Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Способи впровадження FWaaS в систему мережевої безпеки підприємства

Виконавець: студента IV курсу, групи КБ-41

_____ **Гліб ОСТАШИНСЬКИЙ**
(підпис) (ім'я, прізвище)

	Ім'я, прізвище	**Підпис**
Керівник	Олександр ТОРОШАНКО	

Нормоконтроль	Андрій БІГДАН	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-41** (група) **Осташинському Глібу Романовичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Способи впровадження FWaaS в систему мережевої безпеки підприємства

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Концепція FWaaS, брандмауери нового покоління

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з поняттям FWaaS, їх різновидами, функціями цього рішення, дослідити рішення брандмауера нового покоління, розробити план впровадження FWAAS в мережеву безпеку підприємства

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблені рекомендації з вибору функцій FWaaS та впровадження FWaaS в мережеву безпеку підприємства

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ Олександр ТОРОШАНКО
(підпис) (ім'я, прізвище)

Завдання прийняла до виконання _____ Гліб ОСТАШИНСЬКИЙ
(підпис) (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обґрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Дослідження концепції FWAAS	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз існуючих видів брандмауерів та їх порівняння	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження постачальників рішення FWAAS	22.03.2023 – 08.04.2023	*виконано*
7	Створенння рекомендацій щодо впровадження FWAAS в систему мережевої безпеки підприємства	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ Олександр ТОРОШАНКО
(підпис) (ім'я, прізвище)

Завдання прийняв до виконання _____ Гліб ОСТАШИНСЬКИЙ
(підпис) (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 58 сторінок основного тексту, 2 таблиці та 4 рисунки. Список використаних джерел містить 17 найменувань і займає 3 сторінки.

Методи дослідження кваліфікаційної роботи:

- аналіз вітчизняної та зарубіжної наукової літератури;
- аналіз практичного досвіду;
- порівняння;

Об'єктом дослідження є поняття FWaaS

Предметом дослідження в даній роботі є процес впровадження та використання FWaaS

Вивчення та узагальнення вітчизняної і зарубіжної практики. У кваліфікаційній роботі проаналізована існуюча література з налаштування та впровадження FWaaS , виконаний аналіз документації, порівняння, вивчення та узагальнення вітчизняної і зарубіжної практики з теми хмарних брандмауерів, розроблено рекомендації з впровадження FWaaS

В результаті кваліфікаційної роботи були отримані наступні найважливіші та найвагоміші результати:

- Визначено основні переваги впровадження FWaaS в систему мережевої безпеки підприємства, зокрема: зменшення витрат на обладнання, спрощення управління та масштабування, покращення захисту від кіберзагроз.
- Розроблено алгоритм впровадження FWaaS, який складається з аналізу потреб підприємства, вибору постачальника послуг FWaaS, налаштування та інтеграції з існуючою мережевою інфраструктурою, а також контролю та аудиту безпеки.

Ключові слова: Firewall as a Service (FWaaS), система, мережа, безпека, впровадження, методи, безпека мережі, рекомендації, кіберзагроза.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

AES	–	Advanced Encryption Standard
ATP	–	Advanced Threat Protection
API	–	Application Programming Interface
(D)DoS	–	(Distributed) Denial-of-Service
FWaaS	–	Firewall as a service
IEEE	–	Institute of Electrical and Electronics Engineers
IoT	–	Internet-of-Things
IPS	–	Intrusion Prevention System
IaaS	–	Infrastructure as a service
IT	–	Information Technology
mFWaas	–	Mobile Firewall as a Service
NAT	–	Network Address Translation
NGFW	–	Next Generation Firewall
PaaS	–	Platform as a service
pFWaaS	–	Perimeter Firewall as a Service
SaaS	–	Software as a service
SSL	–	Secure Sockets Layer
VM	–	Virtual Machine
vFWaaS	–	Virtual Firewall as a Service
WAF	–	Web Application Firewall

ЗМІСТ

ВСТУП

Сучасні підприємства все більше стикаються з ростом кіберзагроз і надзвичайно важливо забезпечити надійний рівень мережевої безпеки. Швидкий розвиток технологій та зростання обсягів цифрової інформації вимагають ефективних заходів для захисту від кібератак та забезпечення безперебійної роботи бізнес-систем. Одним із потужних інструментів, який набуває все більшої популярності, є Firewall as a Service (FWaaS) - рішення, що надає послугу фаєрвола як хмарний сервіс. Впровадження FWaaS може забезпечити ефективний захист мережевої інфраструктури підприємства від широкого спектру кіберзагроз та зменшити вразливості перед сучасними атаками.

Актуальність та перспективність тематики кваліфікаційної роботи полягає в тому, що зростання кількості та складності кібератак, а також залежність підприємств від надійного функціонування їх мережевих систем створюють потребу в ефективних інструментах захисту. FWaaS є інноваційним підходом, який може допомогти підприємствам забезпечити безпеку мережі та мінімізувати ризики.

Метою кваліфікаційної роботи є вивчення способів впровадження FWaaS в систему мережевої безпеки підприємства з метою забезпечення оптимального рівня захисту, виявлення потенційних переваг та недоліків, а також розробка рекомендацій щодо ефективного впровадження цього рішення.

Об'єктом кваліфікаційної робот є система мережевої безпеки підприємства, а предметом – способи впровадження FWaaS у цю систему.

Для досягнення поставленої мети використовуватимуться такі методи дослідження:

- Аналіз вітчизняної та зарубіжної наукової літератури для вивчення теоретичних аспектів FWaaS та його впровадження в систему мережевої безпеки підприємства.

- Аналіз практичного досвіду та кейс-студій, пов'язаних з впровадженням FWaaS в реальних підприємствах.

Практичне значення одержаних результатів полягатиме в розробці рекомендацій та пропозицій щодо впровадження FWaaS в систему мережевої безпеки підприємства з урахуванням його потенційних переваг та викликів.

РОЗДІЛ 1
ХМАРНІ БРАНДМАУЕРИ

1.1 Поняття FWaaS

FWaaS — це рішення брандмауера, що надається як хмарна послуга, яка дозволяє компаніям спростити IT-інфраструктуру. Він надає можливості брандмауера нового покоління (NGFW), як-от веб-фільтрацію, розширений захист від загроз (ATP), систему запобігання вторгненням (IPS) та безпеку системи доменних імен (DNS).

FWaaS багато в чому схожий на апаратний брандмауер, який у вас буде локально. Однак він має певні переваги, такі як можливість майже миттєво масштабуватися, щоб відповідати мережі, що розширюється. Ви також можете надати нові послуги, які раніше не були вам потрібні.

Все це можливо завдяки тому, що воно базується в хмарі. Тому його можна сформувати відповідно до розміру, конфігурації, попиту та унікальних потреб у безпеці вашої мережі.

Як і рішення NGFW, брандмауер як служба фільтрує мережевий трафік, щоб захистити організації як від внутрішніх, так і зовнішніх загроз. Поряд з функціями брандмауера з визначенням стану, такими як фільтрація пакетів, моніторинг мережі, безпека Інтернет-протоколу (IPsec), підтримка віртуальної приватної мережі рівня безпечних сокетів (SSL VPN) та функції відображення Інтернет-протоколу (IP), FWaaS також має більш глибокі можливості перевірки вмісту, які включають можливість ідентифікувати атаки зловмисного програмного забезпечення та інші загрози.

FWaaS знаходиться між вашою мережею та Інтернетом. Коли трафік намагається проникнути у вашу мережу, рішення FWaaS перевіряє його для виявлення та усунення загроз. Перевірка аналізує інформацію, що міститься в заголовку кожного пакета даних, одержуючи уявлення про те, звідки прийшов пакет

та інші дії, які можуть означати, що він є зловмисним. Схематичний принцип роботи FWaaS можна побачити на рисунку 1.1

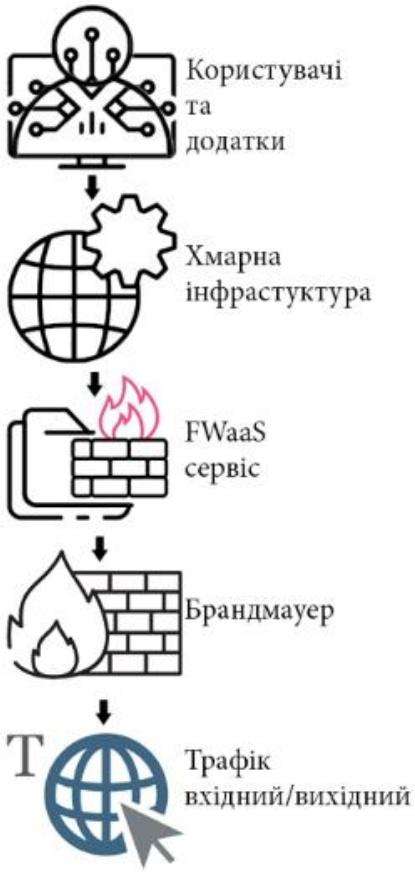

Рисунок 1.1 – Принцип роботи FWaaS

- Користувачі та додатки: це ваші користувачі, які взаємодіють з додатками, розміщеними в обласній інфраструктурі. Вони можуть доступатися до додатків через Інтернет.
- Хмарна інфраструктура: обласна інфраструктура, яка може бути хостингом ваших додатків і забезпечує їх доступність через Інтернет. Наприклад, це може бути інфраструктура хмарного провайдера, такого як Amazon Web Services (AWS), Microsoft Azure або Google Cloud Platform (GCP).
- FWaaS Сервіс: FWaaS-провайдер надає послугу файрвола. Цей сервіс може бути наданий хмарним провайдером або спеціалізованою компанією. Він використовується для настроювання і керування правилами файрвола.

- Брандмауер: брандмауер – це основна частина FWaaS. Він знаходиться в середині інфраструктури і контролює трафік, що проходить через нього. Брандмауер перевіряє правила файрвола, які встановлені FWaaS-провайдером, і приймає рішення щодо дозволу або блокування трафіку.
- Трафік: брандмауер аналізує трафік, що проходить через нього, і перевіряє його з правилами файрвола. Він може блокувати небажаний трафік, що не відповідає правилам, або дозволяти припустимий трафік пройти далі в інфраструктуру.

Таким чином, FWaaS надає хмарну послугу файрвола, яка контролює трафік до вашої хмарної інфраструктури за допомогою настроюваних правил і брандмауера.

В цьому контексті хмарні брандмауери стають новим поколінням брандмауерів, розроблених спеціально для хмарних мереж і здатних фільтрувати трафік між віртуальними машинами та мережевими пристроями.

Наприклад, брандмауер-як-сервіс (FWaaS), який зазвичай застосовується до моделей доставки програмного забезпечення як сервісу (SaaS), має просту конфігурацію, не потребує фізичних або частих ручних оновлень (оскільки він інтегрований у ту ж саму платформу як все-в-одному програмному забезпеченні) і не вимагає поглиблених знань про трафік від користувачів хмари (які не несуть відповідальності за брандмауер та політики безпеки) [1]. Це типовий випадок брандмауерів FWaaS, а також поширена практика більшості популярних хмарних брандмауерів, налаштованих у платформах SaaS (наприклад, брандмауери для веб-додатків (WAF)). Більше традиційні системи безпеки мережі поступово втрачають популярність у сфері безпеки, оскільки вони загалом є більш дорогими з точки зору пристроїв та проектування порівняно з хмарними системами, традиційні та хмамрні схеми брандмауерів можна побачити на рисунку 1.2 та рисунку 1.3.

