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

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Захищена хмарна інфраструктура організації на базі FortigateVM»

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

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

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

_____
(підпис)

Виконав: здобувач вищої освіти групи:
Штагер Богдан
(прізвище, ім'я)

Керівник д. т. н., професор, Кожухівський А.Д.
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

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

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Бакалавр
Спеціальність 125 Кібербезпека
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
«___» _____ 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Штагер Богдан
(прізвище, ім'я)

1. Тема кваліфікаційної роботи:
Захищена хмарна інфраструктура організації на базі FortigateVM

керівник кваліфікаційної роботи Кожухівський Андрій, д.т.н., професор
(прізвище, ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» _____ 2025 року № ____.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 06.06.2025 р.

3. Вихідні дані до кваліфікаційної роботи: У межах даної кваліфікаційної роботи здійснюється розробка, налаштування та аналіз захищеної хмарної інфраструктури з використанням FortigateVM, що має забезпечити конфіденційність, цілісність та доступність даних в умовах сучасних кіберзагроз. Об'єктом дослідження є інформаційна інфраструктура організації, розгорнута у хмарному середовищі, а предметом — механізми забезпечення її кібербезпеки на основі засобів FortigateVM. У ході роботи вирішуються такі завдання: аналізуються актуальні загрози для

хмарних середовищ та обґрунтовується потреба впровадження спеціалізованих засобів захисту; вивчається функціонал FortigateVM як платформи мережевої безпеки; виконується розгортання FortigateVM у віртуалізованому середовищі з подальшим налаштуванням політик безпеки; реалізується інтеграція системи із хмарною мережею для забезпечення фільтрації трафіку, захисту VPN-каналів і виявлення загроз; розробляються практичні рекомендації щодо захисту кінцевих точок і побудови масштабованої інфраструктури.

4. Дата видачі завдання 28.02.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми захисту кінцевих точок організації.	03.03.2025 р.	
2.	Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи.	15.03.2025 р.	
3.	Аналіз методів та засобів захисту кінцевих точок організації на базі FortiEDR.	10.04.2025 р.	
4.	Практична реалізація варіанту захисту кінцевих точок організації на базі FortiEDR.	12.05.2025 р.	
5.	Розроблення рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.	18.05.2025 р.	
6.	Оформлення результатів дослідження.	20.05.2025 р.	
7.	Підготовка доповіді до захисту.	06.06.2025 р.	

Здобувач вищої освіти _____ Богдан Штагер
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій Кожухівський
(підпис)

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача Штагера Богдана
на тему: «Захищена хмарна інфраструктура організації на базі FortigateVM»

Актуальність:

Позитивні сторони:
1.
2.
3.
4.

Недоліки:
1.
2.

Висновок:

Рецензент:

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

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

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

на здобуття освітнього ступеня бакалавра

Направляється здобувач Штагер Богдан до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Захищена хмарна інфраструктура організації на базі FortigateVM».

Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувач Штагер Богдан обрав тему роботи, метою якої було дослідити методи та засоби захисту кінцевих точок організації та розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи Штагер Богдан показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Штагера Богдана на оцінку **"_____"** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Андрій Кожухівський
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Штагер Богдан допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

_____ Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 62 сторінок, 19 рисунків, 3 таблиці, 47 джерел.

Об'єкт дослідження – хмарна інфраструктура організації.

Предмет дослідження – засоби та методи захисту хмарної інфраструктури на базі FortigateVM.

Мета роботи – розробити архітектуру захищеної хмарної інфраструктури з використанням FortigateVM та надати практичні рекомендації щодо її впровадження в умовах сучасних кіберзагроз.

Методи дослідження – аналіз сучасних загроз інформаційній безпеці, опрацювання спеціалізованої літератури, документації Fortinet, вивчення стандартів безпеки, моделювання хмарної інфраструктури з FortigateVM, практичне тестування.

Хмарні середовища активно використовуються в корпоративному секторі, однак з їх популярністю зростає й кількість загроз інформаційній безпеці. Без належного захисту хмарна інфраструктура стає вразливою до атак ззовні та зсередини. У роботі проаналізовано типові загрози безпеці хмарних обчислень, сформульовано принципи побудови захищеної хмарної інфраструктури. Проведено огляд сучасних інструментів захисту та глибоке дослідження можливостей FortigateVM – віртуального міжмережевого екрана, що поєднує функціонал фільтрації трафіку, антивірусного захисту, VPN, IPS/IDS та веб-фільтрації. У практичній частині представлено проект захищеної хмарної мережевої інфраструктури з інтеграцією FortigateVM у середовищі віртуалізації. Проведено налаштування політик безпеки, реалізовано VPN-з'єднання, фільтрацію

трафіку та інші засоби кіберзахисту. На основі досліджень розроблено практичні рекомендації щодо проєктування та впровадження захищеної хмарної інфраструктури із застосуванням FortigateVM.

Галузь використання – побудова безпечних хмарних рішень для захисту корпоративних інформаційних ресурсів.

ХМАРНА ІНФРАСТРУКТУРА, FORTIGATEVM, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРЗАГРОЗИ, ВІРТУАЛІЗАЦІЯ, VPN, ПОЛІТИКИ БЕЗПЕКИ, МІЖМЕРЕЖЕВИЙ ЕКРАН.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VM – віртуальна машина, програмна імітація фізичного комп’ютера.

VLAN – віртуальна локальна мережа, яка дозволяє логічно сегментувати мережу без прив’язки до фізичної інфраструктури.

NGFW – міжмережевий екран нового покоління, що забезпечує глибокий аналіз трафіку, включаючи DPI, IPS, фільтрацію додатків тощо.

IPS – система запобігання вторгненням, яка виявляє і блокує підозрілу активність у мережі.

SSL – протокол захищеного шифрування даних у мережі.

UTM – комплексний підхід до захисту мережі, який об’єднує в одному рішенні кілька засобів кібербезпеки.

GUI – графічний інтерфейс користувача для взаємодії з пристроями або програмами.

CLI – інтерфейс командного рядка, що дозволяє керувати пристроями через текстові команди.

SD-WAN – програмно-визначена мережева архітектура для керування WAN-з’єднаннями.

MFA – багатофакторна автентифікація для підвищення рівня захисту доступу.

FortiOS – операційна система, яка використовується у пристроях Fortinet, зокрема в FortiGate.

FortiGateVM – віртуалізована версія міжмережевого екрану FortiGate, що використовується в хмарному або віртуальному середовищі.

ВСТУП

Актуальність дослідження. У сучасних умовах цифрової трансформації та активного впровадження хмарних технологій, питання інформаційної безпеки набуває особливої актуальності. Організації дедалі частіше обирають хмарні платформи для зберігання, обробки та передачі даних, що, з одного боку, підвищує гнучкість IT-інфраструктури, а з іншого - створює нові виклики в сфері кібербезпеки. Захист хмарної інфраструктури потребує комплексного підходу, який враховує особливості віртуального середовища, віддаленого доступу, використання загальних ресурсів та потенційних вразливостей. Одним з ефективних рішень для реалізації політик безпеки в таких умовах є віртуальний міжмережевий екран FortigateVM, який поєднує у собі функціонал NGFW, IPS, антивірусу, VPN та веб-фільтрації. У межах дослідження буде проведено аналіз основних загроз хмарним середовищам, вивчено функціональні можливості FortigateVM та розглянуто практичні аспекти його розгортання й налаштування з метою забезпечення кібербезпеки організації.

Мета роботи: дослідження та практична реалізація захищеної хмарної інфраструктури організації на базі FortigateVM..

Об’єкт дослідження: хмарна IT-інфраструктура організації.

Предмет дослідження: засоби та методи захисту хмарної інфраструктури на основі FortigateVM.

Завдання:

1. Проаналізувати сучасні загрози хмарним середовищам;
2. Вивчити функціональні можливості FortigateVM;
3. Реалізувати захищену інфраструктуру з використанням FortigateVM;
4. Розробити рекомендацій щодо застосування методів та засобів захисту кінцевих точок організації.

Методи дослідження: аналіз літературних джерел та нормативної документації, системний аналіз, метод порівняння, метод моделювання та проєктування - для створення архітектури захищеної хмарної інфраструктури. Експериментальний метод - для практичного розгортання FortigateVM.

Практичне значення: практичне значення полягає в можливості використання результатів для впровадження сучасної системи захисту хмарної інфраструктури в реальних умовах організаційної IT-інфраструктури.

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ПОБУДОВИ ЗАХИЩЕНОЇ ХМАРНОЇ ІНФРАСТРУКТУРИ

1.1. Сучасні загрози інформаційній безпеці хмарних середовищ

Вивчаючи сучасні загрози інформаційній безпеці хмарних середовищ, можна сказати, що у теперішніх умовах цифрової трансформації дедалі більше організацій здійснюють міграцію IT-інфраструктури до хмарних платформ. Незважаючи на переваги, які надають хмарні сервіси — масштабованість, мобільність, оптимізація витрат — перехід до хмари супроводжується появою нових викликів у сфері інформаційної безпеки. Відкритий доступ до інфраструктур через мережу Інтернет, спільне використання обчислювальних ресурсів, віртуалізація даних та багатокористувацьке середовище формують нову площину ризиків, притаманних саме хмарним обчисленням [12, с. 31].

Однією з основних загроз є несанкціонований доступ до критично важливих ресурсів, що може бути реалізований шляхом підбору облікових даних, перехоплення аутентифікаційних токенів або експлуатації вразливостей в API [1, с. 21].

Через те, що управління ідентичністю користувача часто здійснюється сторонніми провайдерами, виникає ризик втрати контролю над точками доступу та механізмами авторизації. Особливо небезпечною є ситуація, коли облікові записи адміністраторів не захищені багатофакторною автентифікацією.

Ще одним критичним вектором загроз є міжорендаторні атаки, пов’язані з багатокористувацькою природою хмарної платформи. Атаки типу «побічних каналів» або «shared technology vulnerabilities» виникають через недосконале ізолювання ресурсів користувачів, що дозволяє одному орендарю потенційно впливати на роботу іншого [1, с. 22].

Відомі випадки, коли уразливості гіпервізора давали змогу отримати доступ до пам’яті суміжних віртуальних машин.

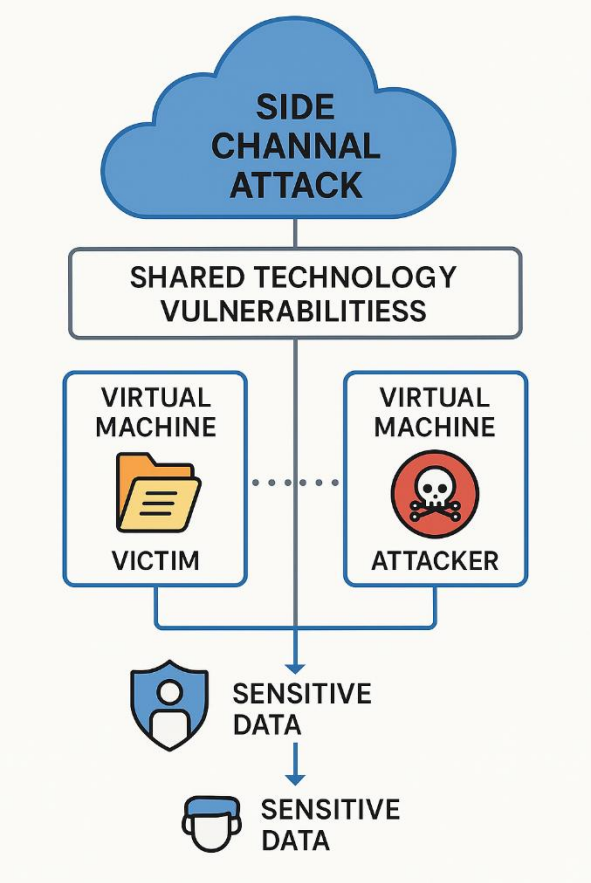

Рис. 1.1. Атаки типу «побічних каналів» або «shared technology vulnerabilities»

Не менш актуальною загрозою є атаки типу «Denial of Service» (DoS) та «Distributed Denial of Service» (DDoS), які в хмарному середовищі можуть спричинити зупинку доступу до сервісів не лише для окремого клієнта, а й для всієї інфраструктури платформи. Розподілені атаки можуть використовувати великі ботнети, що генерують колосальне навантаження на мережу, сервери та балансувальники навантаження [3, с. 78].

