ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ЗХИСТУ ВЕБ-ДОДАТКІВ ЗА ДОПОМОГОЮ FORTIWEB»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Венгерівський В.В.
(прізвище та ініціали)
Керівник Гахов С.О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ 8
……...

ВСТУП ……..…… 9

1 **АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ** 12

1.1 Роль та місце веб-додатків в сучасному інформаційному просторі ……. 12
1.2 Аналіз підходів до захисту веб-додатку організації ……..... 20
1.3 Аналіз існуючих рішень із захисту веб-додатків організації ……..…..... 25

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ В FORTIWEB** ……..……... 30

2.1 Призначення та основні функції брандмауера веб-додатків FortiWeb ……. 30
2.2 Архітектура рішення FortiWeb, призначення основних компонентів …….. 31
2.3 Призначення та застосування основних наборів правил брандмауера веб-додатків ……. 41

3 **РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВЕБ-ДОДАТКІВ ЗА ДОПОМОГОЮ FORTIWEB** 57

3.1 Порядок застосування рішення брандмауера веб-додатків на Fortiweb ……. 57
3.2 Рекомендації щодо налаштування, порядок роботи з Fortiweb …….. 63
3.3 Рекомендації щодо застосування методів та засобів захисту веб-додатків організації ……..…… 71

ВИСНОВКИ ……. 75

ПЕРЕЛІК ПОСИЛАНЬ 78

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 79

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CRS – Core Rule Sets

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

OWASP – Open Web Application Security Project

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Сьогодні сучасні організації широко використовують можливості хмарних платформ для розміщення в них своїх веб-додатків. Веб-додатки піддаються кібератакам зловмисників для досягнення ними різних злочинних цілей, що ще більш загострює проблему забезпечення безпеки інформаційних ресурсів організацій.

Використання незахищених веб-додатків в рази збільшує ризики несанкціонованого доступу до корпоративних ресурсів і порушення працездатності веб-сайтів, що веде до репутаційних, а також, фінансових втрат організацій. Застосування технології Web Application Firewall на сьогоднішній день є найбільш гнучким і точним інструментом для всебічного захисту від веб-загроз.

Вищесказане визначає актуальність теми даної бакалаврської роботи, основний зміст якої становлять дослідження методів та засобів захисту веб-додатків організації на прикладі FortiWeb.

Об'єкт дослідження – захист веб-додатків організації при застосуванні хмарних платформ.

Предмет дослідження – методи та засоби захисту веб-додатків організації в FortiWeb.

Мета роботи – розробити рекомендації щодо захисту веб-додатків організації при застосуванні хмарних платформ.

Наукові завдання:

дослідити сутність проблеми захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати підходи до захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати існуючі рішення із захисту веб-додатків організації при застосуванні хмарних платформ;

проаналізувати методи та засоби захисту веб-додатків організації в FortiWeb;

розкрити порядок захисту веб-додатків організації при застосуванні хмарних

платформ.

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

Практичне значення одержаних результатів: розроблено рекомендації фахівцям з кібербезпеки щодо захисту веб-додатків організації при застосуванні хмарних платформ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ

1.1. Роль та місце веб-додатків в сучасному інформаційному просторі

Для багатьох компаній останні два роки були пов’язані з переходом на віддалену роботу в хмарних корпоративних системах, і командам безпеки додатків довелося адаптуватися до змін у використанні та зростаючої кількості викликів. Дивлячись на це ми можемо зрозуміти що веб-додатки грають важливу роль в сучасному інформаційному просторі і відіграють різні функції та мають своє місце в цьому контексті. Ось кілька ролей та місць, які веб-додатки займають в сучасному інформаційному просторі:

1. Веб-сайти: Веб-сайти є основними елементами веб-простору і надають інформацію, продукти або послуги користувачам. Вони можуть бути різних типів, включаючи сайти компаній, магазини, блоги, новинні портали, освітні ресурси та інші. Веб-сайти надають доступ до інформації та функцій через веб-браузери.

2. Веб-портали: Веб-портали є централізованими місцями, які надають широкий спектр інформації, послуг та функцій користувачам. Вони можуть включати такі елементи, як електронна пошта, календарі, соціальні мережі, форуми, функції співпраці та інші. Веб-портали забезпечують зручний спосіб організації та доступу до різних сервісів та функцій.

3. Веб-додатки для електронної комерції: Веб-додатки для електронної комерції дозволяють користувачам здійснювати покупки товарів та послуг в Інтернеті. Ці додатки надають зручний спосіб перегляду товарів, замовлення, оплати та доставки, що дозволяє підприємствам залучати клієнтів та здійснювати ефективну торгівлю в Інтернеті.

4. Соціальні мережі: Соціальні мережі є популярними веб-додатками, які дозволяють користувачам створювати профілі, спілкуватися, ділитися вмістом та встановлювати контакти з іншими користувачами. Соціальні мережі забезпечують платформу для обміну інформацією, створення спільнот та взаємодії між

користувачами.

5. Освітні та навчальні платформи: Веб-додатки для освіти та навчання надають можливості для дистанційного навчання, електронних курсів, вебінарів та інших форматів освітньої діяльності. Ці додатки дозволяють студентам та викладачам спілкуватися, обмінюватися матеріалами та брати участь у навчальних процесах з будь-якого місця, де є доступ до Інтернету.

6. Веб-додатки для управління проектами та співпраці: Ці додатки дозволяють командам працювати разом, спільно управляти проектами, ділитися документами та іншими матеріалами, обговорювати задачі та виконувати спільні завдання. Вони полегшують співпрацю, збільшують продуктивність та організовують робочі процеси.

7. Веб-додатки для банківських та фінансових послуг: Багато банків та фінансових установ надають веб-додатки для забезпечення доступу до рахунків, переказів коштів, оплати рахунків та інших банківських послуг через Інтернет. Ці додатки забезпечують зручний та безпечний спосіб взаємодії з банківськими послугами.

Отже дивлячись на все вище перераховане ми можемо зрозуміти, що веб-додатки стали невід'ємною частиною сучасного інформаційного простору і відіграють різноманітні ролі в різних сферах життя. Вони дозволяють нам здійснювати операції, спілкуватися, навчатися та працювати в Інтернеті, забезпечуючи зручну та ефективну взаємодію з інформацією та іншими користувачами.

1.2. Аналіз загроз при використанні веб-додатків

Згідно зі звітом Verizon Data Breach Investigations Report за 2020 рік, уразливості веб-додатків були причиною 43% витоків даних у 2019 році. Дивно, але згідно з дослідженням Enterprise Strategy Group, 79% організацій навмисно розмістили вразливий код у виробництві, водночас вважаючи рівень безпеки своїх програм вищим, ніж 7 із 10.

З огляду на те, що середня вартість витоку даних становить 3,86 мільйона доларів США , безпека додатків — це, звичайно, те, що компанії можуть ігнорувати. Цифри зростають — зросли на 12% за останні п’ять років.

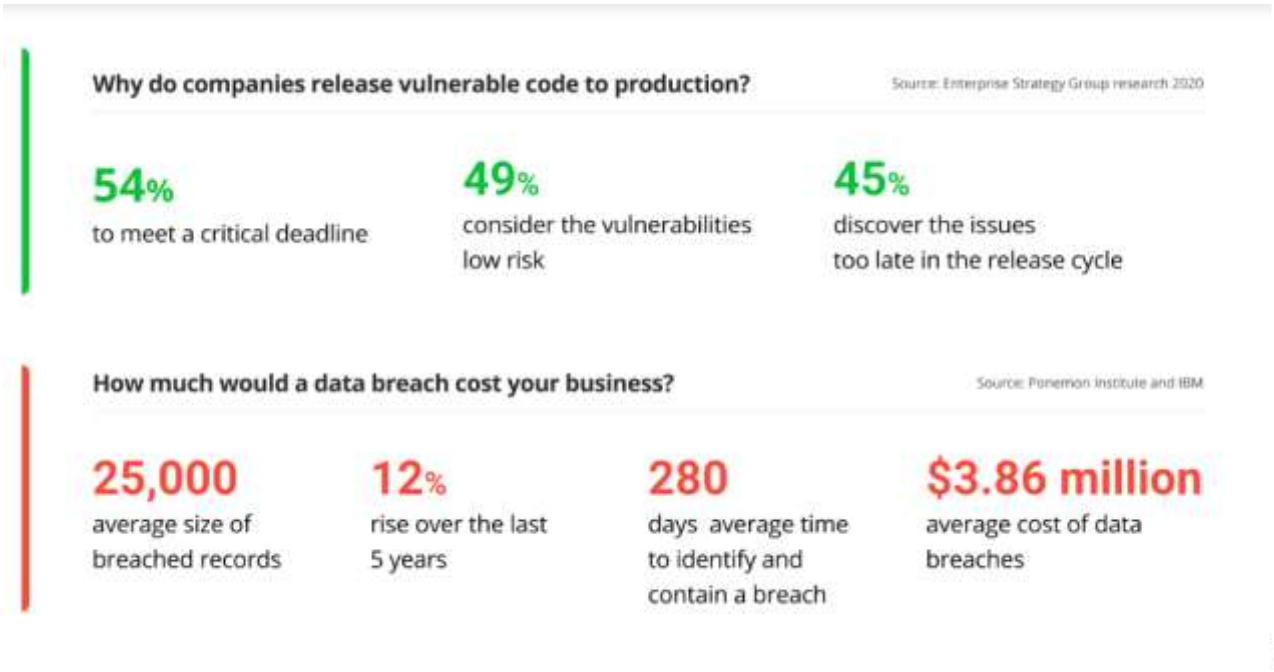

Рис. 1.1. звіт Verizon Data Breach Investigations Report за 2020 рік[2]

Порівняно з іншими IT-активами, веб-додатки особливо вразливі до атак, оскільки вони піддаються впливу Інтернету. Багато векторів атак на веб-програми зосереджені на маніпулюванні введеннями користувачів через веб-форми та машинними введеннями через API.

Уразливості веб-додатків — це слабкі місця в безпеці, які дозволяють суб’єктам загрози маніпулювати вихідним кодом, отримувати несанкціонований доступ, викрадати дані або іншим чином втручатися в нормальну роботу програми.

У документі OWASP Top 10 перелічено найбільш критичні ризики для безпеки веб-додатків. Отже розглянемо кілька загальновідомих векторів атак:

1. SQL-ін’єкція — відбувається, коли зловмисники використовують шкідливий код SQL для маніпулювання серверними базами даних. Результат може включати несанкціонований перелік даних, видалення (видалення) таблиць і неавторизований адміністративний доступ.

2. Міжсайтовий сценарій (XSS) — атака, націлена на користувачів

програми. Його можна використовувати для доступу до облікових записів користувачів, впровадження троянських програм або зміни вмісту сторінки, щоб ввести користувачів в оману або зіпсувати веб-сайт. Інший, більш небезпечний варіант — збережений XSS, коли шкідливий код постійно впроваджується в додаток. Відображений XSS — це коли шкідливі сценарії відображаються з програми в браузер користувача.

3. Віддалене включення файлів (RFI) — віддалене введення файлів на сервер веб-додатків. Це може призвести до виконання зловмисного сценарію та коду в програмах, зламу веб-сервера та крадіжки даних.

4. Міжсайтова підробка запитів (CSRF) — атака, яка може призвести до небажаних переказів коштів, зміни пароля або крадіжки даних. Зловмисник використовує відкритий сеанс користувача, змушуючи браузер користувача несвідомо виконувати дії на сайті, на якому користувач увійшов.

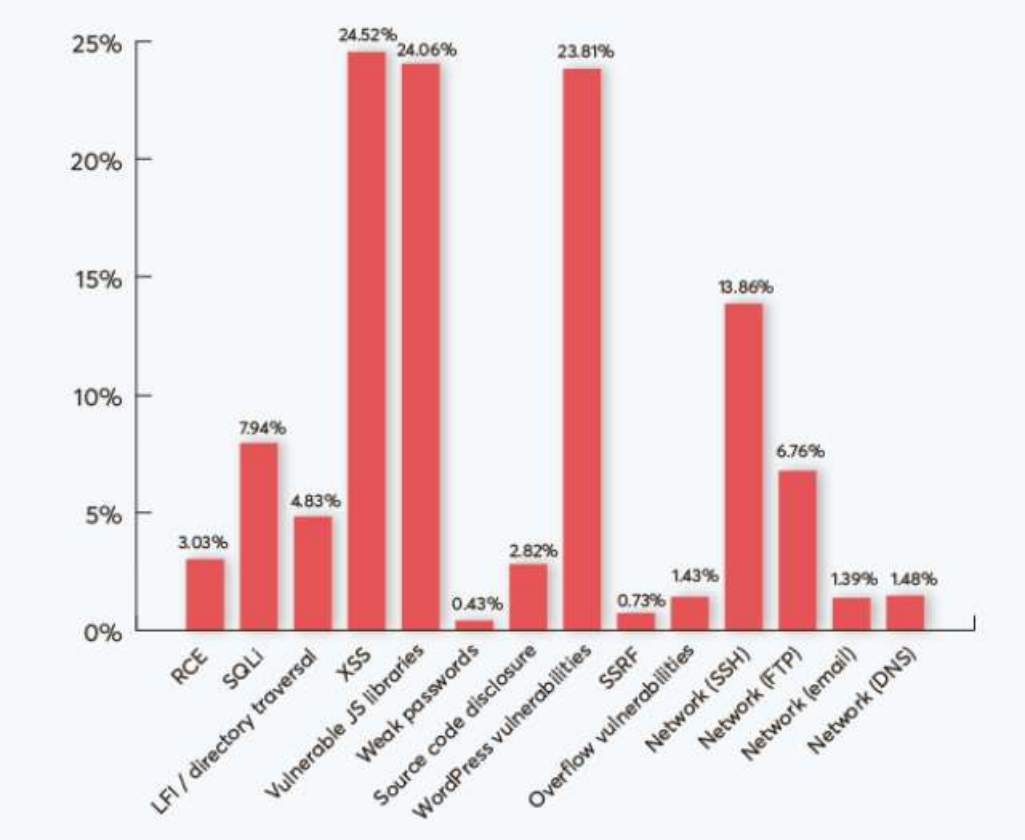

Рис. 1.2. Аналіз вразливостей високого рівня серйозності[8]

Дезінфекція вхідних і вихідних даних додатків, а також впровадження методів безпечного кодування можуть захистити додатки від більшості вразливостей. Однак цього недостатньо. Веб-програми знаходяться в стадії постійної розробки, і тестування безпеки має бути включено до кожного етапу життєвого циклу розробки, щоб визначити та виправити вразливий код на ранніх стадіях.

Крім того, більшість веб-додатків використовують сторонні компоненти з відкритим вихідним кодом, які самі по собі можуть бути вразливими та потребують постійного сканування.

Щоб отримати інформацію про безпеку веб-додатків, зазвичай існує два основних підходи. Їх називають статичне та динамічне тестування безпеки. Вони не виключають одне одного, а повинні доповнювати одне одного.

Ось кілька технологій, які можна використовувати для захисту веб-програм від уразливостей, а також для реагування на атаки, якщо вони трапляються.

Отже, перш за все: безпека в програмах залежить від безпеки в самому проекті. Але коли всі процеси ідеальні — що далі?