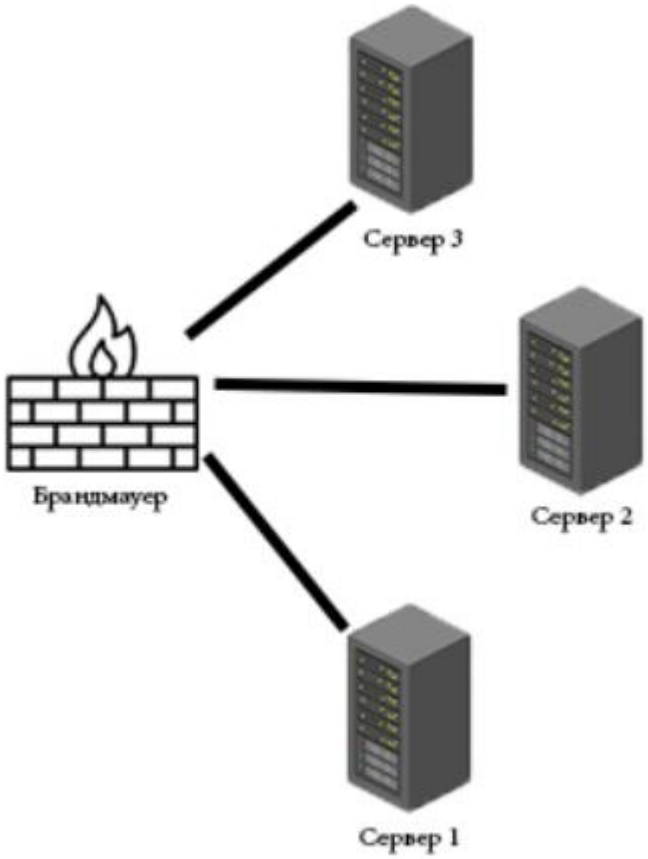

Рисунок 1.2 – Традиційна схема брандмауера

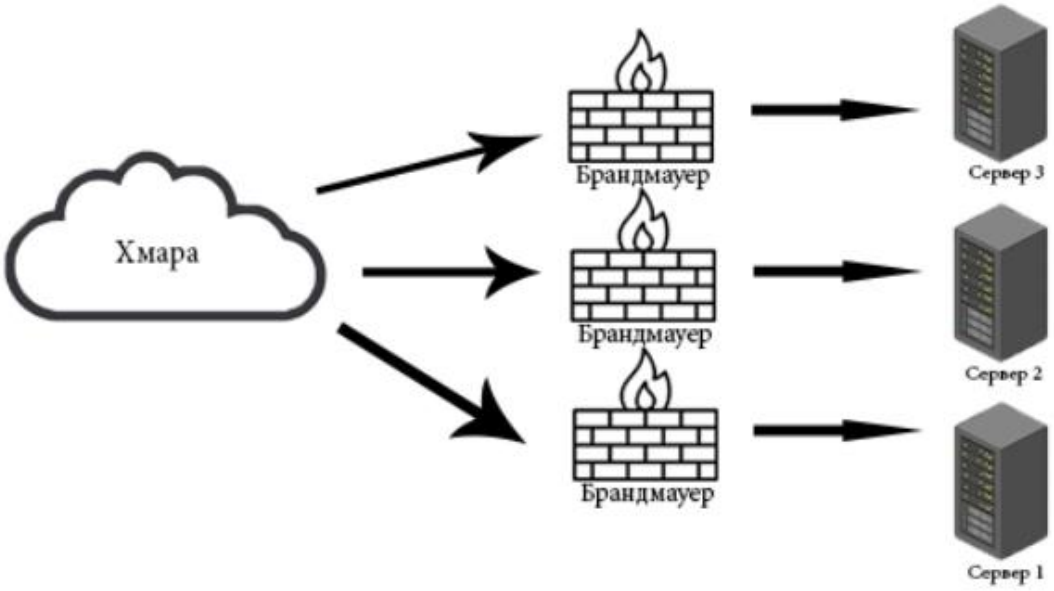

Рисунок 1.3 – Традиційна хмарна система брандмауера (базована)

FWaaS впроваджує інноваційні можливості, розширюючи периметр до всіх авторизованих користувачів, незалежно від їхнього місцезнаходження, часто в поєднанні з віртуальними приватними мережами (VPN). Це дозволяє компаніям підтримувати безпечний зв'язок з віддаленими філіями. Крім того, FWaaS дотримується хмарного принципу планів з оплатою по мірі використання, пропонуючи економічно ефективне рішення. Однак FWaaS в основному розгортається в моделях "Інфраструктура як послуга" (IaaS) і "Платформа як послуга" (PaaS), в той час як платформи "Програмне забезпечення як послуга" (SaaS), як правило, не працюють з цим типом брандмауерів. Таким чином, з'являється перша відмінність між хмарними брандмауерами, призначеними в першу чергу для платформ IaaS і PaaS, такими як брандмауери нового покоління (NGFW), і тими, які в основному використовуються на платформах SaaS, такими як брандмауери для веб-додатків (WAF). Хоча FWaaS не можна розглядати суто як тип брандмауера (його точніше вважати підкатегорією NGFW), WAF і NGFW є основними сучасними категоріями брандмауерів, які зазвичай використовуються в хмарі. Варто зазначити, що віртуальні брандмауери (VF) можна розглядати як попередники цих технологій, що виправдовує їх включення в обговорення [2,3].

1.1.1 Віртуальні брандмауери

Дедалі ширше впровадження віртуальних середовищ в архітектуру корпоративних мереж призвело до високого попиту на віртуальні брандмауери. Ці програмні брандмауери працюють як гіпервізори у віртуальних машинах (ВМ) або як модулі ядра, замінюючи потребу у фізичних пристроях. Вони спеціально розроблені для мережевих систем, які більше орієнтовані на віртуалізовані середовища. Віртуальні брандмауери представляють перше покоління пристроїв, які працюють у віртуалізованих середовищах, в першу чергу у віртуальних машинах, а згодом були поширені на хмарні обчислення.

Брандмауери наступного покоління (NGFW) зазвичай реалізуються в системах "Платформа як послуга" (PaaS) або "Інфраструктура як послуга" (IaaS). З іншого боку,

брандмауери для веб-додатків (WAF) часто зустрічаються в платформах "Програмне забезпечення як послуга" (SaaS), а іноді вони інтегровані в брандмауери SaaS. Мережеву схему віртуального брандмауера можна побачити на рисунку 1.4.

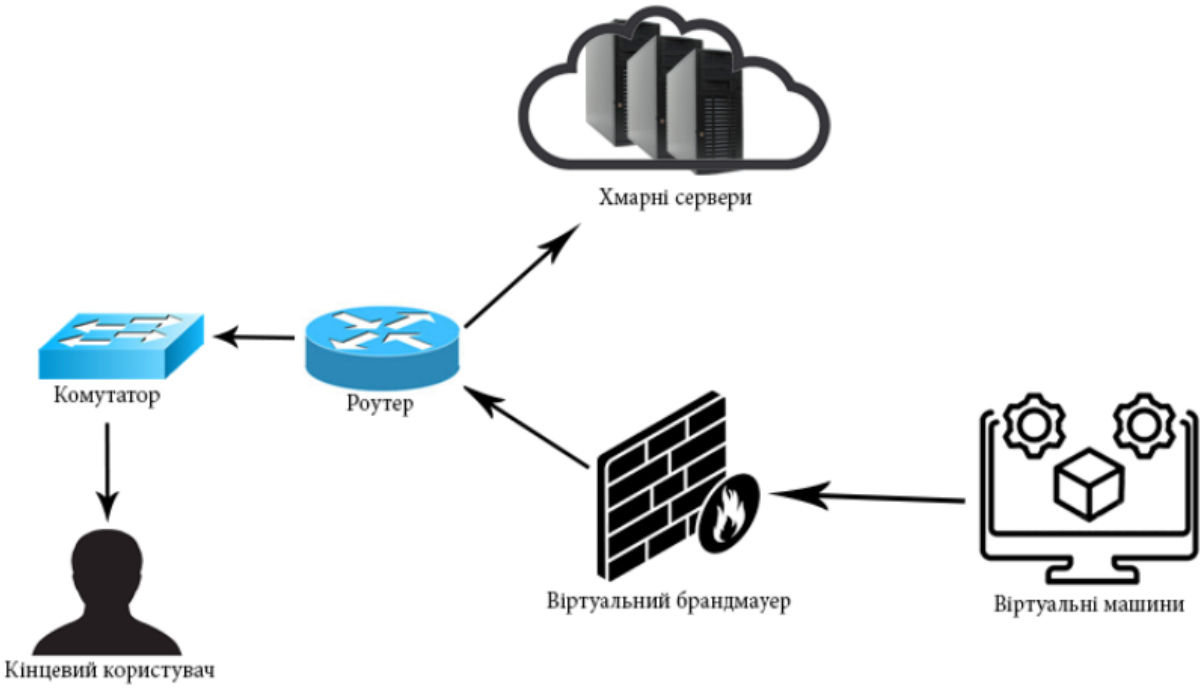

Рисунок 1.4 – Мережева схема віртуального брандмауера

На відміну від інших категорій хмарних брандмауерів, віртуальні брандмауери мають крос-платформне застосування, оскільки їх можна розгортати на всіх хмарних платформах. Вони пропонують перевагу захисту ширшого спектру машин, включаючи окремі сервери та групи віртуальних серверів, завдяки практиці, відомій як мікро-сегментація. Це дозволяє автоматично застосовувати правила брандмауера і політики безпеки до всіх пристроїв, доданих до програми брандмауера.

Однак, є певні потенційні недоліки, які слід враховувати.

По-перше, впровадження віртуального брандмауера в глобальній мережі (WAN), яка використовує бездротові пристрої або програмні технології, що вимагають постійного оновлення, може викликати певні труднощі.

По-друге, подібно до традиційних мережевих IT-систем, віртуальним брандмауерам може бракувати можливостей налаштування.

По-третє, дотримання високих стандартів проектування віртуальних брандмауерів може призвести до додаткових, а іноді й непередбачуваних витрат на розробку.

З точки зору бізнесу, це може призвести до збільшення витрат, а з технічної точки зору - до появи потенційних вразливостей, які нелегко усунути, особливо в гібридних хмарних системах, які часто використовують компанії, що переходять до хмарних технологій.

Тим не менш, віртуальні брандмауери залишаються розумним і портативним рішенням, особливо в контексті розумної охорони здоров'я. Вони пропонують кілька корисних переваг, таких як:

- Покращена продуктивність мережі з точки зору швидкості та зв'язку завдяки гнучкому розміщенню та меншому споживанню ресурсів. Рекомендованою практикою є встановлення брандмауера за кожною віртуальною машиною (далі – ВМ), що працює як керований процес ядра для кожної запущеної ВМ окремо. Така конфігурація допомагає зменшити ризик зловмисних атак на ВМ під час спільного використання мережевих, дискових та обчислювальних ресурсів.
- Віртуальні брандмауери надають додаткову функціональність, яку можна знайти у міжмережевих (маршрутизованих) брандмауерах та брандмауерах на рівні мережевої карти. Брандмауери на рівні мережевої карти підключаються безпосередньо до мережевої карти ВМ і можуть фільтрувати вхідний і вихідний трафік на рівні окремої ВМ.

1.1.2 Брандмауери наступного покоління

Ця категорія брандмауерів набула популярності завдяки зростаючому використанню складних додатків і пов'язаних з ними шкідливих загроз. Традиційним брандмауерам часто не вистачає адаптивності для розпізнавання різних категорій веб-активності, особливо новітніх, які вимагають більш гнучких правил для дозволу або відхилення мережевого трафіку. Платформи "Платформа як послуга" (PaaS) та

"Інфраструктура як послуга" (IaaS) є поширеними моделями доставки таких брандмауерів, оскільки вони мають високі вимоги до безпеки.

