступних розгортаннях.

Bridge IMPVHA: шлюз SecureSphere розгортається в мостовому режимі в існуючих високодоступних розгортаннях, де STP не підтримується комутаторами, є занадто складним у реалізації або використовується з протоколом Rapid Spanning Tree Protocol (RSTP).

Зворотний проксі сервер: шлюз SecureSphere розгортається в режимі зворотного проксі-сервера, коли трафік, призначений для веб-сервера, спочатку проходить через зворотний проксі-сервер.

У режимі зворотного проксі шлюзи SecureSphere можна налаштувати як прозорий зворотний проксі для певних веб-сервісів, тому шлюз SecureSphere може діяти як проксі-сервер для деяких служб, але не для інших.

Шлюзи SecureSphere також можуть бути розгорнуті разом з балансувальниками навантаження.

Варіант розгортання для режиму прослуховування (Sniffing).

У даному режимі розгортання трафік не проходить через пристрій SecureSphere, а лише копіюється до нього. Пристрій прослуховування може контролювати трафік як в Інтернеті, так і в базі даних, а також блокує шкідливий веб-трафік, видаляючи скидання TCP на сервер. Перевага пристрою прослуховування полягає в тому, що він не вносить затримки в трафік веб-додатків або додатків бази даних.

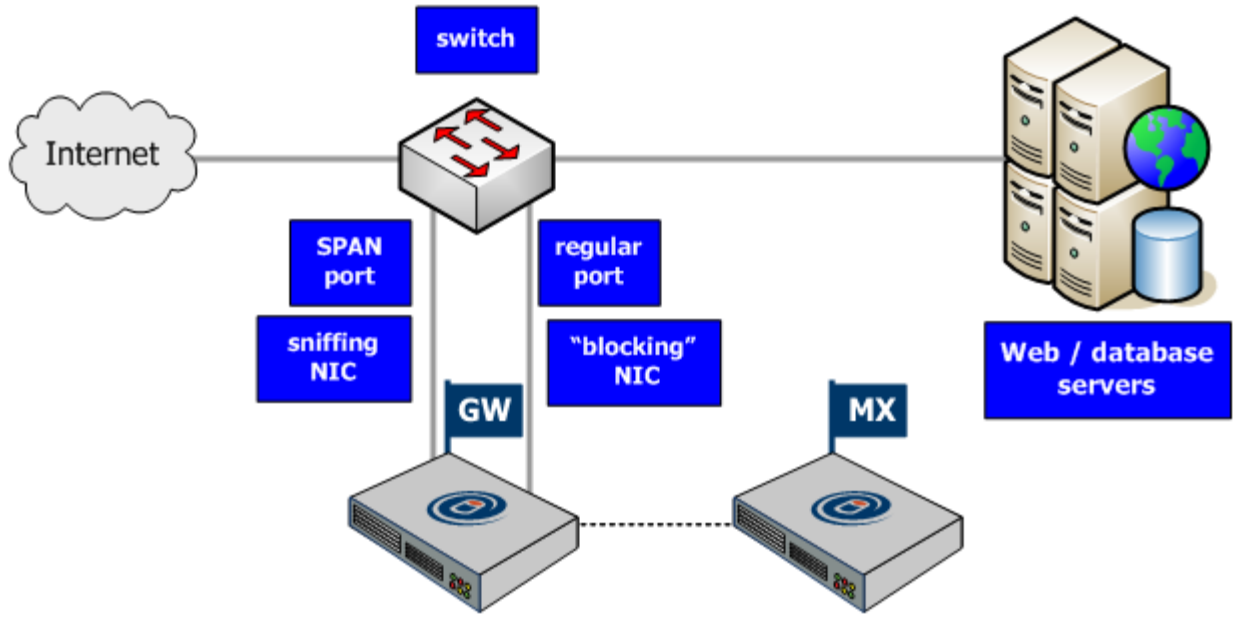

Рис. 3.1. Варіант розгортання для режиму прослуховування [16]

Недоліками режиму прослуховування є:

скидання TCP не є таким надійним методом блокування трафіку, як видалення пакетів;

перевантажені порти SPAN іноді скидають пакети, тому SecureSphere не перевірятиме їх.

Існує два способи прослуховувати трафік: за допомогою SPAN (дзеркального) порту на комутаторі або за допомогою спеціального TAP.

Порт SPAN менш надійний, оскільки він залежить від ресурсів комутатора і має нижчий пріоритет, ніж трафік пересилання, тому він може пропустити пакети. TAP не має цього недоліку.

Варіант розгортання для режиму моста (Bridge).

Під час розгортання моста весь трафік проходить через шлюз SecureSphere, який відстежує трафік і блокує шкідливі з'єднання шляхом відкидання пакетів.

SecureSphere підтримує дві топології мостів: прозорий міст та непрозорий міст з використанням RP (прозорий і непрозорий RP).

Міст може бути невидимим (прозорим) як для клієнтів, так і для серверів, які потім бачитимуть реальні IP-адреси один одного.

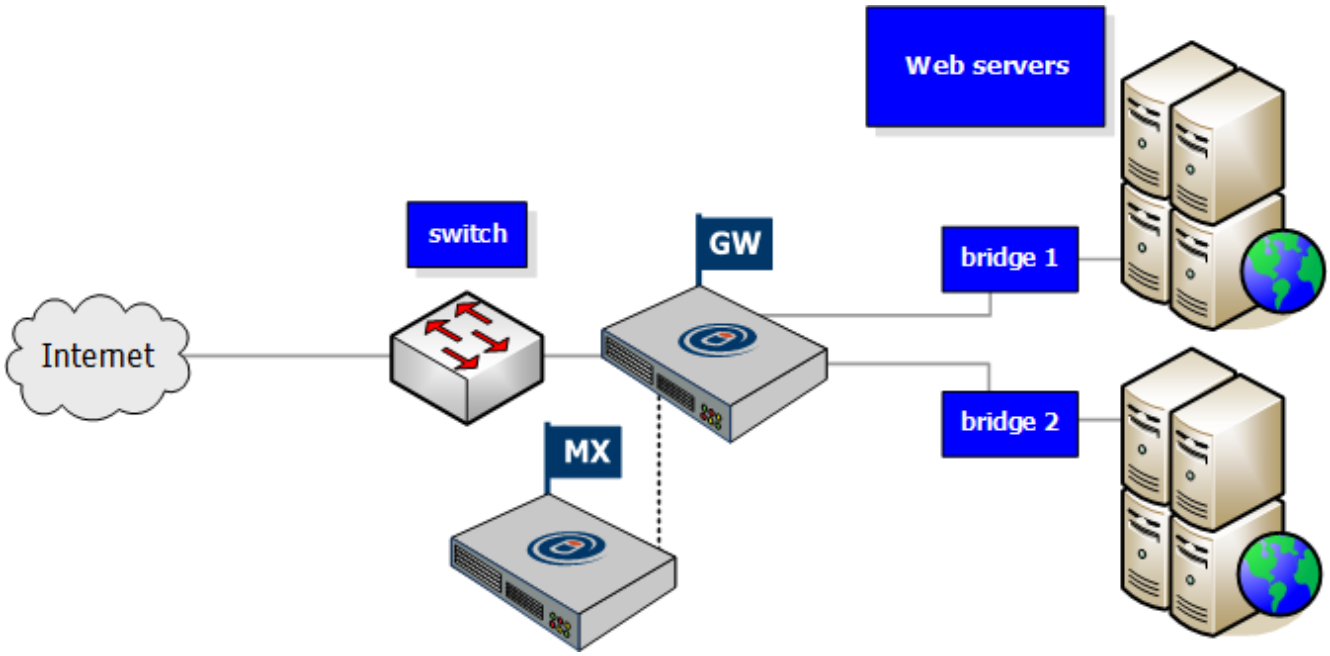

Рис. 3.2. Варіант розгортання для режиму моста [9]

Прозорий міст може бути налаштований для підтримки зв'язку в разі збою. У режимі Fail Open трафік продовжуватиме проходити через міст, але SecureSphere не перевірятиме його.

