Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Дослідження методів захисту відомих хмарних платформ

Виконав: студент II курсу, групи СБд-2
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Шимчук Г.В. (прізвище та ініціали)

Керівник (підпис) Козак Р.О. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т.Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н.В. (прізвище та ініціали)

Рецензент (підпис) Приймак М.В. (прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«____» _____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Шимчуку Григорію Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження методів захисту відомих хмарних платформ

Керівник роботи Козак Руслан Орестович, к.т.н., доцент кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «_01_» _грудня_ 2022 року № _4/7-971_

2. Термін подання студентом завершеної роботи 14 грудня 2022р.

3. Вихідні дані до роботи Наукові публікації про загрози хмарної безпеки та проблем безпеки хмарних середовищ

4. Зміст роботи (перелік питань, які потрібно розробити): Вступ, 1 Інструменти організації безпеки хмарних серверів, 1.1 Розгляд моделей та принципів організації безпеки хмарного серверу, 1.2 Аналіз еталонних архітектур для IaaS, 1.3 Висновок до першого розділу, 2 Варіанти використання моделей архітектури, 2.1 Потік вхідного трафіку у публічній хмарі, 2.2 Потік вихідного трафіку у еталонних архітектурах для публічного IaaS, 2.3 Потік трафіку «схід-захід» у публічному хмарному IaaS, 2.4 Висновок до другого розділу, 3 Практична реалізація, 3.1 Проведення експериментального дослідження на час реакції вторгнень в хмарному сховищі, 3.2 Виявлення вторгнень за допомогою спеціальних агентів, 3.3 Висновок до третього розділу, 4 Охорона праці та безпека в надзвичайних ситуаціях, 4.1 Охорона праці, 4.2 Безпека в надзвичайних ситуаціях, Висновки, Перелік використаних джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів) 1 Титульна сторінка. 2 Тема. Мета. Об'єкт. Предмет дослідження. 3 Завдання дослідження. 4. Повна модель спільної відповідальності для загальнодоступного IaaS, 5. Структурна схема архітектури нульової довіри для публічних і приватних IaaS, 6. Атрибути мікро- та макросегемнтацій, 7. Визначення блейдів безпеки згідно сегментів безпеки, 8 Оптимізований метод для «Lift and Shift», 9. Еталонна архітектура для Microsoft Azure, 10. Еталонна архітектура для GCP, 11. Еталонна архітектура для AWS, 12. Різниця термінологій різних хмарних сервісів, 13. Схематичне зображення хмарного файлового сховища, 14. Класична модель агентів ієрархії з зв'язками по вертикалі, 15 Висновки. 16 Апробація результатів валіфіаційної роботи. 17 Завершальний слайд.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., к.т.н., доцент		
Безпека в надзвичайних ситуаціях	Клепчик В.М., проректор з адміністративно-господарської роботи та будівництва		

7. Дата видачі завдання 14 листопада 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	14.11.2022-15.11.2022	*Виконано*
2.	Підбір наукових джерел про хмарні платформи	16.11.2022-20.11.2022	*Виконано*
3.	Переклад та опрацювання наукових джерел про		
	дослідження методів захисту відомих хмарних		
	платформ	21.11.2022-23.11.2022	*Виконано*
4.	Виконання дослідження щодо аналіз інструментів для		
	організації інфраструктури та безпеки публічної		
	хмари	24.11.2022-27.11.2022	*Виконано*
5.	Оформлення розділу «Інструменти організації		
	безпеки хмарних серверів»	28.11.2022-30.11.2022	*Виконано*
6.	Оформлення розділу «Варіанти використання		
	моделей архітектури»	01.12.2022-04.12.2022	*Виконано*
7.	Оформлення розділу «Практична реалізація»	05.12.2022-07.12.2022	*Виконано*
8.	Виконання завдання до підрозділу «Охорона праці»	08.12.2022-09.12.2022	*Виконано*
9.	Виконання завдання до підрозділу «Безпека в надзви-		
	чай них ситуаціях»	10.12.2022-11.12.2022	*Виконано*
10.	Оформлення кваліфікаційної роботи	12.12.2022-13.12.2022	*Виконано*
11.	Нормоконтроль	14.12.2022-15.12.2022	*Виконано*
12.	Перевірка на плагіат	9.12.2022	*Виконано*
13.	Попередній захист кваліфікаційної роботи	16.12.2022	*Виконано*
14.	Захист кваліфікаційної роботи	23.12.2022	

Студент _____ Шимчук Г.В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Дослідження методів захисту відомих хмарних платформ // Кваліфікаційна робота освітнього рівня «Магістр» // Шимчук Григорій Валерійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБд-2 // Тернопіль, 2022 // С. 74, рис. – 31, табл. – 5, додат. – 3, бібліогр. – 28.