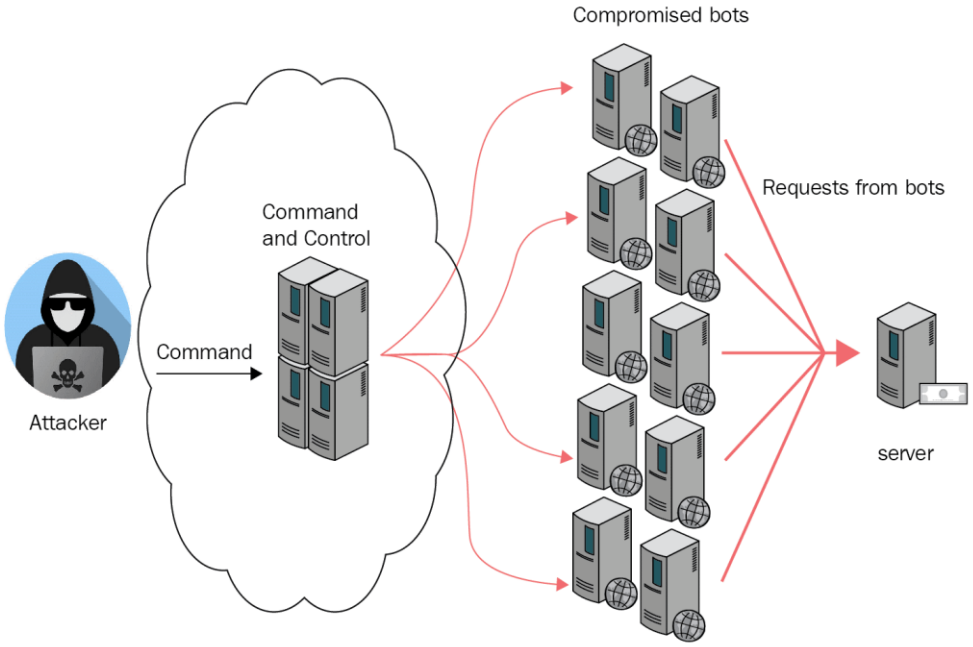

Рис. 1.2. Атаки типу «Denial of Service» (DoS) та «Distributed Denial of Service» (DDoS)

Витік даних, або data leakage, залишається ще однією значною проблемою. Нерідко причиною витоків є неправильна конфігурація доступу до сховищ даних або недостатньо захищені резервні копії. Автоматичне масштабування ресурсів, характерне для хмари, може призводити до неконтрольованого поширення даних у зони з нижчим рівнем захисту [3, с. 79].

У контексті розвитку контейнеризації та мікросервісної архітектури, нові ризики виникають у зв’язку з недостатньо захищеними інтерфейсами обміну між компонентами. Контейнери з неправильно налаштованими правами доступу можуть слугувати точкою входу для атак зсередини хмарного середовища [43, с.

28]. Також зростає загроза експлуатації вразливостей у CICD-пайплайнах, які використовуються для автоматизації розгортання програмного забезпечення.

Таким чином, захист хмарної інфраструктури вимагає урахування багатьох чинників: архітектури доступу, сегментації ресурсів, захисту API, аналізу поведінки користувачів, а також використання спеціалізованих засобів безпеки. Саме такі загрози і мотивують до впровадження комплексних рішень на зразок FortiGateVM — платформи, здатної забезпечити міжмережевий контроль, інспекцію трафіку, захист від вторгнень та централізоване керування політиками безпеки в хмарному середовищі.

1.2. Принципи побудови захищеної хмарної інфраструктури

Досліджуючи принципи побудови захищеної хмарної інфраструктури, ми бачимо, що у сучасних умовах цифрової трансформації дедалі більше організацій впроваджують хмарні обчислення як основу своєї IT-інфраструктури. Попри численні переваги, такі як масштабованість, доступність ресурсів у реальному часі та зниження витрат на фізичне обладнання, хмарне середовище залишається вразливим до широкого спектра кіберзагроз. У зв’язку з цим зростає потреба у впровадженні надійних рішень щодо захисту даних та управління мережею. Одним із найбільш ефективних інструментів для побудови безпечної хмарної інфраструктури є віртуальний міжмережевий екран FortigateVM, що входить до складу лінійки рішень Fortinet [46, с. 12].

FortigateVM — це віртуалізоване мережеве рішення класу NGFW (Next-Generation Firewall), яке забезпечує комплексний захист як для локальних, так і для хмарних середовищ [5, с. 36].

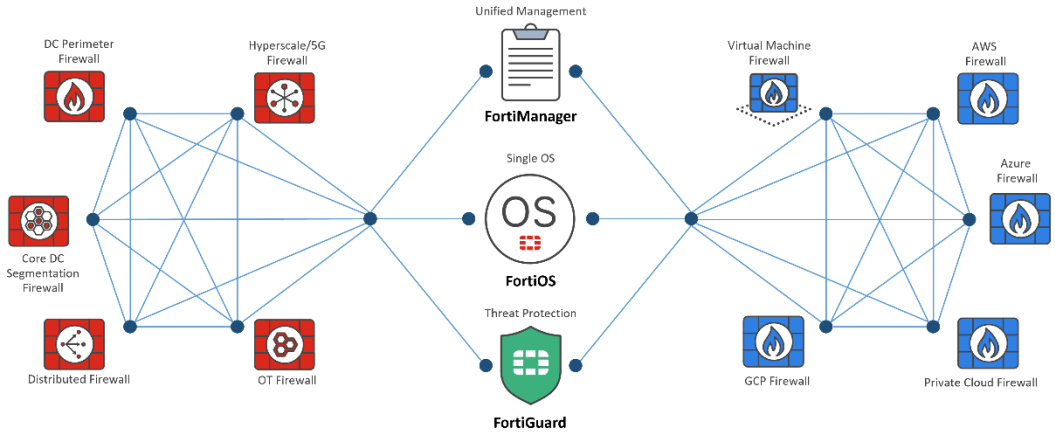

Рис. 1.1. Архітектура інтегрованого мережевого захисту Fortinet

Завдяки можливості розгортання у провідних хмарних провайдерах, таких як Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform та ін., даний програмний продукт надає засоби гнучкої інтеграції в існуючу інфраструктуру організації [3, с. 78]. FortigateVM підтримує функціональність традиційного міжмережевого екрану, а також включає вбудовану систему виявлення та запобігання вторгненням (IPS), веб-фільтрацію, контроль додатків, VPN (віртуальні приватні мережі), антивірусний захист і систему аналітики безпеки.

Ключовим аспектом побудови захищеної хмарної інфраструктури на базі FortigateVM є можливість централізованого управління політиками безпеки та трафіком у режимі реального часу, що дозволяє ефективно реагувати на інциденти, адаптуватися до змін у загрозовому ландшафті, а також забезпечувати відповідність нормативно-правовим вимогам, зокрема стандартам ISO/IEC 27001, NIST та GDPR [2, с. 52]. Архітектура FortigateVM передбачає підтримку сегментації мережі, що забезпечує ізоляцію критично важливих ресурсів та знижує ризик горизонтального розповсюдження шкідливого коду у разі компрометації окремих вузлів.

Додатковою перевагою FortigateVM є інтеграція з системами оркестрації та автоматизації, такими як Terraform, Ansible, Kubernetes та інші, що відкриває можливість реалізації підходів DevSecOps, що сприяє створенню безпечного середовища на всіх етапах життєвого циклу розгортання додатків.

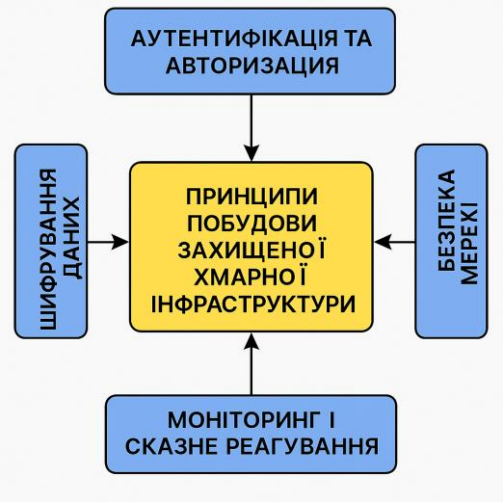

Рис. 1.2. Принципи побудови захищеної хмарної інфраструктури

Тобто, впровадження FortigateVM у хмарному середовищі надає організаціям можливість ефективно інтегрувати переваги віртуалізації, масштабованості та централізованого управління, характерні для хмарних рішень, із потужним інструментарієм сучасної кібербезпеки.

Завдяки широкому спектру функцій — таких як міжмережеве екранування нового покоління, вбудовані системи виявлення та запобігання вторгненням (IPS), управління політиками доступу, захист від шкідливого ПЗ, шифрування трафіку, а також підтримка VPN-з’єднань і сегментації мережі — FortigateVM забезпечує комплексну багаторівневу оборону [2, с. 51].

Дане рішення дозволяє захистити критично важливу корпоративну інформацію від внутрішніх і зовнішніх загроз, запобігати витоку даних, а також забезпечити бізнес-континуїтет у разі виникнення інцидентів безпеки.

Крім того, гнучка архітектура FortigateVM забезпечує швидке масштабування в залежності від змін у завантаженні системи або бізнес-потреб, що особливо важливо для динамічних організацій, які активно використовують гібридну або мультихмарну інфраструктуру. Загалом, використання FortigateVM у хмарному середовищі дозволяє не лише підвищити інформаційну стійкість, а й забезпечити відповідність сучасним вимогам безпеки, стандартам регуляторних органів та найкращим практикам галузі.

1.3. Огляд рішень для захисту хмарної інфраструктури

Виконуючи огляд рішень для захисту хмарної інфраструктури, нами було виявлено, що захист хмарної інфраструктури є одним із найважливіших викликів сучасної інформаційної безпеки, оскільки моделі споживання хмарних сервісів постійно еволюціонують, а обсяг та складність кіберзагроз зростають. Забезпечення конфіденційності, цілісності та доступності даних у хмарному середовищі вимагає інтегрованого підходу, що передбачає використання як традиційних засобів безпеки, так і спеціалізованих хмарних рішень.

Доцільно додати, що існує декілька ключових категорій засобів захисту, які формують комплексну систему безпеки хмарної інфраструктури. До них належать рішення для мережевої безпеки, інструменти управління ідентифікацією та доступом (IAM), системи виявлення та реагування на загрози, сервіси шифрування та контролю даних, а також механізми забезпечення відповідності стандартам (compliance).

Мережеві міжмережеві екрани наступного покоління (NGFW), такі як FortigateVM, Palo Alto VM-Series та Check Point CloudGuard, забезпечують контроль мережевого трафіку, виявлення атак та застосування політик безпеки в хмарних середовищах [5, с. 7]. Дані рішення часто інтегруються з вбудованими

можливостями хмарних провайдерів, що дозволяє посилити захист на рівні віртуальних мереж.

Засоби управління доступом та ідентифікацією, як-от AWS IAM, Azure Active Directory або Google Cloud Identity, відіграють ключову роль у захисті облікових записів та управлінні правами користувачів. Багатофакторна автентифікація, контроль привілейованого доступу (PAM) та принцип найменших привілеїв є критично важливими для мінімізації ризику несанкціонованого доступу [11, с. 6].

Системи моніторингу та виявлення загроз (IDS/IPS, SIEM, XDR) забезпечують своєчасне реагування на інциденти безпеки. До таких рішень належать Microsoft Defender for Cloud, Splunk, IBM QRadar, а також спеціалізовані сервіси хмарних провайдерів. Вони аналізують поведінкові патерни, логі подій і телеметрію, щоб ідентифікувати аномалії та потенційні атаки [10, с. 82].

Особливе значення має застосування шифрування для захисту даних у стані спокою та під час передачі. Рішення для керування ключами (KMS) дозволяють централізовано контролювати криптографічні операції, що є необхідним компонентом захисту конфіденційної інформації [14, с. 55]. Крім того, впроваджуються сервіси для забезпечення відповідності хмарної інфраструктури міжнародним стандартам та регламентам. Інструменти типу AWS Security Hub, Azure Security Center або Prisma Cloud від Palo Alto Networks надають змогу виконувати оцінку ризиків, перевірку політик безпеки та автоматизований аудит відповідності.

Доцільно зауважити, що ефективний захист хмарної інфраструктури базується на поєднанні декількох класів рішень, які взаємодіють між собою для створення багаторівневої архітектури безпеки. Вибір конкретного інструментарію залежить від особливостей обраної моделі хмарних послуг (IaaS, PaaS, SaaS), типу даних, які обробляються, вимог до відповідності та рівня допуску до ризиків у конкретній організації.

На ринку засобів захисту хмарної інфраструктури представлено низку конкурентних рішень, зокрема від таких постачальників, як Palo Alto Networks, Check Point, Cisco, Juniper, Sophos та ін. [41, с. 2]. Однак FortigateVM вирізняється комплексним підходом до безпеки, високою гнучкістю інтеграції у мультихмарне середовище та широким спектром функцій у межах єдиної платформи [14, с. 54].

Однією з головних переваг FortigateVM є уніфікація засобів безпеки в межах так званої концепції Security Fabric [45, с. 3]. Така архітектура дозволяє централізовано керувати політиками безпеки, здійснювати моніторинг, логування та кореляцію подій у різнорідних середовищах — від локальних ЦОД до хмарних і гібридних розгортань. Інші рішення, наприклад Cisco Secure Firewall Threat Defense Virtual або Sophos XG Firewall, можуть потребувати інтеграції з зовнішніми інструментами для досягнення подібного рівня координації, що ускладнює впровадження та адміністрування.

FortigateVM підтримує апаратне прискорення обробки трафіку завдяки використанню технології vSPU (Virtual Security Processing Unit), яка оптимізує продуктивність у віртуальному середовищі, що дозволяє обробляти великі обсяги даних без зниження ефективності навіть у сценаріях з великою кількістю одночасних підключень. Для порівняння, деякі конкуренти обмежені загальною продуктивністю гіпервізора або не мають гнучкого механізму балансування навантаження без залучення сторонніх сервісів [19, с. 38].