Варіант розгортання зворотний проксі.

У режимі прозорого зворотного проксі клієнт не знає про зворотний проксі і підключається безпосередньо до сервера. Шлюз SecureSphere Gateway не бачить клієнт або сервер, які бачать реальні IP-адреси один одного.

Варіант розгортання прозорий зворотний проксі – вибрані веб-сервери.

У даному розгортанні шлюз SecureSphere діє як міст, захищаючи всі сервери (два веб-сервери та сервер баз даних), але для одного з веб-серверів шлюз SecureSphere також діє як прозорий зворотний проксі-сервер.

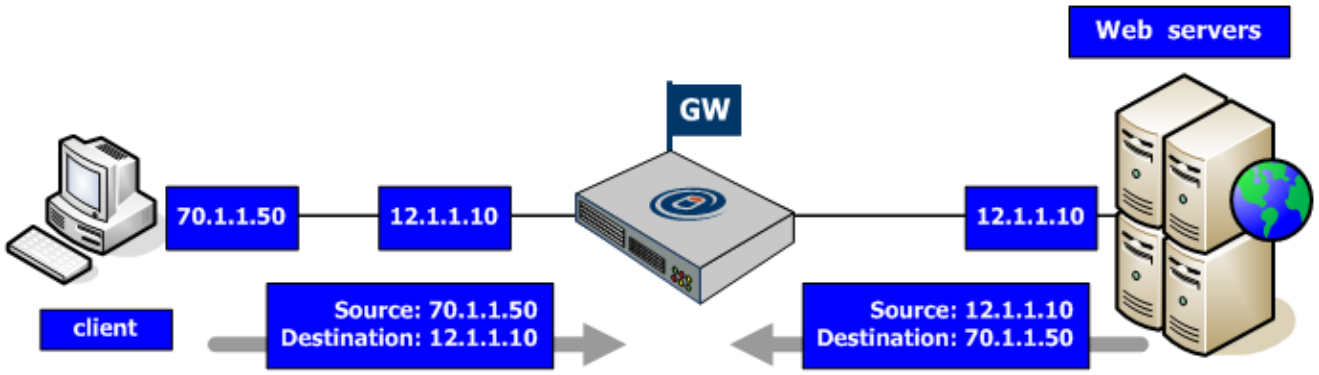

Рис. 3.3. Варіант розгортання прозорого зворотного проксі [16]

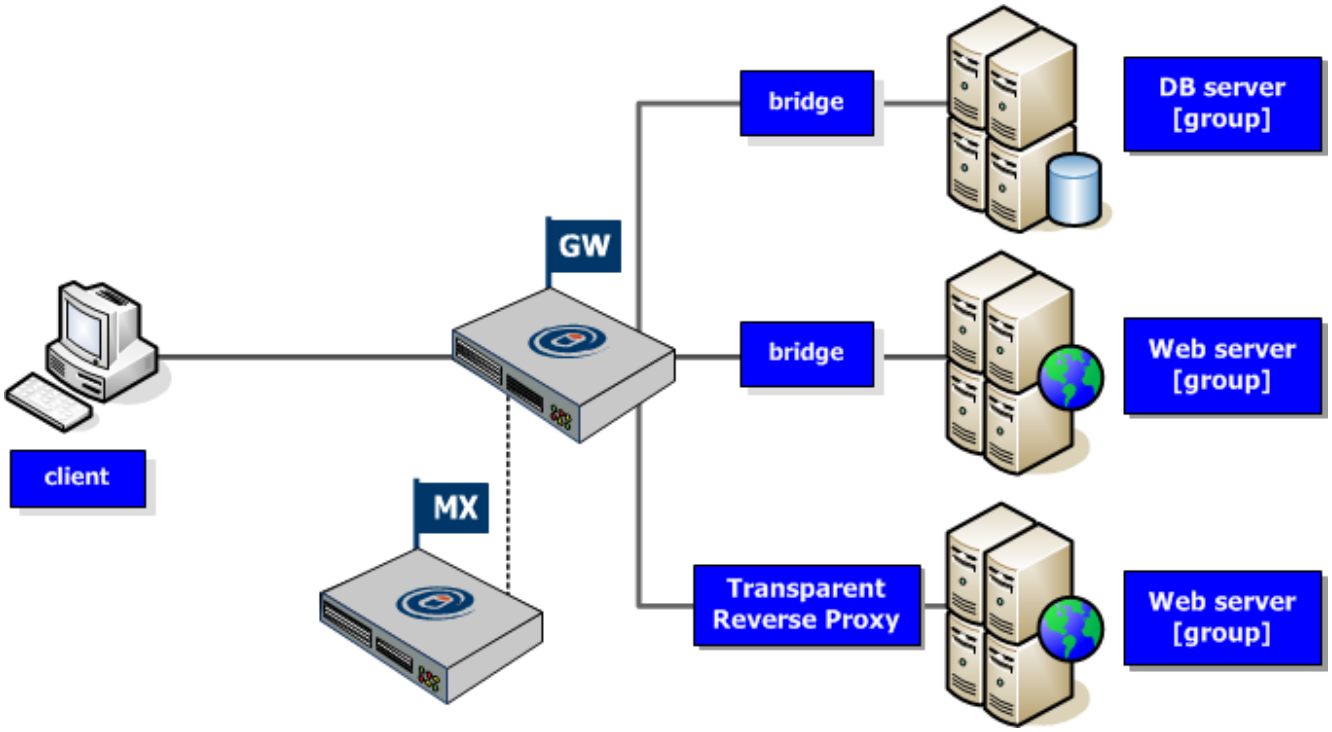

Рис. 3.4. Варіант розгортання прозорого зворотного проксі – вибрані веб-сервери [16]

Варіант розгортання непрозорий зворотний проксі.

У режимі непрозорого зворотного проксі клієнти підключаються до IP-адреси шлюзу SecureSphere, який діє як зворотний проксі для веб-серверів, які він захищає. На відміну від прозорих розгортань, у непрозорих розгортаннях шлюз

SecureSphere є видимим як для клієнта, так і для сервера, тоді як клієнт і сервер не є безпосередньо видимими один для одного.

У розгортанні зворотного проксі клієнт починає сеанс, надсилаючи пакети на вхідну IP-адресу шлюзу SecureSphere. Шлюз SecureSphere Gateway перевіряє пакети і відповідно до правил відкриває друге з'єднання з сервером, змінюючи вихідну IP-адресу пакету на вихідну IP-адресу SecureSphere Gateway, а IP-адресу призначення – на реальну IP-адресу сервера.