Щоб отримати інформацію про безпеку веб-додатків, зазвичай існує два основних підходи. Ми говоримо про статичне та динамічне тестування безпеки. Вони не виключають одне одного, а повинні доповнювати одне одного.

Ось кілька технологій, які можна використовувати для захисту веб-програм від уразливостей, а також для реагування на атаки, якщо вони трапляються.

SAST

Рішення Static Application Security Testing (SAST) сканують ваш вихідний код на наявність вразливостей і ризиків для безпеки. Багато веб-додатків інтегрують сканування коду на кількох етапах розробки — головним чином під час введення нового коду в кодову базу та під час збирання.

SAST зазвичай базується на правилах, і результати сканування зазвичай містять хибні спрацьовування, тому вам потрібно ретельно проаналізувати та відфільтрувати результати, щоб виявити справжні проблеми безпеки.

DAST

Динамічне тестування безпеки додатків (DAST) передбачає тестування розгорнутого або запущеного коду для виявлення вразливостей. Його можна виконувати як вручну, так і автоматично, за допомогою спеціальних інструментів.

Ручне тестування зосереджено на роботі з API програми за допомогою таких інструментів, як Burp suite, Fiddler, Postman. Інструменти автоматизації DAST надсилають велику кількість запитів до коду програми, включаючи несподівані та шкідливі вхідні дані, шукаючи вразливості. Він аналізує результати та визначає слабкі місця безпеки.

Тестування на проникнення – це техніка безпеки, яка поєднує інструменти динамічного сканування та досвід людської безпеки для виявлення прогалин у безпеці веб-додатку.

Пентестери діють як справжні загрозливі особи — використовують вразливості, отримують несанкціонований доступ, викрадають дані та порушують роботу служб. Однак вони роблять це за контрактом із власником веб-додатку в узгодженому обсязі та без завдання реальної шкоди організації.

Порівняно з SAST і DAST цей метод є більш складним для виконання, але він може виявити додаткові ризики, які автоматизовані інструменти можуть пропустити.

XDR

Рішення eXtended detection and response (XDR) — це платформи безпеки нового покоління, які надають командам безпеки єдиний інтерфейс, який дозволяє їм виявляти загрози та реагувати на них, де б вони не були в IT-середовищі.

XDR збирає дані безпеки з усіх рівнів стеку безпеки, включаючи веб-додатки, мережі, приватні та публічні хмари та кінцеві точки. Він застосовує розширену аналітику та автоматизацію для аналізу, сортування та виявлення як відомих, так і невідомих загроз. Найважливіше те, що він безпосередньо інтегрується з інструментами безпеки та може автоматично реагувати на загрози в режимі реального часу.

Найкращі методи безпеки веб-додатків у 2023 році

Ось декілька практичних порад, якими можна скористатися для підвищення

безпеки веб-програм.

Аутентифікація та контроль доступу

Хоча це може здатися очевидним, багато веб-додатків не реалізують базові заходи контролю доступу. Переконайтеся, що ви дотримуєтесь цих принципів:

Використовуйте надійні паролі — використовуйте безпечне відновлення пароля, установіть розумну політику терміну дії та ротації паролів і, бажано, використовуйте багатофакторну автентифікацію;

Примусова повторна автентифікація під час доступу до конфіденційних можливостей або виконання транзакцій;

Використовуйте принцип найменших привілеїв (POLP) і надайте кожному користувачеві лише ті привілеї, які йому необхідні для виконання своєї ролі в системі;

Використовуйте SSL і шифрування та переконайтеся, що паролі та облікові дані завжди зашифровані, як у стані спокою, так і під час передачі;

Відстежуйте облікові записи користувачів і блокуйте користувачів або вимагайте зміни пароля, якщо ви виявите підозрілу активність;

Уникайте неправильних конфігурацій безпеки

Яку б CMS або структуру веб-розробки ви не використовували, є багато можливостей для неправильної конфігурації. Слідкуйте за такими проблемами:

Завжди встановлюйте надійні паролі адміністратора та змінюйте імена користувачів за умовчанням;

Захистіть файли та каталоги з конфігурацією або конфіденційним вмістом;

Не залишайте порти відкритими, якщо вони не потрібні без потреби;

Регулярно оновлюйте до останньої стабільної версії всі програмні бібліотеки, плагіни та саму структуру;

Регулярно перевіряйте всі свої пакети на вразливі місця;

Слідкуйте за вразливими місцями безпеки та оновленнями, які впливають на ваше програмне забезпечення та інфраструктуру;

Використовуйте захищений зв'язок і мережеві протоколи;

Переконайтеся, що цифрові сертифікати актуальні;

Використання бібліотек і компонентів із відкритим кодом у розробці програмного забезпечення є майже повсюдним: приблизно 99% програм мають принаймні один компонент із відкритим кодом, згідно зі Звітом про безпеку та аналіз ризиків із відкритим кодом за 2020 рік.

У деяких галузях, як-от роздрібна торгівля, охорона здоров'я та освіта, протягом 2020 року спостерігалося експоненційне зростання доходів, головним чином через поведінку споживачів і зміни в соціальній взаємодії під час COVID. Оскільки ці галузі використовували більше відкритого коду у своїх програмах, вони мали найбільшу кількість вразливостей і вразливостей із високим ризиком. Визначення того, які компоненти з відкритим вихідним кодом є безпечними, повинно бути першочерговим завданням для будь-якої групи безпеки програми.

Управління винятками

Винятки — це аспект безпеки веб-додатків, який зазвичай забувають. Часто спостерігаються винятки або помилки, які відображають користувачеві трасування довгого стеку — ця інформація надзвичайно цінна для зловмисників. Ви ніколи не повинні показувати користувачеві нічого, крім повідомлення про помилку, яке пояснює, що пішло не так, і що вони можуть зробити, щоб вирішити цю проблему.

Переконайтеся, що ви плануєте свою веб-програму як для «щасливого», так і «нещасливого» сценаріїв кожної операції користувача. Передбачте всі можливі помилки та обробляйте їх зі значущими винятками. Це запобіжить зловмисникам використовувати крайні випадки, щоб спричинити неочікувану поведінку.

Обережно поводьтеся з контейнерами

Слідуючи останнім тенденціям веб-розробки , багато програм працюють у контейнерах за допомогою Docker. Контейнери можуть створити серйозні проблеми з безпекою, якщо ними не керувати належним чином. Зверніть увагу на такі правила безпеки:

Надійні зображення – під час створення контейнера завжди використовуйте надійні базові зображення та скануйте зображення на наявність вразливостей (навіть ваші власні) перед їх використанням;

Використовуйте секрети – дуже погано зберігати облікові дані або іншу

конфіденційну інформацію безпосередньо в образі контейнера, оскільки вона буде відкрито доступна в будь-якому контейнері, створеному з цього зображення. Натомість використовуйте механізм секретів у Docker або Kubernetes для зберігання конфіденційної інформації.

Ніколи не надавайте кореневий доступ — контейнер, який має кореневий доступ у системі, також надасть кореневий доступ зловмиснику, якщо контейнер скомпрометовано. Завжди визначте користувача у своїх зображеннях і уникайте використання таких опцій, як «привілейований контейнер» у Kubernetes.

Сегментація мережі гарантуйте, що контейнери можуть отримувати доступ до інших систем, лише якщо їм це дійсно необхідно. Запускайте контейнери в захищеній підмережі та уникайте їх доступу до Інтернету, якщо це не є абсолютно необхідним.

Гарантія якості та тестування

Тестування безпеки є важливим для безпеки веб-додатків. Дотримуйтесь цих практичних порад:

Використовуйте статичне та динамічне сканування — скануйте вихідний код на наявність вразливостей під час розробки за допомогою статичного тестування безпеки додатків (SAST) і в робочому стані за допомогою динамічного тестування безпеки додатків (DAST).

Використовуйте тестування на проникнення. Ви можете використовувати легке тестування на проникнення як сервісне рішення (PTaaS) або для великомасштабних додатків, а також періодичне повномасштабне тестування на проникнення сертифікованим етичним хакером.

Використовуйте CI/CD – кожного разу, коли ви оновлюєте свою програму, запускайте свій код через процес автоматизованого тестування та розгортайте його автоматично, щоб переконатися, що ви не створюєте ризиків для безпеки через проблеми з установкою.

Візьміть до уваги відповідність – більшість організацій у світі підпадають під дію регламенту Європейського Союзу GDPR. Програми, які обробляють дані кредитної картки, підпадають під дію стандарту PCI/DSS. Перевірте, чи існують

додаткові стандарти відповідності або правила, які впливають на вашу програму, і застосуйте необхідні заходи.

У більшості випадків наш звичайний процес розгортання в CI/CD включає наступні 5 кроків:

1. Сканувати вихідний код на наявність порушень стилю коду.
2. Сканувати бібліотеки сторонніх розробників на наявність проблем із безпекою.
3. Запустіть модульний тест.
4. Підготуйте новий вихідний код для розгортання.
5. Створіть і розгорніть нові образи Docker у вибраному середовищі. Усі конфіденційні облікові дані, необхідні для запуску веб-програми, зберігаються в безпечному сховищі CI/CD.

Розгортання буде зупинено, якщо будь-який із цих кроків не вдасться. Це гарантує стабільні оновлення та стабільне безпечне середовище.

1.3. Аналіз існуючих рішень із захисту веб-додатків

Незважаючи на те, що рішення Web Application Firewall в світі вже встигли набрати достатню популярність, і такі компанії як Amazon надають захищенні сервіси на базі продуктів даного класу, на ринку України для багатьох використання WAF ще в новинку. Сильними гравцями на ринку є Fortinet з рішення FortiWeb і Imperva з SecureSphere Web Firewall Application.

FortiWeb – це WAF, який захищає розміщення веб-додатків від атак, спрямованих на відомі та невідомі експлойти

Використовуючи багаторівневі та кореляційні методи виявлення, FortiWeb захищає програми від відомих вразливостей та загроз нульового дня. Служба безпеки веб-додатків від FortiGuard Labs використовує інформацію, засновану на останніх вразливостях додатків, ботах, підозрілих URL-адресах та шаблонах даних, а також спеціалізованих евристичних механізмах виявлення для забезпечення веб додатків. FortiWeb також пропонує функцію машинного навчання, яка дозволяє автоматично виявляти шкідливий веб-трафік. Окрім виявлення відомих атак, ця функція може виявити потенційно невідомі атаки нульового дня для забезпечення захисту веб-серверів у режимі реального часу.

Порівнюємо 7 WAF лідерів магічного квадранта Gartner за характеристиками

Рішень WAF на ринку досить багато і на будь-який смак. Щоб вибрати продукт, який ідеально підходитиме саме для вашої компанії, слід звернути увагу на функціонал – у різних вендорів сервіси трохи відрізняються. Нижче наведено огляд лідерів ринку WAF програмних рішень, пристроїв та хмарних служб, визначений Magic Quadrant for Web Application Firewall у 2018 року. Більш детальну інформацію про них можна отримати в порівняльній таблиці ROI4CIO, де можна порівняти 28 WAF за 32 характеристиками. А в нашому огляді ми спробуємо висвітлити основні властивості і переваги 7 найпопулярніших WAF продуктів. І все це в алфавітному порядку.

Akamai Kona Web Application Firewall

Kona Web Application Firewall від Akamai (дешевша урізана версія Kona Site

Defender) підходить клієнтам, яким потрібна хмарна служба WAF, особливо коли клієнти вже використовують Akamai в якості CDN. Порівняно дорогий продукт, але розроблений компанією (Кембридж, 7500 чоловік), команда розробників якої займається виключно питаннями безпеки веб-додатків. Akamai надає керований SOC, який може відслідковувати інциденти. Виробник застосовує автоматичну аналітику та сортування всього трафіку, який він обробляє, щоб клієнти налаштовували свої підписи та збирали інформацію про загрози для створення нових засобів захисту. Оскільки WAF Akamai доступний лише в якості хмарної служби, для організацій, яким просто не подобаються рішення для хмарної безпеки, або коли оцінки потенційних клієнтів визначають, що дотримання та нормативні обмеження обмежують його використання, Akamai не підійде.

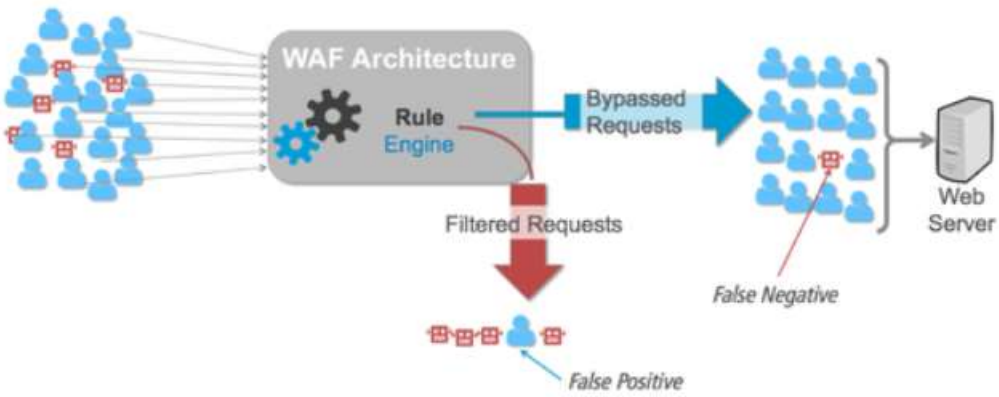

Рис. 1.3. Архітектура Akamai Kona WAF[5]

Barracuda Web Application Firewall

Barracuda Web Application Firewall – ефективна комплексна система, призначена для забезпечення безпеки веб-додатків та сайтів для підприємств середнього бізнесу. Barracuda WAF дає потужну відсіч зловмисникам, які експлуатують слабкі місця у протоколах та додатках для розкрадання даних, порушення роботи сервісів або дефейсу веб-сайтів. Лінія WAF випускається вендором для фізичних або віртуальних пристроїв, а також доступна на платформах Microsoft Azure, AWS та Google Cloud Platform (GCP). З випуском пристрою WAF 1060 Barracuda тепер підтримує пропускну здатність до 10 Гбіт/с.

Barracuda залишається одним з найкращих WAF у Microsoft Azure.

Barracuda Cloud WAF як послуга включає захист від DDoS без додаткової оплати. Технічна підтримка здійснюється на хорошому рівні та отримує високу оцінку клієнтів.

Інтерфейс користувача оцінюється клієнтами як user-friendly. І тут хороша новина для російськомовних – рішення від Barracuda WAF має не лише англійський, а й російський інтерфейс.

Продукт від Barracuda здатний забезпечити захист від наступних атак: впровадження SQL коду, міжсайтовий скриптинг (XSS), підробка сесій та переповнення буфера, запобігає розкраданню інформації за рахунок моніторингу всіх вихідних даних на наявність витоків будь-яких секретних відомостей (номерів рахунків у банках, особистої користувальницької інформації, паролів та іншого).

Системний адміністратор зможе вчасно детектувати атаки DoS- і DDoS завдяки спеціальній функції, що контролює швидкість передачі даних. Потужний вбудований антивірус дозволяє перевірити будь-які дані та файли, що імпортуються в систему, на предмет різного шкідливого коду.