Ще одним важливим аспектом є глибока інтеграція FortigateVM з платформами автоматизації та DevOps-інструментами. Підтримка API, шаблонів конфігурацій (CloudFormation для AWS, ARM для Azure, Terraform для мультихмарних сценаріїв) і CI/CD-інструментів сприяє гнучкому та швидкому впровадженню політик безпеки вже на етапі розробки, що особливо важливо для організацій, що практикують підхід «інфраструктура як код» та прагнуть мінімізувати людський фактор.

Функціонал FortigateVM включає повноцінний вбудований IDS/IPS, систему фільтрації контенту, захист від DDoS-атак, антивірус, контроль додатків та веб-брандмауер (WAF), що знижує потребу у придбанні додаткових ліцензій або налаштуванні зовнішніх служб. У той час як продукти конкурентів часто обмежені певними модулями безпеки, FortigateVM надає всеохопний набір функцій у рамках єдиної віртуальної машини [19, с. 40].

Також важливо відзначити розвинуту систему звітності та візуалізації, доступну через FortiAnalyzer, яка дозволяє здійснювати глибокий аналіз інцидентів, генерувати звіти для аудитів і виявляти приховані загрози завдяки аналітиці на основі штучного інтелекту. Аналогічні можливості конкурентних рішень зазвичай доступні лише через окремі продукти, що потребує додаткової інтеграції та витрат.

Одже, FortigateVM демонструє конкурентну перевагу завдяки поєднанню високої продуктивності, повноцінного набору функцій безпеки, зручності розгортання та централізованого управління, що робить його одним із найефективніших рішень для забезпечення захищеності хмарної інфраструктури в умовах сучасного динамічного IT-середовища.

РОЗДІЛ 2 FORTIGATEVM ЯК ІНСТРУМЕНТ ДЛЯ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ

2.1. Архітектура FortigateVM та її функціональні можливості

Розглядаючи архітектуру FortigateVM та її функціональні можливості, можна сказати, що вона є віртуалізованим рішенням від компанії Fortinet, що виконує роль міжмережевого екрана наступного покоління (NGFW) та виконує комплекс функцій з управління безпекою у хмарному середовищі. Дане рішення призначене для розгортання у приватних, публічних та гібридних хмарах і є адаптованим до платформ віртуалізації, таких як VMware ESXi, KVM, Microsoft Hyper-V, а також до провідних хмарних провайдерів: Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) [35, с. 14].

Архітектура FortigateVM базується на мікросервісному підході, який дозволяє масштабувати функціональність залежно від навантаження та потреб організації. Основою функціональної структури є віртуальна машина, що містить модулі для обробки трафіку, інспекції пакетів, а також системи управління політиками. Представлена архітектура доповнюється підтримкою віртуальних інтерфейсів (vNIC), які використовуються для маршрутизації, фільтрації трафіку та інтеграції з віртуальними мережами хмарного середовища [21, с. 9].

Функціональні можливості FortigateVM охоплюють низку ключових напрямів безпеки. По-перше, це міжмережевий екран з можливістю глибокої інспекції пакетів (DPI), що дозволяє аналізувати трафік на рівні прикладного протоколу, виявляючи шкідливі дії навіть у зашифрованому потоці [20, с. 4]. Система контролю додатків (Application Control) забезпечує можливість дозволяти або блокувати використання окремих програм чи сервісів, виходячи з бізнес-політик.

По-друге, FortigateVM включає вбудовану систему запобігання вторгненням (IPS), яка використовує сигнатурний та евристичний аналіз для виявлення атак. IPS може автоматично блокувати підозрілу активність, запобігаючи експлуатації вразливостей [36, с. 5]. Технологія FortiGuard забезпечує регулярне оновлення баз даних сигнатур, що дозволяє підтримувати високий рівень актуальності захисту.

По-третє, FortigateVM підтримує функціональність віртуальних приватних мереж (VPN), включаючи IPsec та SSL VPN, що дозволяє забезпечити захищений доступ до внутрішніх ресурсів організації для віддалених користувачів та офісів, навіть у випадку використання загальнодоступних каналів передачі даних [28, с. 6].

Таблиця 2.1.

Архітектура та функціональні можливості FortigateVM

Компонент/Підсистема	Опис	Функціональні можливості
VCPU / Обчислювальні ресурси	Віртуальні процесорні ядра, виділені для FortigateVM	Обробка трафіку, запуск системних служб, оптимізація продуктивності
Віртуальні мережеві інтерфейси (vNIC)	Мережеві інтерфейси для підключення до зовнішніх/внутрішніх мереж	Підтримка зон безпеки, маршрутизація, сегментація мережі
FortiOS (операційна система)	Програмна платформа Fortinet, що виконує всі функції NGFW	Управління політиками, IPS, VPN, маршрутизація, NAT, фільтрація

Модуль управління (Management Plane)	Інтерфейс адміністрування через GUI, CLI, API	Налаштування, моніторинг, логування, інтеграція з FortiManager
Модуль обробки трафіку (Data Plane)	Канал для обробки користувацького трафіку	Інспекція пакетів, DPI, антивірус, веб-фільтрація
Функція FortiGuard Services	Хмарний сервіс оновлень і баз знань від Fortinet	IPS-сигнатури, фільтрація веб-контенту, антивірус, геолокаційна фільтрація
VPN-модуль	Інструменти створення захищених з'єднань	Підтримка IPsec та SSL VPN для безпечного доступу користувачів до мережі
IPS/IDS-система	Система виявлення та запобігання вторгненням	Аналіз трафіку в реальному часі, блокування атак, журналювання інцидентів
Антивірусний механізм	Компонент для виявлення шкідливого ПЗ	Сканування в реальному часі, блокування заражених файлів
Логування та моніторинг	Збір і збереження інформації про події	Аналіз журналів, інтеграція з SIEM, попередження про інциденти

Додатково до основних функцій FortigateVM надає механізми фільтрації веб-контенту (Web Filtering), антивірусного сканування трафіку в реальному часі, а також інтеграцію з системами виявлення шкідливих об'єктів на основі машинного навчання [32, с. 4]. Усі ці компоненти можуть бути централізовано керовані за допомогою FortiManager та FortiAnalyzer, що дає змогу реалізувати єдину політику безпеки та забезпечити моніторинг в реальному часі з можливістю глибокого аналізу інцидентів.

Архітектура FortigateVM також передбачає інтеграцію з технологіями автоматизації (Terraform, Ansible) та підтримує API для взаємодії з іншими компонентами інфраструктури, що, в свою чергу дозволяє адаптувати систему до сценаріїв DevOps/DevSecOps та підвищити швидкість розгортання і масштабування рішень безпеки [39, с. 3].

Отже, FortigateVM сьогодні виконує значно більше, ніж базові функції традиційного міжмережевого екрана - комплексний віртуалізований мережевий безпековий шлюз, який інтегрується в хмарну інфраструктуру як повноцінний захисний компонент із широкими можливостями налаштування та адаптації.

На відміну від класичних апаратних рішень, FortigateVM має високий рівень масштабованості — як вертикальної (в межах одного середовища), так і горизонтальної (при розгортанні у багатохмарних або гібридних структурах), що дозволяє ефективно відповідати на зміну обсягу трафіку, навантаження або вимог до безпеки [25, с. 8]. Адаптивність системи проявляється у здатності швидко змінювати конфігурації, застосовувати політики безпеки до нових сервісів, динамічно оновлювати бази даних загроз і виявляти нетипову активність у реальному часі.

Інтегрованість FortigateVM з хмарними платформами (Azure, AWS, GCP) та іншими рішеннями (SIEM, EDR, VPN, SD-WAN) дозволяє будувати гнучкі, міжплатформені системи захисту, що відповідають вимогам сучасних корпоративних середовищм [26, с. 7]. Крім того, FortigateVM підтримує

автоматизовані сценарії реагування на інциденти, централізований моніторинг і детальну аналітику, що підвищує ефективність управління безпекою.

Таким чином, FortigateVM є не просто інструментом фільтрації трафіку, а стратегічним елементом архітектури інформаційної безпеки, який дозволяє своєчасно й ефективно реагувати на загрози нового покоління, зберігаючи стабільність, керованість і надійність хмарної інфраструктури організації.

2.2. Варіанти розгортання FortigateVM у хмарних середовищах (Azure, AWS, GCP, локальна віртуалізація)

Розглядаючи варіанти розгортання FortigateVM у хмарних середовищах, ми бачимо, що гнучкість FortigateVM полягає у можливості його розгортання в різноманітних віртуалізованих середовищах — як у межах приватної інфраструктури, так і в публічних хмарах, що забезпечує адаптивність до потреб конкретної організації, незалежно від обраної моделі обчислень — IaaS, PaaS або гібридного підходу [33, с. 2].

У середовищі Microsoft Azure FortigateVM доступний як готовий шаблон у Marketplace, що дає змогу швидко здійснити розгортання у кілька кліків із попередньо налаштованими параметрами безпеки. Azure дозволяє інтегрувати FortigateVM з такими сервісами, як Azure Virtual Network, Network Security Groups (NSG), Azure Load Balancer, а також з Azure Active Directory для централізованого управління доступом [33, с. 4]. Підтримується масштабування за рахунок використання Virtual Machine Scale Sets (VMSS), що дає змогу автоматично додавати чи вилучати вузли без втрати функціональності. Див. рис. 2.1.

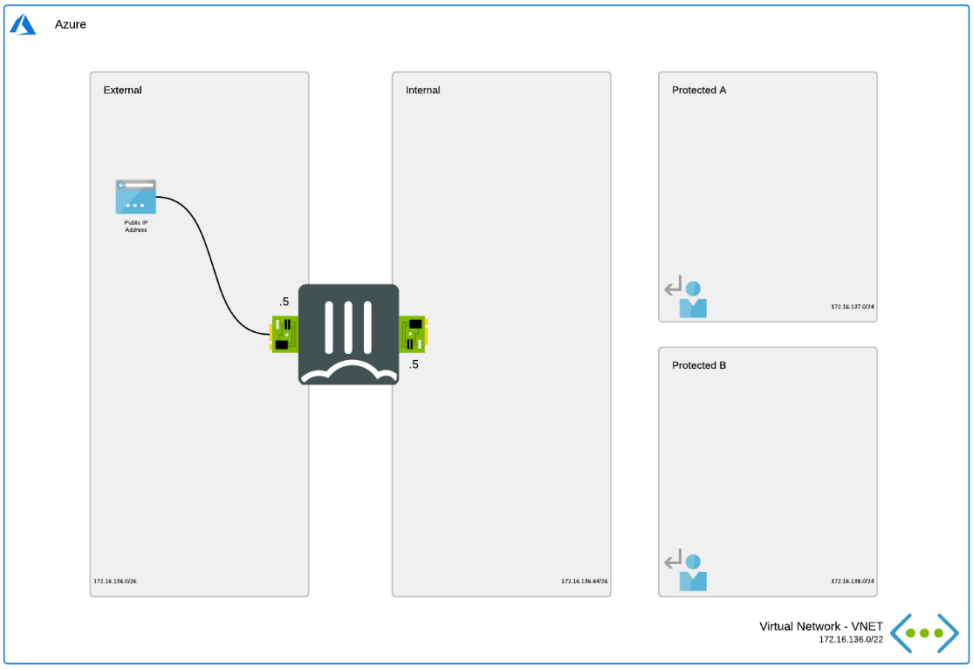

Рис. 2.1. Розгортання Fortigate VM у хмарному середовищі Azure

У Amazon Web Services (AWS) FortigateVM розгортається як EC2-інстанс з інтеграцією у VPC (Virtual Private Cloud). Він може працювати в режимі міжмережевого екрана на рівні інтернет-шлюзу або бути частиною архітектури із зонуванням — наприклад, у демілітаризованій зоні (DMZ) [31, с. 12]. FortigateVM підтримує сервіси AWS, такі як Elastic Load Balancing (ELB), Auto Scaling Groups, Route 53, CloudWatch та CloudFormation, що дозволяє здійснювати інфраструктуру як код та налаштовувати автоматичний контроль стану пристроїв безпеки. Див. рис.2.2.