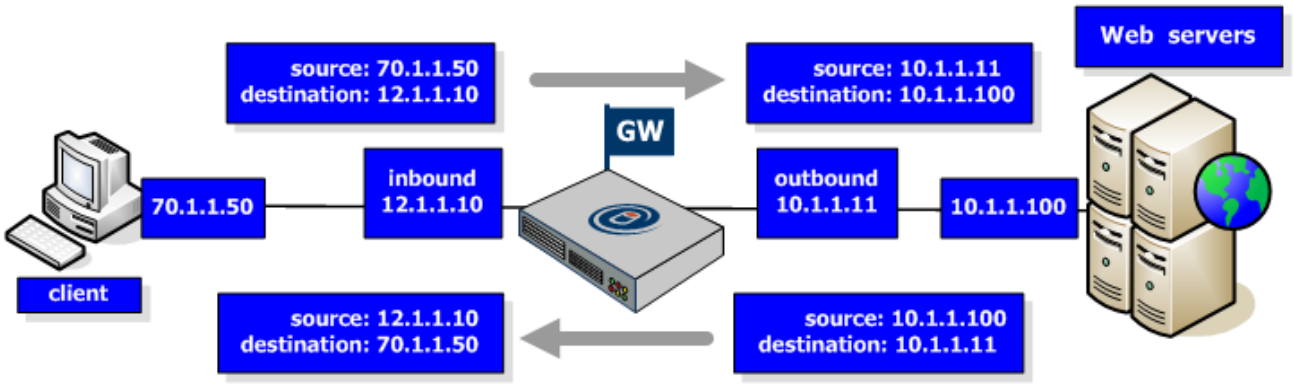

Рис. 3.5. Варіант розгортання непрозорого зворотного проксі [16]

Сервер надсилає зворотні пакети шлюзу SecureSphere Gateway, який перевіряє пакети та пересилає їх клієнту, змінюючи вихідну IP-адресу на вхідні IP-адреси SecureSphere Gateway, а IP-адресу призначення – на IP-адресу клієнта.

З точки зору клієнта, сервер є вхідною IP-адресою SecureSphere Gateway. З точки зору сервера, клієнтом є вихідна IP-адреса шлюзу. SecureSphere Gateway не діє як міст. Зворотний проксі прослуховує вказані порти та ігнорує весь інший трафік.

Варіант розгортання зворотний проксі з балансиром навантаження.

Балансувальники навантаження мають ряд переваг:

висока доступність – якщо один із шлюзів SecureSphere виходить з ладу, балансувальник навантаження спрямовує трафік на один із інших шлюзів;

збільшена пропускна здатність – оскільки навантаження на обробку розподіляється між SecureSphere Gateways, доступна більша загальна пропускна здатність.

Зворотний проксі може бути реалізований за допомогою балансирів навантаження.

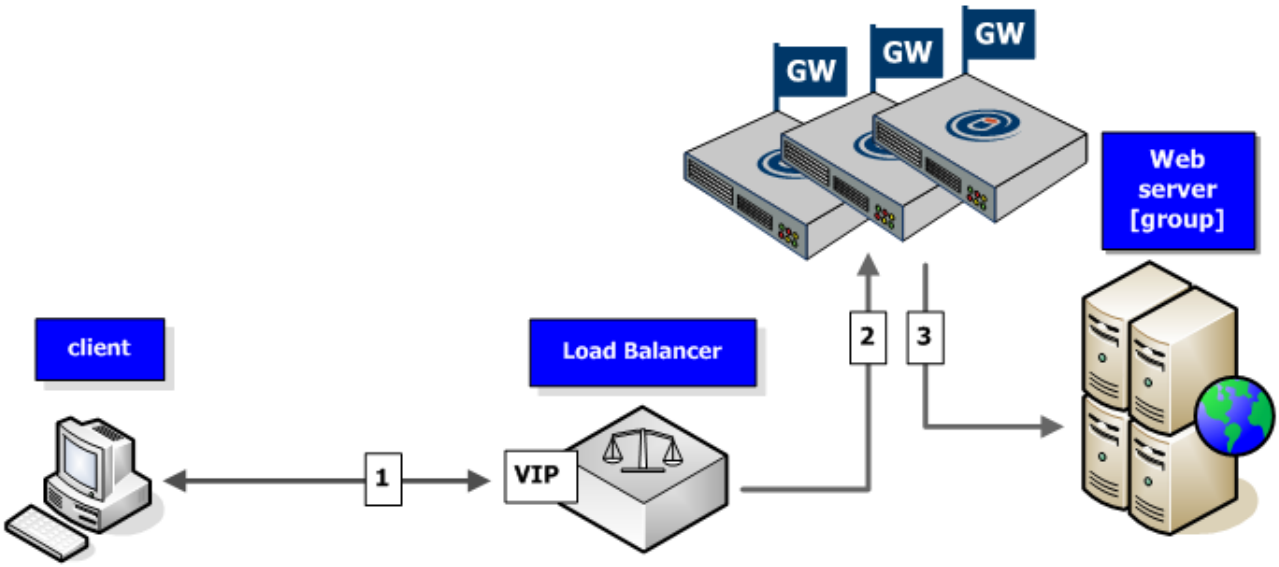

Рис. 3.6. Варіант розгортання зворотний проксі з балансиром навантаження [16]

Клієнт підключається до зовнішньої VIP (Virtual IP) адреси Load Balancer. Балансувальник навантаження відкриває підключення до зворотного проксі на одному із шлюзів SecureSphere. Зворотний проксі-сервер перевіряє пакети і на основі правил надсилає з'єднання на один із веб-серверів. Зворотний рух йде зворотним шляхом.

Необхідно зазначити, що варіант розгортання SecureSphere визначає відповідну множину доступних до реалізації функцій.

3.2. Реалізація функцій моніторингу рішенням Imperva WAF

Моніторинг є ключовим етапом життєвого циклу керування даними програми SecureSphere (Imperva WAF). SecureSphere оснащено зручним монітором, який чітко відображає згенеровану інформацію в центральному місці. Інформація в реальному часі, яка генерується, включає системні події, сповіщення, порушення, заблоковані джерела, стан шлюзу, системні попередження та інформацію про

архівування [5].

Робоча область моніторингу містить ряд параметрів, які представляють різні аспекти моніторингу в SecureSphere [5].

Моніторинг моделей у SecureSphere. Процес моніторингу подій, сповіщень і порушень може мати багато аспектів. Залежно від конкретної реалізації може існувати кілька різних типів користувачів з різними ролями в моніторингу сповіщень. Ми можемо визначити фактичну серйозність конкретних сповіщень на відміну від номінальної серйозності, визначеної SecureSphere, визначити, чи є сповіщення помилковим спрацьовуванням чи атакою, і багато іншого. У цьому розділі розглядаються різні типи користувачів SecureSphere, а також кілька варіантів використання на основі різних реалізацій SecureSphere.

Розуміння сповіщень, подій і порушень. Життєвий цикл моніторингу SecureSphere включає кілька етапів і складається з ряду будівельних блоків, щоб тримати фахівців в курсі подій, що відбуваються у корпоративній системі. Щоб зрозуміти, як SecureSphere відстежує та захищає трафік, важливо розуміти ці будівельні блоки та вміти їх розрізняти.

Виявлення події, яка порушує політику безпеки відстежуваного трафіку. Самі події безпеки не відображаються в SecureSphere, а лише їхні результуючі сповіщення та порушення. Подія безпеки включає такі етапи, як показано в архітектурі моніторингу (рисунок 3.7).

На рисунку 3.7 показано архітектуру моніторингу SecureSphere. Ліва частина схеми ілюструє архітектуру SecureSphere, а права – архітектуру сповіщень і те, що відображається на панелі інструментів.

1. Мережеву подію виявляє SecureSphere Gateway у вхідному трафіку або агент, встановлений на сервері в мережі. Шлюз визначає, що це подія безпеки.