Barracuda Web Application Firewall повністю сумісний з більшістю поширених ідентифікаційних систем (Active Directory, eDirectory), які підтримують LDAP RADIUS. Крім того, тут є функція двофакторної ідентифікації: система підтримує аутентифікатори користувача та токени (RSASecureID), щоб гарантувати надійний захист аутентифікації клієнтів.

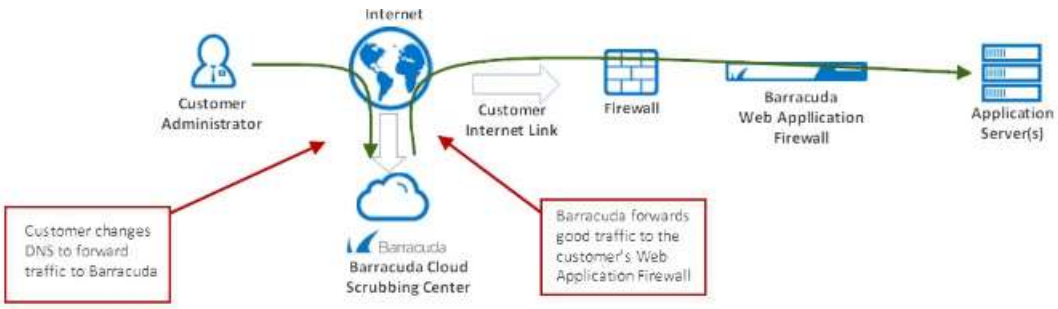

Рис. 1.4. Архітектура Barracuda WAF[6]

Cloudflare WAF

Cloudflare web application firewall (WAF) корпоративного класу в хмарі захищає веб-застосунки від поширених вразливостей, таких як атаки з використанням SQL-ін'єкцій, міжсайтовий скриптинг та міжсайтові підробки, без змін в існуючій інфраструктурі. Порівняно недорогі плани обслуговування є зручними для невеликих компаній. Є дорожчі індивідуальні плани для великих компаній – Enterprise. Модель самообслуговування, що використовується компанією, дозволяє клієнтам швидко та легко налаштовувати конфігурації за допомогою майстрів. Тому клієнти високо оцінюють простоту обслуговування.

Cloudflare (Сан-Франциско, 700 співробітників) розробляє захисту від DDoS та пропозиції CDN. Cloudflare — провайдер із пропускною здатністю 15 Тбіт/с та 152 дата-центрами по всьому світу. Ця інфраструктура не тільки підтримує високу продуктивність додатків, але й забезпечує найсучасніші засоби захисту.

Нещодавнє додавання Cloudflare Workers дозволяє замовникам розміщувати веб-програми в інфраструктурі Cloudflare, що має бути привабливим для невеликих організацій. Постачальник також надає доступну кнопку «Я під атакою». Це автоматично включає набір захистів та зручно для екстреного реагування.

Cloudflare пропонує WAF тільки як хмарний сервіс. Для організацій з обмеженнями на хмарні послуги та організацій, для яких потрібні локальні фізичні або віртуальні пристрої, продукт не підходить.

Рис. 1.5. Архітектура Cloudflare WAF [7]

Imperva SecureSphere Web Application Firewall

Imperva WAF рішення призначені для застосування у державному секторі, а також у великому та середньому бізнесі. SecureSphere може поставлятись як фізичні, так і віртуальні пристрої. Він також доступний як хмарний сервіс та хмарний сервіс WAF Incapsula на AWS і Microsoft Azure. Imperva (Редвуд-Шорс, Каліфорнія) також пропонує керовані набори правил AWS WAF.

Максимальна пропускна здатність старшої моделі, що підтримується, досягає 10 Гбіт/с. Крім HTTP/HTTPS, є підтримка веб-стандартів WebSockets, XMS і JSON. Продукти цікаві синхронним застосуванням кількох технологій кіберзахисту: контролем протоколів на аномальну поведінку, динамічним профільуванням, аналізом через сигнатури, відстеженням сесій. Для всіх продуктів Imperva надається якісна підтримка, оцінена клієнтами.

Брандмауер для веб-додатків компанії Imperva складається з двох основних модулів:

SecureSphere Web Application Firewall - захист веб-застосунків від кібератак;

ThreatRadar - репутаційна база даних (ThreatRadar дозволяє оперативно блокувати трафік, що йде від підозрілих джерел, ще до моменту здійснення будь-якого шкідливого впливу);

Imperva пропонує гнучке ліцензування для організацій, які використовують як локальні, так і хмарні програми. Це дозволяє виробнику орієнтуватися на ширше коло варіантів використання та організацій, а також краще керувати переходом від пристрою WAF до хмарної служби WAF.

Клієнти SecureSphere повідомляють, що консоль управління залишається складною при використанні більш просунутих можливостей, для розгортання часто потрібні професійні послуги для ефективного впровадження.

Для ефективного захисту застосовуються механізми на основі сигнатур безкоштовної open-source системи запобігання вторгненням Snort, а також власним SQL-сигнатурам, що генеруються дослідницьким центром ADC (Application Defense Center). З точки зору стійкості до відмов, тут є підтримка

кластеризації Active-Active і Active-Passive.

SecureSphere WAF оснащений невбудовуваним сніфером, прозорим проксі-сервером і зворотним проксі-сервером, має відмінну підтримку SSL. Так продукт забезпечує пасивне розшифрування SSL, підтримку сесій, встановлених на клієнтських сертифікатах, термінацію та детермінацію (тобто аналіз трафіку SSL без термінації). Важливо, що технологія містить апаратні модулі, що прискорюють обробку SSL.

Для формування еталонної моделі безпеки тут застосовано метод класифікації правил та застосування детальних сигнатур (з використанням правил міжмережевого екранування, створення сигнатур та обробки порушень протоколів). Для адаптації WAF до програми, що змінюється, реалізована можливість зміни профілю веб-додатків, створеного в режимі машинного навчання. Разом з тим є налаштування профілю веб-додатків у ручному режимі.

Реалізований у SecureSphere WAF генератор звітів, надає системним адміністраторам звіти відповідно до вимог стандартів ІБ. Також тут є можливість генерувати власні кастомізовані звіти (у тому числі і за розкладом) та експортувати до різних форматів.

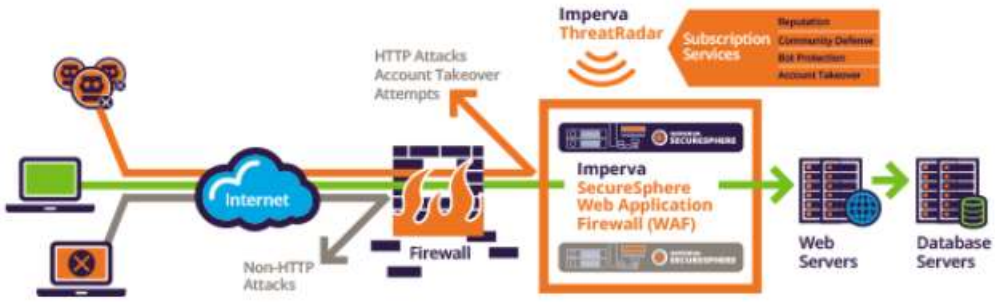

Рис. 1.6. Imperva SecureSphere WAF

На мою думка, що у майбутньому статистика кіберзлочинів перевищуватиме статистику злочинів поза мережею. І вже зараз нехтувати захистом від атак не варто, ці інвестиції окупаються цілком і повністю. Рішення WAF - маленька, але важлива цегла у вашій лінії оборони від зловмисників.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВЕБ-ДОДАТКІВ ОРГАНІЗАЦІЇ В FORTIWEB

2.1. Призначення та основні функції брандмауера веб-додатків

Fortiweb являє собою міжмережевий екран рівня веб-додатків (WAF), який реалізує захист від атак, спрямованих на експлуатацію відомих і невідомих вразливостей, і допомагає відповідати вимогам галузевих стандартів.

Завдяки використанню багаторівневої системи виявлення загроз на базі штучного інтелекту, а також методів кореляції подій Fortiweb забезпечує захист застосунків від відомих вразливостей і загроз нульового дня.

Захист веб-додатків від десяти найпоширеніших загроз за версією OWASP, зокрема від міжсайтингового скриптингу та впровадження SQL-коду.

Захист API від експлуатації зловмисниками, фільтрація на основні політики. Безшовна інтеграція безпеки API в процес розробки та пацплайн CI/CD.

Захист веб-сайтів, мобільних додатків і API від автоматизованих атак, тачно розділяючи хороших і поганих ботів, блокуючи останніх. Механізми протидії ботам надають інструменти контролю та візуалізації запитів без необхідності введення CAPTCHA або відповідей на запитання.

Fortiweb забезпечує багаторівневий захист веб-додатків від усього спектра загроз, включно з 10 найпоширенішими та найнебезпечнішими типами атак за версією OWASP. На першому рівні використовуються традиційні механізми для виявлення і блокування шкідливих запитів: сигнатури, IP репутації, валідація протоколу тощо. На другому рівні Fortiweb використовує механізм машинного навчання для виявлення аномалій, спираючись на генеровану Fortiweb математичну модель додатка, що захищається. Модель формується і оновлюється рішенням самостійно, виключаючи необхідність у ручному доналаштуванні правил фільтрації.

В умовах активної цифрової трансформації API інтерфейси стали ще більш

популярними. Вони є невід'ємною частиною інфраструктури мобільних додатків та інтеграції бізнес-систем. Доступність, поширеність і важливість виконуваних функцій робить API привабливою ціллю для зловмисників. Захист API веб-додатків є одним із ключових призначень FortiWeb. FortiWeb дає змогу імпортувати схему API веб-додатка (OpenAPI, XML або JSON) і автоматично сформувати позитивну модель безпеки для захисту від API експлойтів. Механізм валідації схеми API FortiWeb можна інтегрувати в конвеєр розроблення та доставлення застосунків (CI/CD) для автоматичної перегенерації позитивної моделі безпеки під час кожного оновлення API застосунку

FortiWeb захищає веб-ресурси, API, додатки, користувачів і чутливу інформацію від автоматизованих ботів, автозбирачів даних із сайтів та інших інструментальних атак. Поєднуючи механізми машинного навчання, політики порогових значень для запитів, пасток для ботів, біометричний аналіз, FortiWeb ефективно блокує атаки ботів, зводячи до нуля негативний вплив на легітимних користувачів. Складаючи профіль користувача, FortiWeb може відрізнити запити людини, бота і зловмисника, мінімізуючи необхідність використання CAPTCHA. Інструменти графічної аналітики FortiWeb дають змогу компаніям легко диференціювати атаки, хороших ботів і легітимних користувачів.

Машинне навчання покращує виявлення атак і збільшує операційну ефективність. Здатність FortiWeb виявляти поведінкові аномалії в запитах до конкретного додатка, що захищається, дає змогу блокувати раніше невідомі експлойти і запобігати атакам нульового дня, націленим на додаток. В операційному плані машинне навчання FortiWeb позбавляє вас трудомістких завдань, як-от усунення помилкових спрацьовувань або ручне налаштування правил WAF. FortiWeb постійно оновлює математичну модель запитів у міру розвитку вашого застосунку, тому немає необхідності вручну оновлювати правила під час кожному оновленні. FortiWeb дає вам змогу швидше випускати в реліз нові функції веб додатків, а також економить ресурси фахівців, підвищуючи операційну ефективність

Машинне навчання FortiWeb точно виявляє аномалії та визначає, які з них є

атаками. На відміну від наявних моделей виявлення, використовуваних іншими постачальниками WAF, які сприймають кожну аномалію, як загрозу, FortiWeb з високою точністю виключає хибно-позитивні спрацьовування і перехоплює типи атак, які недоступні аналогічним пристроям.

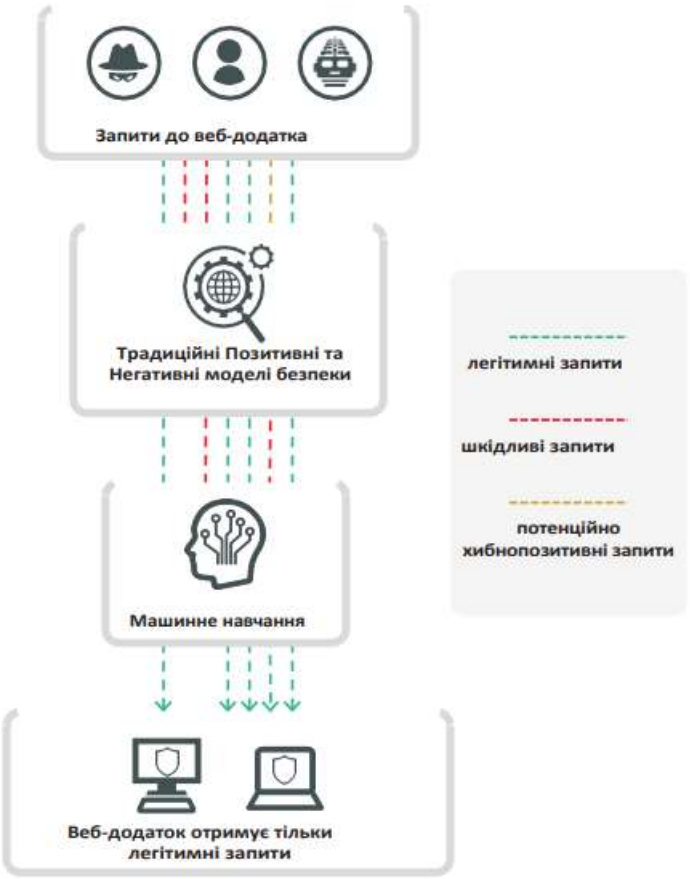

Рис. 2.1. Особливості захисту Fortiweb

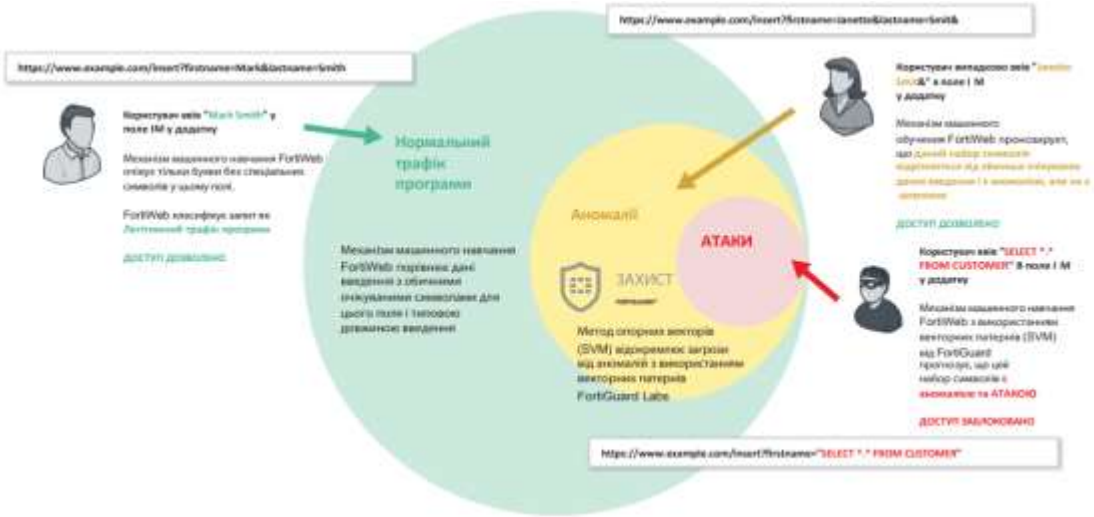

Рис. 2.2. Інтелектуальний механізм машинного навчання FortiWeb

2.2 Архітектура рішення FortiWeb, призначення основних компонентів

Тісна інтеграція з Fortinet Security Fabric і сканерами вразливостей сторонніх виробників У міру розвитку ландшафту загроз багато нових загроз вимагають комплексного підходу до захисту веб-додатків. Розвинені стійкі загрози, націлені на організації, можуть набувати різних форм порівняно з традиційними одновекторними атаками, і можуть обійти захист, який здійснюється тільки одним пристроєм. Інтеграція FortiWeb з FortiGate і FortiSandbox розширює основні можливості захисту WAF за допомогою синхронізації та обміну інформацією про загрози як у разі глибокого сканування підозрілих файлів, так і в разі поширення заражених внутрішніх джерел. FortiWeb забезпечує інтеграцію зі сканерами вразливостей від сторонніх виробників, включно з Acunetix, HP Weblnspect, IBM AppScan, Qualys, IBM QRadar і WhiteHat для формування віртуальних патчів. Уразливості, виявлені сканером, автоматично перетворюються на правила безпеки FortiWeb для захисту застосунку до того моменту, поки розробники не зможуть внести їх до коду застосунку.