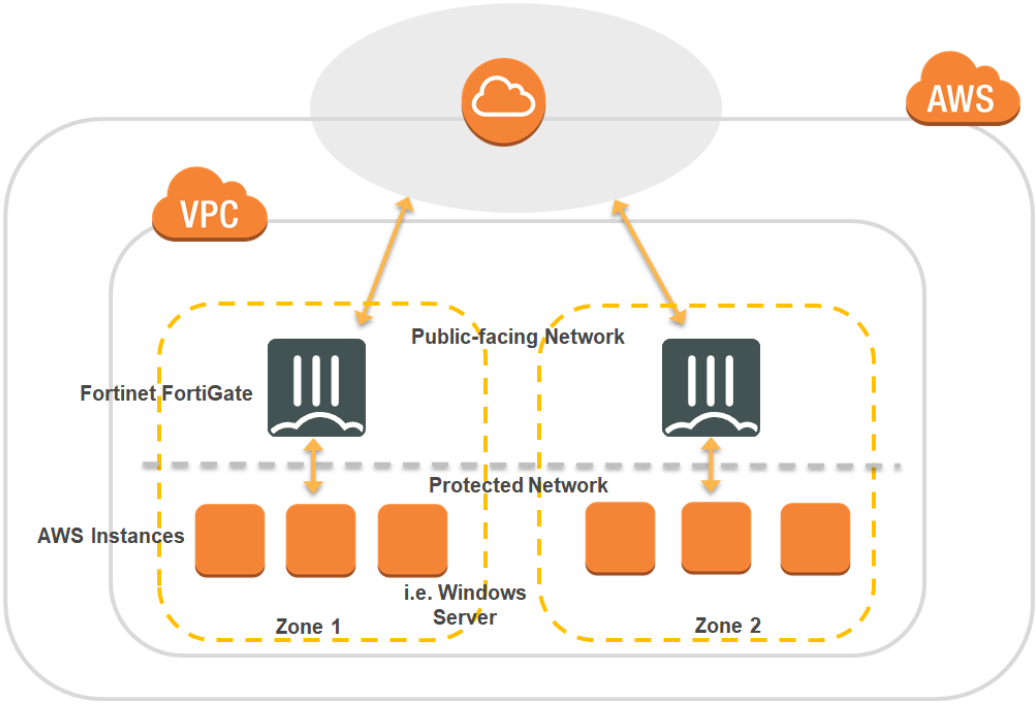

Рис. 2.2. Розгортання Fortigate VM у хмарному середовищі AWS

У Google Cloud Platform (GCP) FortigateVM доступний як шаблон у Google Cloud Marketplace та підтримує інтеграцію з Google VPC, Cloud Armor, Identity and Access Management (IAM), а також Stackdriver для логування й моніторингу [38, с. 11]. Розгортання можливе як у зонованих, так і в багаторегіональних конфігураціях з балансуванням навантаження та високою доступністю (HA). FortigateVM у GCP часто використовується в сценаріях міжрегіональної маршрутизації трафіку між кластерами Kubernetes або у мультихмарних зв'язках (interconnect). Див. рис. 2.3.

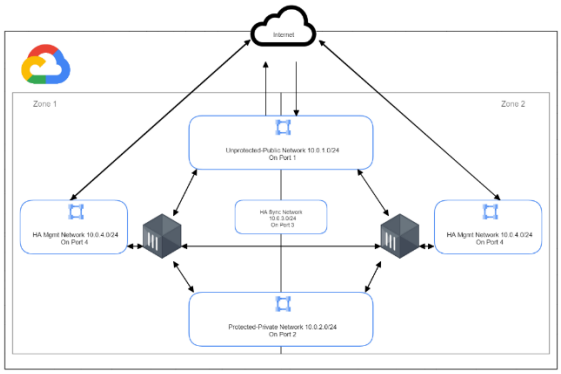

Рис. 2.3. Розгортання Fortigate VM у хмарному середовищі GCP

У контексті локальної віртуалізації FortigateVM розгортається на гіпервізорах VMware ESXi, Microsoft Hyper-V, KVM або Oracle VirtualBox. Такий підхід часто використовується в лабораторіях, тестових середовищах, а також у приватних хмарах (наприклад, OpenStack). У локальному середовищі FortigateVM може виконувати роль шлюзу безпеки, сегментатора мережі або VPN-концентратора, інтегруючись із внутрішніми службами авторизації, системами SIEM та засобами моніторингу [44, с. 9].

Важливо відзначити, що незалежно від середовища, FortigateVM підтримує розгортання у режимі високої доступності (HA), як у активному–пасивному, так і у кластерному активному режимі, що дає змогу забезпечити безперервність захисту навіть у разі збоїв окремих компонентів інфраструктури.

Загалом, універсальність FortigateVM у виборі середовища розгортання дає змогу організаціям реалізовувати політики безпеки незалежно від локації обчислювальних ресурсів, що є особливо актуально у випадках використання гібридних чи мультихмарних стратегій, де необхідно забезпечити єдиний контроль доступу, моніторинг та реагування на загрози в межах розподіленої інфраструктури.

Таблиця 2.1.

Варіанти розгортання FortigateVM у хмарних середовищах

Середовище	Спосіб розгортання	Особливості інтеграції	Переваги
MICROSOFT AZURE	Через Azure Marketplace	Інтеграція з Azure Virtual Network, підтримка Auto	Гнучке масштабування, простота налаштувань,

	або ARM шаблони	Scaling, використання Azure Load Balancer, підтримка платформи Azure Security Center	висока інтеграція з сервісами Microsoft
AMAZON AWS	Через AWS Marketplace або CloudFormation	Інтеграція з VPC, підтримка Auto Scaling Group, Route Tables, IAM, CloudWatch	Підтримка гібридної архітектури, централізований моніторинг, відповідність вимогам AWS Well-Architected
GOOGLE CLOUD (GCP)	Через Google Cloud Marketplace або Deployment Manager	Підключення до VPC, підтримка хмарного NAT, інтеграція з GCP Logging, Cloud Armor	Збалансована продуктивність, підтримка регіонального розгортання, глибока інтеграція з Google сервісами
ЛОКАЛЬНА ВІРТУАЛІЗАЦІЯ (VMWARE, HYPER-V, KVM)	За допомогою ISO/OVF/RAW образів FortigateVM	Встановлюється як окрема віртуальна машина з налаштуванням мережевих інтерфейсів, NAT, VPN	Повний контроль над середовищем, незалежність від публічної хмари, гнучкість конфігурації

2.3. Політики безпеки, VPN, фільтрація трафіку, антивірус, IPS

Вивчаючи питання політики безпеки, можна сказати, що FortigateVM забезпечує глибокий та багаторівневий захист інформаційних систем у хмарному середовищі шляхом впровадження політик безпеки, інструментів фільтрації та інспекції трафіку, а також систем запобігання загрозам. Його функціональність дозволяє реалізувати концепцію Zero Trust та забезпечити відповідність сучасним стандартам кібербезпеки.

Політики безпеки (Security Policies) є основним інструментом контролю взаємодії між об'єктами мережі. Вони визначають правила доступу на основі джерела, призначення, портів, додатків, географічного розташування, а також користувачів або груп, інтегрованих через системи ідентифікації (наприклад, LDAP, SAML, RADIUS) [37, с. 4]. FortigateVM дозволяє створювати динамічні політики з логічними умовами, а також застосовувати їх до віртуальних доменів (VDOM), що забезпечує сегментацію мережі на логічні ізольовані середовища із власними правилами доступу [15, с. 19].

Особливе значення мають VPN-технології, що реалізуються в FortigateVM на базі протоколів IPsec та SSL. IPsec VPN дозволяє створювати захищені тунелі між філіями або між хмарними майданчиками, забезпечуючи конфіденційність і цілісність даних. SSL VPN, у свою чергу, надає користувачам можливість безпечного віддаленого доступу до внутрішніх ресурсів через веб-браузер або клієнтське ПЗ, з можливістю автентифікації, шифрування та обмеження доступу на основі ролей. У FortigateVM реалізовано гнучке управління сесіями VPN, включаючи підтримку мультифакторної автентифікації (MFA), журналювання, обмеження часу сесії та контроль активності [8, с. 66].

Фільтрація трафіку (Web and Application Filtering) виконується на рівні прикладного трафіку та дозволяє блокувати доступ до небажаного або

шкідливого контенту. FortigateVM підтримує категоризацію вебсайтів на основі оновлюваних баз FortiGuard, а також розпізнавання додатків (Application Control), що дозволяє регулювати використання хмарних сервісів, месенджерів, файлообмінників тощо, що важливо з огляду на ризики, пов’язані з Shadow IT та витоками даних через сторонні платформи [8, с. 67].

Антивірусна система FortigateVM реалізує сканування трафіку в реальному часі, використовуючи сигнатурний аналіз, евристику та механізми на основі поведінкових шаблонів [29, с. 16]. Вона здатна виявляти відомі та нульові загрози, блокувати шкідливі вкладення в електронній пошті, перехоплювати заражені файли в HTTP(S), FTP або SMTP трафіку, а також працювати у зв’язці з FortiSandbox для глибшого аналізу підозрілих об’єктів у контрольованому середовищі.

Таблиця 2.2.

Антивірусна система FortigateVM: функціональні можливості

Компонент / Технологія	Призначення	Особливості реалізації
Сканування трафіку в реальному часі	Аналіз вхідного та вихідного трафіку для виявлення загроз	Працює з HTTP(S), FTP, SMTP, POP3, IMAP
Сигнатурний аналіз	Виявлення загроз за відомими сигнатурами вірусів і шкідливого ПЗ	Постійну актуалізацію забезпечує FortiGuard
Евристичний аналіз	Виявлення нових або модифікованих загроз, що мають підозрілу структуру	Аналізує поведінкові та кодові аномалії

Аналіз поведінкових шаблонів	Виявлення загроз на основі дій, що імітують шкідливу поведінку	Особливо ефективно проти нульових атак (zero-day)
Фільтрація вкладень електронної пошти	Перевірка вкладень у SMTP, POP3, IMAP	Автоматичне блокування шкідливих документів, архівів та скриптів
Інтеграція з FortiSandbox	Поглиблений аналіз підозрілих файлів у віртуальному ізольованому середовищі	Запускає файли у пісочниці для виявлення прихованих загроз
Підтримка HTTPS-інспекції	Аналіз зашифрованого трафіку без втрати безпеки	Розшифровує та перевіряє SSL-сесії на шкідливий контент

Система виявлення та запобігання вторгненням (IPS) у FortigateVM функціонує як інтелектуальний бар’єр, який аналізує вхідний і вихідний трафік на предмет відомих атак, експлойтів, порушень протоколів або аномальної поведінки. IPS підтримує оновлювані сигнатури, а також дозволяє створювати власні правила [7, с. 11]. Завдяки технології flow-based inspection можливе швидке прийняття рішень у режимі реального часу з мінімальною затримкою трафіку.
Усі вищезгадані механізми об'єднуються в єдину систему за допомогою централізованого управління через FortiManager та аналітики безпеки на базі FortiAnalyzer. В свою чергу, це дає змогу корелювати події, виявляти складні багатовекторні атаки та автоматизувати реакцію на інциденти.

Отже, функціональні можливості FortigateVM охоплюють усі основні компоненти сучасного кіберзахисту хмарної інфраструктури, що робить його універсальним і високоефективним інструментом для забезпечення інформаційної безпеки в організаціях різного масштабу. У складі рішення

реалізовано глибоку фільтрацію трафіку, контроль доступу до мережевих ресурсів за допомогою гнучких політик, шифрування даних у каналі передачі (IPSec/SSL VPN), а також постійний моніторинг активності з використанням механізмів виявлення аномалій і вторгнень (IPS/IDS). У разі виявлення підозрілої активності FortigateVM автоматично активує сценарії реагування, ізоляції вузлів або блокування трафіку, мінімізуючи потенційний вплив інцидентів.

Крім того, FortigateVM підтримує інтеграцію з SIEM-платформами, централізованими засобами управління безпекою та логами, що дозволяє здійснювати аналітичний контроль над усіма процесами у реальному часі. Завдяки цьому рішення відповідає вимогам як традиційної корпоративної інфраструктури, так і динамічних хмарних середовищ із розподіленими ресурсами та підвищеним ризиком зовнішніх і внутрішніх загроз [9, с. 93].

Таким чином, комплексний підхід до безпеки, який реалізує FortigateVM, дає змогу ефективно впроваджувати політики інформаційної безпеки відповідно до міжнародних стандартів, одночасно підтримуючи гнучкість, масштабованість та високу готовність до реагування в умовах постійно змінюваного IT-ландшафту.

РОЗДІЛ 3 РОЗГОРТАННЯ ТА НАЛАШТУВАННЯ ЗАХИЩЕНОЇ ХМАРНОЇ ІНФРАСТРУКТУРИ

3.1. Проектування безпечної мережевої інфраструктури з FortigateVM

Проєктування безпечної мережевої інфраструктури в хмарному середовищі вимагає врахування багатьох аспектів, зокрема логічної сегментації, контролю доступу, маршрутизації, шифрування та моніторингу [30, с. 2]. Використання FortigateVM як центрального елемента безпеки дозволяє реалізувати модель захищеного периметра із підтримкою сучасних принципів — зокрема Zero Trust, Defense-in-Depth та Least Privilege Access. Див. рис. 3.1.