2. Подія безпеки надсилається на сервер управління SecureSphere.

3. Порушення генерується для кожної порушеної політики.

4. Порушення аналізуються, співвідносяться, а потім призначаються сповіщенням. SecureSphere корелює та агрегує порушення на основі відомих атак. Це допомагає ідентифікувати атаки під час їх виникнення.

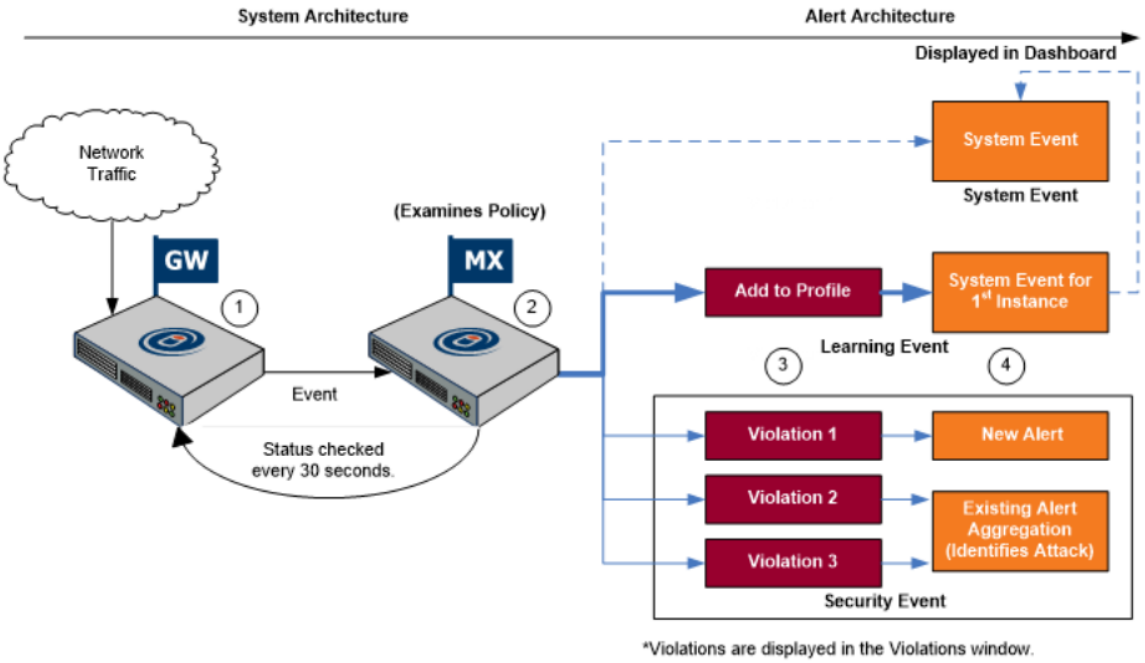

Рис. 3.7. Архітектура моніторингу SecureSphere [5]

Приклад: SecureSphere виявляє, що користувач порушив політику, яка визначає, хто може отримати доступ до певних даних. Порушення реєструється, створюється сповіщення безпеки та відображається у вікні сповіщень.

Порушення є ознакою того, що відбулася подія безпеки, яка порушує політику. Одна подія безпеки може викликати кілька порушень. Порушення відображаються у вікні «Порушення», підсумковий список порушень також можна побачити на панелі «Деталі» у вікні «Сповіщення». Порушення генерується для кожної порушеної політики, якщо тільки група серверів не перебуває в активному режимі та політика блокування вже порушена подією, після чого транзакція блокується, і подальші дії не виконуються.

Приклад: SecureSphere виявляє сигнатуру атаки SQL-ін’єкції (подія безпеки), яка порушує політику. Створюється порушення, створюється сповіщення, яке відображається у вікні сповіщень. Крім того, порушення відображається у вікні «Порушення».

Контрольний список моніторингу. Відстеження поточного стану корпоративної системи включає ряд стандартних завдань.

Робота з панеллю інструментів. Панель інструментів (рисунок 3.8) є

центральним монітором для всіх даних, згенерованих у SecureSphere. Він підсумовує різні типи даних, що відстежуються в центрі, і надає першу вказівку щодо атак, які відбуваються, системних подій та інших проблем, з якими може зіткнутися система. Дані відображаються майже в режимі реального часу (кожні кілька секунд).

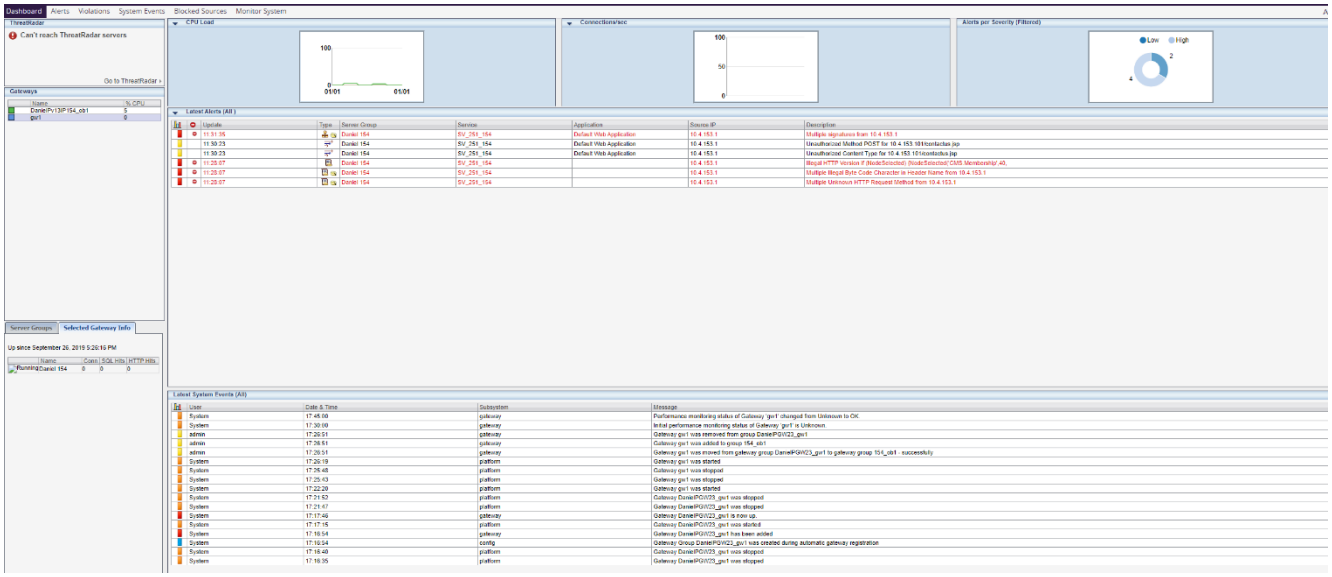

Рис. 3.8. Панель інструментів SecureSphere

Управління сповіщеннями. Сповіщення – це повідомлення про те, що порушення або група порушень (політики безпеки) відбулися в контрольованому трафіку. Одна атака безпеки може містити довгу послідовність порушень, кожне з яких створює окреме сповіщення і призводить до шторму попереджень. Щоб співвіднести оповіщення в логічну групу, запобігти штормів попереджень і допомогти в ідентифікації атак, SecureSphere об’єднує порушення на основі типу атаки, а потім відображає агреговані порушення як попередження у вікні попереджень.