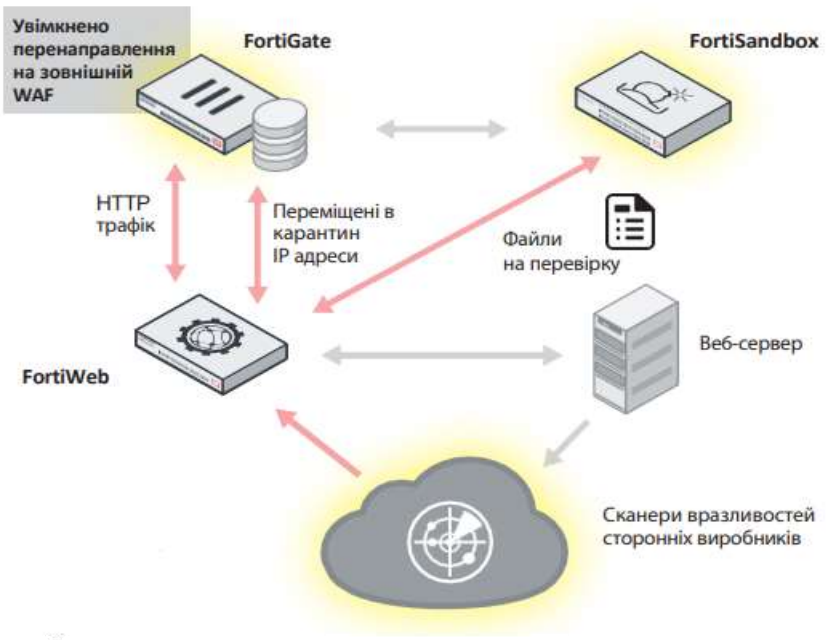

Рис. 2.3 Інтеграція з іншими елементами архітектури інформаційної безпеки Fortinet Security Fabric

Вирішення проблеми помилкових спрацьовувань Хибно-позитивні спрацьовування можуть мати вкрай руйнівні наслідки і часто призводять до того, що багато адміністраторів послаблюють правила безпеки міжмережевих екранів для веб-додатків до такої міри, що багато хто з них стає засобом моніторингу, а не надійною платформою для запобігання загрозам. Механізми штучного інтелекту FortiWeb унеможливлюють хибні спрацьовування без необхідності трудомісткого управління білими списками і тонкого налаштування політик. При забезпеченні практично 100% точності, дворівневі механізми, що навчаються, виявляють аномалії, а потім визначають, чи є вони атаками, на відміну від інших виробників, які блокують усі аномалії незалежно від їхньої суті. У поєднанні з іншими захисними механізмами FortiWeb практично виключає помилкові спрацьовування.

Звітність і розширена графічна аналітика FortiWeb містить набір інструментів графічної аналітики FortiView. Він візуалізує ключові елементи конфігурації, карту атаки, категоризує події безпеки відповідно до класифікації OWASP, технічні параметри клієнтських запитів. FortiView дає змогу в режимі реального часу виявляти джерела підозрілої активності та атак, агрегувати допоміжну інформацію про користувача та клієнтський пристрій.

Захист за допомогою FortiGuard Відзначені нагородами сервіси FortiGuard Labs від компанії Fortinet є основою FortiWeb під час забезпечення безпеки додатків. Служба репутації IP адрес FortiWeb захищає вас від відомих джерел атак, якот ботнети, спамери, анонімні проксі-сервери та джерела, помічені в поширенні шкідливого ПЗ. Для FortiWeb розроблено спеціалізовані сервіси FortiGuard: сигнатури прикладного рівня, моделі загроз машинного навчання, підозрілі шаблони URL, шкідливі боти, оновлення сканера вразливостей, модуль антивірусної фільтрації. Сервіс захисту облікових даних (Credential Stuffing Defense) перевіряє спроби входу відповідно до списку скомпрометованих облікових даних FortiGuard і може блокувати вхід із використанням вкрадених ідентифікаторів. Підписка на хмарний сервіс FortiSandbox Cloud дає змогу FortiWeb інтегруватися з хмарним сервісом-пісочницею від Fortinet для глибокого

аналізу поведінки підозрілих файлів.

Підтримка публічних і приватних хмар FortiWeb максимально гнучкий з точки зору підтримки інфраструктури публічних і приватних хмар. Віртуальні FortiWeb підтримують всі функції апаратної реалізації та доступні в середовищах віртуалізації VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Docker, AWS, Azure, Google Cloud, а також як сервіс WAF в AWS, Azure і Google Cloud.

Рис. 2.4. Інтерфейс FortiView для FortiWeb

Архітектура FortiWeb показано на рис.2.5.

FortiWeb -VM розгортається в таких середовищах:

VMware ESXi (див. ілюстрацію);

Microsoft Hyper-V;

Платформа хмарних обчислень OpenStack;

KVM;

Citrix XenServer;

Докер;

Відкрийте Xen;

FortiWeb -мережа VMтопологія.

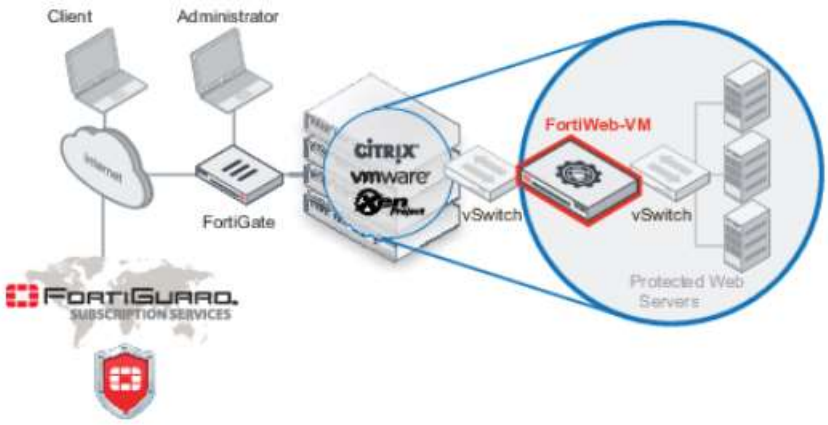

Рис. 2.5. Архітектура FortiWeb

1.3 Призначення та застосування основних наборів правил брандмауера веб додатків

FortiWeb є спеціалізованим брандмауером для веб-додатків, який надає рішення для захисту веб-додатків від різноманітних загроз, таких як SQL-ін'єкції, кросс-сайтові скриптові атаки (XSS), викрадення сесій, вразливості веб-додатків та багато інших.

Основні набори правил FortiWeb включають такі функції та застосування:

Правила фільтрації веб-трафіку: FortiWeb може використовувати правила для фільтрації HTTP-запитів та відповідей на основі різних параметрів, таких як URL, методи HTTP, заголовки, параметри запиту та багато іншого. Це дозволяє блокувати атаки, що базуються на певних вразливостях веб-додатків;

Правила виявлення вразливостей: FortiWeb має набір правил для виявлення вразливостей веб-додатків, таких як SQL-ін'єкції, XSS атаки, витік інформації та інші. Вони дозволяють ідентифікувати потенційно небезпечний трафік та блокувати атаки, спрямовані на ці вразливості;

Правила заборони доступу та авторизації: FortiWeb може використовувати правила для контролю доступу до веб-додатків, включаючи авторизацію користувачів, обмеження доступу до конкретних ресурсів та функцій, обробку сесій і багато іншого. Це допомагає запобігти несанкціонованому доступу до веб-додатків та зберегти конфіденційні дані;

Правила захисту від DDoS-атак: FortiWeb має функціонал для виявлення та захисту веб-додатків від атак типу Distributed Denial of Service (DDoS). Він може використовувати правила для розпізнавання підозрілого трафіку, а також встановлювати обмеження на кількість запитів або швидкість трафіку з одного джерела;

Правила моніторингу та журналювання: FortiWeb дозволяє налаштовувати правила для моніторингу активності веб-додатків та записування журналів подій. Це дозволяє виявляти та аналізувати аномалії, потенційні атаки та інші події, що можуть позначати наявність загроз;

Ці набори правил FortiWeb допомагають забезпечити безпеку веб-додатків, виявляти та блокувати атаки, контролювати доступ та захищати конфіденційні дані користувачів. Вони дозволяють адміністраторам мережі налаштовувати індивідуальні правила для веб-додатків залежно від їх потреб та загроз, з якими вони стикаються.

Конфігурація FortiWeb

Крок 1. Запит LDAP

Перейдіть до «Користувач» > «Віддалений сервер» > «Сервер LDAP» і створіть новий запис(Рис. 2.6.).

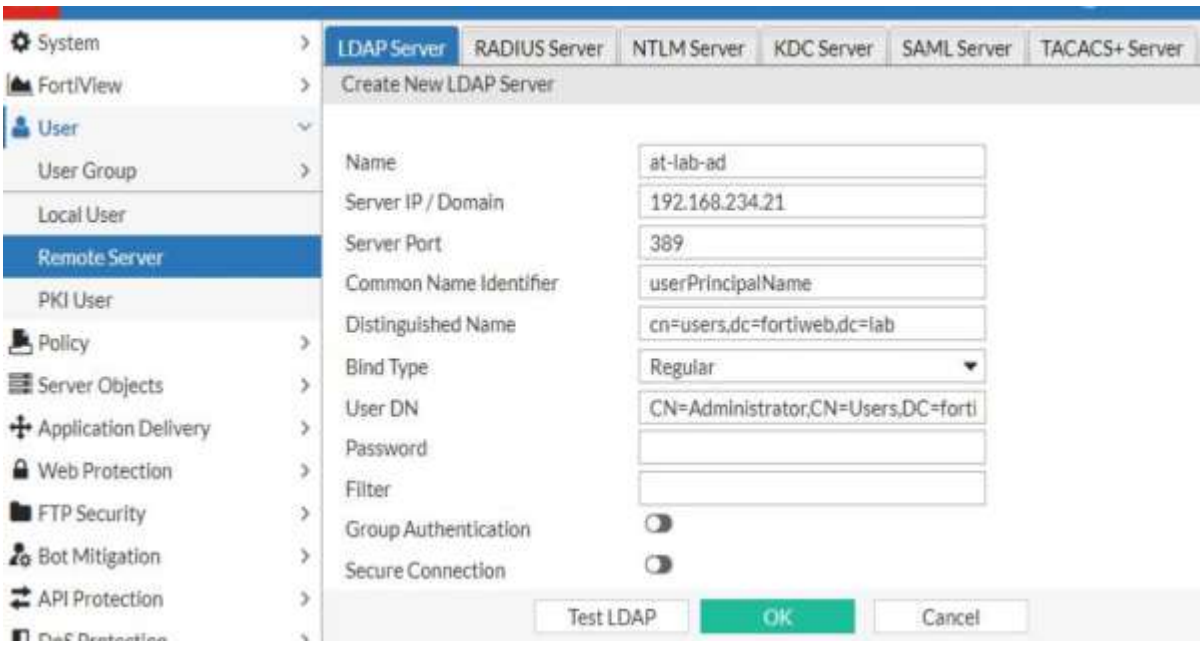

Рис. 2.6. Запит LDAP

У цьому прикладі користувачі входять, використовуючи свою повну адресу електронної пошти. Тому значення ідентифікатора загального імені є полем Active Directory userPrincipalName.

(Для інших програм або конфігурацій може знадобитися інша інформація для входу.)

Щоб отримати поле відмінного імені :

1. На контролері домену запустіть інструмент adsiedit.msc.
2. Натисніть Дія > Підключитися до .
3. Натисніть OK .
4. Перейдіть до папки CN=Users.
5. Виберіть користувача (наприклад, CN=Administrator), а потім виберіть його властивості.
6. Покрутіть униз до поля «Відмінна назва», щоб переглянути значення для використання у FortiWeb.

Щоб отримати додаткові відомості про створення запиту LDAP,

Крок 2. Пул серверів автентифікації

Перейдіть до пункту Доставка програми > Публікація сайту > Пул серверів автентифікації

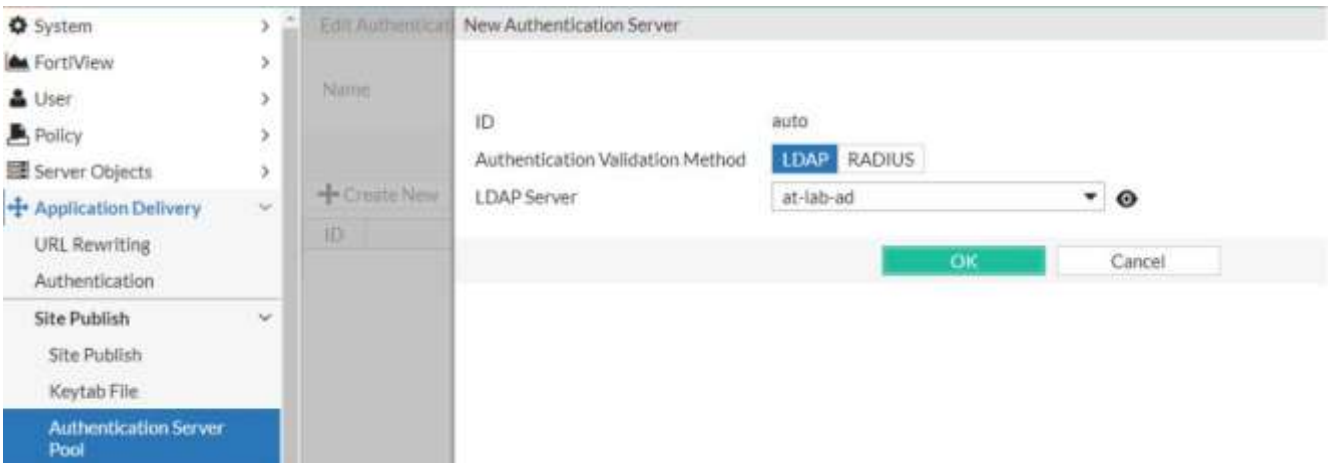

Рис. 2.7. Створення нового пулу серверів і додавання в пул сервер LDAP.