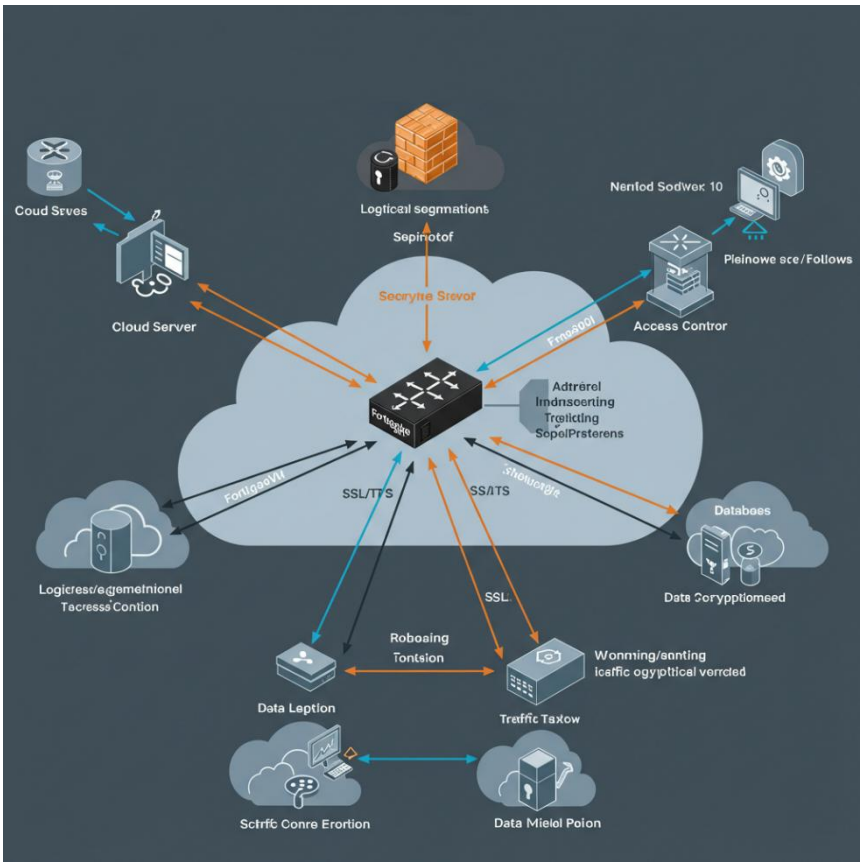

Рис. 3.1. Архітектура безпеки хмарної мережі

Процес проєктування починається з визначення функціональної структури інфраструктури, яка має включати зони з різним рівнем доступу та критичності: зовнішню публічну DMZ-зону, внутрішню приватну мережу, адміністративний сегмент, а також інтерфейс для віддалених користувачів або філій [13, с. 4]. FortigateVM виконує роль шлюзу між цими зонами, здійснюючи інспекцію, шифрування та контроль трафіку на міжзональному рівні. Див. рис. 3.2.

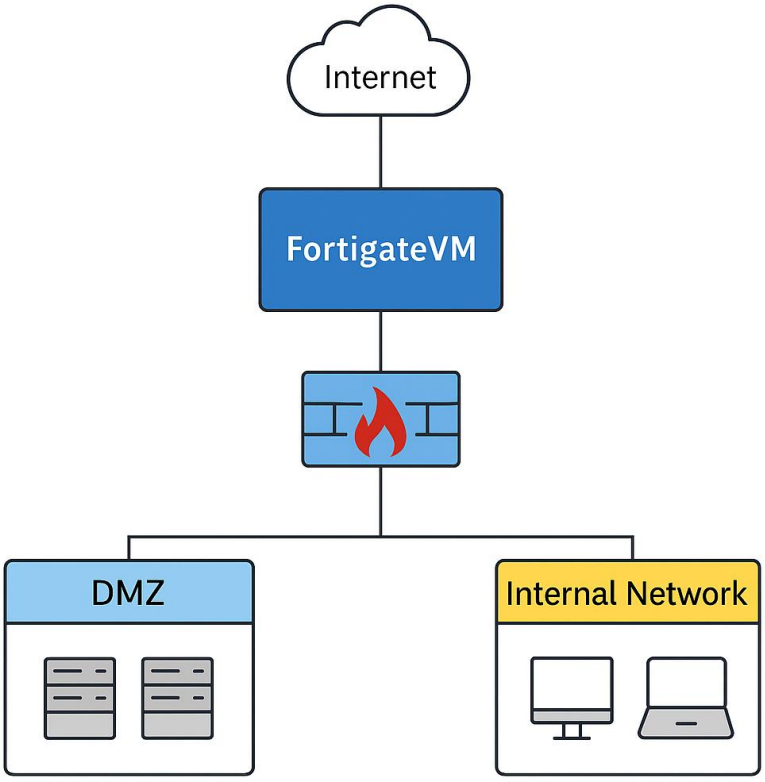

Рис. 3.2. Проєктування безпечної мережевої інфраструктури з різними зонами безпеки та FortigateVM як шлюзом

У хмарному середовищі (наприклад, Azure або AWS) інфраструктура проєктується у межах логічної топології, побудованої на базі віртуальних мереж (VNet/VPC) та підмереж [23, с. 18]. FortigateVM розміщується у спеціальній підмережі (security subnet), через яку маршрутується увесь вхідний та вихідний трафік [4, с. 12]. Для досягнення високої доступності можуть використовуватись схеми з двома інстансами FortigateVM у режимі active-passive із застосуванням Load Balancer або Route Tables з моніторингом стану.

Ключовим елементом безпечного проєктування є впровадження політик міжмережевого екранування [17, с. 38]. У середовищі FortigateVM вони створюються на основі принципу Whitelist — дозволяється лише необхідний трафік, решта блокується за замовчуванням. Наприклад, доступ до внутрішньої бази даних ззовні заборонено, а до вебсерверу — лише на портах 80/443 з IP-адрес довірених джерел. Див. рис. 3.3.

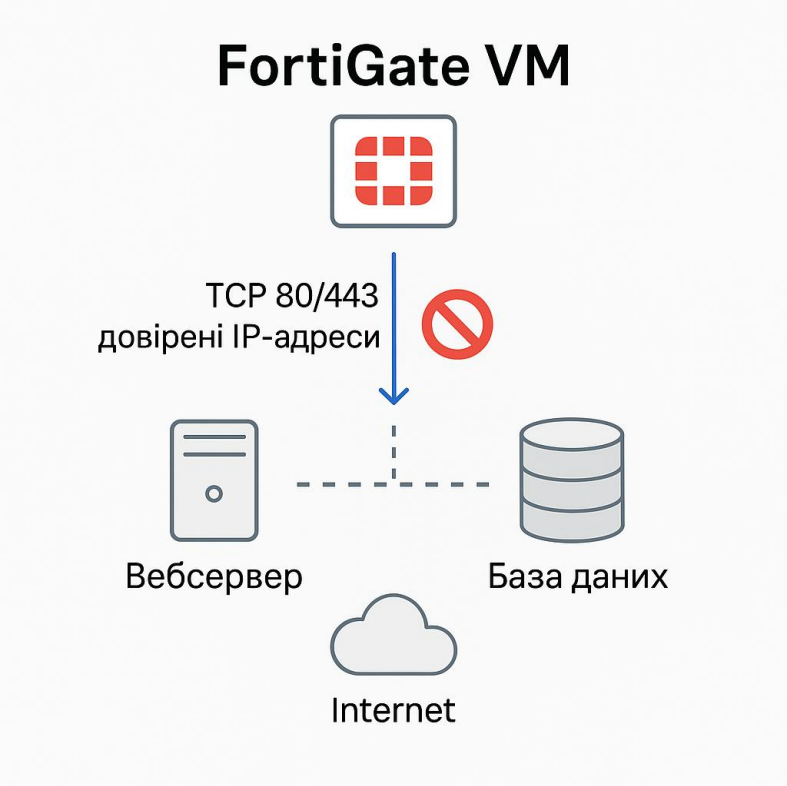

Рис. 3.3. Обмеження доступу до внутрішніх ресурсів у хмарній інфраструктурі

Особливу увагу приділяється інтеграції VPN — як у вигляді Site-to-Site з іншими майданчиками, так і SSL VPN для безпечного доступу працівників до внутрішніх ресурсів [24, с. 6]. Важливо реалізувати систему багатофакторної автентифікації, обмеження сесій та моніторинг активності користувачів.

У межах проєктування передбачено підключення FortigateVM до системи журналювання та моніторингу подій, зокрема FortiAnalyzer або аналогічних

SIEM-платформ, що дозволяє виконувати аналіз загроз у реальному часі, кореляцію інцидентів та побудову графіків навантаження на мережу.

Ще одним елементом безпечної архітектури є розгортання фільтрів на рівні додатків (Web Filtering, Application Control), антивірусного сканування та системи виявлення вторгнень (IPS). Вони активуються на відповідних політиках безпеки залежно від зон та типів трафіку, політика для публічного вебсерверу може включати SSL-інспекцію, WAF-функції та обмеження доступу до адміністративного інтерфейсу лише з певних адрес [34, с. 3].

Одже, проєктування захищеної хмарної інфраструктури з використанням FortigateVM базується на багаторівневій архітектурі з чітким розмежуванням зон, визначенням політик доступу, шифруванням каналів та аналітикою безпеки. Даний підхід дозволяє створити надійне та масштабоване середовище, здатне протистояти сучасним кіберзагрозам та відповідати вимогам нормативних стандартів безпеки.

3.2. Практичне розгортання FortigateVM у віртуалізованому середовищі

На сучасному етапі розвитку інформаційних технологій використання віртуалізованих середовищ є невід’ємною складовою проєктування гнучких та масштабованих інфраструктур кіберзахисту [40, с. 2]. У рамках нашого дослідження проведено практичне розгортання віртуального міжмережевого екрану FortigateVM у середовищі віртуалізації, що забезпечує основну платформу для реалізації функцій захисту мережевої інфраструктури організації.

Першочерговим етапом розгортання є підготовка гіпервізора [40, с. 3]. У межах роботи використано середовище VMware ESXi 7.0, що дозволяє реалізувати високий рівень ізоляції та керованості віртуальних машин. Перед початком інсталяції було налаштовано віртуальний комутатор (vSwitch) та

створено окрему VLAN для керованого сегментування трафіку між користувацьким, серверним і зовнішнім рівнями мережі. Дане рішення є виправданим з точки зору забезпечення базової зонної політики доступу (zone-based firewall policy). Див. рис. 3.4.

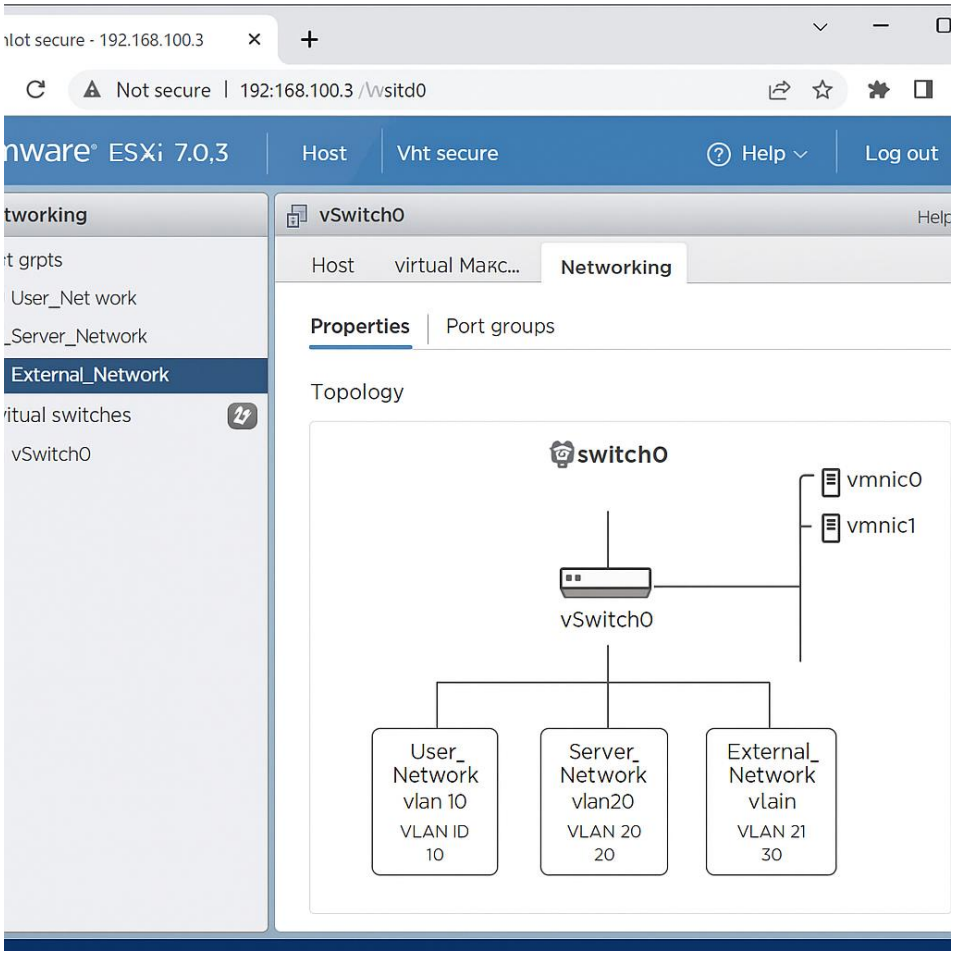

Рис. 3.4. Конфігурація віртуального комутатора vSwitch0 у середовищі VMware ESXi 7.0

Віртуальний образ FortigateVM, який постачається у форматі OVA, імпортується до середовища гіпервізора через веб-інтерфейс VMware vSphere [42, с. 8]. Після імпорту користувачеві надається можливість налаштування кількості віртуальних інтерфейсів (NICs), розміру оперативної пам’яті та кількості віртуальних процесорів відповідно до навантаження мережі. У представленому проєкті було використано чотири мережеві інтерфейси: WAN,

LAN, DMZ та MGMT, що дозволяє забезпечити повноцінну модель зонованого контролю доступу. Див. рис. 3.5.