Сповіщення є ключовим аспектом SecureSphere Data Lifecycle Management. Вони містять узагальнену інформацію, яка допомагає аналізувати події, що відбуваються у корпоративній мережі, і попереджає вас про підозрілу або проблемну діяльність.

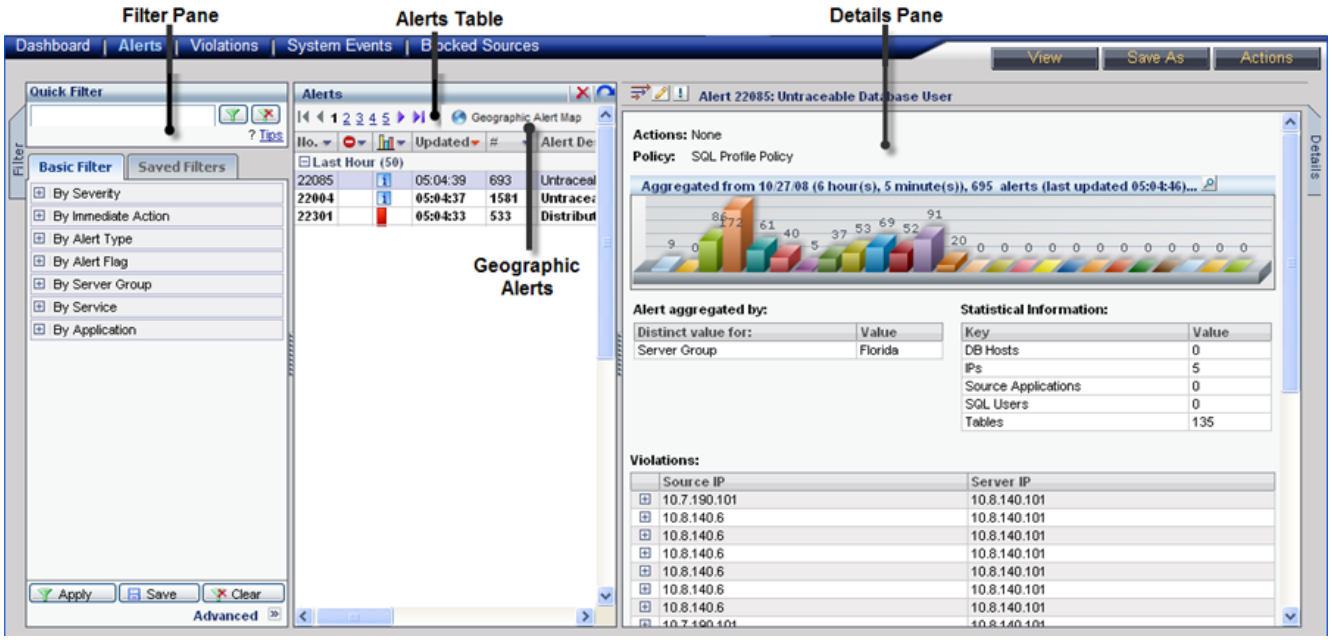

Рис. 3.9. Вікно сповіщень SecureSphere

Робочий процес роботи зі сповіщеннями включає наступні етапи:

1. сканування сповіщення з високим рівнем серйозності у вікні сповіщень;

2. перегляд описів сповіщень та інші деталі та спробувати зрозуміти, яку загрозу це становить;

3. необхідно спробувати визначити, чи є сповіщення хибно-позитивним;

4. якщо сповіщення здається важливим, клацніть сповіщення, щоб відобразити порушення, які спричинили сповіщення, на панелі деталей та проаналізуйте його вміст;

5. якщо ми вважаємо, що сповіщення заслуговує додаткового вивчення, ми можемо переглянути деталі порушення;

6. треба визначити, чи становлять загрозу порушення, що викликають попередження. Виконайте такі дії, як додавання винятку, зміна політики, яка створила сповіщення, щоб відповідати бажаній обробці подібних подій у майбутньому, або додавання поведінки до профілю SecureSphere;

7. крім того, ми можемо позначити сповіщення, щоб допомогти в управлінні. Ми можемо позначити сповіщення як «Важливі», «Підтверджені» або «Відхилені»;

8. нарешті, ми можемо видалити сповіщення, щоб видалити їх із вікна сповіщень. Сповіщення видаляються назавжди, хоча їхні вихідні порушення

завжди зберігаються в системі;

9. ми можемо переглядати Контрольний список інших елементів для перегляду.

Управління порушеннями. Порушення – це попередження про подію, яка порушує політику, визначену в SecureSphere. На відміну від сповіщень, порушення надають конкретну вказівку на подію, яка відбулася, включно з низкою деталей щодо порушеного трафіку. Це допоможе нам проаналізувати порушення та визначити, яку загрозу вони можуть становити для корпоративних даних.

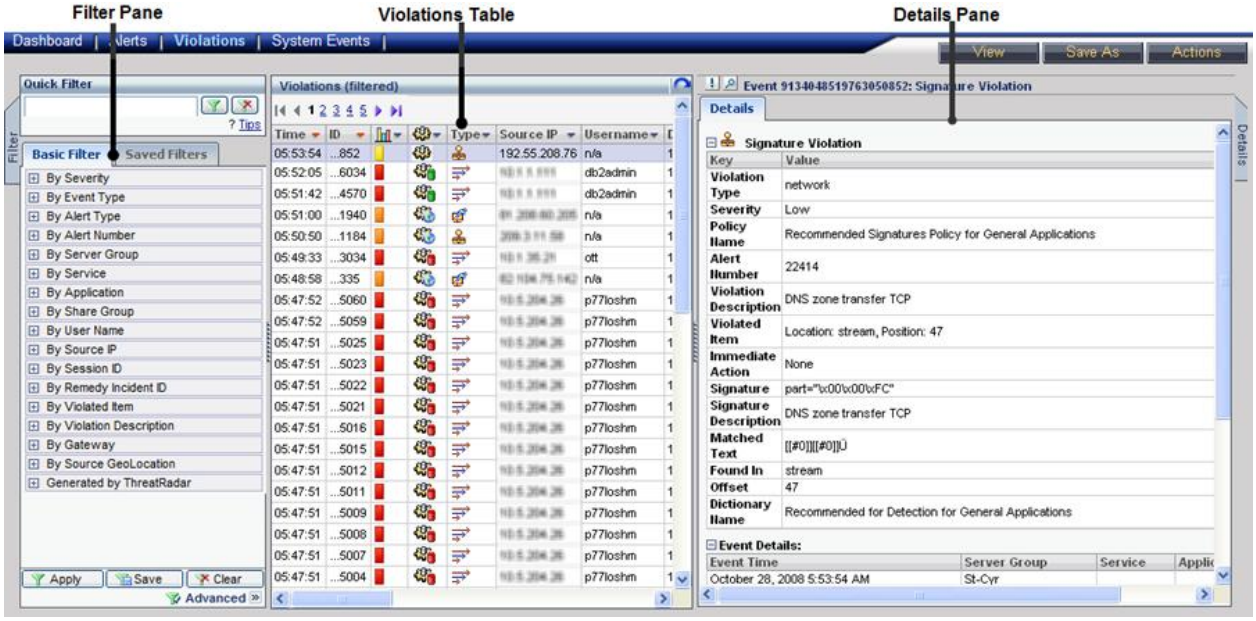

Рис. 3.10. Вікно управління порушеннями

Порушення містять відомості про подію безпеки. Зазвичай спочатку отримується сповіщення про цю подію на інформаційній панелі або у вікні сповіщень, а потім можна детальніше переглянути порушення, пов’язані з певним сповіщенням. Порушення надають детальну інформацію щодо атаки, щоб допомогти визначити обставини атаки, наприклад IP-адресу зловмисника, цільову службу та багато іншого. Потім ці дані можна використовувати, щоб визначити, чи становить порушення ризик для ваших даних, чи порушення не повинно було бути згенеровано, і потрібно точно налаштувати SecureSphere. Тонка настройка виконується шляхом редагування політики безпеки, додавання порушення як

винятку, додавання його до профілю або створення звіту про порушення та консультації з відповідними SME (наприклад, веб-майстрами).