Крок 3. Правило публікації на сайті

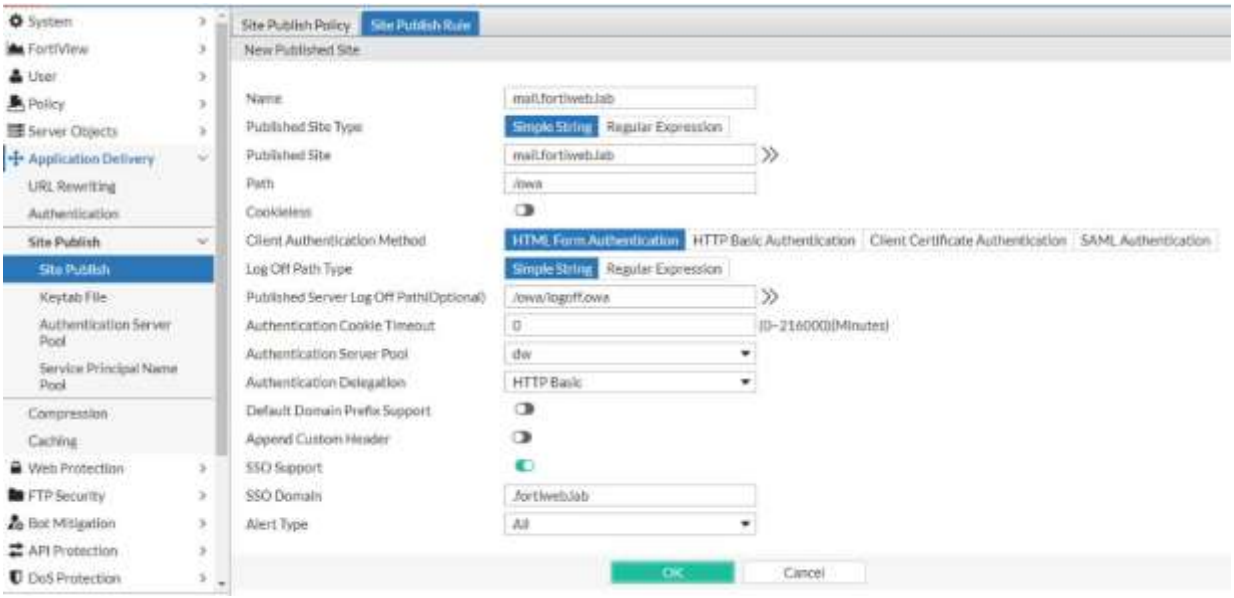

Рис. 2.8. Створення правила публікації на сайті

Ім’я – це унікальний ідентифікатор правила.

Опублікований сайт і шлях визначають URL-адресу, яку клієнт використовує для доступу до OWA. FortiWeb перехоплює запити на цю URL-адресу та змушує клієнтів пройти попередню автентифікацію.

Оскільки шлях для OWA починається з /owa, URL-адреса така:

HTTPS://mail.fortiweb.lab/owa

Published Server Log Off Path визначає шлях, який FortiWeb використовує для виходукористувача.ДляOWAце/owa/logoff.owa.

Примітка. Для Exchange 2016 CU1 і пізніших версій шлях виходу більше не підтримується корпорацією Майкрософт, через що FortiWeb не може розпізнати транзакцію виходу. Для Exchange 2016 CU1 доступне таке обхідне рішення:

Відредагуйте

"Exchange\V15\ClientAccess\Owa\prem\15.1.1034.26\scripts\microsoft.owa.core.models.js".

Додайте цей рядок.

$(document).ready(function(){ $('._ho2_2').click(function () { $('body > div:last-child ._abs_c div[role=menu] > div > div:last-child > button').on('click', function () { window.location.href= './logoff.owa' }) }) });

Зберегти та скинути

Без застосування цього обхідного шляху, наданого спільнотою, FortiWeb не зможе ідентифікувати запити на вихід із системи, а це означає, що термін дії файлу cookie сеансу закінчується, лише коли користувач закриває свій браузер і не використовує опцію «Відновити попередній сеанс» під час повторного відкриття браузера.

Метод автентифікації клієнта визначає, як FortiWeb пропонує клієнту ввести облікові дані автентифікації. Наприклад, за допомогою базової автентифікації HTTP або попередньо визначеної форми (показано праворуч).

Сервер LDAP — це конфігурація LDAP, яку ви створили раніше.

Делегування автентифікації визначає, чи надсилає FortiWeb облікові дані, які вводить клієнт, на внутрішній сервер.

Наприклад, виберіть «Без делегування», якщо веб-програма не має власної автентифікації або використовує автентифікацію на основі форми HTML. Виберіть базову автентифікацію HTTP, щоб використовувати авторизацію HTTP: заголовки з кодуванням Base64 для пересилання облікових даних клієнта до веб-програми.

Оскільки FortiWeb зберігає облікові дані протягом сеансу, він може пересилати облікові дані на інші сервери додатків, не вимагаючи від клієнта повторного введення пароля. Щоб увімкнути цю функцію, виберіть Підтримка SSO та вкажіть значення домену SSO.

Тип сповіщення визначає, які події входу FortiWeb записує до журналу подій (жодних, лише невдалих, лише успішних чи всіх).

Крок 4. Політика публікації сайту

Використовуйте політику публікації сайту, щоб додати правила публікації сайту до профілю веб-захисту. Політика публікації на сайті дозволяє додавати до політики кілька правил публікації на сайті.

Щоб створити нову політику, перейдіть до пункту Доставка програми > Публікація сайту > Політика публікації сайту. Створіть новий запис, введіть назву

політики та натисніть кнопку OK. Потім ви можете додати одне або кілька правил публікації сайту до політики.

Крок 5. Правило X-Forwarded-For

Оскільки режимом роботи є зворотний проксі, адресою джерела всіх з'єднань від FortiWeb до внутрішнього сервера є IP-адреса одного з інтерфейсів FortiWeb.

Щоб надати IP-адресу клієнта в журналі внутрішнього сервера, ви можете переслати IP-адресу клієнта в запиті в заголовку X-Forwarded-For:

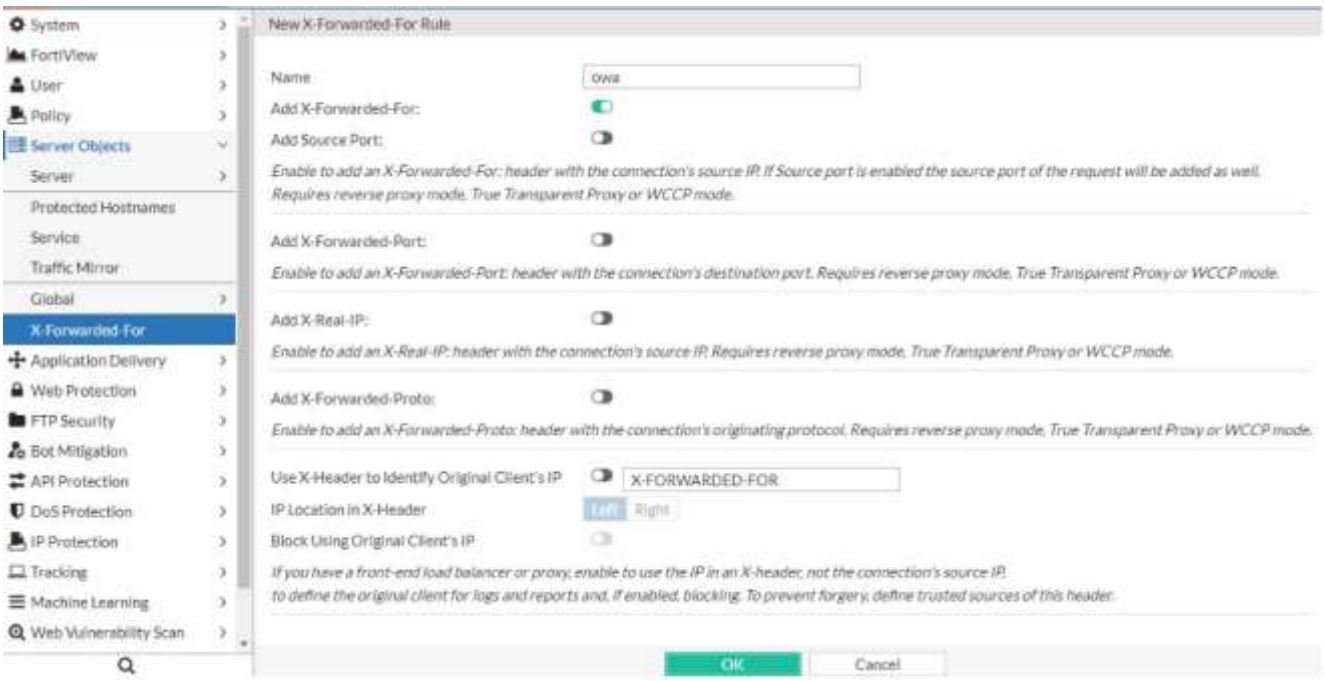

Рис. 2.9. Налаштування правила X-Forwarded-For

Перейдіть до об'єктів сервера > X-Forwarded-For > X-Forwarded-For і створіть новий запис. Введіть назву та виберіть Додати X-Forwarded-For .

(Ці налаштування також надають альтернативні методи включення цієї інформації в запити.)

Крок 6 - Профіль веб-захисту

Перейдіть до «Політика» > «Профіль веб-захисту» > «Вбудований профіль захисту».

Замість створення нового профілю ви можете клонувати попередньо визначений профіль для Exchange 2013, а потім налаштувати клонований профіль відповідно до свого середовища.

Введіть ім’я, увімкніть керування сеансом і виберіть створений раніше профіль X-Forwarded-For .

У нижній частині конфігурації профілю в розділі «Доставка програми» для «Публікація сайту» виберіть політику публікації на сайті, яку ви створили раніше.

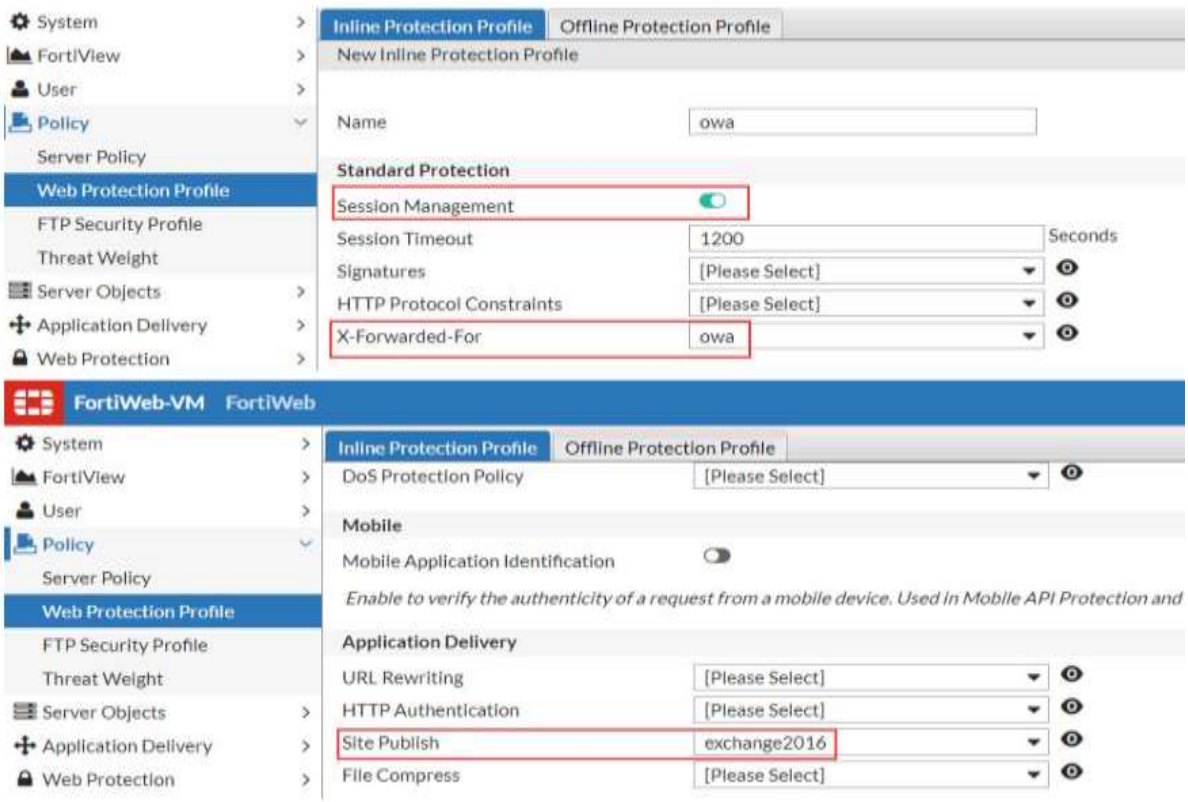

Рис. 2.10 Профіль веб-захисту

Крок 7 - Віртуальний сервер

Перейдіть до«Об’єкти сервера» > «Сервер» > «Віртуальний сервер» і створіть новий запис, який визначає IP-адресу, яку FortiWeb прослуховує для з’єднань з Інтернету.

Крок 8 - Пул серверів

Перейдіть до Об’єкти сервера > Сервер > Пул серверів. Створіть новий пул, який є пулом одного сервера (за замовчуванням). Потім додайте нового члена пулу, вказавши IP-адресу сервера, на якому працює опублікована програма.

Крок 9 - Сертифікати

Щоб завантажити сертифікати або створити запити на підписання сертифікатів, перейдіть до Система > Сертифікати > Локальні .

Якщо у вас є офіційний підписаний сертифікат, завантажте сертифікат центру підпису (CA). Залежно від ваших повноважень ви також завантажуєте проміжні ЦС.

Посібник з адміністрування FortiWeb містить детальну інформацію про завантаження сертифікатів. Наприклад, див. «Як розвантажити або перевірити HTTPS».

Крок 10 – Політика сервера

Перейдіть до «Політика» > «Політика сервера» > «Політика сервера» та створіть новий запис.

Виберіть об’єкти конфігурації, які ви створили раніше:

Віртуальний сервер;

Пул серверів;

Сертифікат;

Профіль веб-захисту (вбудований);

FortiWeb тепер прослуховує вказану IP-адресу та перехоплює з’єднання, призначені для URL-адреси, визначеної в правилі публікації сайту (у цьому прикладі HTTPS://mail.fortiweb.lab/owa). Клієнт повинен успішно пройти автентифікацію, перш ніж він зможе надсилати будь-які подальші запити на сервер додатків.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАХИСТУ ВЕБ-ДОДАТКІВ ЗА ДОПОМОГОЮ FORTIWEB

3.1 Порядок застосування рішення брандмауера веб-додатків на Fortiweb

У цій темі зібрані поради щодо точного налаштування та найкращі практичні вказівки, які допоможуть вам налаштувати пристрої FortiWeb для найбільш безпечної та надійної роботи. Хоча багато функцій є необов'язковими або гнучкими, тому їх можна використовувати багатьма способами, деякі методи загалом є гарною ідеєю, оскільки вони зменшують ускладнення, ризик або можливі проблеми.