Брандмауери наступного покоління (Next-Generation Firewalls, NGFW) охоплюють цілий ряд можливостей, які дозволяють їм застосовувати політики мережевої безпеки і надавати розширені функціональні можливості. У стандартному режимі NGFW діють як універсальне рішення, що включає в себе можливості традиційних брандмауерів. У розширеному режимі NGFW включає складні системи запобігання вторгненням (IPS) і працює автономно на різних рівнях моделі OSI, від 2-го до 7-го. Це робить NGFW потужним рішенням для брандмауера. Додаткові можливості NGFW включають фільтрацію веб-сайтів, антивірусну перевірку, якість обслуговування (QoS), аналіз пропускної здатності та антивірусні можливості. NGFW також може генерувати звіти про трафік на хмарних сервісах і відповідно адаптувати свої правила, використовуючи білі та чорні списки.

Однак, щоб забезпечити широкий захист і перевірку на прикладному рівні з детальним контролем мережевого трафіку, NGFW повинен включати в себе певні функції, які наразі не охоплені в повній мірі. Ці функції включають контроль зашифрованого трафіку, перемикання портів, контроль на основі додатків та ідентифікаційних даних, фільтрацію URL-адрес, захист від витоку даних, примусову WAN-маршрутизацію, потужніші можливості оптимізації QoS, управління мережею Wi-Fi та комплексні політики мережевої безпеки для всіх підключених пристроїв. Крім того, NGFW часто вважається складною системою, яка вимагає значних інвестицій для ефективного використання її функціональних можливостей, що може бути необхідним не для всіх організацій [4].

1.1.3 Брандмауер веб-додатків

Брандмауер веб-додатків (WAF) – це рішення для забезпечення безпеки, призначене для роботи на прикладному рівні моделі OSI. Він спеціально розроблений для підвищення веб-безпеки і відіграє важливу роль у захисті стандартних інфраструктур, таких як веб-сервери, веб-додатки, обробка сеансів, файли cookie та

інші компоненти, які зазвичай асоціюються з веб-додатками. WAF надає такі важливі функції, як інструменти моніторингу журналів і методи безпеки, як шифрування URL-адрес.

Однією з основних цілей WAF є захист від поширених атак, які в першу чергу націлені на рівень веб-додатків. Він використовує різні контрзаходи, включаючи перевірку безпечного ведення журналів, шифрування SSL, перевірку даних на переповнення буфера і захист від таких атак, як SQL-ін'єкції, LDAP-ін'єкції, XML-атаки, впровадження коду, міжсайтовий скриптинг, контрабанда HTTP-запитів і захист файлів cookie. Зі зростанням значення хмарних мереж, брандмауер веб-додатків був поширений на хмарні рішення WAF. Ці хмарні WAF зберігають основні характеристики WAF, але пропонують еластичність, масштабованість і модель оплати за фактом використання. Однак розгортання хмарних WAF пов'язане з певними ризиками і складнощами, особливо при усуненні помилкових спрацьовувань, які можуть негативно вплинути на бізнес і спричинити додаткові витрати. Порівняння видів брандмауерів можна побачити в таблиці 1.1 [5,6].

Таблиця 1.1

Порівняння видів брандмауерів

Брандмауер	**Рівень OSI**	**Плюси**	**Мінуси**
Віртуальний брандмауер	Рівень 2	Застосовується трансверсально на хмарних платформах. Забезпечує захист на ширшому діапазоні машин.	Обмеження реалізації в WAN-мережах з використанням Wi-Fi пристроїв/програмних засобів технології Потрібні додаткові витрати на проектування щоб уникнути впливу на мережу.
Брандмауери наступного покоління (NGFW)	Рівні 2-7	Ширший захист на рівні OSI, сумісність з Intrusion Detection System (IDS) / Системою запобігання вторгненням (IPS), контроль доступу. Можливості списків, розширені розвідка загроз.	Занадто багато складнощів і високі необхідні інвестиції. Деякі функціональні можливості не призначені для стандартних мережевих середовищ (хмарних і не хмарних).

продовження табл. 1.1

Брандмауер	**Рівень OSI**	**Плюси**	**Мінуси**
Брандмауер веб-додатків	Рівні 7	Дуже специфічне рішення проти основних зловмисних атак на рівні на рівні додатків з можливостями адаптації для цільового рівня. Шифрування та примусовий режим SSL режим для встановлення безпечних з'єднання.	Для уникнення помилкових позитивних виявлень необхідні високопрофесійні навички у вирішенні проблем.

1.2 Використання FWaaS в сучасній Україні

В умовах сучасної України, де війна та пандемія COVID-19 створюють виклики для підприємств, багато бізнесів почали використовувати SaaS для економії витрат, гнучкості та віддаленого доступу. SaaS, або Software as a Service це модель розподілу програмного забезпечення, де програми надаються в якості сервісу через Інтернет. Замість того, щоб придбувати та встановлювати програмне забезпечення на своїх власних серверах, користувачі можуть отримувати доступ до програм через хмару.

У моделі SaaS відповідальність за встановлення, налаштування та підтримку програмного забезпечення на серверах лежить на постачальнику послуг (SaaS-провайдері). Користувачі мають зручний доступ до програмного забезпечення через веб-браузер або спеціальний клієнтський інтерфейс, що позбавляє їх необхідності проходити складні процедури інсталяції та обслуговування.

Існує кілька спільних аспектів використання FWaaS та SaaS на підприємстві:

Хмарна інфраструктура - FWaaS використовує хмарні ресурси для розгортання та управління брандмауерами, тоді як SaaS надає хмарні додатки та сервіси. В обох випадках компанії можуть використовувати хмарні облікові записи, інструменти та інфраструктуру.

- Централізований доступ та управління є спільними аспектами як SaaS, так і FWaaS. SaaS дозволяє користувачам отримувати доступ до додатків і даних з будь-якого місця через Інтернет, тоді як FWaaS дозволяє адміністраторам централізовано керувати брандмауерами і політиками безпеки в мережі.
- Оптимізація ресурсів – ще одна спільна перевага використання FWaaS і SaaS. Використовуючи ці сервіси, підприємства можуть заощадити ресурси, які в іншому випадку були б потрібні для розгортання та управління власною інфраструктурою брандмауерів та додатків. Замість того, щоб інвестувати в обладнання або ліцензії, підприємства можуть використовувати SaaS і FWaaS на основі оплати за використання. Це дозволяє організаціям більш ефективно розподіляти свої ресурси і зосередитися на основних бізнес-операціях.

1.3 Різновиди моделей FWaaS та їх характеристики

1.3.1 Віртуальний Firewall as a Service (vFWaaS)

Віртуальний Firewall as a Service (vFWaaS) є модифікацією концепції FWaaS, де фаєрволи виконуються у віртуальному середовищі замість фізичних пристроїв. Основна ідея полягає у використанні віртуалізації для розгортання та управління фаєрволами у хмарних середовищах або в інфраструктурі "програмне забезпечення-віртуалізація" (Software-Defined Infrastructure, SDI) [7].

Основні переваги віртуального FWaaS:

- Гнучкість: віртуальні фаєрволи можуть бути легко масштабовані та налаштовані в залежності від потреб мережі. Вони дозволяють швидко реагувати на зміни в обсязі трафіку та атакуватися в режимі реального часу.
- Ефективність використання ресурсів: віртуальні фаєрволи можуть бути розгорнуті на існуючому апаратному забезпеченні або в хмарному середовищі, що дозволяє ефективно використовувати ресурси. Вони також дозволяють розділяти фізичне апаратне забезпечення між різними віртуальними інстанціями фаєрволу.

- Централізоване управління: за допомогою vFWaaS можна централізовано управляти політиками безпеки та конфігураціями фаєрволів. Це дозволяє швидко впроваджувати зміни, уникати помилок та забезпечувати єдність у політиках безпеки.
- Безпека: віртуальні фаєрволи можуть використовувати сучасні методи виявлення загроз, а також інтегруватися з системами виявлення вторгнень (IDS) та системами управління загрозами (TMS). Це дозволяє забезпечувати комплексний захист мережі.
- Економічна ефективність: використання віртуальних фаєрволів дозволяє знизити витрати на придбання та підтримку фізичного апаратного забезпечення. Вони також дозволяють платити лише за використані ресурси, що робить їх економічно вигідними для багатьох організацій.

Однак, впровадження vFWaaS також має свої виклики, такі як необхідність міцного забезпечення віртуального середовища, впровадження механізмів ізоляції та контролю доступу, а також забезпечення високої доступності та надійності системи. Тому дослідження в цій області присвячені розробці та вдосконаленню рішень для вирішення цих викликів.

1.3.2 Периметр Firewall as a Service (pFWaaS)

Периметр Firewall as a Service (pFWaaS) відноситься до концепції FWaaS, яка зосереджується на забезпеченні захисту мережі на рівні її периметру. В основі pFWaaS лежить ідея розміщення фаєрволів у хмарних середовищах або на вузлах розташування хмарних провайдерів, що забезпечує централізований контроль над трафіком, який проходить через мережу.

Основні аспекти, пов'язані з pFWaaS:

- Захист периметру: pFWaaS надає можливість створювати і налаштовувати фаєрволи для захисту зовнішнього периметру мережі. Вони фільтрують та аналізують вхідний та вихідний трафік, виявляють та блокують загрози, такі як вторгнення, шкідливі програми та DDoS-атаки.

- Централізоване управління: pFWaaS дозволяє централізовано керувати політиками безпеки та конфігураціями фаєрволів на різних вузлах мережі. Це спрощує управління та забезпечує однорідність застосування правил безпеки.
- Масштабованість: pFWaaS забезпечує можливість масштабування фаєрволів для вирішення великих обсягів трафіку та забезпечення швидкодії. Він може адаптуватись до зростаючих потреб мережі та забезпечувати ефективне управління трафіком.
- Ефективність використання ресурсів: використання pFWaaS дозволяє ефективно використовувати ресурси, оскільки фаєрволи розгортаються у хмарних середовищах або на вузлах хмарних провайдерів. Це дозволяє уникнути витрат на фізичне апаратне забезпечення та підтримку.
- Безпека: pFWaaS забезпечує централізовану систему безпеки на периметрі мережі. Він дозволяє виявляти та блокувати загрози, контролювати доступ до ресурсів мережі та забезпечувати захист від атак зовнішніх загроз.
- Сумісність з існуючою інфраструктурою: pFWaaS може бути інтегрований з існуючими мережевими компонентами та інфраструктурою. Це дозволяє плавну міграцію та використання вже наявних ресурсів без необхідності повного перепроектування мережі.
- Аналітика та звітність**:** pFWaaS може надавати аналітичні дані та звіти про трафік, загрози та події безпеки. Це допомагає виявляти вразливості, реагувати на атаки та робити висновки для подальшого вдосконалення безпеки мережі.

Враховуючи різні переваги та можливості, pFWaaS стає популярним вибором для організацій, що шукають безпечні та ефективні рішення для захисту мережі на периметрі [8].

1.3.3 Firewall as a Service для мобільних пристроїв (mFWaaS)

Firewall as a Service для мобільних пристроїв (mFWaaS) є концепцією, що спрямована на надання функцій файрволу для захисту мобільних пристроїв, таких як смартфони та планшети. mFWaaS дозволяє користувачам мобільних пристроїв

отримувати захист мережі, контролювати доступ до ресурсів та забезпечувати безпеку проти загроз.