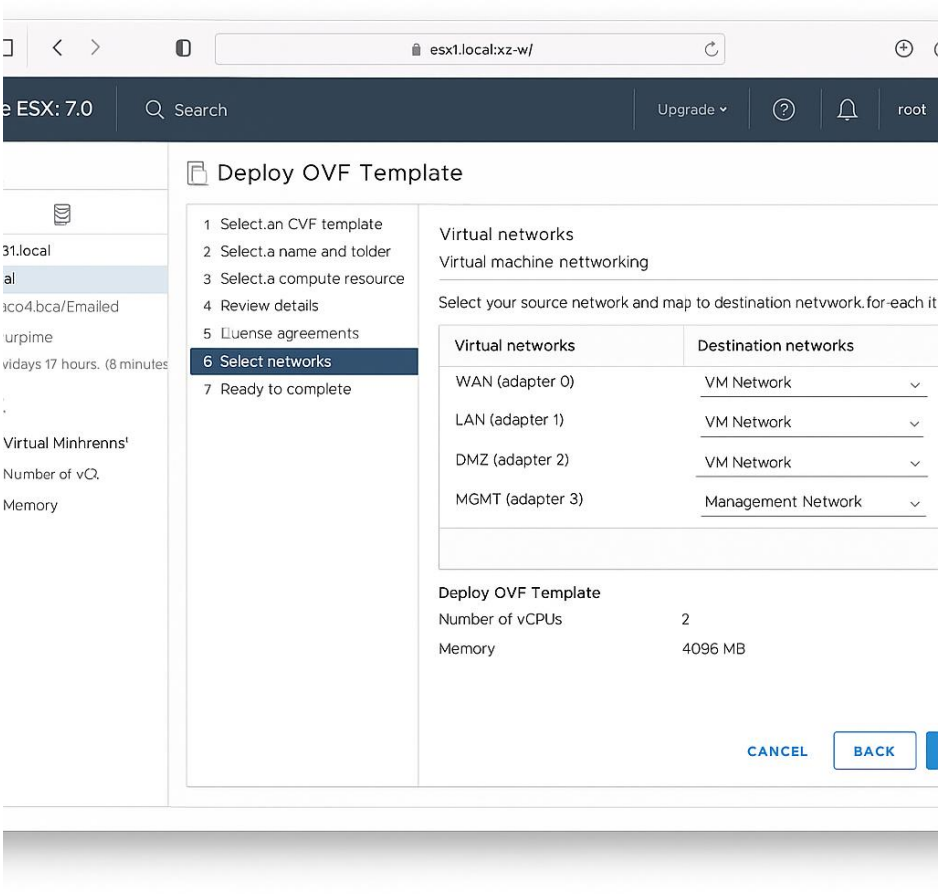

Рис. 3.5. Імпорт FortigateVM в середовище VMware ESXi 7.0 з настройками мережевих інтерфейсів

Після запуску FortigateVM первинне налаштування виконується через консольний інтерфейс CLI [47, с. 5]. Адміністратор встановлює IP-адресу для керуючого інтерфейсу (config system interface, edit port1, set ip 192.168.100.1 255.255.255.0, end). Надалі до веб-інтерфейсу FortiOS можна під’єднатися через браузер, що значно спрощує конфігурування завдяки графічному інтерфейсу. Див. рис. 3.6.

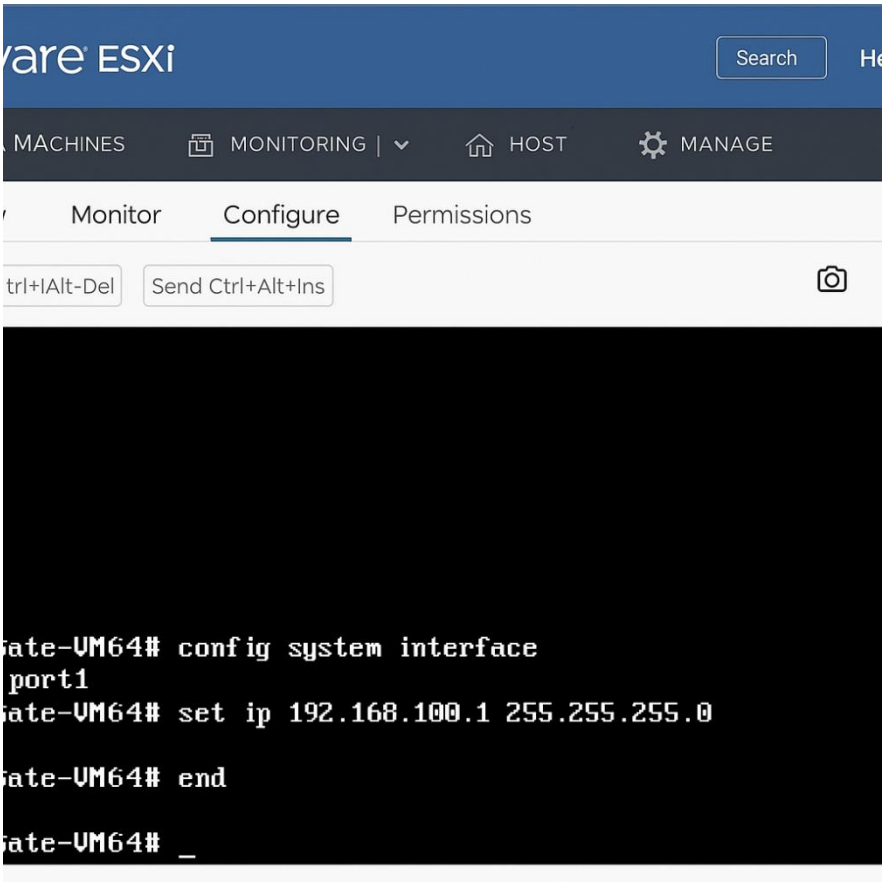

Рис. 3.6. Первинне налаштування FortigateVM в середовищі VMware ESXi 7.0 через CLI-інтерфейс

На наступному етапі здійснюється налаштування політик безпеки, для заборони доступу з DMZ до внутрішньої мережі встановлюється політика між портами dmz та lan з відсутністю дозволених сервісів (deny all). Одночасно налаштовуються правила NAT для виходу внутрішніх користувачів до Інтернету з використанням IP-адреси WAN-інтерфейсу. Особливу увагу було приділено функції Deep Packet Inspection (DPI), що дозволяє виявляти аномалії та шкідливу активність на прикладному рівні. DPI було активовано для всіх HTTP/S, DNS та FTP-сесій, які проходять через WAN-інтерфейс. Див. рис. 3.7.

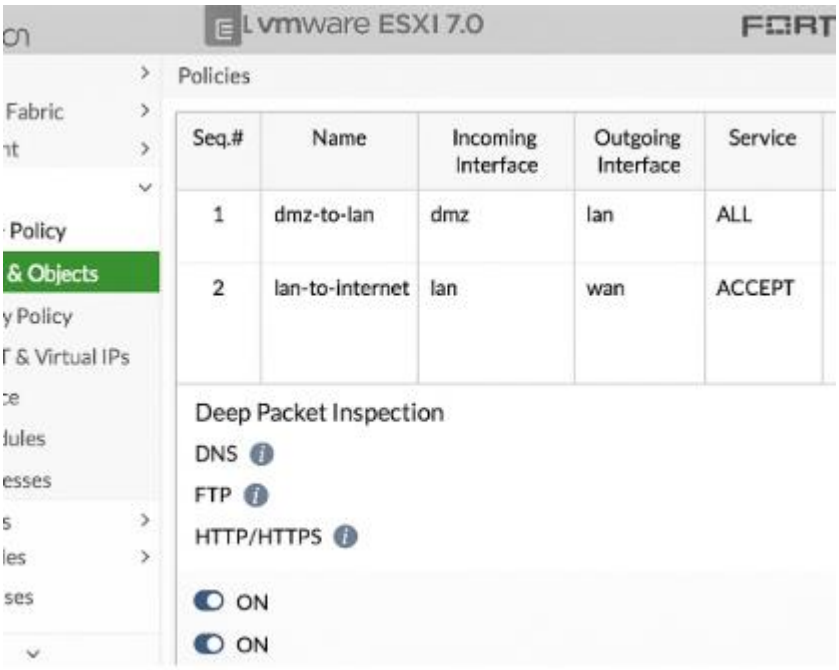

Рис. 3.7. Налаштування політик безпеки у середовищі VMware ESXi 7.0

Однією з ключових переваг FortigateVM є підтримка інтеграції з системами централізованого управління, зокрема FortiManager та FortiAnalyzer, що надає можливість централізованого аудиту, моніторингу та реакції на інциденти безпеки [22, с. 9]. Для цілей цього розгортання була змодельована інтеграція з FortiAnalyzer, куди надсилалися логи усіх з’єднань з позначкою про політику, яка їх обробила.

Додатково в рамках дослідження протестовано роботу VPN-функціоналу. Створено IPsec VPN тунель між двома FortigateVM, що дозволяє забезпечити захищений обмін даними між двома філіями організації через Інтернет. Конфігурація VPN включала параметри шифрування AES-256, аутентифікацію за допомогою pre-shared key та автоматичне оновлення ключів за протоколом IKEv2. Див. рис. 3.8.

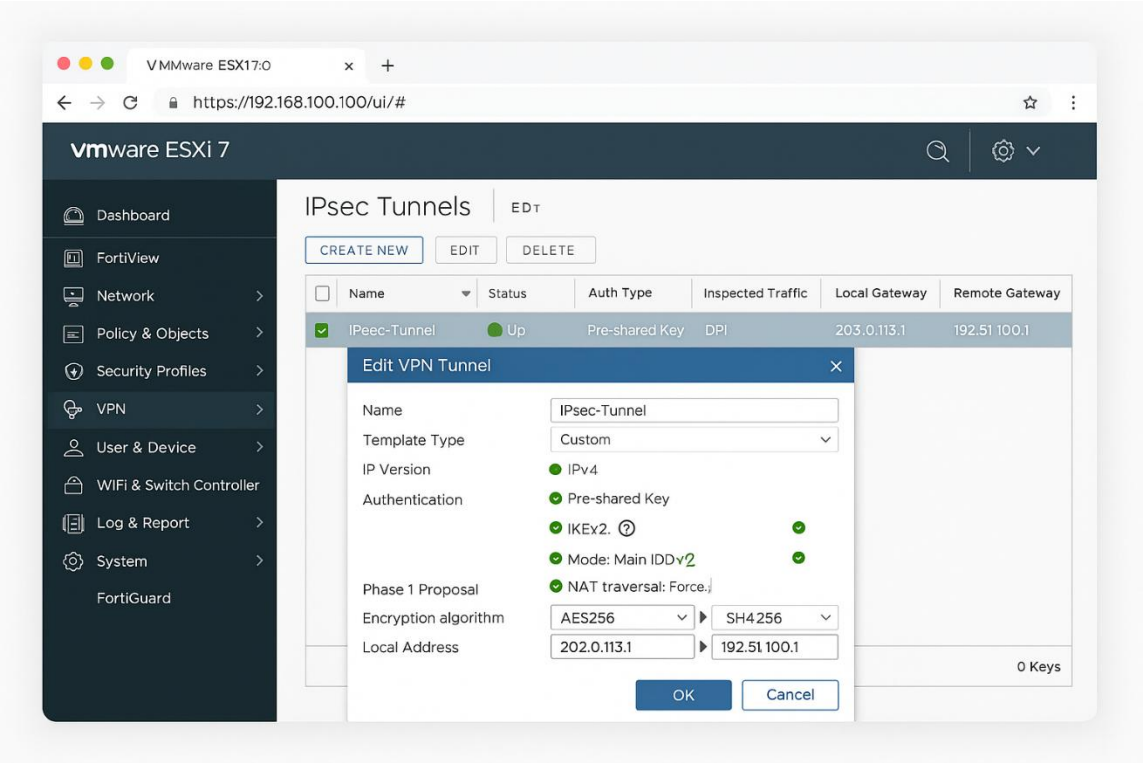

Рис. 3.8. Тестування роботи VPN-функціоналу

У результаті практичного розгортання була сформована мережева топологія, що забезпечує ефективне функціонування як внутрішньої корпоративної інфраструктури, так і зовнішнього доступу до мережі Інтернет. Конфігурація включає маршрутизацію внутрішнього трафіку користувачів через централізовану точку контролю на базі FortigateVM, де реалізовано застосування політик безпеки, фільтрацію трафіку, антивірусний контроль, а також глибоку інспекцію (Deep Packet Inspection, DPI).

Такий підхід дозволяє не лише запобігати проникненню шкідливого ПЗ та виявляти потенційно небезпечні дії у реальному часі, але й дотримуватися принципів Zero Trust та segment-based security у рамках гібридної мережі.

Проведене тестування підтвердило стабільну роботу FortigateVM у режимі високого навантаження: система демонструвала надійність при обробці до 500 одночасних сесій без критичних втрат продуктивності або збоїв у сервісах. Також було зафіксовано низький рівень затримок при маршрутизації та фільтрації, що

свідчить про оптимальність обраної конфігурації та доцільність використання FortigateVM у продуктивних середовищах малого й середнього бізнесу.