FortiWeb розроблений для підвищення безпеки ваших веб-сайтів і веб-додатків, і після повного налаштування він може автоматично закривати діри, якими зазвичай користуються зловмисники для компрометації системи.

У цьому розділі наведено поради щодо подальшого підвищення безпеки.

Топологія

Щоб захистити ваші веб-сервери, установіть пристрій або пристрої FortiWeb між веб-серверами та брандмауером загального призначення, таким як FortiGate. FortiWeb доповнює, а не замінює брандмауери загального призначення. Прилади FortiWeb розроблено спеціально для боротьби із загрозами HTTP/HTTPS; Брандмауери загального призначення мають більше функцій для захисту на нижніх рівнях мережі.

Переконайтеся, що веб-трафік не може обійти пристрій FortiWeb у складному мережевому середовищі.

Визначте IP-адреси інших надійних балансувальників навантаження або веб-проксі, щоб запобігти підробці заголовків HTTP, таких як X-Forwarded-For:і X-Real-IP:

Вимкніть усі мережеві інтерфейси, які не повинні отримувати трафік.

Наприклад, якщо адміністративний доступ зазвичай здійснюється через порт1, Інтернет підключено до порту2, а веб-сервери підключено до порту3, ви повинні вимкнути («вивести») порт4. Це запобіжить зловмиснику з фізичним доступом

підключити кабель до порту 4 і таким чином отримати доступ, якщо конфігурація ненавмисно це дозволяє.

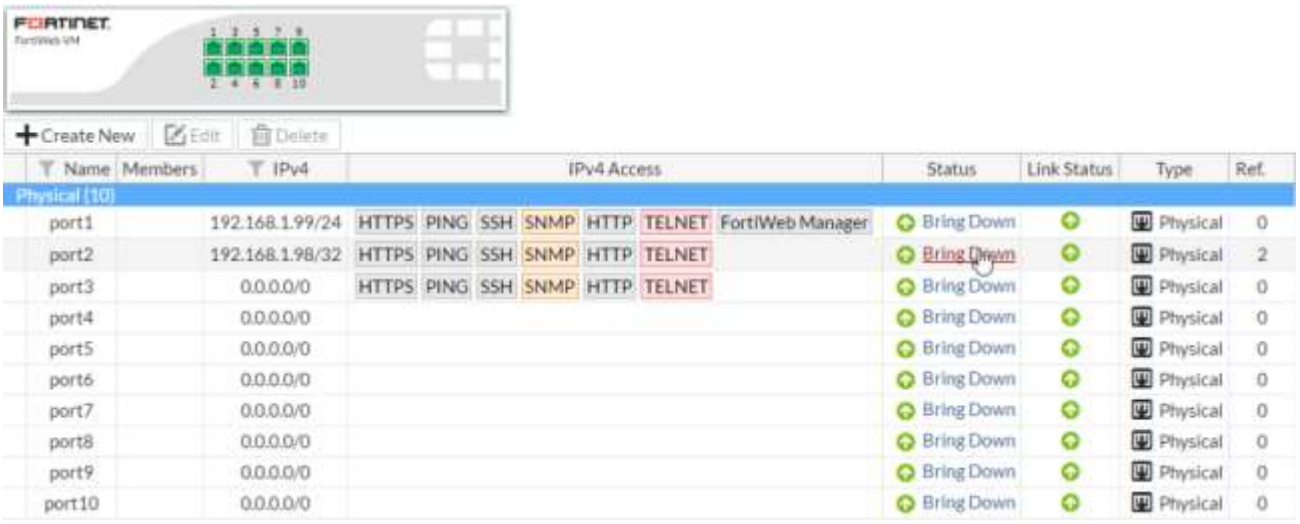

Рис. 3.1. Вимкнення порту 2 у Мережа > Інтерфейс

Доступ адміністратора

Якнайшвидше під час початкового налаштування FortiWeb дайте адміністратору за замовчуванням adminпароль. Цей обліковий запис суперадміністратора має найвищий можливий рівень дозволів, і доступ до нього має бути обмежено якомога меншою кількістю людей.

Регулярно змінюйте всі паролі адміністратора. Встановіть політику (наприклад, кожні 60 днів) і дотримуйтесь її. Ви можете натиснути піктограму «Змінити пароль» , щоб відкрити діалогове вікно пароля.

Замість того, щоб дозволяти адміністративний доступ до пристрою FortiWeb з будь-якого джерела, обмежте його довіреними внутрішніми хостами. (Записи IPv6 ::/0 ігноруватимуться, але вам слід налаштувати всі записи IPv4.) . На тих комп’ютерах, які ви призначили для керування, застосуйте суворі політики виправлення та безпеки. Завжди шифруйте паролем будь-яку резервну копію конфігурації FortiWeb , яку ви завантажуєте на ці комп’ютери, щоб пом’якшити інформацію, яку зловмисники можуть отримати від будь-якого потенційного зламу. Не використовуйте профіль доступу адміністратора за умовчанням для всіх нових адміністраторів. Створіть один або кілька профілів доступу з обмеженими дозволами відповідно до обов’язків нових облікових записів адміністратора.

За замовчуванням вхід адміністратора, який не використовується більше п’яти хвилин, закінчується. Ви можете змінити цей період на довший у Idle Timeout , але Fortinet не рекомендує цього. Залишений без нагляду веб-інтерфейс користувача або сеанс CLI може дозволити будь-кому, хто має фізичний доступ до

вашого комп’ютера, змінити налаштування FortiWeb . Невеликі тайм-аути простою зменшують цей ризик.

Паролі адміністратора мають містити принаймні 8 символів і містити як цифри, так і літери.

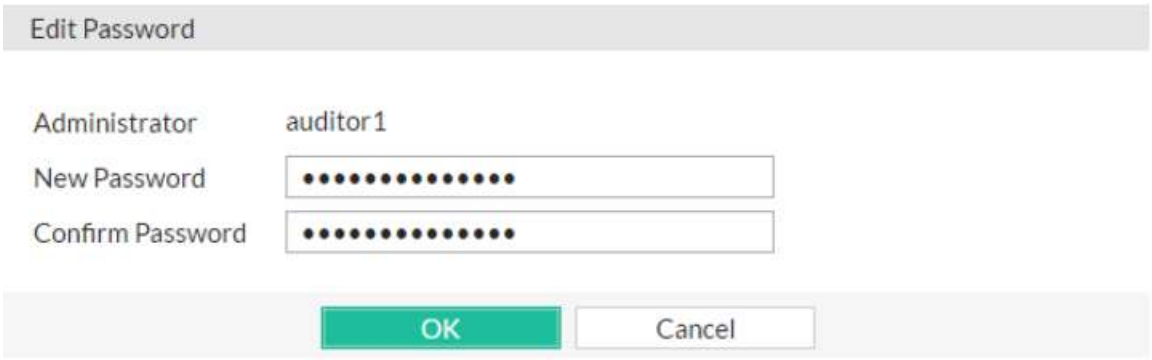

Рис. 3.2. Діалогове вікно «Змінити пароль» у «Система» > «Адміністратор» > «Адміністратори».

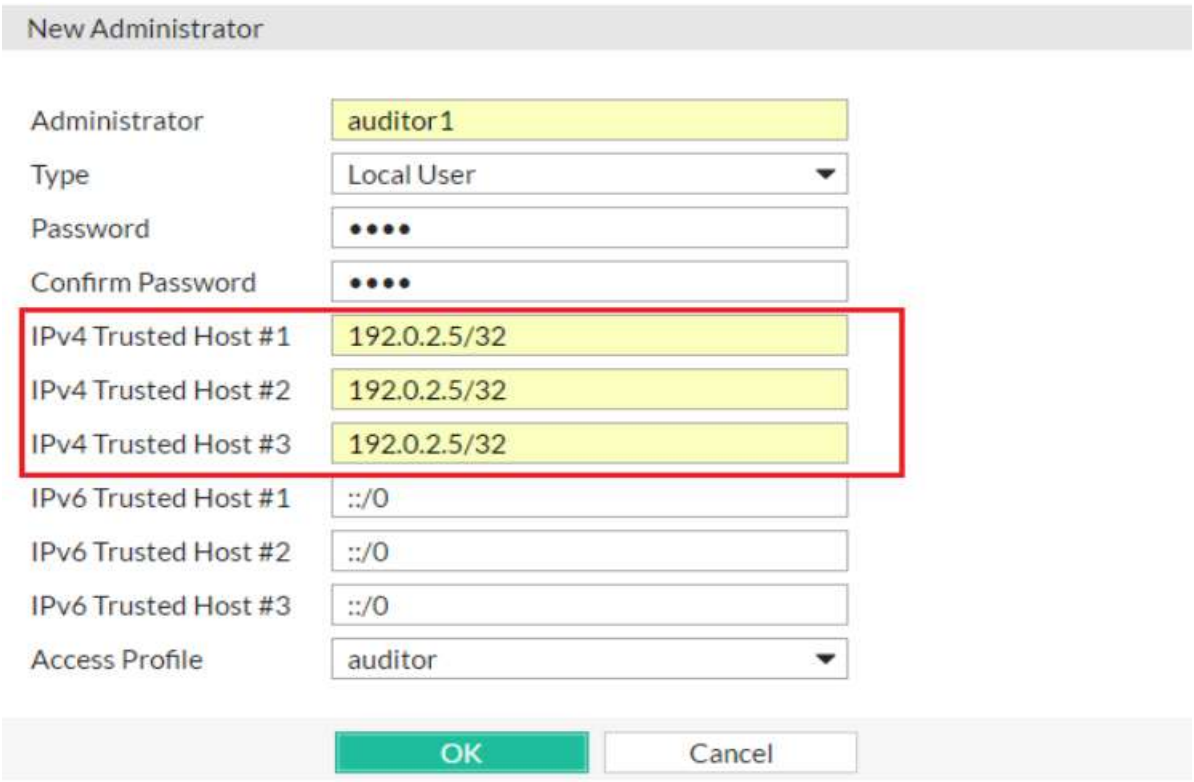

Рис. 3.3. Створити нове діалогове вікно в меню «Система» > «Адміністратор» > «Адміністратори».

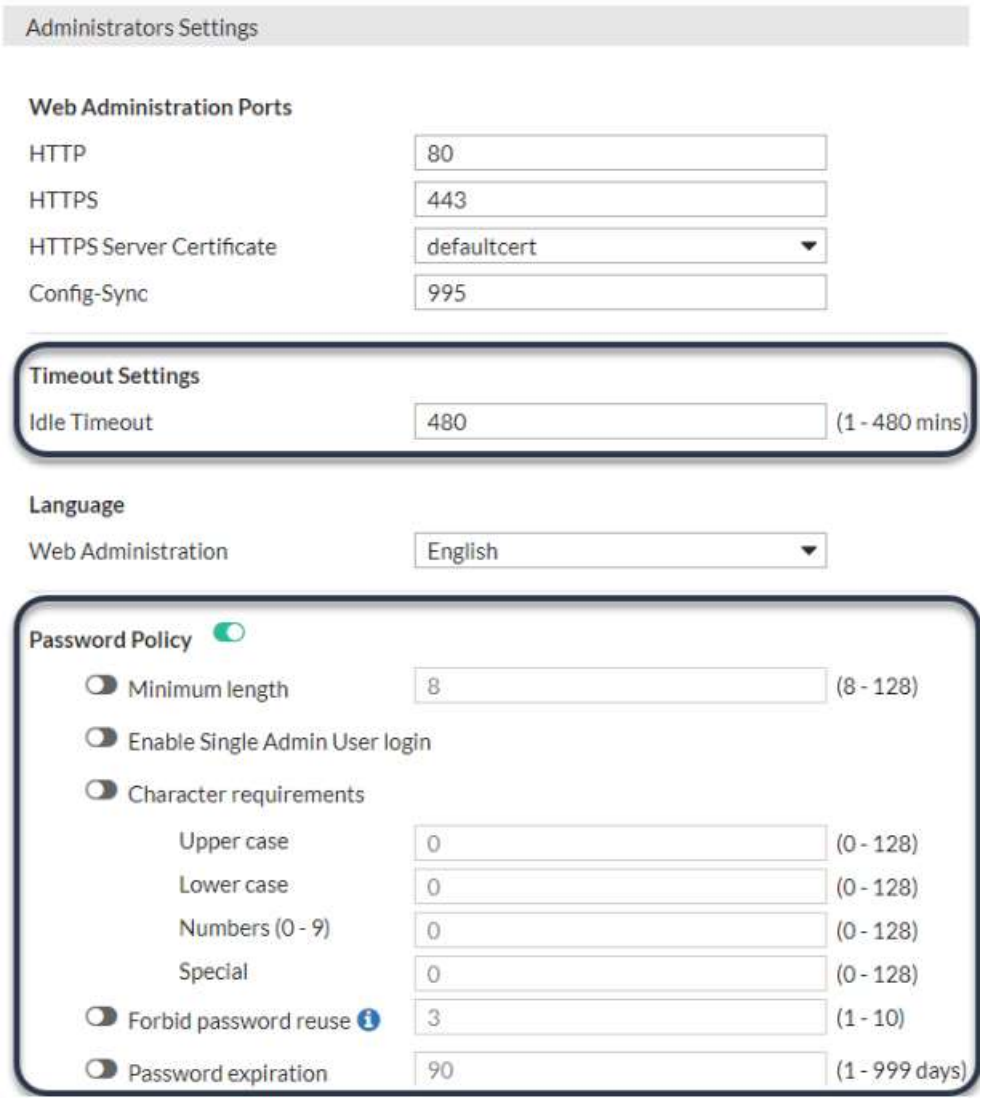

Рис. 3.4. Посилення паролів і час простою Система > Адміністратор > Налаштування

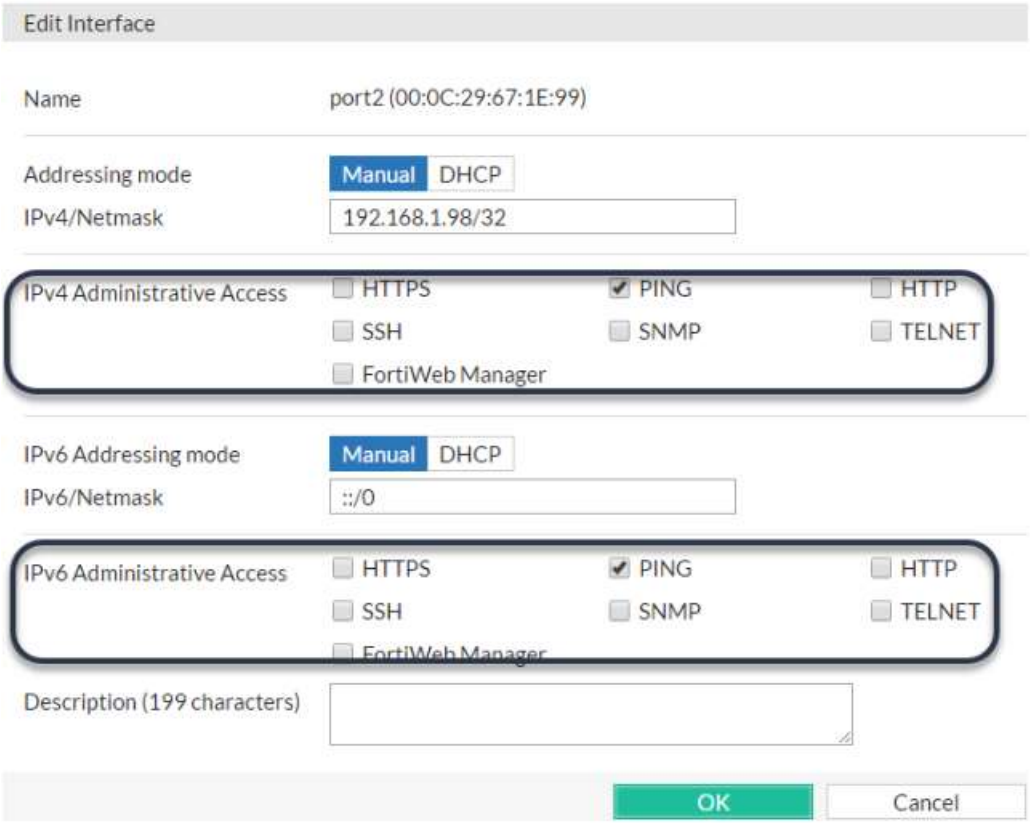

Рис. 3.5. Обмежити адміністративний доступ до одного мережевого інтерфейсу і дозволити лише протоколи доступу до керування, необхідні в Мережа > Інтерфейс

Використовуйте лише найбезпечніші протоколи. Вимкніть PING , за винятком усунення несправностей. Вимкніть HTTP , SNMP і налаштування мережі, якщо мережевий інтерфейс не підключається лише до довіреної приватної адміністративної мережі.