Основні аспекти, пов'язані з mFWaaS:

- Захист від загроз: mFWaaS надає можливість виявляти та блокувати загрози, такі як шкідливі програми, фішингові атаки, зловмисний трафік та інші види мобільних загроз. Він дозволяє створювати правила безпеки та політики доступу для захисту пристроїв та даних користувачів.
- Контроль доступу: mFWaaS дозволяє контролювати доступ до ресурсів мережі з мобільних пристроїв. Він може встановлювати правила та обмеження на рівні мережевого рівня, щоб обмежити доступ до певних додатків, сайтів або сервісів з мобільного пристрою.
- Інтеграція з хмарними сервісами: mFWaaS може бути інтегрований з хмарними сервісами для забезпечення безпеки та захисту даних в хмарних середовищах. Він може використовувати аналітику та інтелектуальні алгоритми для виявлення незвичайної активності та загроз у мобільних додатках та сервісах.
- Управління та конфігурація: mFWaaS забезпечує можливість централізованого управління та конфігурації файрволу на мобільних пристроях. Адміністратори мережі можуть встановлювати правила безпеки, оновлювати політики та моніторити стан безпеки пристроїв з централізованого інтерфейсу.
- Оптимізація ресурсів: mFWaaS може оптимізувати використання ресурсів мобільних пристроїв, таких як батарея, обсяги даних та обчислювальні ресурси. Він може регулювати споживання ресурсів залежно від потреб та пріоритетів безпеки.

mFWaaS стає важливим рішенням для захисту мобільних пристроїв у сучасному світі, де використання мобільних додатків та доступ до мережі є широко поширеними. Забезпечення безпеки та контролю над мобільним трафіком стає дедалі більш важливим завданням, і mFWaaS надає рішення для цих потреб.

Firewall as a Service з контролем доступу до даних (dFWaaS): ця модель використовується для контролю доступу до даних, які зберігаються в хмарному

середовищі. Вона дозволяє користувачам налаштувати політики доступу до даних, забезпечуючи контроль над тим, хто має доступ до яких даних.

Політика Firewall as a Service (polFWaaS): ця модель використовується для налаштування політик безпеки в хмарному середовищі. Вона забезпечує користувачам можливість налаштувати правила безпеки, які будуть застосовуватися до всього трафіку, що надходить до хмарного середовища [9,10].

1.4 Переваги та недоліки FwaaS

FWaaS дозволяє клієнтам частково або повністю перенести перевірку безпеки в хмарну інфраструктуру. Завдяки безпеці в хмарі вашим рішенням керує постачальник хмари, який підтримуватиме апаратну інфраструктуру, яка забезпечує ваше рішення. Ваша угода про надання послуг міститиме деталі з описом типів функцій, до яких ви матимете доступ, залежно від обраної вами підписки. Багатьом компаніям потрібна архітектура на основі послуг, оскільки вона дає їм свободу розширюватися на вимогу, не турбуючись про надання нового обладнання.

Підтримка апаратних брандмауерів не вписується в бюджети багатьох компаній або операційний процес, що робить FWaaS привабливим варіантом. Зручність, яку надає постачальник усіх оновлень і коригування налаштувань, дозволяє організаціям вивільняти критичні ресурси, час та енергію для інших, критично важливих завдань.

За допомогою FWaaS розподілені сайти та користувачі організації підключаються до єдиного логічного глобального брандмауера з уніфікованою політикою безпеки, що керується програмою, що дозволяє їм краще масштабувати безпеку. Брандмауер як постачальник послуг надає всім співробітникам доступ до ресурсів, які захищають широкий спектр пристроїв, що робить FWaaS єдиним рішенням для всіх, незалежно від розміру організації.

Це робить FWaaS основоположним компонентом будь-якої архітектури межі служби безпечного доступу (SASE), оскільки забезпечує функціональність NGFW без великих капітальних витрат (CapEx), пов’язаних із інвестиціями в інфраструктуру локальної глобальної мережі (WAN). При локальному налаштуванні оновлення

системи передбачає пошук найкращих компонентів і порівняння їх один з одним перед покупкою. Потім, після розставання з цінними коштами для придбання товару, організація має переконатися, що персонал ознайомлений з тим, як він працює, як його обслуговувати та як забезпечити належне оновлення. Для багатьох компаній це важке навантаження. За допомогою FWaaS все це бере на себе постачальник [11].

FWaaS використовує переваги вдосконалення програмного забезпечення та хмарних технологій, щоб забезпечити широкий спектр мережевої безпеки та можливостей перевірки, які надаються користувачам на вимогу будь-де. Завдяки внутрішньому налаштуванню ваша IT-команда має бути в курсі останніх програмного забезпечення та технологічних розробок, які впливають на світ мережевої безпеки. Деяким компаніям потрібен FWaaS просто для того, щоб забезпечити найновіший і найкращий захист. Коли постачальник захищає вашу мережу, ви, швидше за все, матимете передові технології та методології, ніж якби ви поклали цю відповідальність на своїх співробітників.

Для компаній, які шукають гнучкі рішення безпеки, FWaaS надає кілька явних переваг. Щоб зберегти гнучкість, багато організацій відходять від традиційних внутрішніх опцій і довіряють захист своєї мережі постачальнику FWaaS.

Уніфікована політика безпеки, розгорнута через хмару.

Уніфікована безпека передбачає поєднання кількох ініціатив безпеки під однією парасолькою. Таким чином, загальна служба здатна захистити організацію від різноманітних загроз. Уніфікована архітектура безпеки може включати навмисне резервування, яке є результатом двох або більше заходів безпеки, які здатні зупинити загрозу того самого типу. Керування цим у хмарі спрощує налаштування. Замість того, щоб шукати, купувати, налаштовувати та керувати кожним аспектом вашої уніфікованої архітектури, постачальник послуг подбає про все це за вас.

Гнучке розгортання та Модель споживання операційних витрат (OpEx).

Розгортання власного рішення може бути складним і тривалим. Є багато рухомих частин, пов’язаних із обладнанням та інших. У FWaaS, з іншого боку, розгортанням займається постачальник. Часто це можна зробити швидко і практично без роботи з боку компанії. У ситуаціях, коли потрібні спеціальні конфігурації,

організація повинна лише надати необхідну інформацію постачальнику, який потім може налаштувати розгортання [12].

Ваша модель споживання операційних витрат також повинна мати гнучкість. Рідко трапляються випадки, коли показники операційних витрат організації статичні – їх потрібно мати можливість коригувати в міру виникнення потреб. За допомогою FWaaS ви можете знайти способи отримати максимальну віддачу від вашого бюджету і навіть способи обмежити витрати на операційні витрати, забезпечуючи при цьому необхідну безпеку.

Спрощене розгортання та обслуговування.

Розгортання нового локального пакета безпеки – або навіть одного інструмента безпеки – може потребувати великих витрат часу та ресурсів.

Покращена масштабованість

Масштабувати рішення FWaaS просто. Вам просто потрібно обговорити свої нові потреби зі своїм провайдером. Потім вони можуть порадити вам на основі цілей вашого бізнесу. Крім того, коли ви масштабуєтеся за допомогою FWaaS, відносно легко повернутися до старої конфігурації, якщо нове рішення виявиться непотрібним або надмірним.

Підвищена гнучкість

За допомогою FWaaS ви можете вирішити, коли і як ви хочете розгорнути захист на основі процесів і активів, які ви хочете захистити. Ви також можете вирішити, де в хмарному ланцюжку даних ви хочете розмістити свої засоби захисту. Ви також можете використовувати FWaaS для захисту рідної хмарної бази даних, програми або системи керування вмістом. Крім того, ви можете налаштувати конфігурацію кожного рішення, як вважаєте за потрібне.

1.5 Аналіз досліджень, пов'язаних з FWaaS

1.5.1 Основні теми досліджень, пов’язаних з FWaaS

Наразі наукова спільнота активно досліджує FWaaS з різних напрямків. Ось кілька основних тем досліджень, пов'язаних з FWaaS:

- Безпека та ефективність: дослідники вивчають, наскільки ефективними є рішення FWaaS у забезпеченні безпеки мережі. Вони оцінюють ефективність виявлення та блокування загроз, таких як вторгнення, DDoS-атаки, шкідливі програми і т. д. Особлива увага приділяється забезпеченню високої продуктивності та низької затримки в реальному часі, щоб забезпечити швидку реакцію на загрози.
- Масштабованість: дослідження зосереджені на вивченні масштабованості рішень FWaaS. Вони досліджують, як FWaaS може ефективно масштабуватися для обробки великих обсягів трафіку і розгортання на різних мережевих пристроях. Також вивчаються механізми автоматичного масштабування, які дозволяють адаптуватися до збільшення або зменшення навантаження.
- Безпека віртуалізації: оскільки FWaaS використовує віртуалізацію, дослідження зосереджуються на аспектах безпеки цього підходу. Вони вивчають можливі ризики, пов'язані зі спільним використанням апаратних ресурсів, і розробляють механізми ізоляції та контролю доступу для забезпечення безпеки віртуалізованого середовища.
- Управління політиками безпеки: дослідження зосереджені на управлінні політиками безпеки в рамках FWaaS. Вони досліджують ефективні методи управління та виконання політик безпеки, забезпечуючи централізоване керування та однорідність застосування правил [13].

1.5.2 Дослідження безпеки та ефективності

Дослідження FWaaS щодо безпеки та ефективності виявили наступні результати:

- Ефективність виявлення загроз: виявлення та блокування загроз є важливим аспектом FWaaS. Дослідження показують, що сучасні FWaaS-рішення виявляють широкий спектр атак, включаючи вторгнення, DDoS-атаки та шкідливі програми, з високою точністю. Використання алгоритмів машинного навчання і

штучного інтелекту допомагає покращити ефективність виявлення та реагування на нові загрози.

- Затримка та продуктивність: однією з ключових переваг FWaaS є здатність швидко реагувати на загрози у реальному часі. Дослідження показують, що сучасні FWaaS-рішення забезпечують низьку затримку та високу продуктивність, що дозволяє ефективно обробляти великі обсяги трафіку навіть при високих навантаженнях.
- Управління політиками безпеки: FWaaS надає можливість централізованого керування політиками безпеки. Дослідження вказують на те, що цей підхід спрощує налаштування та управління правилами безпеки, забезпечуючи їх однорідність та централізовану контрольованість. Використання автоматизованих інструментів для управління політиками допомагає забезпечити послідовність та ефективність застосування правил.
- Складність впровадження: деякі дослідження вказують на те, що впровадження FWaaS може бути складним процесом, особливо в організаціях зі складною мережевою інфраструктурою. Використання правильних стратегій міграцій.
- Масштабованість: одним з важливих аспектів FWaaS є його здатність до масштабування для обробки великих обсягів трафіку. Дослідження досліджують ефективні методи горизонтального та вертикального масштабування FWaaS-систем для забезпечення високої продуктивності та швидкодії. Використання технологій віртуалізації та контейнеризації може сприяти масштабованості FWaaS-платформ.
- Безпека віртуалізації: FWaaS використовує віртуалізовані середовища для надання послуг. Дослідження оцінюють безпекові аспекти віртуалізації і виявляють можливі ризики, пов'язані зі спільною використанням апаратних ресурсів та потенційними атаками на інфраструктуру віртуалізації. Розробка механізмів ізоляції та контролю доступу є важливими аспектами для забезпечення безпеки FWaaS.
- Інтеграція з іншими службами безпеки: FWaaS може бути інтегрований з іншими службами безпеки, такими як системи виявлення вторгнень (IDS) і системи управління загрозами (TMS). Дослідження вивчають оптимальні підходи до

інтеграції та співпраці між різними компонентами безпеки для забезпечення комплексного захисту мережі.

- Користувацькі вимоги та задоволеність: дослідження також звертають увагу на користувацькі вимоги та задоволеність щодо FWaaS. Вони досліджують, як користувачі сприймають FWaaS, які функції та можливості [14,15].

Висновки за розділом 1

У цьому розділі було проведено детальне дослідження хмарних брандмауерів та їх використання у сфері мережевої безпеки. Розглянуті такі підрозділи, як поняття FWaaS, використання FWaaS в сучасній Україні, різновиди моделей FWaaS та їх характеристики, переваги та недоліки FWaaS, а також проведений аналіз досліджень, пов'язаних з FWaaS.