Як приклад, припустімо, політика визначає, що втручання в файли *cookie* є порушенням, яке потребує подальших дій. Якщо SecureSphere виявляє, що файл *cookie* було змінено, він генерує повідомлення про порушення зі списком деталей порушення, таких як IP-адреса користувача, вміст файлу *cookie* або назва політики, яка порушується. Потім ми можемо проаналізувати ці деталі, щоб визначити, чи має місце атака, чи файл *cookie* може бути змінено в рамках його обробки, а політику, яка спричинила порушення, потрібно точно налаштувати.

Порушення мають різні форми. Вони можуть варіюватися від порушення сигнатури, коли SecureSphere визначила сигнатуру атаки, як-от ін’єкція SQL, до порушення файлів *cookie*, коли SecureSphere визначила, що файл cookie було ін’єктовано під час спроби перехопити сеанс, і багато іншого. Щойно сталося порушення, обставини порушення відображаються на панелі подробиць із вичерпною інформацією в текстовому форматі. Панель подробиць є контекстно-залежною та змінюється залежно від порушення, яке переглядається, і типу його вихідної події.

Керування заблокованими джерелами. Заблоковані джерела – це джерело повідомлень, які були поміщені на карантин через порушення політики безпеки та заблоковані у доступі до робочого середовища в результаті подальшої дії. Джерела можуть бути заблоковані за ідентифікатором сеансу, IP-адресою або користувачем і можуть бути заблоковані на певний період часу. Це дає адміністратору достатньо часу, щоб перевірити подію, щоб визначити, чи є вона загрозою, або вирішити, що це дійсний трафік, і розблокувати її.

Фільтрування сповіщень і порушень. SecureSphere містить широкий спектр елементів, які використовуються в повсякденних операціях. Фільтрування дозволяє легко шукати ці елементи. Наприклад, ви можете шукати звіт, який ви створили про виконання завдань, призначених у SecureSphere. Фільтрація дозволяє легко фільтрувати елементи за різноманітними категоріями.

Веб-сторінки помилок і сторінки відповідей у сповіщеннях. Сервери часто

стають мішенню зловмисних атак. Зазвичай ці атаки породжують порушення в SecureSphere і обробляються відповідно. Хоча якщо сервер не налаштовано належним чином, навіть якщо генерується порушення, можуть відображатися сторінки помилок, які випадково розкривають конфіденційну інформацію, таку як поточні операційні системи, встановлені пакети оновлень та інша системна інформація, яку хакери можуть використовувати для отримання доступу до системи. Крім того, конфіденційні дані можуть ненавмисно відображатися в повідомленнях про помилки під час повідомлення про загальні помилки. Наприклад, дані кредитної картки можуть відображатися користувачам системи, які інакше мали б бути замасковані.

Щоб відстежувати дані, які були піддані впливу зовнішніх елементів, випадково витікали або не були належним чином захищені, SecureSphere зберігає сторінку відповіді (джерело HTML) повністю, а потім дає змогу переглядати її на вкладці, розташованій із порушеннями.

Управління системними подіями. Системні події – це події, які відбулися в системі, наприклад, вхід в систему, або прямий результат системних змін, таких як оновлення підпису, зміни конфігурації, активація налаштувань, створення профілів, автоматичне оновлення профілю, запуск/зупинка сервера, діяльність з архівування, системні помилки або попередження (наприклад, перевищення визначених порогових значень) тощо. Системні події можуть мати наслідки для безпеки або відповідності, і тому їх потрібно відстежувати приблизно так само, як сповіщення та порушення.

3.3. Рекомендації щодо захисту корпоративних веб-додатків і API

У [17] зазначається, що зловмисники наполегливо намагаються використовувати вразливості веб-додатків, прагнучи отримати несанкціонований доступ до конфіденційних даних. Ось чому сприйняття та дотримання найкращих практик безпеки програм (AppSec) є важливими. Веб-додатки більш вразливі до атак порівняно з іншими IT-активами. Основна причина полягає в тому, що вони

легкодоступні та доступні через Інтернет. Використання онлайн-форм і API для маніпулювання введенням інформації машиною та користувачем є поширеною стратегією, яку використовують зловмисники для націлювання на веб-додатки.

API є унікальною поверхнею для атаки завдяки таким характеристикам [18]:

API обмінюються даними між системами. Кінцеві користувачі отримують доступ до веб-додатків через веб-браузер;

API використовують інший формат (зазвичай JSON) для транспортування даних. Веб-додатки приймають введені користувачем дані та візуалізують дані з серверної частини (за допомогою HTML, CSS і JavaScript);

API отримують прямий доступ до серверних систем, часто слугуючи посередником між сучасними веб-додатками та їхніми серверними базами даних і серверами;

успішні транзакції API передбачають законний доступ;

API легко не помітити, оскільки вони не видимі для кінцевих користувачів.

Порівняно з безпекою веб-додатків, безпека API вимагає значного бізнес-контексту, різних методів виявлення, глибшого контролю перевірки доступу та інтелектуального захисту від зловживань [18].

Методологія виявлення для безпеки API відрізняється від безпеки веб-додатків навіть категоріями вразливостей, що збігаються, як-от ін’єкційні атаки та ризики доступу. Наприклад, кожна операція API повинна перевіряти особу абонента та дозволи перед виконанням будь-якої роботи від імені абонента [18].

Рекомендації щодо захисту корпоративних веб-додатків і API:

Необхідно застосовувати практики безпечного кодування, які є основою безпеки веб-додатків. Розробники повинні дотримуватися методів безпечного кодування, щоб зменшити ризик уразливостей і помилок, якими можуть скористатися зловмисники. Прикладами безпечного кодування є:

перевірка введених даних: перевіряйте всі введені користувачем дані, щоб запобігти таким атакам, як впровадження SQL і міжсайтовий сценарій (XSS);

параметризовані запити: використовуйте параметризовані запити, щоб запобігти атакам SQL-ін’єкцій;

уникайте жорсткого кодування паролів і облікових даних: надійно зберігайте конфіденційну інформацію, таку як паролі та облікові дані;

використовуйте криптографічні бібліотеки та функції: реалізуйте безпечні алгоритми шифрування для захисту конфіденційних даних;

проводьте регулярні перевірки коду, щоб виявити й усунути потенційні проблеми безпеки.

Необхідно застосовувати протоколи SSL/TLS. Протоколи SSL/TLS необхідні для захисту веб-додатків. SSL і TLS гарантують, що зв'язок між клієнтом і сервером зашифрований, що запобігає зловмисникам від перехоплення та читання конфіденційних даних. Впровадження сертифікатів SSL/TLS гарантує, що всі дані, що передаються між клієнтом і сервером, зашифровані та безпечні.