Буферне зміцнення

Під час аналізу трафіку HTTP-парсер FortiWeb повинен витягувати та буферизувати кожну частину запиту чи відповіді. Буфер дозволяє FortiWeb сканувати та/або переписувати його, перш ніж прийняти рішення про блокування чи пересилання готового трафіку. Буфери не нескінченні — через фізичні обмеження, притаманні всій оперативній пам’яті, їм виділяється максимальний розмір. Якщо частина запиту чи відповіді завелика, щоб поміститися в буфер, FortiWeb має пропускати або блокувати трафік без подальшого аналізу цієї частини.

Практично кажучи, хоча надмірні запити не є поширеними, коли вони є, вони можуть бути нешкідливими. Типовим прикладом є завантаження фільмів. GET Іншим прикладом є HTTP- запити, що містять багато запитів до бази даних із зашифрованими значеннями. У цих випадках зміцнення буфера може призвести до багатьох помилкових спрацьовувань під час звичайного використання. Слід уникати таких помилкових спрацьовувань, оскільки потік інформації може відвернути вас від справжніх атак.

З точки зору атак, великі DoS-атаки від одного зловмисника є непрактичними: якщо атакуючий хост повинен використовувати власну пропускну здатність або процесор швидше, ніж веб-сервер може це обробити, атака не спрацює. Тому трафік запиту DoS навряд чи буде надмірним.

Однак рішучі зловмисники часто створюють занадто великі запити, щоб замаскувати експлойт. Тактика підсилення атаки нешкідливими даними, щоб вивести корисне навантаження за межі буфера сканування, популярна серед більш обізнаних і вмотивованих зловмисників APT, а також серед дослідників із чорним капелюхом, які створюють пакети експлойтів для Metasploit та інших інструментів, які в кінцевому підсумку потрапляють до рук сценаристів. . Подібно до атак на переповнення буфера, ці атаки з доповненням намагаються обійти та використати внутрішні обмеження. Якщо запит не може поміститися в буфер, це може бути атака з доповненням.

Щоб визначити відповідні обмеження HTTP, спочатку спостерігайте за нормальним трафіком. Порівняйте його з кількістю буферів і максимальними розмірами FortiWeb

3.2 Рекомендації щодо налаштування, порядок роботи з Fortiweb

Планування топології мережі

Щоб отримувати трафік, призначений для веб-серверів, які захищатиме ваш пристрій FortiWeb , зазвичай потрібно встановити пристрій FortiWeb між веб-

серверами та всіма клієнтами, які мають до них доступ.Конфігурація мережі має гарантувати, що весь мережевий трафік, призначений для веб-серверів, має спочатку проходити до або через пристрій FortiWeb (залежно від режиму роботи). Зазвичай клієнти отримують доступ до веб-серверів з Інтернету через брандмауер, наприклад FortiGate, тому пристрій FortiWeb слід встановити між веб-серверами та брандмауером показано на рис. 3.1.

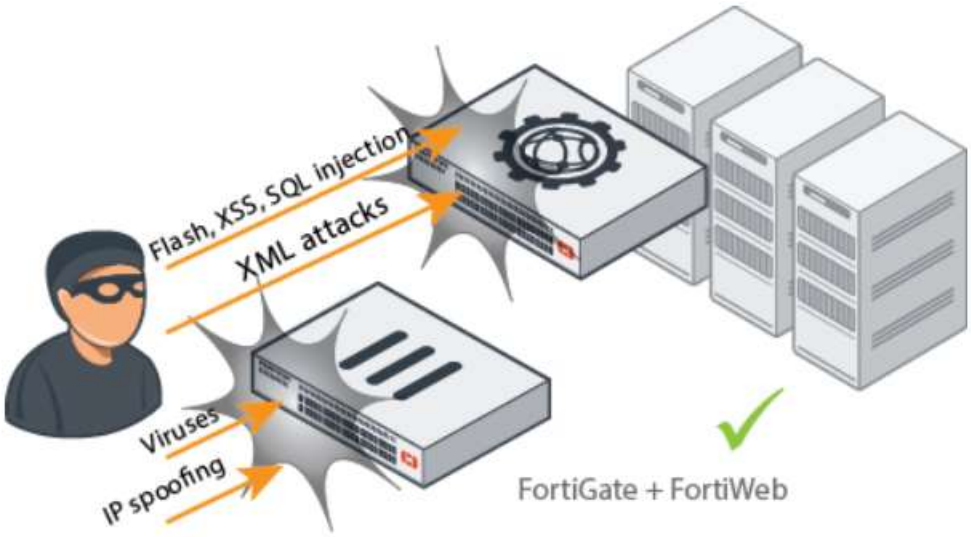

Рис. 3.6. Приклад правильного встановлення пристроїв FortiGate та FortiWeb

Встановіть брандмауер загального призначення, наприклад FortiGate, на додаток до пристрою FortiWeb . Якщо цього не зробити, ваші веб-сервери можуть стати вразливими для атак, які не базуються на HTTP/HTTPS. Пристрої FortiWeb не є міжмережевими екранами загального призначення, і якщо ви ввімкнете переадресацію на основі IP, вони дозволять проходити трафік без HTTP/HTTPS без перевірки.В ідеалі заходи контролю та захисту мають дозволяти лише веб-трафіку досягати FortiWeb і ваших веб-серверів. FortiWeb і FortiGate доповнюють один одного для підвищення безпеки.

Інші деталі топології та функції залежать від режиму роботи пристрою FortiWeb . Наприклад, пристрої FortiWeb , що працюють у режимі Offline Protection або в будь-якому з прозорих режимів, не можуть виконувати трансляцію мережевих адрес (NAT) або балансування навантаження; Пристрої FortiWeb , що

працюють у режимі зворотного проксі, можуть.

Зовнішні балансувальники навантаження:

Зазвичай вам слід розгортати FortiWeb перед балансувальником навантаження (наприклад, FortiBalancer, FortiADC або будь-яким іншим пристроєм, який застосовує вихідний NAT), щоб FortiWeb знаходився між балансувальником навантаження та клієнтами показано на рис. 3.2. Це має важливі наслідки:

Спрощена конфігурація;

Нескановний трафік не досягне балансувальника навантаження, покращуючи його продуктивність і безпеку;

На IP-рівні, з точки зору FortiWeb , HTTP-запити правильно виглядатимуть так, що вони надходять із справжньої IP-адреси клієнта, а не (через SNAT) балансувальника навантаження

Інакше IP-адреси зловмисників і законних клієнтів можуть бути приховані балансувальником навантаження.

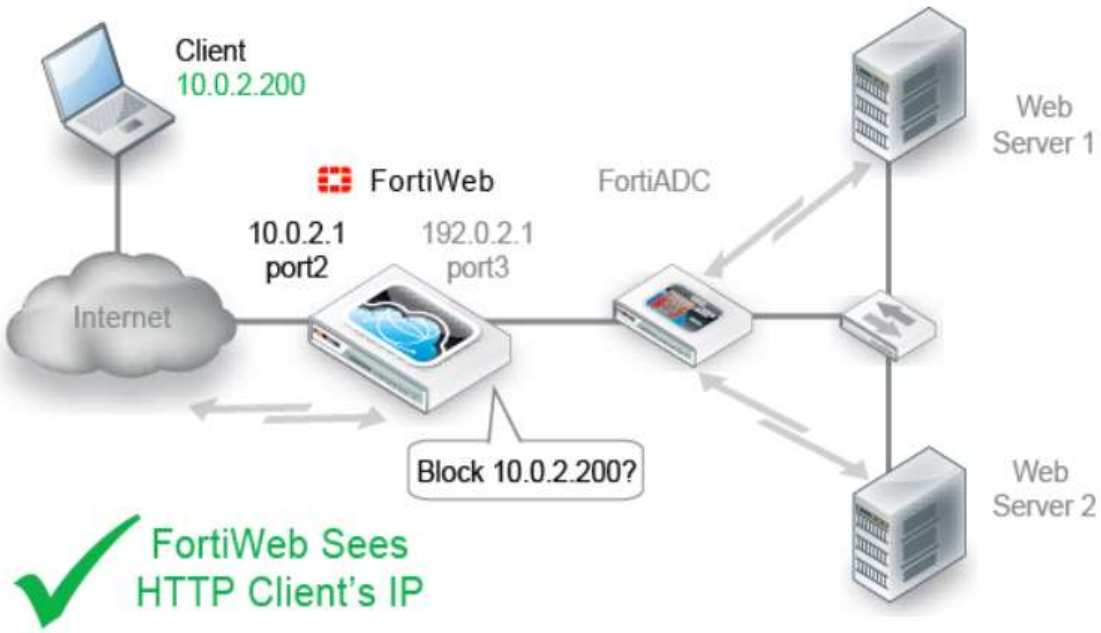

Рис. 3.7. приклад топології мережі з балансувальником навантаження

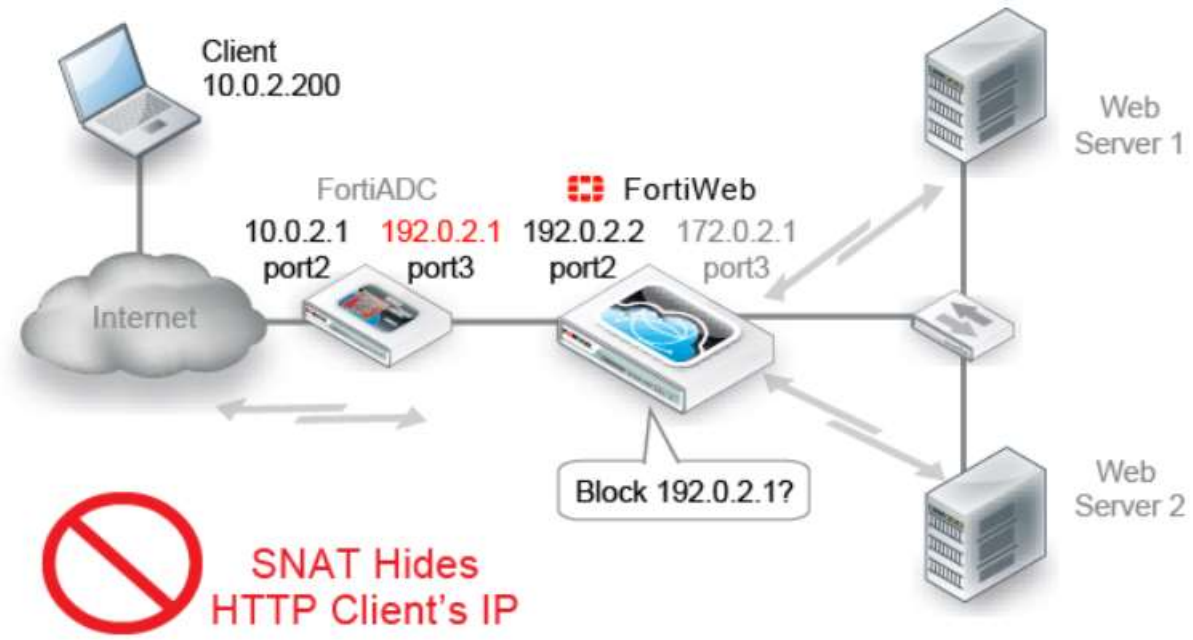

Рис. 3.8. приклад неправильної конфігурації

Щоб запобігти такій неправильній конфігурації (рис 3.2.), ви повинні налаштувати свої пристрої так, щоб компенсувати, якщо FortiWeb знаходиться позаду балансувальника навантаження. Налаштуйте балансувальник навантаження так, щоб він не мультиплексував HTTP-запити від різних клієнтів у кожне TCP-з'єднання за допомогою FortiWeb .

FortiWeb часто застосовує блокування на рівні TCP/IP-з'єднання, що може призвести до блокування невинних HTTP-запитів, якщо балансувальник навантаження передає їх у рамках того самого TCP-з'єднання як атаку. Таким чином, це може спричиняти періодичні невдалі запити. Щоб врахувати це, налаштуйте балансувальник навантаження на вставлення або додавання X-заголовка X-Forwarded-For:, X-Real-IP:або іншого HTTP. Також налаштуйте FortiWeb на пошук початкової IP-адреси зловмисника або клієнта в цьому HTTP-заголовку, а не в IP-сеансі.

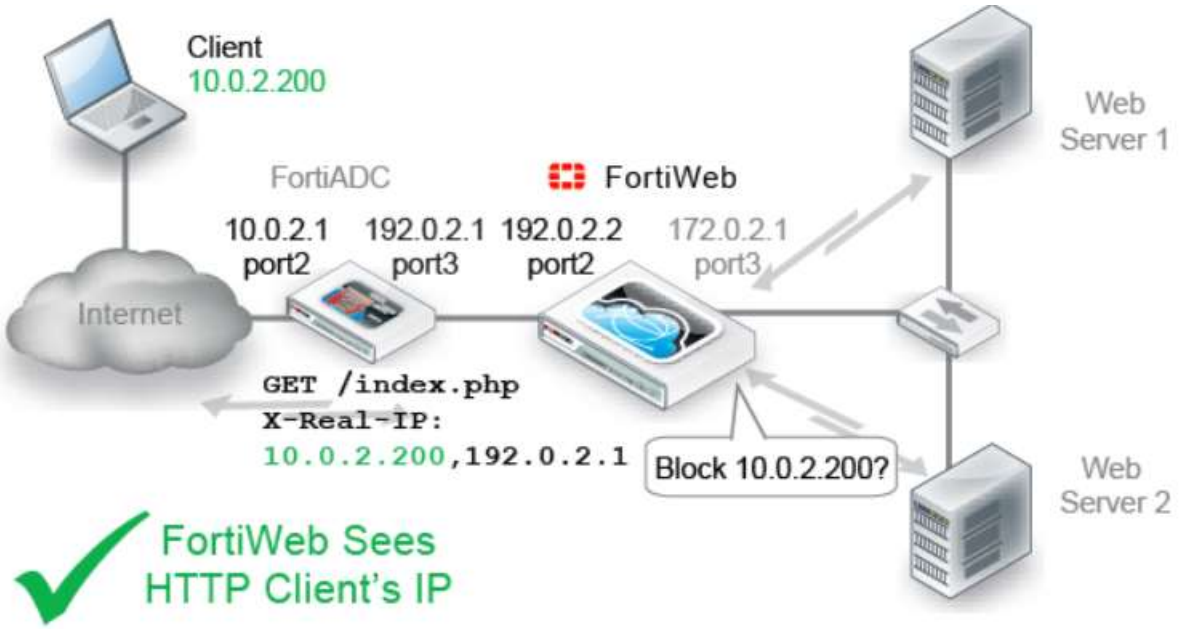

Рис. 3.9. приклад правильної конфігурації

Не встановлюйте жодних дій для Period Block , якщо балансувальник навантаження або будь-який інший пристрій перед FortiWeb застосовує SNAT, якщо ви не налаштували блокування на основі HTTP X-заголовків. Періодичне блокування на основі IP-адреси джерела на рівні IP призведе до того, що невинні запити, переслані пристроєм SNAT після атаки, блокуватимуться до закінчення періоду блокування. Таким чином, це може спричинити періодичні збої в роботі служби.