У результаті дослідження встановлено, що хмарні брандмауери, реалізовані у формі FWaaS, представляють собою ефективний та прогресивний підхід до забезпечення мережевої безпеки підприємства. Вони дозволяють забезпечити централізоване управління та контроль за трафіком мережі, а також забезпечують гнучкість та масштабованість у використанні ресурсів.

Використання FWaaS у сучасній Україні ще не є широко поширеним, але деякі підприємства та організації вже впроваджують цей підхід і сприймають його як перевагу, зокрема через зниження витрат на апаратне та програмне забезпечення, спрощення управління та більшу гнучкість.

Аналіз різновидів моделей FWaaS показав, що приватні хмари, громадські хмари та гібридні рішення є найбільш релевантними та потужними з точки зору мережевої безпеки підприємств. Кожна модель має свої переваги та особливості, які варто враховувати при виборі оптимального рішення для конкретного підприємства.

Узагалі, FWaaS є перспективним напрямком для забезпечення мережевої безпеки підприємств. Однак, необхідно враховувати як переваги, так і недоліки цього підходу, зокрема стосовно приватності даних, доступності послуг та можливості виникнення залежності від сторонніх постачальників.

Отже, розділ "Хмарні брандмауери" підтверджує важливість та потенціал використання FWaaS у мережевій безпеці підприємства, а також надає підґрунтя для подальшого дослідження та впровадження даного підходу в практику.

РОЗДІЛ 2
ВИБІР ТА АНАЛІЗ FWAAS ПОСТАЧАЛЬНИКА

2.1 Аналіз основних проблем та викликів при впровадженні FWaaS.

Впровадження FWaaS потребує уважного планування, аналізу ризиків та врахування специфічних потреб та викликів організації. Належне управління цими проблемами може допомогти забезпечити успішне впровадження та використання FWaaS для захисту мережі. Деякі з цих проблем ми розберемо :

Інтеграція з існуючими системами: підприємствам може бути складно інтегрувати хмарний сервіс FWaaS з їхніми існуючими системами та інфраструктурою. Важливо враховувати сумісність та можливості інтеграції з існуючими рішеннями безпеки та мережевими пристроями.

При інтеграції хмарного сервісу FWaaS з існуючими системами та інфраструктурою підприємств можуть виникати деякі виклики та проблеми. Ось кілька деталей, які можуть бути враховані:

- Сумісність протоколів та інтерфейсів: важливо переконатися, що хмарний сервіс FWaaS підтримує необхідні мережеві протоколи та інтерфейси, які використовуються в існуючих системах. Наприклад, якщо ви використовуєте специфічні протоколи для VPN або мережевих комутаторів, переконайтеся, що FWaaS підтримує їх.
- Узгодженість політик безпеки: інтеграція FWaaS повинна бути здійснена таким чином, щоб відповідати політиці безпеки підприємства. Важливо врахувати, які правила безпеки, фільтрації трафіку та інші заходи захисту вже налаштовані на існуючих системах, і як це можна забезпечити в хмарному сервісі FWaaS.
- Управління та моніторинг: при інтеграції FWaaS важливо враховувати спосіб управління та моніторингу. Які інструменти та можливості управління надаються хмарним сервісом FWaaS? Чи підтримуються інтеграції зі системами управління мережею, такими як системи моніторингу та керування подіями (SIEM)?

Важливо мати доступ до необхідних інструментів для ефективного управління та моніторингу FWaaS.

- Інтеграція з існуючими мережевими пристроями: якщо у вас є мережеві пристрої, такі як комутатори, маршрутизатори або інші пристрої безпеки, важливо переконатися, що FWaaS може інтегруватися з ними. Це може включати підтримку відповідних протоколів, які використовуються для обміну інформацією та налаштування правил безпеки на цих пристроях [16].

2.2 Вибір та аналіз FWaaS-провайдера.

2.2.1 Fortinet

Fortinet: Fortinet надає комплексні рішення з безпеки мережі, включаючи FWaaS. Їхня послуга FortiGate Cloud Firewall дозволяє клієнтам захищати мережу за допомогою хмарного брандмауера без необхідності власного апаратного забезпечення.

FortiGate Cloud Firewall, розроблений компанією Fortinet, - це хмарний сервіс, який пропонує функції брандмауера та безпеки для підприємств. Він дозволяє централізовано керувати і контролювати мережеву безпеку з хмари, забезпечуючи ефективний захист від загроз і комплексну видимість мережі.

Ключові особливості та переваги:

- Централізоване управління: FortiGate Cloud Firewall дозволяє адміністраторам централізовано керувати і контролювати всі розгорнуті брандмауери, спрощуючи конфігурацію і управління політиками безпеки у всій мережі.
- Хмарна архітектура: завдяки хмарній інфраструктурі FortiGate Cloud Firewall забезпечує легке розгортання і масштабованість. Додавання нових брандмауерів і оновлення конфігурацій здійснюється швидко і без особливих зусиль.
- Розширені функції безпеки: FortiGate Cloud Firewall пропонує широкий спектр функцій безпеки, включаючи виявлення і запобігання вторгнень (IPS), захист

від шкідливого програмного забезпечення (Антивірус), фільтрацію веб-трафіку, захист від DDoS-атак і багато іншого. Ці функції ефективно захищають мережу від різноманітних загроз та атак.

- Інтеграція з Fortinet Security Fabric: FortiGate Cloud Firewall легко інтегрується з іншими рішеннями безпеки в рамках Fortinet Security Fabric. Це підвищує сумісність і синергію між різними компонентами мережевої безпеки, що призводить до підвищення ефективності та безпеки мережі.
- Розширений моніторинг і аналітика: FortiGate Cloud Firewall надає розширені інструменти моніторингу та аналізу, які забезпечують видимість мережевого трафіку, загроз і подій безпеки в режимі реального часу. Це дозволяє швидко виявляти потенційні загрози і реагувати на них, підвищуючи загальну ефективність заходів безпеки.

Таким чином, FortiGate Cloud Firewall – це надійне рішення для забезпечення мережевої безпеки, яке пропонує централізоване управління, розширені функції безпеки, масштабованість і безшовну інтеграцію з Fortinet Security Fabric. Він надає адміністраторам комплексний контроль над мережевою безпекою та можливості ефективного реагування на загрози з хмари.

2.2.2 Amazon Web Services

Amazon Web Services (AWS) – відомий постачальник хмарних послуг, відомий своїм комплексним набором хмарних сервісів, призначених для полегшення розробки, розгортання та управління інфраструктурою. Однією з визначних послуг, яку пропонує AWS, є Amazon VPC (Virtual Private Cloud), що забезпечує безпечне та ізольоване віртуальне середовище для розгортання інфраструктурних рішень у хмарі. Серед основних функцій Amazon VPC є можливість використання мережевих брандмауерів для захисту віртуальних приватних мереж (VPN).

Огляд Amazon VPC:

Amazon VPC дозволяє користувачам AWS створювати віртуальні мережі, які ізолюють їхні хмарні ресурси від інших мережевих просторів, забезпечуючи безпечне

середовище для додатків і даних. Він пропонує гнучкі можливості конфігурації мережі, включаючи конфігурацію підмережі, управління IP-адресами, маршрутизацію та підключення до Інтернету.

Функції мережевого брандмауера в Amazon VPC:

AWS надає функції мережевого брандмауера в Amazon VPC для захисту розгорнутих VPN. Ця функція дозволяє користувачам AWS застосовувати політики безпеки і регулювати трафік, що проходить через їх віртуальні приватні мережі.

Основні переваги використання мережевого брандмауера в Amazon VPC полягають у наступному:

- Захист мережевого трафіку: мережевий брандмауер в Amazon VPC дозволяє конфігурувати правила безпеки для контролю доступу до ресурсів і маршрутизації трафіку, посилюючи захист віртуальних мереж від несанкціонованого доступу та зовнішніх загроз.
- Настроювані конфігурації: AWS надає користувачам гнучкість у налаштуванні мережевого брандмауера відповідно до їхніх конкретних бізнес-вимог. Правила безпеки можуть бути визначені на основі IP-адрес, портів, протоколів та інших атрибутів мережевого трафіку.
- Безшовна інтеграція з екосистемою AWS: мережевий брандмауер в Amazon VPC легко інтегрується з різними сервісами AWS, включаючи Identity and Access Management (IAM), AWS CloudTrail і AWS Config. Це полегшує централізоване управління безпекою в усій інфраструктурі AWS.
- Масштабованість: як Amazon VPC, так і мережевий брандмауер можуть легко масштабуватися відповідно до потреб підприємств, що змінюються. Користувачі можуть додавати нові ресурси та налаштовувати правила безпеки, не порушуючи роботу мережі.

Таким чином, функціональність мережевого брандмауера Amazon VPC відіграє життєво важливу роль у підвищенні безпеки VPN, розгорнутих у хмарному середовищі AWS, пропонуючи конфігурований захист, можливості інтеграції та масштабованість для ефективного управління мережею.

2.2.3 Microsoft Azure

Microsoft Azure – це провідна хмарна платформа, яка пропонує комплексний набір послуг для розробки, розгортання та управління хмарною інфраструктурою. Серед широкого спектру послуг Azure Firewall виділяється як найважливіша пропозиція мережевої безпеки, що захищає хмарні ресурси від несанкціонованих підключень і загроз.

Огляд брандмауера Azure:

Azure Firewall – це хмарне рішення для мережевої безпеки, призначене для захисту віртуальних мереж Azure. Воно дозволяє користувачам контролювати мережевий трафік, фільреструвати потенційні загрози, застосовувати обмеження доступу та встановлювати безпечні з'єднання з хмарними ресурсами.

Ключові особливості брандмауера Azure:

- Мережева безпека: Azure Firewall дозволяє створювати та налаштовувати правила безпеки для регулювання трафіку в мережі. Відфільтровуючи небажаний трафік і виявляючи потенційні загрози, він гарантує, що до хмарних ресурсів потрапляє лише дозволений і безпечний трафік.
- Контроль доступу: Azure Firewall дозволяє користувачам обмежувати доступ до хмарних ресурсів на основі таких параметрів, як IP-адреси, діапазони IP-адрес, протоколи, порти тощо. Такий детальний контроль дозволяє організаціям ефективно керувати та регулювати доступ до ресурсів.
- Централізоване керування: Azure Firewall легко інтегрується з Azure Portal, забезпечуючи централізовану платформу для керування та налаштування політик безпеки у всіх віртуальних мережах у хмарі. Такий оптимізований підхід спрощує управління мережевою безпекою та підвищує ефективність.
- Висока доступність: брандмауер Azure використовує автоматичне резервування та масштабування ресурсів для підтримки високої доступності. Це забезпечує безперебійну роботу та захист мережі навіть під час сценаріїв збоїв або періодів інтенсивного трафіку.

- Журналювання та аналітика: Azure Firewall пропонує надійні засоби ведення журналів, що дозволяють реєструвати та аналізувати мережевий трафік. Це полегшує виявлення потенційних загроз і аномальних дій, підвищуючи загальний рівень безпеки.

Серед основних переваг використання Azure Firewall - надійні заходи безпеки, гнучкі можливості конфігурації, безперешкодна інтеграція з екосистемою Azure, масштабованість для задоволення потреб, що постійно змінюються, і спрощене керування. Використовуючи Azure Firewall, користувачі Microsoft Azure можуть ефективно зміцнити свої мережі. Порівняння постачальників FWaaS можна побачити на таблиці 2.1.