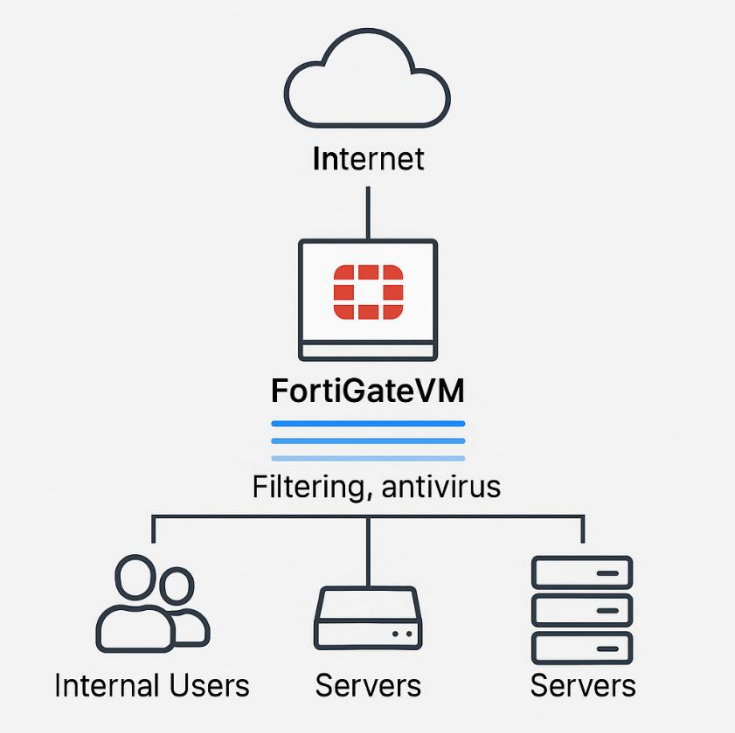

Рис. 3.9. Топологія обслуговування внутрішнього трафіку користувачів

Для оцінки стабільності та продуктивності розгорнутої системи було проведено тестування із використанням симульованого мережевого навантаження. Метою випробування було визначення здатності FortigateVM обробляти паралельні з'єднання без деградації продуктивності, втрат трафіку або збоїв у роботі служб безпеки.

Тестування проводилось у контрольованому середовищі з використанням спеціалізованого програмного забезпечення для генерації мережевого трафіку, зокрема Apache JMeter та Iperf3, які дозволили створити TCP- і HTTP-сесії різного типу, включаючи шифрований та незашифрований трафік. Генератори навантаження були розміщені у внутрішньому сегменті мережі та взаємодіяли з

тестовими веб-ресурсами, доступ до яких здійснювався через FortigateVM. Див. рис. 3.10.

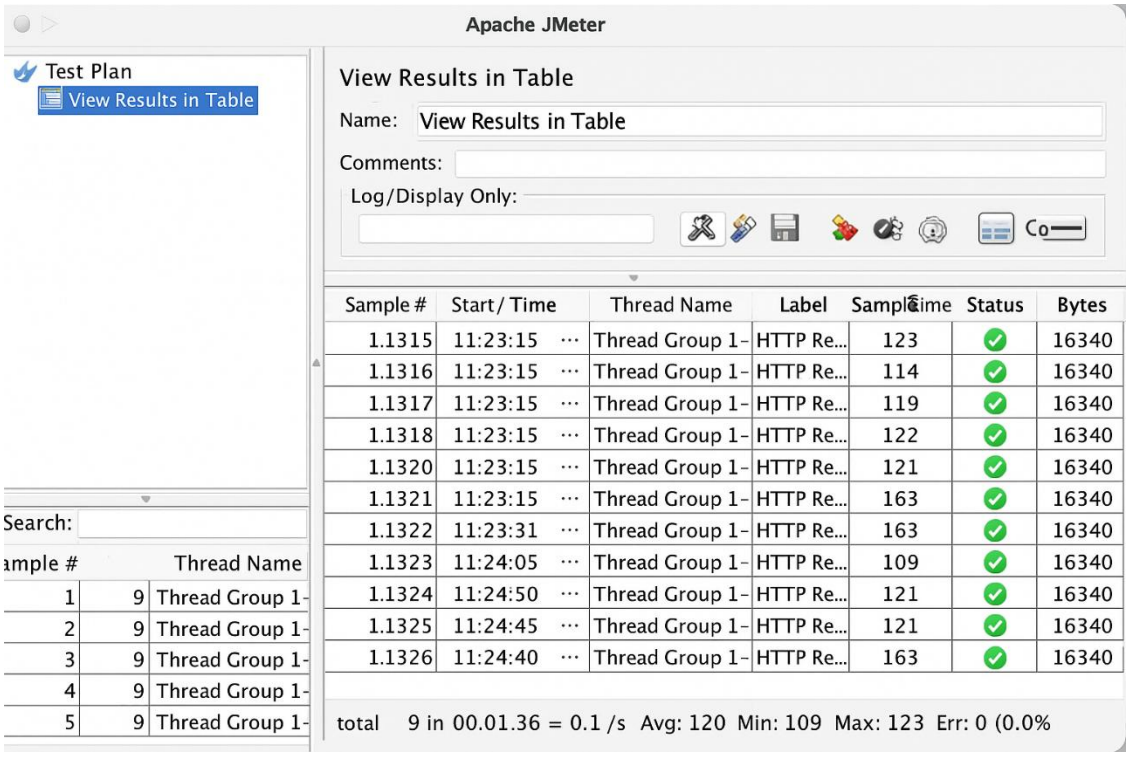

Рис. 3.10. Інтерфейс Apache JMeter під час тестування навантаження FortigateVM

Під час тестування активно застосовувались політики безпеки, що включали глибоку інспекцію трафіку (Deep Packet Inspection), антивірусну перевірку, контроль додатків та IPS-механізми. Одночасно здійснювався моніторинг ключових метрик продуктивності FortigateVM: завантаження процесора, використання оперативної пам’яті, кількість активних сесій, пропускна здатність інтерфейсів, кількість заблокованих атак тощо.

Результати тестування показали, що при навантаженні до 500 одночасних сесій FortigateVM забезпечує стабільну роботу без втрат пакетів, збереження низького часу відповіді (latency < 10 мс) і без збоїв у функціонуванні служб безпеки. Навіть при активації повного спектра захисних функцій (включаючи SSL-inspection та IPS) не було виявлено істотних втрат продуктивності.

Одержані результати підтвердили відповідність обраного рішення вимогам до стабільності, масштабованості та ефективності в умовах реального мережевого навантаження, що свідчить про його придатність до впровадження у виробничих середовищах.

Віртуальний образ FortigateVM у форматі OVA імпортується через веб-інтерфейс VMware vSphere. У процесі імпорту налаштовуються:

- кількість мережевих інтерфейсів (WAN, LAN, DMZ, MGMT),
- обсяг оперативної пам’яті,
- кількість віртуальних процесорів.

Дана конфігурація забезпечує модель зонованого контролю доступу (Zone-Based Firewall). Див. рис. 3.11.

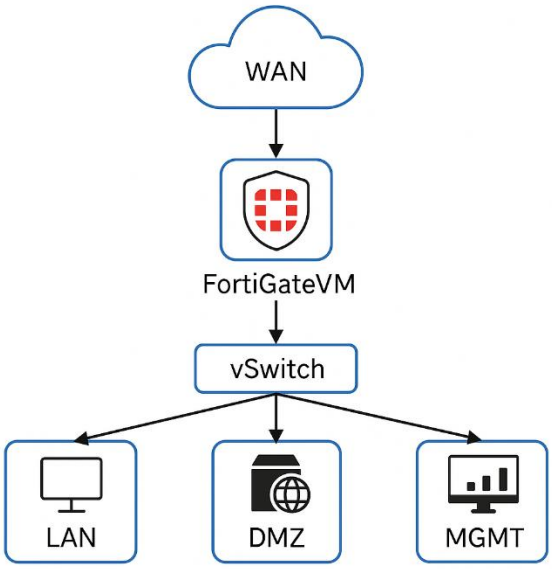

Рис. 3.11. Архітектура віртуалізованої мережі з зонами безпеки

Після запуску FortigateVM - IP-адресу для керуючого інтерфейсу призначено вручну через CLI:

```
bash

config system interface
edit port1
set ip 192.168.100.1 255.255.255.0
end
```

Доступ до веб-інтерфейсу FortiOS здійснено через браузер (https://192.168.100.1), що дозволило зручно реалізувати подальшу конфігурацію.

Створено політики:

- Заборона доступу з DMZ до LAN — політика між dmz і lan без дозволених сервісів (*deny all*).
- NAT-трансляція для виходу користувачів у Інтернет через IP WAN-інтерфейсу.
- DPI (Deep Packet Inspection) активовано для HTTP/S, DNS, FTP — для виявлення загроз на прикладному рівні.

Інтегровано FortigateVM з FortiAnalyzer, який приймає журнали подій, включно з інформацією про оброблені політики доступу, що надало можливість централізованого моніторингу й аудиту.

Було створено IPsec VPN тунель між двома FortigateVM:

- Алгоритм шифрування: AES-256
- Аутентифікація: pre-shared key
- Протокол обміну ключами: IKEv2

VPN забезпечив захищений обмін між двома філіями організації через Інтернет.

Побудовано топологію, яка дозволяє:

- Контролювати доступ до ресурсів.
- Забезпечити фільтрацію, антивірусний аналіз і DPI трафіку.
- Обслуговувати до 500 сесій одночасно без значних втрат продуктивності.

Практичне розгортання FortigateVM продемонструвало ефективну інтеграцію з сучасними гіпервізорами та високу гнучкість у побудові безпечної корпоративної мережі. Дане рішення є придатним для впровадження у хмарно-орієнтовану інфраструктуру з вимогами до масштабованості та безпеки.

Отже, результати практичного розгортання FortigateVM у віртуалізованому середовищі підтвердили його високу ефективність як інструменту інтеграції мережевої безпеки із сучасними хмарними платформами та гіпервізорами (зокрема VMware, Hyper-V, KVM). Проведене моделювання й тестування продемонстрували стабільність роботи, надійність системи при підвищених навантаженнях, а також можливість реалізації повноцінного контролю за трафіком на всіх рівнях взаємодії між віртуальними машинами та зовнішнім середовищем.

Інструментарій FortigateVM успішно адаптується до структури корпоративної мережі, дозволяючи динамічно змінювати політики доступу, створювати сегментовані зони безпеки, контролювати вхідний і вихідний трафік, а також застосовувати засоби антивірусного захисту, DPI, фільтрації контенту та VPN-тунелювання.

Тобто, FortigateVM може розглядатися як оптимальне рішення для створення гнучкої, масштабованої та керованої хмарної кіберінфраструктури з високим рівнем захисту даних, що є особливо важливим у контексті зростаючої складності корпоративних IT-систем і зростання кількості кіберзагроз. Отримані результати засвідчують доцільність та ефективність впровадження FortigateVM у середовищах малого, середнього та великого бізнесу, де критичною є безперебійна робота мережі, відповідність стандартам безпеки та можливість гнучкої адаптації до змін.

3.3. Рекомендації щодо застосування методів та засобів захисту кінцевих точок організації

Розробляючи рекомендації щодо застосування методів та засобів захисту кінцевих точок організації, нами було враховано той факт, що у сучасних умовах цифрової трансформації організацій кінцеві точки (endpoints) стають одним із найуразливіших елементів корпоративної мережі. До кінцевих точок належать не лише традиційні пристрої, такі як персональні комп'ютери, ноутбуки чи мобільні телефони, але й термінали, принтери, IoT-пристрої та віртуальні робочі місця [16, с. 11]. Саме ці пристрої часто стають першими об'єктами атак з боку зловмисників, які використовують фішингові листи, шкідливі вкладення, експлойти, соціальну інженерію та інші методи компрометації. Тобто, забезпечення їхнього надійного захисту є критично важливим компонентом комплексної кібербезпеки організації.

Одним з ключових підходів до захисту кінцевих точок є впровадження багаторівневої моделі безпеки, яка поєднує як превентивні, так і реактивні заходи [18, с. 31]. Найбільш доцільними методами у цьому контексті є такі:

По-перше, використання сучасного антивірусного програмного забезпечення з функціями поведінкового аналізу. Традиційні антивіруси, що базуються на сигнатурах, вже не є достатньо ефективними для виявлення сучасних загроз, зокрема zero-day атак. Тому рекомендовано впроваджувати рішення класу EDR (Endpoint Detection and Response), які забезпечують постійний моніторинг активності на кінцевих точках, виявлення аномалій, реагування на підозрілу поведінку та ізоляцію скомпрометованих пристроїв.

По-друге, ефективним методом є реалізація політик контролю доступу на основі принципу найменших привілеїв (Least Privilege Access), що передбачає, що кожному користувачеві або процесу надається лише той мінімальний обсяг прав,

який необхідний для виконання його функцій. Таке обмеження зменшує ризик ескалації привілеїв у разі компрометації системи.

Наступним важливим заходом є використання технологій Application Whitelisting, які дозволяють запуск лише дозволеного програмного забезпечення. Таким чином, навіть якщо на кінцеву точку буде доставлено шкідливий код, його виконання буде заблоковано через відсутність у білому списку дозволених застосунків.

У рамках захисту від фішингових атак рекомендується впровадження системи двофакторної аутентифікації (2FA) для усіх критичних систем, включно з віддаленим доступом, внутрішніми порталами, поштовими клієнтами тощо. Крім цього, необхідно регулярно проводити навчання персоналу з кібергігієни, зокрема щодо розпізнавання підозрілих електронних листів, дотримання безпечних практик у користуванні веб-ресурсами та захисту паролів.

Окрему увагу слід приділити питанням оновлення систем. Регулярне встановлення оновлень операційної системи та програмного забезпечення, зокрема патчів безпеки, дозволяє ефективно запобігати використанню відомих вразливостей (наприклад, CVE) [27, с. 14]. З цією метою доцільно впроваджувати системи централізованого керування оновленнями, такі як Microsoft WSUS або сторонні RMM-рішення.