Як вибрати режим роботи Багато речей, зокрема:

Підтримувані функції FortiWeb;

Необхідна топологія мережі;

Позитивна/негативна модель безпеки;

Конфігурація веб-сервера;

Відрізняються за режимом роботи. Виберіть режим, який найкраще відповідає потребам вас і ваших клієнтів. Оскільки це такий ключовий фактор, уважно обміркуйте наслідки, перш ніж зробити свій вибір. Перенастроювання мережі може зайняти багато часу, якщо ви зміните режими пізніше.

3.3 Загальні рекомендації щодо забезпечення захисту

Попросіть професіоналів «атакувати» вашу програму

Який кращий спосіб ознайомитися з ризиками безпеки вашого веб-сайту , ніж знайти їх самостійно або за допомогою професіонала? Це один із найкращих методів безпеки веб-додатків, щоб бути в курсі всього, що відбувається на вашому сайті.Розуміючи методи, які зловмисники можуть використовувати у вашій веб-програмі, ви можете ефективно захистити точки входу.

Якщо ви плануєте зробити це самостійно, важливо переконатися, що ви нічого не порушуєте за допомогою автоматичного сканування . Крім того, можуть виникнути проблеми, коли ваш хостинг може заборонити ваш IP під час атаки на ваш сайт. Звичайно, будь-яке тестування має проводитися в ізольованому середовищі. Належне тестування безпеки веб-додатків передбачає отримання додаткової інформації про наступне:

Атаки SQL ін'єкції;

Міжсайтовий скриптинг;

Небезпечна десеріалізація;

Порушена автентифікація;

Підробка міжсайтових запитів;

Викриття конфіденційних даних;

Зрештою хакери знайдуть ці вразливості. Побий їх до цього.

Стежте за блогами безпеки веб-додатків і вивчайте їх

Якщо у вас відносно невелика команда або ви працюєте над розробкою додатків поодинці, вам доведеться оновити тактику безпеки. Ви вже читаєте це, тож ви точно робите правильні речі. Тим не менш, досліджуйте різні авторитетні блоги безпеки веб-додатків , щоб дізнатися більше, оскільки галузь і технології додатків змінюються. Хакери роблять ставку на те, щоб бути на крок попереду вас і вашої команди. Найкращий спосіб боротися з уразливими місцями — бути на вершині основ, а також нових небезпек, які з’являються з часом.

Завжди створюйте резервні копії даних

У випадку порушення безпеки або зараження зловмисним програмним забезпеченням і вам потрібно відновити веб-сайт, було б катастрофою не зберігати оновлену версію вашого веб-сайту. Коли прийде час знову виходити в прямому ефірі, ви будете раді, що все приховали. Тому створюйте резервні копії даних якомога частіше. Варто зазначити, що більшість хост-провайдерів нададуть резервні копії зі своїх серверів на випадок подібної події.

Часто скануйте свій веб-сайт на наявність вразливостей

Перевірки безпеки та сканування слід проводити регулярно, щоб бути в курсі безпеки веб-додатків. Було б доцільно проводити сканування безпеки на своїх веб-сайтах принаймні раз на тиждень. Ви також повинні виконувати сканування після кожної зміни, яку ви вносите у свою програму. Варто зазначити, що сканери безпеки, навіть дуже хороші, не зможуть виявити все. Сканери або евристичні, або засновані на шаблонах, а зловмисне програмне забезпечення завжди розроблено таким чином, щоб бути невидимим для сканерів. Деякі сканери краще виявляють зловмисне програмне забезпечення, деякі борються з помилковими спрацьовуваннями, а багато з них взагалі не працюють. Ви все одно повинні самостійно дізнаватися про недоліки та вразливості безпеки.

Інвестуйте в експертів з безпеки

Це дуже мудро, а також одна з найкращих практик безпеки веб-додатків. Самостійно залишатися в курсі безпеки веб-додатків дуже важко. Хоча всі наведені нами поради, безперечно, корисні, ви можете виявитися розсіяними, намагаючись не відставати від нових вразливостей. Експерт із безпеки або фірма, що надає послуги з безпеки, може виконувати сканування й перевірки безпеки, а також відстежувати наявність у вашій веб-програмі нових і небезпечних уразливостей. Просто переконайтеся, що ви провели серйозне дослідження , перш ніж інвестувати в будь-яку конкретну компанію чи спеціаліста-фрілансера.

Очистіть вихідні дані користувача

Як ми вже говорили раніше, дуже багато розробників вважають безпеку запізнілою думкою. Насправді це має бути частиною процесу розробки з самих ранніх стадій розробки. Ми це розуміємо. Ви зосереджуєтеся на тому, щоб ці

функції були зручними для користувачів. Можливо, ви вважаєте, що у вас немає часу чи ресурсів, щоб інвестувати в безпеку веб-додатків. Все-таки це велика помилка. Про безпеку слід думати до того, як веб-програма стане доступною для громадськості.

Тримайте все в актуальному стані

Дуже важливо постійно оновлювати все програмне забезпечення, яке у вас є. Не робити цього – великий ризик для вашої компанії. Хакери щодня уважно стежать за недоліками безпеки та шукають можливі експлойти. Записуйте кожен плагін, який у вас є, і оновлюйте його, коли вони доступні. Для сайтів WordPress ви можете використовувати функцію автоматичного оновлення для вразливих плагінів.

Використовуйте платформу безпеки веб-додатків, наприклад Patchstack

Patchstack — чудовий інструмент для захисту та моніторингу веб-додатків, особливо для розробників. Оскільки за допомогою Patchstack ви можете захистити весь свій портфель клієнтів – захищайте скільки завгодно сайтів. Перевірте ціни та тарифні плани тут. Тож ви можете захистити свої веб-програми, заощадити час і гроші та допомогти виділитися серед конкурентів.

Встановіть дуже надійну політику паролів

Ніхто не любить паролі, і ніхто не любить створювати нові паролі. Ось чому ми використовуємо інструменти керування паролями. Життя набуває набагато більшого сенсу після початку його використання.

Інструменти керування паролями корисні з кількох причин:

По-перше , ви не запам’ятаєте кожен свій пароль. Дуже поганою практикою є використання одного пароля в кількох облікових записах. Використовувати слово- пароль у будь-якому разі погано, але ми поговоримо про це пізніше.

За допомогою інструментів керування паролями ви можете легко отримати доступ до всіх своїх паролів з одного місця за допомогою одного головного ключа

По-друге , використовуйте парольні фрази або згенеруйте випадковий ключ за допомогою програми керування паролями. Важливо, щоб усі ваші паролі були унікальними. Хороший менеджер паролів випадковим чином згенерує ваші паролі

для вас і збереже їх у безпеці. Немає значення, який менеджер паролів ви використовуєте, якщо ви ним користуєтеся. Ми рекомендуємо LastPass і KeePass – перевірте їх. KeePass трохи хитріший, але LastPass широко використовується та має хороший інтерфейс користувача. Ще один — Dashlane, якщо вам потрібен третій варіант і ви не використовуєте Linux. Це твій вибір. По-третє – майстер-ключ. Замість використання пароля використовуйте парольну фразу , яка набагато довша. Використовуйте кілька цифр, великих і малих літер. І щоб було зрозуміло: за допомогою фрази-паролу вам слід створити коротке речення, але переконайтеся, що це те, що ви запам'ятаєте.

Окрім надійних паролів – використовуйте 2FA

Двофакторна автентифікація (2FA), яка також називається багатофакторною або багатоетапною перевіркою, — це механізм автентифікації для подвійної перевірки вашої особи. Це те, що ще більше захистить ваші облікові записи та запропонує вам додатковий рівень захисту, окрім паролів. Кіберзлочинцям важко отримати другий фактор автентифікації. Це різко зменшить їхні шанси на успіх.

2FA є обов'язковим для:

Ваша робоча або особиста електронна адреса;

Ваші облікові записи хмарного сховища (Google Drive, Dropbox);

Інтернет-банкінг;

Облікові записи в соціальних мережах (Facebook, Twitter, LinkedIn);

Програми для спілкування (Slack, Skype);

Інтернет-магазини (PayPal, Amazon);

- І навіть для програм керування паролями

Тут ви можете знайти деякі мобільні програми, які можна використовувати для двофакторної автентифікації: Google Authenticator (доступний для Android, iOS, Blackberry). Authy (для Android, iOS, але також доступний як програма для робочого столу та розширення для браузера). Microsoft Authenticator (Windows Phone 7).

10. Використовуйте шифрування SSL (HTTPS) для своїх сторінок входу

Використання шифрування SSL (або навіть краще TLS) повинно бути

обов’язковим і пріоритетним у захисті веб-додатків. HTTPS може належним чином захистити вразливу інформацію, яку можна використати, як-от номери соціального страхування, номери кредитних і дебетових карток, а також дані для входу для членів команди та користувачів. За допомогою HTTPS інформація, яка розміщується у веб-програмі, шифрується, тому для хакерів марна спроба перехопити інформацію. Крім того, відсутність сертифіката HTTPS часто позначається браузерами, як-от Chrome, як небезпечна, що відлякує багатьох потенційних користувачів. HTTPS захищає особисті дані, просто й просто.

11. Не економте на безпечному хості

Що таке безпека веб-додатків без безпечного хосту ? Будь-який вартий уваги веб-розробник знає, що для розміщення будь-якої веб-програми слід використовувати надійну компанію з веб-хостингу з привабливою справжньою репутацією. Хороший спосіб визначити, чи є хостингова компанія гідною, — це перевірити відгуки про компанію на кількох сайтах, які не пов’язані з самою хостинговою компанією. Зверніть увагу на їхні сторінки продуктів і блог, якщо вони є. Чи активно говорять про нові загрози безпеці веб-додатків? Чи часто вони оновлюють свою платформу для підвищення безпеки? Чи хороша їх технічна підтримка? Не бійтеся витрачати багато часу на дослідження хостів для вашої веб-програми.

ВИСНОВКИ

В роботі проведено дослідження проблеми захисту веб-додатків в сучасному інформаційному просторі як складової частини забезпечення кібербезпеки її інформаційних ресурсів.

FortiWeb — це брандмауер веб-додатків (WAF), який захищає розміщені веб-додатки від атак, спрямованих на відомі та невідомі експлойти. Використовуючи багаторівневі та корельовані методи виявлення, FortiWeb захищає програми від відомих уразливостей і загроз нульового дня. Служба безпеки веб-додатків від FortiGuard Labs використовує інформацію, засновану на останніх уразливостях програм, роботах, підозрілих URL-адресах і шаблонах даних, а також спеціалізовані евристичні механізми виявлення для забезпечення безпеки ваших програм.

Проаналізовано існуючи рішення із захисту веб-додатків озганізації при застосуванні хмарних платформ. Рішення брандмауера веб-додатків (Web Application Firewall) в світі вже встигли набрати достатню популярність, і такі компанії як Amazon і Fortinet Під час дослідження були вивчені основні загрози, з якими стикаються веб-додатки, такі як атаки на вразливості, перехоплення аутентифікаційних даних, атаки на API та інші. Було проведено аналіз можливостей FortiWeb у контексті захисту веб-додатків і визначено його переваги та можливості. Використання FortiWeb дозволяє організаціям ефективно захистити свої веб-додатки від різноманітних загроз та забезпечити безпеку клієнтів та даних. Інтеграція FortiWeb в існуючу інфраструктуру дозволяє забезпечити цілісний захист веб-додатків, аналізувати трафік, виявляти аномалії та вчасно реагувати на потенційні загрози. FortiWeb надає широкий набір функцій, таких як інтелектуальне виявлення загроз, система виявлення вторгнень (IDS), система запобігання вторгнень (IPS), захист від DDoS-атак, контроль доступу та шифрування, що дозволяють ефективно забезпечувати безпеку веб-додатків Досліджено призначення та застосування основних наборів правил брандмауера

веб-додатків. Захист веб-додатків відбувається за допомогою правил, визначених на основі основних наборів правил OWASP 3.2, 3.1, 3.0 або 2.2.9. Для кожної системи правил можна вимикати окреме правило або можна встановити певні дії за окремим правилом. Розроблено рекомендації фахівцям з кібербезпеки щодо застосування методів та засобів захисту веб-додатків організації при застосуванні хмарних платформ.

Таким чином, застосування рекомендацій із захисту веб-додатків організації при застосуванні хмарних платформ має забезпечити кібербезпеку інформаційних ресурсів організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. FortiWeb 7.2.2. Administration Guide. Fortinet Document Library. [Електронний ресурс] Режим доступу: https://docs.fortinet.com/document/fortiweb/7.2.2/administration-guide/60895/introduction
2. How to Secure Web Applications From Vulnerabilities in 2023. [Електронний ресурс] - Режим доступу: https://mobidev.biz/blog/best-practices-to-secure-web-applications-from-vulnerabilities
3. 11 Ways To Improve Your Web Application Security. [Електронний ресурс] - Режим доступу: https://patchstack.com/articles/web-application-security/
4. OWASP Top 10 – 2017.The Ten Most Critical Web Application Security Risks [Електронний ресурс] - Режим доступу: https://owasp.org/www-project-top-ten/2017/Top_10
1. Akamai App & API Protector: Maximize Security Through Simplicity [Електронний ресурс] - Режим доступу: https://www.akamai.com/blog/news/akamai-app-and-api-protector-maximize-security-through-simplicity
2. Cloudflare Product Cheat Sheet [Електронний ресурс] - Режим доступу: https://www.cloudflare.com/static/6f129010d43216d460e308819acce421/Cloudflare_Product_Cheat_Sheet.pptx.pdf
3. Impreva. v14.4 Web Application Firewall User Guide [Електронний ресурс] - Режим доступу: https://docs.imperva.com/bundle/v14.4-web-application-firewall-user-guide/page/70414.htm
4. Acunetix Web Application Vulnerability Report 2020

[Електронний ресурс] - Режим доступу: https://www.acunetix.com/white-papers/acunetix-web-application-vulnerability-report-2020/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)