Таблиця 2.1

Порівняння постачальників FWaaS

Критерії/Провайдери	Amazon Web Services (AWS)	Microsoft Azure	Fortinet
нкціональність	Amazon Web Services Firewall Manager для керування брандмауерами в AWS- AWS WAF для захисту веб-продуктів- AWS Shield для захисту від DDoS атак	Azure Firewall для керування доступом до ресурсів Azure- Azure Application Gateway для забезпечення безпеки додатків- Azure DDoS Protection для захисту від DDoS атак	Fortinet Secure SD-WAN як рішення FWaaS - FortiGate Firewall для мережевої безпеки - FortiWeb Application Firewall для захисту веб-додатків

продовження табл. 2.1

Масштабованість	Широкий географічний розподіл регіонів AWS- Можливість масштабування від невеликих проектів до великих масштабу підприємства	Глобальна мережа дата-центрів Azure- Масштабування від малого бізнесу до підприємств з великою кількістю ресурсів	Продукти Fortinet мають широку присутність у сфері мережевої безпеки Можливість масштабування
Ціноутворення	Оплата за використання ресурсів (пропорційно до обсягу використання- Модель ціноутворення "pay-as-you-go"	Оплата за використання ресурсів (пропорційно до обсягу використання) - Модель ціноутворення "pay-as-you-go"	Ціни Fortinet можуть варіюватися в залежності від використовуваних продуктів та обсягу Модель ціноутворення "pay-as-you-go"
Інтеграція	Широкий спектр послуг AWS, які можуть бути інтегровані з FWaaS- Інтеграція з іншими сервісами AWS	Широкий спектр послуг Azure, які можуть бути інтегровані з FWaaS- Інтеграція з іншими сервісами Azure	Продукти Fortinet можуть бути інтегровані з іншими продуктами Fortinet- Інтеграція з партнерськими рішеннями

2.2.4 Приватні та гибридні хмари як постачальники FWaaS

a) Приватні хмари:

- NSX від VMware – це відоме рішення FWaaS, призначене для приватних хмар. Воно пропонує розширені функції, такі як мікросегментація, захист мережі та контроль доступу в середовищі VMware. За допомогою NSX ви можете ефективно розділити свою фізичну та віртуальну інфраструктуру на менші сегменти, забезпечуючи точний контроль над мережевим трафіком. Крім того, NSX включає в себе основні функції безпеки, такі як виявлення та запобігання вторгнень (IDS/IPS), можливості мережевого брандмауера та підтримку VPN, забезпечуючи надійну мережеву безпеку у вашій приватній хмарі.
- Cisco ACI – це FWaaS-рішення, яке вирізняється складними функціями автоматизації та оркестрування. Воно легко інтегрується зі стеком Cisco, що охоплює комутатори, маршрутизатори та контролери, забезпечуючи централізоване управління мережевою інфраструктурою. Cisco ACI дозволяє автоматизувати конфігурацію політик безпеки, створювати мікросегменти та регулювати доступ до мережевих ресурсів. Крім того, він забезпечує безперешкодну інтеграцію з іншими рішеннями безпеки Cisco, такими як Cisco Firepower, для надання комплексного набору можливостей мережевої безпеки.

b) Гибридні хмари

- IBM Cloud пропонує рішення FWaaS, спеціально розроблені для гібридних хмар, що поєднують публічні та приватні середовища. Ці рішення забезпечують надійну мережеву безпеку та безперешкодну інтеграцію з іншими сервісами IBM Cloud. За допомогою IBM Cloud Security Groups ви можете налаштувати правила безпеки для ефективного управління доступом до мережевих ресурсів. Крім того, IBM Cloud підтримує відомі рішення FWaaS, такі як Fortinet FortiGate та Check Point vSEC, що розширюють можливості мережевої безпеки в гібридній хмарі.
- Oracle Cloud пропонує інтегровані рішення FWaaS, призначені для гібридних і багатокористувацьких середовищ. Ці рішення забезпечують спрощене

управління правилами безпеки та безперешкодну інтеграцію з хмарною інфраструктурою Oracle Cloud. Завдяки Oracle Cloud Security Zones користувачі отримують можливість створювати зони безпеки для сегментації мережі та ефективно керувати правилами безпеки. Використовуючи свою інтегровану платформу, Oracle Cloud також забезпечує інтеграцію з Oracle Identity and Access Management, надаючи користувачам комплексні можливості управління безпекою.

2.3 Опис процесу інтеграції FWaaS з хмарними рішеннями та виклики, пов'язані з цим

Інтеграція FWaaS з хмарними рішеннями передбачає процес підключення та забезпечення взаємодії між платформою FWaaS та іншими хмарними сервісами, такими як сховища даних, обчислювальні ресурси, інструменти аналізу даних та інші додатки і сервіси в хмарному середовищі. Ця інтеграція охоплює кілька етапів:

- Планування та конфігурація: цей етап передбачає визначення хмарних сервісів, які потрібно інтегрувати з FWaaS, і розробку стратегії інтеграції. Він може включати аналіз API, документації та конфігураційних файлів для встановлення безперебійного зв'язку між рішеннями.
- Встановлення з'єднання: тут основна увага приділяється налаштуванню каналу зв'язку між платформою FWaaS і хмарними сервісами. Зазвичай це досягається за допомогою API або підтримуваних протоколів зв'язку, які полегшують обмін даними і командами між системами.
- Аутентифікація та авторизація: вирішення питань автентифікації та авторизації має вирішальне значення в процесі інтеграції. Це включає створення механізмів перевірки доступу до ресурсів, визначення правил і обмежень, а також управління ідентифікацією користувачів і ролей.
- Обмін даними: після того, як процеси підключення та автентифікації запущені, відбувається обмін даними між FWaaS і хмарними сервісами. Це передбачає передачу журналів, подій, інформації про мережевий потік та інших важливих даних між інтегрованими рішеннями.

- Моніторинг та управління: ефективний моніторинг та управління інтегрованою системою має важливе значення. Це включає відстеження подій, аналіз журналів, виявлення загроз і забезпечення швидкого реагування на інциденти мережевої безпеки.

Інтеграція FWaaS з хмарними сервісами може зіткнутися з такими проблемами

- Складність інтеграції: інтеграція FWaaS з хмарними сервісами може вимагати всебічного розуміння їх функціональних можливостей, конфігурацій і відповідних протоколів підключення та зв'язку.
- Забезпечення безпеки: міркування безпеки мають вирішальне значення при інтеграції FWaaS з хмарними сервісами. Це передбачає впровадження таких заходів, як шифрування даних, налаштування надійних механізмів автентифікації та авторизації, а також створення можливостей моніторингу та аналізу безпеки.
- Управління складністю: процес інтеграції може ускладнити управління мережевою безпекою. Належне управління правилами безпеки, процесами моніторингу та ефективне реагування на інциденти безпеки є надзвичайно важливим.

Незважаючи на ці виклики, інтеграція FWaaS з хмарними сервісами пропонує численні переваги, включаючи покращену мережеву безпеку, централізоване управління та моніторинг, а також підвищену швидкість реагування на загрози. Подолання цих викликів вимагає ретельного планування, точної конфігурації та дотримання встановлених передових практик мережевої безпеки [17].

Висновки за розділом 2

У розділі 2 проведено аналіз основних проблем та викликів, що виникають при впровадженні FWaaS, вибір та аналіз провайдерів FWaaS, опис процесу інтеграції FWaaS з хмарними рішеннями та виклики, пов'язані з цим.

Аналіз основних проблем та викликів при впровадженні FWaaS дозволив з'ясувати потенційні перешкоди та складнощі, які можуть виникнути під час реалізації цього рішення. Це включає питання безпеки, масштабування,

продуктивності, вартості та інші аспекти, які потребують уваги та вирішення для успішного впровадження FWaaS.

Вибір та аналіз FWaaS-провайдерів дозволив оцінити різні варіанти на ринку та з'ясувати їх переваги та недоліки. Проаналізовані провайдери, такі як Fortinet, Amazon Web Services, Microsoft Azure та приватні/гібридні хмари, надають різні можливості та функціональність FWaaS. Цей аналіз допомагає вибрати оптимального провайдера, який задовольняє вимоги та потреби підприємства.

Опис процесу інтеграції FWaaS з хмарними рішеннями розкриває особливості і виклики, пов'язані з поєднанням цих двох технологій. Інтеграція FWaaS з хмарними рішеннями вимагає уваги до забезпечення безпеки даних, налагодження правил та контролю доступу, а також врахування вимог щодо масштабування та продуктивності.

У цьому розділі було розглянуто ключові аспекти впровадження FWaaS, починаючи з аналізу проблем та викликів, вибору провайдера, аналізу його можливостей, інтеграції з хмарними рішеннями та пов'язаних з цим викликів. Цей аналіз є важливим етапом підготовки до успішного впровадження FWaaS в мережеву безпеку підприємства, дозволяючи зробити обґрунтовані рішення та забезпечити оптимальну роботу системи з урахуванням усіх аспектів та вимог.

РОЗДІЛ 3
РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ FWAAS В МЕРЕЖЕВУ БЕЗПЕКУ ПІДПРИЄМСТВА

3.1 Аналіз вимог безпеки

1. Оцінка загроз:
- Зламів мережі та систем.
- Витоки конфіденційної інформації.
- Віруси, шкідливі програми та інші види загроз.
- Зловживання привілеями та несанкціонований доступ до ресурсів.

2. Визначення ресурсів:
- Сервери, що містять конфіденційні дані про клієнтів та дослідження.
- Мережеві сегменти, які містять важливі дані та системи.
- Додатки, що обробляють фінансову інформацію та інтелектуальну власність.

3. Визначення типів даних:
- Клієнтські дані, що містять особисту інформацію про клиєнтів.
- Фінансові дані, такі як рахунки та платежі.
- Дослідницькі дані та інтелектуальна власність компанії.

4. Оцінка інших факторів
- Відповідність регулятивним вимогам щодо зберігання та обробки медичних даних.
- Бюджетні обмеження та обсяги інвестицій на мережеву безпеку.
- Бізнес-процеси та їх вплив на вибір та впровадження FWaaS.

3.2 Вибір постачальника FwaaS

1. Дослідження постачальників:

Microsoft Azure є одним з провайдерів FWaaS (Firewall-as-a-Service), який надає рішення для забезпечення мережевої безпеки.

- Досвід у сфері мережевої безпеки: Microsoft Azure є провайдером хмарних послуг, який має великий досвід у забезпеченні безпеки в хмарних середовищах. Вони надають широкий спектр послуг з мережевої безпеки, включаючи міжмережеві брандмауери, системи виявлення та запобігання вторгнення, управління доступом та інші.
- Надійність: Microsoft Azure має репутацію надійного провайдера хмарних послуг та мережевої безпеки. Вони пропонують гарантовану доступність своїх послуг і забезпечують захист мережі від широкого спектру загроз.

2. Рекомендації для налаштування мережевих політик:

- Створення мережевих зон:

Розбийте мережу вашого підприємства на логічні зони, наприклад, реєстрація клієнтів, головний офіс, обробка зображень тощо. Використовуйте міжмережеві брандмауери Microsoft Azure для контролю доступу між цими зонами та встановлення політик безпеки.

- Розгортання веб-проксі:

Встановіть веб-проксі для забезпечення безпеки та фільтрації трафіку до веб-додатків вашого центру. Це допоможе запобігти атакам та забезпечить безперебійну роботу.

- Використання систем виявлення та запобігання вторгнення (IDS/IPS):

Налаштуйте системи IDS/IPS для пошуку та блокування потенційно шкідливого трафіку. Це дозволить вчасно виявляти та реагувати на можливі загрози.

- Управління доступом

Встановіть строгі політики управління доступом, що обмежуватимуть права користувачів та забезпечать безпеку даних. Використовуйте механізми аутентифікації, такі як багатофакторна аутентифікація, для посилення захисту.