Необхідно проводити регулярні оновлення та виправлення. Вразливості програмного забезпечення є поширеним способом зламати веб-додатки зловмисниками. Постачальники програмного забезпечення випускають виправлення та оновлення для усунення цих вразливостей, тому важливо постійно оновлювати програмне забезпечення.

Переконайтеся, що ви регулярно перевіряєте наявність оновлень і виправлень для всіх компонентів програмного забезпечення вашої веб-програми, включаючи веб-сервер, операційну систему, базу даних і будь-які сторонні бібліотеки та фреймворки, які ви використовуєте.

Необхідно використовувати брандмауер веб-додатків (WAF). WAF – це важливий інструмент безпеки, який допомагає захистити веб-додатки від різноманітних атак, зокрема впровадження SQL, міжсайтових сценаріїв (XSS) та інших поширених веб-атак.

Брандмауер веб-додатків (WAF) функціонує як фільтр трафіку HTTP, який захищає зв'язок між сервером і клієнтом. Запобігаючи проникненню зловмисних запитів у ваші бази даних і скомпрометуючи їх, він діє як важлива лінія захисту від кіберзагроз.

Необхідно використовувати надійні механізми автентифікації. Автентифікація – це процес підтвердження особи користувача. Слабкі механізми

автентифікації, такі як паролі, які легко вгадати або використати повторно, можуть зробити корпоративний веб-додаток вразливим до атак грубої сили, коли зловмисники використовують автоматичні інструменти для вгадування імен користувачів і паролів.

Щоб запобігти цим атакам, слід застосувати надійні механізми автентифікації, такі як двофакторна автентифікація (2FA) або багатофакторна автентифікація (MFA). Ці механізми вимагають від користувачів додаткової інформації, такої як код, надісланий на їхній телефон, або біометричний фактор, крім пароля.

Необхідно дотримуватися принципу найменших привілеїв. Принцип найменших привілеїв стверджує, що користувачі, процеси та системи повинні мати лише мінімальний доступ, необхідний для виконання своїх функцій. Цей принцип може допомогти зменшити вплив атак і обмежити шкоду, яку можуть завдати зловмисники.

Щоб застосувати принцип найменших привілеїв, слід надати користувачам і процесам мінімальні дозволи, необхідні для виконання їхніх завдань, і видалити будь-які непотрібні дозволи. Також необхідно обмежувати доступ до конфіденційних даних, таких як облікові дані для входу та фінансова інформація, лише для уповноваженого персоналу.

Необхідно використовувати перевірку введення. Перевірка введених даних – це процес перевірки введених користувачем даних, щоб переконатися, що вони дійсні та безпечні для використання. Неможливість перевірити введені користувачем дані може призвести до вразливості системи безпеки, наприклад впровадження SQL, міжсайтового сценарію (XSS) і впровадження команд.

Щоб запобігти цим вразливостям, слід запроваджувати перевірку введених даних для всіх введених користувачами даних, включаючи поля форми, рядки запитів і файли cookie. Також необхідно постійно удаляти введені користувачем дані, щоб видалити будь-які потенційно небезпечні символи чи код.

Необхідно керувати сеансом користувача. Керування сеансами користувачів – це критично важливий аспект безпеки веб-додатків, який передбачає керування

та контроль сеансів користувачів для запобігання несанкціонованому доступу. Викрадення сеансу та фіксація сеансу є двома поширеними атаками, які можуть скомпрометувати сеанси користувача.

Викрадення сеансу відбувається, коли зловмисник викрадає ідентифікатор сеансу користувача (унікальний ідентифікатор, призначений сеансу користувача), що дозволяє йому взяти під контроль сеанс і отримати доступ до конфіденційних даних або виконувати несанкціоновані дії. Фіксація сеансу відбувається, коли зловмисник встановлює ідентифікатор сеансу користувача на заздалегідь визначене значення, що дозволяє йому взяти під контроль сеанс, коли користувач входить.

Щоб запобігти захопленню сеансу та атакам на фіксацію, веб-додатки повинні запроваджувати належне керування сеансом користувача. Для керування сеансом користувача необхідно:

використовуйте надійні ідентифікатори сеансу. Ідентифікатор сеансу має бути досить довгим і складним, щоб зловмисникам було важко вгадати або застосувати грубу силу. Використання випадково згенерованих ідентифікаторів сеансу може допомогти запобігти захопленню сеансу та атакам фіксації;

застосовуйте повторне генерування ідентифікаторів сеансу. Ідентифікатори сеансу слід генерувати повторно після входу користувача або виконання будь-яких конфіденційних дій. Це гарантує, що ідентифікатор сеансу часто змінюється, що ускладнює зловмисникам захоплення або фіксацію сеансу;

встановлюйте час закінчення сеансу. Сеанси повинні мати час закінчення, після якого користувач автоматично виходить із системи. Це допомагає запобігти використанню зловмисниками ідентифікатора сеансу, який був активним протягом тривалого часу;

запроваджуйте двофакторну автентифікацію. Впровадження двофакторної автентифікації може додати додатковий рівень безпеки для сеансів користувачів, ускладнюючи зловмисникам захоплення або фіксацію сеансу;

слідкуйте за активністю користувача. Регулярний моніторинг активності користувача може допомогти виявити будь-яку незвичайну поведінку, яка може

свідчити про викрадення сеансу або атаку фіксації. Будь-яка підозріла діяльність має бути негайно розслідувана та вжито відповідних заходів.

Необхідно обробляти та обліковувати помилки. Належна обробка помилок і ведення журналу є важливими для виявлення та усунення проблем безпеки у веб-додатках. Помилки та винятки можуть надати зловмисникам цінну інформацію про вразливі місця програми, тому вкрай важливо обробляти помилки та належним чином реєструвати їх. Впровадження належної обробки помилок і журналювання може допомогти виявити й усунути потенційні проблеми безпеки до того, як вони стануть серйозними.

Необхідно проводити безпечне завантаження файлів. Завантаження файлів може становити значну загрозу безпеці, якщо з ними поводитися неправильно. Зловмисники можуть завантажувати шкідливі файли, які можуть поставити під загрозу безпеку всієї програми. Застосуйте безпечні механізми завантаження файлів, щоб забезпечити можливість завантаження лише авторизованих файлів і запобігти зловмисникам завантажувати шкідливі файли.

Отже, безпека веб-додатків є критично важливим аспектом захисту конфіденційних даних і забезпечення загальної функціональності додатків. Зі збільшенням кількості кіберзагроз важливо застосовувати найкращі методи безпеки веб-додатків, щоб запобігти несанкціонованому доступу та витоку даних.

Приділяючи належну увагу ми можемо значно покращити безпеку веб-додатків та зменшити ризик витоку даних та інших кіберзагроз. Важливо пам’ятати, що безпека веб-додатків – це безперервний процес, який вимагає регулярних оновлень і моніторингу, щоб забезпечити постійний захист конфіденційних даних. Зробивши безпеку веб-додатків головним пріоритетом, ми можемо надати своїм користувачам безпечний і захищений досвід роботи в Інтернеті та захистити свою організацію від потенційної фінансової та репутаційної шкоди.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення кібербезпеки веб-додатків організації. Вразливості веб-додатків – це недоліки безпеки, які зловмисники використовують для маніпулювання вихідним кодом, отримання несанкціонованого доступу, викрадення даних або порушення функціональності додатка. Список OWASP Top 10 визначає найбільш критичні ризики для безпеки веб-додатків.Проведено аналіз існуючих методів та засобів забезпечення безпеки веб-додатків та API. Захист веб-додатків і API розширює можливості WAF до чотирьох основних функцій: WAF; розподілений захист від відмови в обслуговуванні (DDoS); управління ботом; захист API.