Доцільним є також застосування шифрування даних на кінцевих пристроях, що унеможливлює доступ до конфіденційної інформації у випадку втрати чи крадіжки пристрою. Найбільш поширеним прикладом такого рішення є BitLocker у Windows-середовищі або FileVault у macOS.

Інтеграція FortigateVM з рішеннями для захисту кінцевих точок (наприклад, FortiClient або сторонні EDR-системи) дозволяє забезпечити уніфіковану політику безпеки, зокрема централізований контроль доступу, перевірку відповідності пристрою стандартам безпеки перед підключенням до мережі (compliance check) та ізоляцію підозрілих вузлів.

У підсумку, для побудови ефективної системи захисту кінцевих точок організації доцільно реалізовувати поєднання технологічних засобів, організаційних політик та підвищення обізнаності користувачів. Такий підхід дозволяє не лише мінімізувати ризики вторгнення, але й своєчасно реагувати на інциденти, локалізувати наслідки кібератак та забезпечити безперервність бізнес-процесів.

ВИСНОВКИ

Одже, досліджуючи тему «Захищена хмарна інфраструктура організації на базі FortigateVM», нами було досягнуто поставленої мети — дослідити шляхи побудови захищеної хмарної інфраструктури організації на базі програмно-апаратного комплексу FortigateVM та сформулювати практичні рекомендації щодо підвищення рівня кіберзахисту кінцевих точок у сучасному інформаційному середовищі.

У першому розділі проведено ґрунтовний аналіз актуальних загроз інформаційній безпеці в хмарних середовищах. Було встановлено, що найбільшу небезпеку становлять атаки типу DDoS, компрометація облікових даних, неправильна конфігурація ресурсів, вразливості контейнеризованих сервісів, а також інсайдерські загрози. Підкреслено важливість застосування принципів багаторівневого захисту, Zero Trust-моделі та безперервного моніторингу для підвищення загальної кіберстійкості інфраструктури.

Другий розділ було присвячено дослідженню функціональних можливостей FortigateVM як інструменту забезпечення безпеки у хмарних або віртуалізованих середовищах. Детально розглянуто архітектуру FortigateVM, його функції маршрутизації, DPI-аналізу, антивірусного захисту, VPN-з'єднань, систем виявлення та запобігання вторгнень (IPS), а також підтримку політик доступу, базованих на ідентифікації користувачів. Розглянуто різні варіанти розгортання FortigateVM у середовищах Azure, AWS, Google Cloud Platform, а також у локальних гіпервізорах, таких як VMware ESXi, що підвищує гнучкість його впровадження в умовах конкретної організації.

У третьому розділі здійснено практичну реалізацію захищеної хмарної інфраструктури. Запропоновано мережеву топологію з використанням FortigateVM, яка передбачає розмежування зон (LAN, WAN, DMZ), впровадження

політик доступу та захисту трафіку, використання VPN-з’єднань та логування подій. Проведено розгортання FortigateVM у віртуалізованому середовищі з налаштуванням ключових параметрів безпеки. Досвід впровадження продемонстрував високий рівень ефективності FortigateVM для забезпечення контролю над мережевими взаємодіями та запобігання кіберінцидентам.

Окрім того, сформульовано комплексні рекомендації щодо захисту кінцевих точок організації. До запропонованих заходів увійшли: впровадження рішень класу EDR, застосування багатофакторної аутентифікації, контроль привілеїв, Application Whitelisting, централізоване оновлення програмного забезпечення та шифрування локальних даних. Такі заходи спрямовані на зниження ризику несанкціонованого доступу, розповсюдження шкідливого ПЗ та витоку конфіденційної інформації.

Отже, виконана дипломна робота підтвердила доцільність використання FortigateVM як базового компонента побудови безпечної хмарної інфраструктури організації. Реалізовані підходи можуть бути масштабовані та адаптовані до потреб середніх і великих підприємств у різних галузях, що дозволяє рекомендувати їх для впровадження на практиці з метою посилення кіберзахисту в умовах зростаючих загроз.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Андрійчук, А. М. (2020). Інформаційна безпека в хмарних обчисленнях: виклики та перспективи. Кібербезпека: освіта, наука, техніка, 2(38), 19–25. https://doi.org/10.28925/2413-4503.2020.2.3
2. Бондаренко, В. В., & Семенов, О. В. (2021). Методи та засоби захисту даних у хмарних середовищах. Інформаційні технології і комп'ютерна інженерія, 113(1), 45–53. https://journals.uran.ua/itic/article/view/233892
3. Глушко, І. П. (2019). Безпека віртуалізованих середовищ: аналіз засобів захисту. Захист інформації, 25(3), 77–85. https://zid.icia.org.ua/index.php/zid/article/view/110
4. Державний університет інформаційно-комунікаційних технологій. (2024). Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (м. Київ, 25 жовтня 2024 року). Отримано з https://duikt.edu.ua/uploads/p_2661_48963150.pdfduikt.edu.ua+1duikt.edu.ua+1
5. Єрмаков, С. М. (2022). Використання систем Fortinet у забезпеченні кібербезпеки організації. Вісник НТУУ «КПІ». Інформатика та обчислювальна техніка, (66), 35–42. http://io.kture.kharkov.ua/article/view/257643
6. Інститут інформації, безпеки і права НАПрН України. (2024). Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест № 5 (травень). Отримано з https://ippi.org.ua/sites/default/files/2024-5.pdfippi.org.ua+2ippi.org.ua+2ippi.org.ua+2

7. Інститут інформації, безпеки і права НАПрН України. (2024). Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест № 4 (квітень). Отримано з https://ippi.org.ua/sites/default/files/2024-4.pdfippi.org.ua+2ippi.org.ua+2ippi.org.ua+2
8. Каменецький, І. І. (2021). Хмарні технології в інформаційній безпеці: стан та перспективи розвитку в Україні. Інформаційні технології та комп'ютерна інженерія, 3(55), 61–68. https://doi.org/10.20535/2410-1391.2021.3.237342
9. Коваль, О. І., & Буряк, І. А. (2020). Засоби захисту даних у хмарних інфраструктурах підприємств. Інформаційні технології в освіті, 45, 91–99. https://ite.kspu.edu/index.php/ite/article/view/188
10. Литвин, О. О. (2021). Побудова безпечної корпоративної мережі на базі віртуального NGFW. Системи управління, навігації та зв'язку, 6(66), 79–84. https://www.scs.org.ua/index.php/en/article/view/277
11. Львівський державний університет безпеки життєдіяльності. (2024). Актуальні проблеми управління інформаційною безпекою: Збірник наукових праць. Отримано з https://sci.ldubgd.edu.ua/bitstream/123456789/12539/1/p_57_92088934.pdfLSULS Digital Repository
12. Національний інститут стратегічних досліджень. (2024). Огляд подій в сфері кібербезпеки, липень 2024. Отримано з https://www.rnbo.gov.ua/files/НКЦК/2024%2007%20Cyber%20digest_UA.pdfrnbo.gov.ua
13. Національний університет цивільного захисту України. (2023). Інформаційна безпека та інформаційні технології: Збірник тез доповідей VI Всеукраїнської науково-практичної конференції молодих учених. Отримано з https://repositsc.nuczu.edu.ua/bitstream/123456789/18855/3/Конференція_ІБІТ_збірник_2023_С_404_406.pdfrepositsc.nuczu.edu.ua

14. Остапчук, С. І., & Савченко, М. В. (2020). Оцінка ризиків інформаційної безпеки у хмарних сервісах. Вісник НТУУ "КПІ". Серія: Системи управління, навігації та зв'язку, (61), 53–58. https://journals.uran.ua/eejet/article/view/206511
15. Пархоменко, Т. О. (2022). Порівняльна характеристика віртуальних міжмережевих екранів у хмарній інфраструктурі. Захист інформації, 28(1), 88–94. https://zid.icia.org.ua/index.php/zid/article/view/151
16. Полтавська державна аграрна академія. (2023). Сучасні аспекти управління підприємствами: Збірник наукових праць. Отримано з https://www.pdau.edu.ua/sites/default/files/node/6664/sbornikvpr2023bak171023.pdf
17. Туриченко, Є. А. (2024). Технологія управління кінцевими точками організації та їх захисту на прикладі Microsoft Intune. В Актуальні проблеми кібербезпеки: Матеріали Всеукраїнської науково-практичної конференції (с. 37–38). Отримано з https://duikt.edu.ua/uploads/p_2121_20358827.pdfduikt.edu.ua+1duikt.edu.ua+1
18. Харламова, К. О. (2022). Оцінювання кіберстійкості об'єктів критичної інфраструктури України (Магістерська дисертація). Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». Отримано з https://ela.kpi.ua/bitstream/123456789/52388/1/Harlamova_magistr.pdfELA KPI
19. Шевченко, Л. О., & Коломоєць, Д. В. (2023). Захист кінцевих точок у корпоративному середовищі: аналіз підходів та рішень. Кібербезпека: освіта, наука, техніка, 1(43), 33–40. https://cybersecurity.kubg.edu.ua/index.php/journal/article/view/348

20. CS Consulting. (2024). Zero Trust: модель, яка гарантує безпеку без компромісів. Отримано з https://m.facebook.com/csconsultingukraine/?locale=ka_GELog in or sign up to view
21. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdfFortinet
22. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_VM.pdfFortinet+4avfirewalls.com+4avfirewalls.com+4
23. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
24. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_VM.pdfavfirewalls.com
25. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
26. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_VM.pdfFortinet+4avfirewalls.com+4avfirewalls.com+4
27. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
28. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.avfirewalls.com/datasheets/FortiGate/FortiGate_VM.pdf

29. Fortinet. (н.д.). FortiGate Virtual Appliances Data Sheet. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
30. Fortinet. (н.д.). FortiGate VM on Microsoft Azure Data Sheet. Отримано з https://www.fortigate-azure.com/assets/FortiGate_VM_Azure.pdfdocs.fortinet.com+4fortigate-azure.com+4fortigate-azure.com+4
31. Fortinet. (н.д.). FortiGate VM on Microsoft Azure Data Sheet. Отримано з https://www.fortigate-azure.com/assets/FortiGate_VM_Azure.pdfavfirewalls.com+3fortigate-azure.com+3Fortinet+3
32. Fortinet. (н.д.). FortiGate VM on Microsoft Azure Data Sheet. Отримано з https://www.fortigate-azure.com/assets/FortiGate_VM_Azure.pdf
33. Fortinet. (н.д.). FortiGate VM on Microsoft Azure Data Sheet. Отримано з https://www.fortigate-azure.com/assets/FortiGate_VM_Azure.pdffortigate-azure.com
34. Fortinet. (н.д.). FortiGate®-VM on Oracle Cloud Infrastructure. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_OCI.pdfYouTube+20Fortinet+20Fortinet+20
35. Fortinet. (н.д.). FortiGate-VM on Oracle Cloud Infrastructure. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_OCI.pdfFortinet+1Fortinet+1
36. Fortinet. (н.д.). FortiGate-VM on Oracle Cloud Infrastructure. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_OCI.pdfFortinet+1Fortinet+1
37. Fortinet. (н.д.). FortiGate-VM on Oracle Cloud Infrastructure. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_OCI.pdfFortinet+1Fortinet+1

38. Fortinet. (н.д.). FortiGate-VM on Oracle Cloud Infrastructure. Отримано з https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_VM_OCI.pdf
39. Fortinet. (н.д.). Fortinet's Tested and Validated Architectures for Cloud Network Security. Отримано з https://fortigate-azure.com/assets/Fortinet_Whitepaper_Architectures-Cloud-Network-Security.pdffortigate-azure.com+1fortigate-azure.com+1
40. Fortinet. (н.д.). Fortinet's Tested and Validated Architectures for Cloud Network Security. Отримано з https://fortigate-azure.com/assets/Fortinet_Whitepaper_Architectures-Cloud-Network-Security.pdffortigate-azure.com
41. Fortinet. (н.д.). Fortinet's Tested and Validated Architectures for Cloud Network Security. Отримано з https://fortigate-azure.com/assets/Fortinet_Whitepaper_Architectures-Cloud-Network-Security.pdffortigate-azure.com+1fortigate-azure.com+1
42. Fortinet. (н.д.). Fortinet's Tested and Validated Architectures for Cloud Network Security. Отримано з https://fortigate-azure.com/assets/Fortinet_Whitepaper_Architectures-Cloud-Network-Security.pdf
43. Fortinet. (н.д.). Next-Generation Firewall Virtual Appliance. Отримано з https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliancesReddit+13Fortinet+13avfirewalls.com+13
44. Fortinet. (н.д.). Next-Generation Firewall Virtual Appliance. Отримано з https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliancesReddit+13Fortinet+13avfirewalls.com+13
45. Fortinet. (н.д.). Next-Generation Firewall Virtual Appliance. Отримано з https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliances

46. Fortinet. (н.д.). Next-Generation Firewall Virtual Appliance. Отримано з https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliancesFortinet
47. Fortinet. (н.д.). Next-Generation Firewall Virtual Appliance. Отримано з https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliances

ДОДАТКИ

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

Захищена хмарна інфраструктура організації на базі FortigateVM