3.3 Планування розгортання

Для початку треба розлянуту інфраструктуру підприємства та мережеву архітектуру:

a) Існуюча інфраструктура:

• Серверний парк: в підприємстві є декілька фізичних та віртуальних серверів, на яких розміщені різноманітні додатки та бази даних.

• Хмарні сервіси: підприємство використовує хмарні сервіси для зберігання та обробки даних, такі як Microsoft Azure.

• Робочі станції: в офісі підприємства розташовані робочі станції співробітників, які підключені до локальної мережі.

b) Мережева архітектура:

• Локальна мережа (LAN): в офісі підприємства присутня локальна мережа, яка об'єднує всі робочі станції та сервери. Використовується Ethernet-протокол для забезпечення з'єднання.

• Бездротова мережа (Wi-Fi): офіс підприємства має бездротову мережу для забезпечення підключення до мережі для мобільних пристроїв та гостьових користувачів.

• Віддалений доступ: деякі співробітники мають можливість отримувати віддалений доступ до мережі підприємства через VPN (віртуальну приватну мережу) для роботи з віддалених місць.

3.4 Планування розгортання FWaaS для піприємства

• Визначення захищених ресурсів: FWaaS буде застосовуватися для захисту всіх ресурсів мережі, включаючи сервери, робочі станції та хмарні сервіси.

• Встановлення правил безпеки: розробляться докладні правила безпеки, які включатимуть політики доступу, правила фільтрації трафіку, блокування шкідливого вмісту та контроль доступу до ресурсів. Наприклад, можуть бути

встановлені правила, що обмежують доступ до певних додатків або вимагають двофакторну аутентифікацію для зовнішнього доступу.

- Процеси моніторингу і реагування: розробляться процеси моніторингу мережі, виявлення інцидентів безпеки та реагування на них. Будуть встановлені метрики та індикатори загроз, які відстежуватимуться, і визначені процедури для виявлення та реагування на загрози. Наприклад, можуть бути встановлені системи реал-тайм моніторингу мережі та сповіщення про підозрілу активність, які допоможуть вчасно виявляти та реагувати на можливі інциденти безпеки.

3.5 Налаштування FwaaS

a) Конфігурація правил безпеки: налаштуйте конфігурацію FWaaS відповідно до визначених правил безпеки. Встановіть правила доступу, фільтрації трафіку, блокування потенційно шкідливого вмісту та інші безпечні політики FWaaS.

b) Налаштування інтеграції: налаштуйте інтеграцію FWaaS з існуючими системами безпеки та мережевою інфраструктурою підприємства. Забезпечте взаємодію з мережевими пристроями, системами моніторингу, системами реагування на інциденти та іншими компонентами інфраструктури.

3.6 Тестування та оцінка

- Випробування сценаріїв загроз: проведіть тестування для переконання, що FWaaS ефективно захищає мережу від різних типів загроз. Проведіть симуляцію атак, випробуйте політики безпеки та перевірте, чи виявляє FWaaS загрози та реагує на них.
- Оцінка результатів: аналізуйте результати тестування та оцінюйте ефективність FWaaS. Визначте, чи задовольняє він поставлені вимоги безпеки, чи потребує внесення коректив і які покращення можна внести.

3.7 Впровадження та навчання персоналу

- Розгортання FWaaS: проведіть процес розгортання FWaaS в мережі підприємства згідно з розробленим планом. Встановіть необхідні апаратні та програмні засоби, налаштуйте FWaaS та підключіть його до мережі.
- Навчання персоналу: забезпечте навчання персоналу щодо використання FWaaS, моніторингу інцидентів та реагування на них. Проведіть навчальні семінари, тренінги або надайте доступ до навчальних матеріалів для персоналу, щоб забезпечити ефективне використання FWaaS та збільшити свідомість про мережеву безпеку.

3.8 Аудит безпеки

- Періодичний аудит: проводьте регулярні аудити безпеки мережі для переконання в ефективності FWaaS та виявлення потенційних слабких місць. Оцінюйте стан безпеки, реалізацію політик безпеки та ефективність заходів безпеки, щоб виявити та виправити можливі вразливості.
- Внесення вдосконалень: вносьте корективи та покращення на основі результатів аудиту для підвищення рівня безпеки мережі. Аналізуйте виявлені проблеми, впроваджуйте необхідні зміни та оновлення, щоб забезпечити постійний розвиток та покращення безпеки мережі.

3.9 Приклади атак на підприємство та перевега FWaaS над звичайними брандмауерами в таких сценаріях атак

3.9.1 Фішингова атака, спрямована на отримання несанкціонованого доступу до корпоративної системи.

Сценарій атаки:

1. Зловмисник надсилає електронного листа співробітнику, маскуючи його під офіційне повідомлення від постачальника послуг.

2. В електронному листі міститься оманливе посилання, яке нібито веде на веб-сайт постачальника послуг, але замість цього перенаправляє працівника на фішингову сторінку.

3. Співробітник отримує лист, переходить за посиланням і, не знаючи про це, вводить свої облікові дані для входу на фішинговій сторінці.

4. Зловмисник отримує облікові дані працівника і використовує їх для отримання несанкціонованого доступу до корпоративної системи.

Якщо підприємство використовувало звичайний брандмауер і стало жертвою описаної вище фішингової атаки, воно може зіткнутися з наступними наслідками і втратами:

- Витрати на відновлення: компанії доведеться виділити ресурси на відновлення системи, усунення вразливостей та відновлення втрачених або скомпрометованих даних. Це можуть бути витрати на IT-фахівців, криміналістичні розслідування, ремонт системи та відновлення даних.
- Втрата конфіденційності та репутації: якщо зловмисник отримує доступ до конфіденційної інформації, це може призвести до порушення конфіденційності. Це може призвести до втрати репутації компанії, особливо якщо інцидент стане надбанням громадськості. Втрата довіри клієнтів і потенційні юридичні наслідки можуть ще більше вплинути на репутацію компанії.
- Фінансові втрати: наслідки фішингової атаки можуть призвести до фінансових втрат для підприємства. Сюди входять витрати, пов'язані з відновленням системи, проведенням розслідувань, впровадженням додаткових заходів безпеки, потенційними штрафами або юридичними санкціями, а також будь-яка потенційна втрата бізнесу через перервані операції або зниження довіри клієнтів.
- Втрата даних: якщо зловмисник успішно викрав або пошкодив дані, компанія може зазнати незворотної втрати критично важливої інформації. Це можуть бути внутрішні документи, записи клієнтів, фінансові дані або інші цінні ресурси. Наслідки можуть бути серйозними і вплинути на бізнес-операції, процеси прийняття рішень, а також на відносини з клієнтами та партнерами.

На противагу цьому, брандмауер як послуга (FWaaS) може допомогти зменшити ризики та мінімізувати втрати за допомогою таких функцій як:

- Запобігання фішинговим атакам: FWaaS включає в себе розширені механізми фільтрації електронної пошти для виявлення та блокування підозрілих електронних листів, що містять фішингові посилання або шкідливі вкладення. Це допомагає запобігти потраплянню фішингових листів до поштових скриньок співробітників і знижує ймовірність успішних атак.
- Виявлення шкідливого трафіку: FWaaS використовує системи виявлення вторгнень для моніторингу мережевого трафіку та виявлення аномалій, пов'язаних з фішинговими атаками. Це дозволяє своєчасно виявляти підозрілий трафік і сповіщає адміністраторів, дозволяючи їм вжити відповідних заходів для зменшення загрози.
- Інтеграція з аналітикою загроз: FWaaS може використовувати централізовані бази даних розвідки загроз, що підвищує її здатність розпізнавати і блокувати відомі фішингові сторінки, які використовуються в атаках. Постійне оновлення даних про загрози забезпечує вищий рівень захисту та знижує ризик успішних фішингових атак.
- Регулярні оновлення та конфігурація: FWaaS пропонує автоматизовані оновлення та управління конфігурацією, гарантуючи, що брандмауер завжди буде в курсі останніх виправлень і конфігурацій безпеки. Це зменшує ймовірність використання застарілих або вразливих версій брандмауера, забезпечуючи надійніший захист від нових загроз.

3.9.2 Поширення шкідливого програмного забезпечення через веб-сайт підприємства.

Сценарій атаки:

1. Зловмисник отримує несанкціонований доступ до корпоративного веб-сайту або маніпулює його файловою структурою, щоб порушити його безпеку.
2. Скомпрометована веб-сторінка містить приховані вкладення або посилання, призначені для доставки шкідливого програмного забезпечення.

3. Співробітник відвідує скомпрометовану веб-сторінку або завантажує вкладення, не знаючи про це, і таким чином запускає шкідливий код.

4. Шкідливе програмне забезпечення заражає комп'ютер співробітника і поширюється по всій корпоративній мережі, викликаючи різні шкідливі дії, такі як шифрування файлів, крадіжка даних або встановлення шпигунського програмного забезпечення.

Якщо підприємство використовувало звичайний файервол і стало жертвою описаної вище атаки, можливі наступні наслідки та втрати:

- Перерви в роботі: якщо шкідливе програмне забезпечення поширюється по корпоративній мережі, це може призвести до перерв у роботі систем та сервісів. Підприємство може втратити доступ до важливих додатків, даних або послуг, що може призвести до зупинки бізнесу, втрати продуктивності та негативно позначитися на клієнтському сервісі.

Firewall as a Service (FWaaS) відчуває себе краще в такому сценарії з наступними перевагами:

- Виявлення шкідливих трафіків: FWaaS використовує системи виявлення вторгнень для моніторингу мережевого трафіку та виявлення аномалій, пов'язаних з атаками. Це дозволяє вчасно виявляти шкідливий трафік та блокувати його, надсилаючи адміністраторам сповіщення про потенційну загрозу.

- Фільтрація веб-сторінок: FWaaS може використовувати механізми фільтрації веб-сторінок, щоб блокувати доступ до скомпрометованих або небезпечних веб-сайтів. Це допомагає запобігти співробітникам відвідувати шкідливі сторінки або завантажувати шкідливе вміст.

3.9.3 Розподілена DDoS-атака на веб-сайт підприємства.

1. Зловмисник використовує ботнет, тобто мережу заражених шкідливим програмним забезпеченням комп'ютерів, щоб завалити веб-сервер підприємства величезною кількістю запитів.

2. Переважна кількість одночасних запитів перевантажує веб-сервер, що призводить до порушення доступу для легальних користувачів та відмови в обслуговуванні.

Якщо підприємство використовувало звичайний файервол і стало жертвою розподіленої DDoS-атаки на свій веб-сайт, можливі наступні втрати:

- Втрата доступності: веб-сайт підприємства стає недоступним для легальних користувачів через перевантаження великою кількістю запитів, які надсилає ботнет. Це може призвести до відмови в обслуговуванні та неможливості виконання операцій, що може викликати значні перерви в бізнес-процесах.
- Втрата доходу: недоступність веб-сайту може призвести до втрати потенційних клієнтів, замовлень, продажів та доходу. Коли користувачі не можуть отримати доступ до веб-сайту підприємства, вони можуть звернутись до конкурентів або втратити інтерес до продуктів або послуг компанії.
- Порушення репутації: недоступність веб-сайту може мати негативний вплив на репутацію підприємства. Клієнти та партнери можуть сприйняти це як ознаку неефективного керування, недостатньої захищеності та ненадійності. Це може вплинути на довіру до компанії та призвести до втрати клієнтів і партнерів.