Досліджено підходи до забезпечення безпеки веб-додатків та API. Брандмауери веб-додатків (Web Application Firewall, WAF) є критично важливим захистом для веб-сайтів, мобільних додатків і API. Вони відстежують, фільтрують і блокують пакети даних до та з веб-додатків, захищаючи їх від загроз. WAF розроблено (навчено) для виявлення та захисту від небезпечних недоліків безпеки, які найчастіше зустрічаються в веб-трафіку. Це робить їх необхідними для онлайн-бізнесу, як-от роздрібна торгівля, банки, охорона здоров’я та соціальні мережі, яким необхідно захищати конфіденційні дані від несанкціонованого доступу. WAF можна розгортати як мережеві, хостові або хмарні рішення, забезпечуючи видимість даних додатків на прикладному рівні HTTP.

Проаналізано існуючі рішення для захисту корпоративних веб-додатків і API. Брандмауери веб-додатків (WAF) можуть відстежувати, фільтрувати та блокувати підозрілий або небажаний трафік HTTP до та з веб-служби чи додатка. Він спеціально аналізує трафік між Інтернетом і веб-додатком. Використовуючи модель OSI, рішення WAF забезпечуватимуть захист на прикладному рівні (також відомий як рівень 7). У той час як проксі-сервери можуть захистити ідентичність кінцевої точки користувача за допомогою посередника, WAF працює інакше. Вони діють як зворотні проксі-сервери, захищаючи сервер від впливу та вимагаючи від

користувачів навігації WAF перед доступом до сервера чи додатка.

Розглянуто варіанти побудови системи захисту системи захисту веб-додатків та API на базі Imperva WAF. Шлюз SecureSphere можна розгорнути або як вбудований, коли трафік проходить через нього, або як шлюз, що перевіряє, де трафік не проходить через шлюз, а копіюється та направляєтться до нього для аналізу.

Розглянуто порядок реалізації функцій моніторингу рішенням Imperva WAF. Моніторинг є ключовим етапом життєвого циклу керування даними програми SecureSphere (Imperva WAF). SecureSphere оснащено зручним монітором, який чітко відображає згенеровану інформацію в центральному місці. Інформація в реальному часі, яка генерується, включає системні події, сповіщення, порушення, заблоковані джерела, стан шлюзу, системні попередження та інформацію про архівування.

Розроблено рекомендації фахівцям з кібербезпеки щодо застосування методів та засобів захисту веб-додатків та API. Безпека веб-додатків є критично важливим аспектом захисту конфіденційних даних і забезпечення загальної функціональності додатків. Зі збільшенням кількості кіберзагроз важливо застосовувати найкращі методи безпеки веб-додатків, щоб запобігти несанкціонованому доступу та витоку даних.

Отже, приділяючи належну увагу ми можемо значно покращити безпеку веб-додатків та зменшити ризик витоку даних та інших кіберзагроз. Важливо пам’ятати, що безпека веб-додатків – це безперервний процес, який вимагає регулярних оновлень і моніторингу, щоб забезпечити постійний захист конфіденційних даних. Зробивши безпеку веб-додатків головним пріоритетом, ми можемо надати своїм користувачам безпечний і захищений досвід роботи в Інтернеті та захистити свою організацію від потенційної фінансової та репутаційної шкоди.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2024 Imperva Bad Bot Report. URL: https://www.imperva.com/resources/resource-library/reports/2024-bad-bot-report/

2. Kinza Yasar. Web application firewall (WAF). TechTarget. URL: https://www.techtarget.com/searchsecurity/definition/Web-application-firewall-WAF

3. What is a WAF? Cisco. URL: https://www.cisco.com/site/us/en/learn/topics/security/what-is-web-application-firewall-waf.html

4. What Is WAF. Imperva. URL: https://www.imperva.com/learn/application-security/what-is-web-application-firewall-waf/

5. Imperva. Web Application Firewall User Guide. v15.2. URL: https://docs.imperva.com/bundle/v15.2-waf-user-guide/page/70414.htm

6. Anton Lohvynenko. 8 Web Application Security Best Practices: Fortifying Your Product for Sustainable Growth. Security Web Dev, Updated on Nov 25, 2024. URL: https://mobidev.biz/blog/best-practices-to-secure-web-applications-from-vulnerabilities

7. What Is Web Application Security? The Cloud Native Experts, April 17, 2024. URL: https://www.aquasec.com/cloud-native-academy/application-security/web-application-security/

8. Web Application Security. Imperva. URL: https://www.imperva.com/learn/application-security/web-application-security/

9. How to Secure Web Applications: Best Practices and Strategies. Stfalcon Team, 24.04.2023. URL: https://stfalcon.com/en/blog/post/building-secure-web-applications-best-practices-and-strategies

10. What is Web Application Security? Everything you Need to Know. CyberTalents. URL: https://cybertalents.com/blog/web-application-security

11. Saurabh Barot. Web Application Security Guide. Aglowid, 22 August 2024. URL: https://aglowiditsolutions.com/blog/web-application-security-guide/

12. Caitlin Harris, Laura Iannini. The Top 11 Web Application Firewalls. Expert

Insights. Last updated on Nov 14, 2024. URL: https://expertinsights.com/insights/the-top-web-application-firewalls/

13. Cloud WAF Service. Radware. URL: https://www.radware.com/products/cloud-waf-service/

14. Radware Cloud WAF Service. URL: https://roi4cio.com/catalog/product/radware-cloud-waf-service

15. Security Automations for AWS WAF. Implementation Guide. URL: https://docs.aws.amazon.com/solutions/latest/security-automations-for-aws-waf/architecture-overview.html

16. Imperva. WAF Administration Guide. v15.2. URL: https://docs.imperva.com/bundle/v15.2-waf-administration-guide/page/9284.htm

17. How to Secure Your Web Application from Vulnerabilities: Best Practices to Follow. ZeroThreat. Updated Date: Sep 11, 2024. https://zerothreat.ai/blog/best-practices-for-secure-web-app-development

18. The CISO's Guide to API Security. Ebook. Cloudflare. URL: https://cf-assets.www.cloudflare.com/slt3lc6tev37/6VKdAmxsP0FiN5ICN1dpRP/72c75712cf8e1d1239f5de450770f175/The_CISO_Guide_to_API_Security_-_eBook.pdf?_ga=2.17838905.1878513775.1686768047-

19. Imperva 10 Things Every Web Application Firewall Should Provide. White Paper. Thales Trusted Cyber Technologies. URL: https://www.thalestct.com/wp-content/uploads/2024/04/imperva-10-things-every-WAF-should-provide-wp-tct-3-29-24.pdf

20. Imperva Cloud Web Application Firewall. Datasheet, Imperva. URL: https://www.imperva.com/resources/datasheets/Cloud-Web-Application-Firewall_DATASHEET_2024.pdf

21. Imperva Web Application Firewall (WAF) Gateway. Product Brief. Thales Trusted Cyber Technologies. URL: file:///C:/Users/User/Downloads/imperva-waf-gateway-pb-tct-3-28-24.en.uk.pdf

22. КУБРАК Олена Сергіївна, Технологія захисту корпоративних веб-додатків і API на базі Imperva Web Application Firewall. Всеукраїнська наукова

конференція «Актуальні проблеми кібербезпеки». Державний університет інформаційно-комунікаційних технологій. 25 жовтня 2024. Тези доповідей. С. 149-153. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)