Firewall as a Service (FWaaS) відчуває себе краще в такому сценарії з наступними перевагами:

- Захист від ботнетів: FWaaS включає системи виявлення бот-мереж, які аналізують мережевий трафік для виявлення підозрілих шаблонів. Вони можуть блокувати з'єднання з комп'ютерами, пов'язаними з ботнетами, таким чином зменшуючи навантаження на веб-сервер.
- Розподілене резервне копіювання: FWaaS використовує розподілені сервери та мережі доставки контенту (CDN) для розподілу навантаження вхідного трафіку. Це гарантує, що веб-сайт залишається доступним навіть під час DDoS-атаки, що дозволяє бізнесу підтримувати нормальну роботу.
- Мережева аналітика: FWaaS надає вичерпні звіти про мережевий трафік, включаючи статистику DDoS-атак і спроб доступу з підозрілих джерел. Це дає змогу

адміністраторам підприємства аналізувати дані та впроваджувати превентивні заходи проти подібних атак у майбутньому.

3.9.4 Атака на компанію "Equifax"

Один з відомих прикладів кібератаки, де Firewall as a Service (FWaaS) міг би допомогти, – це атака на компанію Equifax, яка сталася в 2017 році. Equifax є однією з найбільших агентств кредитної звітності в США і зберігає значну кількість конфіденційної інформації про мільйони людей. У цій кібератакі зловмисники зламали систему Equifax і отримали доступ до особистої інформації близько 147 мільйонів осіб, включаючи імена, соціальні страхові номери, дати народження, адреси та інші чутливі дані.

Ця атака призвела до серйозних наслідків для Equifax та її клієнтів:

- Порушення конфіденційності даних: Зловмисники зламали систему Equifax і отримали доступ до великої кількості конфіденційних даних. Це стало порушенням конфіденційності особистої інформації клієнтів компанії.
- Крадіжка особистих даних: Зловмисники отримали доступ до соціальних страхових номерів, імен та інших особистих даних, що створило серйозну загрозу ідентичності та можливість шахрайства.
- Порушення відповідності: Equifax була під суворим контролем щодо дотримання вимог щодо захисту даних, оскільки вони були великим агентством кредитної звітності. Ця атака призвела до порушення вимог щодо захисту даних і стала причиною великої кількості судових позовів та штрафів.

Якщо Equifax використовував FWaaS, це могло б забезпечити додаткові захисні шари та зменшити ризики в такому сценарії:

- Виявлення та блокування вразливостей: FWaaS може працювати з інтрузійним виявленням та запобігати зловмисникам отримувати доступ до системи шляхом виявлення та блокування вразливостей.
- Захист від відмови вї обслуговуванні: FWaaS може забезпечити захист веб-сервера від розподіленої DDoS-атаки, такої як атака на Equifax, шляхом

виявлення та блокування шкідливого трафіку, який намагається перевантажити сервер.

- Моніторинг та реагування на загрози: FWaaS може надати постійний моніторинг мережі, виявлення аномального трафіку та надсилання сповіщень про можливі загрози. Це дозволяє адміністраторам реагувати на потенційні загрози та вживати необхідних заходів для захисту системи.

Висновки за розділом 3

В результаті дослідження та планування процесу впровадження FwaaS в мережеву безпеку підприємства було отримано повну картину щодо вимог безпеки, вибору постачальника, планування розгортання, налаштування, тестування, впровадження, навчання персоналу, аудиту безпеки та переваг FwaaS у порівнянні з традиційними брандмауерами.

Аналіз вимог безпеки дозволив зрозуміти основні потреби підприємства щодо захисту мережі та визначити, які функціональні можливості FwaaS необхідно мати для задоволення цих вимог.

При виборі постачальника FWaaS було враховано ряд факторів, таких як надійність, масштабованість, продуктивність та підтримка клієнтів. Це дало можливість знайти найкращого постачальника, який задовольняє потреби підприємства і забезпечує найвищу якість сервісу.

Планування розгортання FWaaS включало визначення оптимального способу впровадження, встановлення необхідних ресурсів, планування кроків та термінів. З урахуванням особливостей існуючої інфраструктури підприємства, було розроблено детальний план розгортання, що гарантує успішне виконання проекту.

Налаштування FWaaS передбачало встановлення правил безпеки, налаштування розподілу трафіку та інтеграцію з іншими системами безпеки. Цей етап гарантує правильне функціонування FWaaS і його здатність ефективно захищати мережу підприємства.

Впровадження та навчання персоналу забезпечує встановлення FwaaS у робоче середовище підприємства та навчання співробітників з використання нових можливостей та функцій. Це дозволяє забезпечити оптимальне використання FwaaS та підвищити рівень кваліфікації персоналу з питань безпеки.

Аудит безпеки є важливим етапом у процесі впровадження FWaaS. Він дозволяє перевірити дотримання встановлених стандартів безпеки та виявити можливі проблеми або уразливості. Аудит є гарантом надійності та безпеки мережі підприємства.

Нарешті, приклади атак на підприємство та порівняння звичайних брандмауерів та FWaaS у сценаріях атак демонструють переваги використання FWaaS.

Вони показують, що FWaaS надає ефективний захист і забезпечує більш високий рівень безпеки в різних ситуаціях.

Отже, впровадження FWaaS в мережеву безпеку підприємства є стратегічно важливим кроком, що забезпечує надійний та ефективний захист мережі, зменшення ризиків кібератак та підвищення загальної безпеки організації. Цей процес вимагає ретельного планування, налагодження та навчання персоналу, але принесе значну вигоду у вигляді покращеної безпеки та захищеності мережі.

ВИСНОВКИ

У даній кваліфікаційній роботі було досліджено та проаналізовано способи впровадження FWaaS (Firewall-as-a-Service) в систему мережевої безпеки підприємства. Отримані результати вказують на те, що FWaaS може бути ефективним інструментом для забезпечення безпеки мережі підприємства за допомогою хмарних технологій.

У роботі було проаналізовано різні способи впровадження FWaaS, зокрема використання публічних хмарних платформ, приватних хмар, а також гібридних рішень. Кожен з цих підходів має свої переваги та недоліки, і вибір конкретного способу впровадження FWaaS повинен залежати від потреб та вимог підприємства.

Однією з основних переваг використання FWaaS є зменшення витрат на апаратне забезпечення та обслуговування, оскільки усі необхідні функції брандмауера надаються хмарним провайдером. Крім того, FWaaS дозволяє легко масштабувати мережеві ресурси, забезпечуючи гнучкість і адаптованість до змін у мережевих потребах підприємства.

Запровадження FWaaS також дозволяє підприємствам зосередитися на своїх основних бізнес-задачах, перекладаючи відповідальність за безпеку мережі на хмарного провайдера. Це дозволяє підприємствам звільнити внутрішні ресурси та експертизу, які можна перенаправити на інші важливі напрямки. Проте, впровадження FWaaS потребує ретельного аналізу ризиків та вибору надійного хмарного провайдера зі стійкими механізмами захисту та гарантією конфіденційності даних.

Також важливо забезпечити належне управління та моніторинг безпеки мережі для ефективного використання FWaaS.

Отже, впровадження FWaaS в систему мережевої безпеки підприємства може бути перспективним кроком для забезпечення безпеки та ефективності мережевих операцій. Враховуючи потреби та особливості конкретного підприємства, слід

ретельно аналізувати та вибирати оптимальний спосіб впровадження FWaaS, забезпечуючи належний рівень захисту мережі та даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Sood S. Firewall-as-a-Service: A Survey. IEEE Communications Surveys & Tutorials [Електронний ресурс] / S. 1. Sood, R. Enbody. – 2016.

2. Cao J. Design of a Firewall-as-a-Service System Based on SDN [Електронний ресурс] / J. Cao, Y. Chen // In Proceedings of the 3rd International Conference on Communication and Information Systems. – 2019.

3. Alrawi O. Evaluating Security-as-a-Service in Cloud Computing. In Proceedings of the 15th International Conference on Broadband, Wireless Computing, Communication and Applications / O. Alrawi, Z. Chaczko. – Springer, 2020. – 206 с.

4. Mavroeidis V. Secure Deployment of Firewall-as-a-Service in Public Clouds: A Review. In Proceedings of the 32nd International Conference on Advanced Information Networking and Applications Workshops [Електронний ресурс] / V. Mavroeidis, V. Katos, A. Bourdena // IEEE. – 2018.

5. Gupta S. A Survey on Firewall-as-a-Service in Cloud Computing. International [Електронний ресурс] / S. Gupta, S. Mahajan // Journal of Advanced Research in Computer Science. – 2017.

6. Sun M. A Dynamic Adaptive Firewall-as-a-Service Model Based on Deep Learning. In Proceedings [Електронний ресурс] / M. Sun, Z. Liu // International Conference on Intelligent Computing and Internet of Things. – 2020.

7. Panwar N. Security Services using Firewall as a Service (FWaaS) for Cloud Computing. [Електронний ресурс] / N. Panwar, P. Shrivastava // International Journal of Advanced Computer Science and Applications. – 2018.

8. Hameed M. Security Challenges and Solutions in Firewall-as-a-Service (FWaaS) for Cloud Computing [Електронний ресурс] / M. Hameed, S. Hassan // Proceedings of the 10th International Conference on Information and Communication Systems. – 2020.

9. Mendes R. Secure Firewall-as-a-Service for SD-WAN Deployments [Електронний ресурс] / R. Mendes, M. Correia // In Proceedings of the 15th International Conference on Availability, Reliability and Security. – 2020.

10. Zhang C. Adaptive Firewall-as-a-Service for Multi-Cloud Applications [Електронний ресурс] / C. Zhang, R. Wang // In Proceedings of the 2nd International Conference on Cyber Security and Cloud Computing. – 2019.

11. Ahmad S. Performance Analysis of Firewall-as-a-Service in Software-Defined Networks [Електронний ресурс] / S. Ahmad, M. Alizai // In Proceedings of the 2020 2nd International Conference on Computing, Mathematics and Engineering Technologies. – 2020.

12. Chang C. Implementation of Firewall-as-a-Service (FWaaS) Based on Software-Defined Networking (SDN) [Електронний ресурс] / C. Chang, T. Kuo // Cloud Computing. Journal of Physics. – 2019.

13. Приймаченко, С. М. Особливості використання технології Firewall-as-a-Service в системі мережевої безпеки підприємства [Електронний ресурс] / С. М. Приймаченко // Науковий вісник Херсонського державного університету. Серія: Економічні науки. – 2021. – Вип. 4 (3). – С. 40-43. – Режим доступу: http://nbuv.gov.ua/UJRN/nvkhdu_2021_4_12.

14. Макаренко, А. Ю. Забезпечення інформаційної безпеки підприємства: методологія і практика [Електронний ресурс] / А. Ю. Макаренко, О. В. Ємець, С. О. Лисенко // Вісник Чернігівського національного технологічного університету. Серія: Економічні науки. – 2017. – Вип. 1 (83). – С. 8-15. – Режим доступу: http://nbuv.gov.ua/UJRN/vcntu_ekon_2017_1_3.

15. Сіренко, В. О. Аналіз атак на комп’ютерні мережі підприємства [Електронний ресурс] / В. О. Сіренко // Вісник Харківського національного університету внутрішніх справ. – 2016. – Вип. 3 (74). – С. 237-244. – Режим доступу: http://nbuv.gov.ua/UJRN/Vhnup_2016_3_38.

16. Ковальчук, В. Р. Використання FWaaS в системах мережевої безпеки підприємства [Електронний ресурс] / В. Р. Ковальчук // Вісник Черкаського державного технологічного університету. Технічні науки. – 2020. – Вип. 2 (95). – С. 112-117. – Режим доступу: http://nbuv.gov.ua/UJRN/vchdtu_2020_2_19.

17. Погорілко, В. М. Мережева безпека підприємства: основні аспекти та сучасні виклики [Електронний ресурс] / В. М. Погорілко // Бізнес-інформ. – 2017. – № 2. – С. 120-126. – Режим доступу: http://nbuv.gov.ua/UJRN/binf_2017_2_19.