Ключові слова: ХМАРА, ХМАРНІ СЕРВІСИ, ХМАРНІ СЕРВЕРИ, АРХІТЕКТУРА, БЕЗПЕКА, ВІДДАЛЕНИЙ ДОСТУП, МОДЕЛЬ, IAAS.

Кваліфікаційна робота присвячена дослідженню методів захисту відомих хмарних платформ.

У першому розділі проводиться аналіз інструментів для організації інфраструктури та безпеки публічної хмари: розгляд еталонних архітектур, опис моделей та принципів побудови серверу. Також проводиться характеристика моделі надання хмарних послуг IaaS та сегмент її безпеки.

В другому розділі розглядаються варіанти використання описаних інструментів у організації публічного та локального трафіку хмарного серверу, віддаленого доступу до корпоративних ресурсів та віртуального робочого столу. Також, відбувається розгляд можливостей керування безпекою у налаштованій хмарі.

У третьому розділі проведені експериментальні дослідження на час реакції вторгнень в хмарному сховищі, наведено опис виявлення вторгнень за допомогою спеціальних агентів.

ANNOTATION

Study of methods of protection known cloud platforms // Qualification work of the educational level “Master” // Grygorii Shymchuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBd-2 group // Ternopil, 2022 // P. 74, fig. - 31, tables - 5, annexes - 3, references - 28.

Key words: cloud, cloud services, cloud servers, architecture, security, remote access, model, IAAS

The qualification work is devoted to the study of methods of protecting well-known cloud platforms.

In the first section, the analysis of tools for the organization of public cloud infrastructure and security is carried out: consideration of reference architectures, description of models and principles of server construction. The characterization of the IaaS cloud service provision model and its security segment are also carried out.

The second section considers options for using the described tools in the organization of public and local cloud server traffic, remote access to corporate resources, and a virtual desktop. Also, there is consideration of security management capabilities in the configured cloud.

In the third chapter, experimental studies on the reaction time of intrusions in cloud storage are conducted, a description of intrusion detection using special agents is provided.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CISO – Chief Information Security Officer (керівник відділу IT-безпеки, директор з IT-безпеки).

CIO – Chief Information Officer (головний менеджер з інформатизації, директор з інформаційних технологій).

CSO – Chief Security Officer (директор із комп'ютерної (інформаційної) безпеки, начальник служби інформаційної безпеки; особа, відповідальна за інформаційну безпеку організації).

CRM – Customer relationship management (Управління відносинами з клієнтами).

ZTNA – Zero Trust Network Access (Мережевий доступ з нульовою довірою).

SOA – Service-oriented architecture (Сервіс-орієнтована архітектура).

VPN – Virtual Private Network (Віртуальне приватне мережеве підключення).

VPC – Virtual Private Cloud (Віртуальна приватна хмара).

IRM – Integrated Risk Management (Інтегроване управління ризиками).

IT – Information Technology (інформаційні технології).

OT – Operational Technology (операційні технології).

IOT – Internet of Things (Інтернет речей).

ESG – Environmental, social, and governance (Екологічне, соціальне та корпоративне управління).

VM – Virtual Machine (Віртуальна машина).

LVM – Local Virtual Machine (Локальна віртуальна машина).

AWS – Amazon Web Services (Веб-сервіси Амазон).

ПЗ – програмне забезпечення.

БД – база даних.

ХТ – хмарні технології.

ЗМІСТ

ВСТУП

Актуальність теми. Хмарна безпека – це категорія IT, що, як прогнозується, буде мати найбільш швидкий та потужний ріст протягом наступних декількох років. Враховуючи, що організації збільшують фокус на метод екологічного, соціального та корпоративного управління (ESG), сторонній ризик, ризик кібербезпеки та ризик конфіденційності, спеціалісти Gartner прогнозують, що ринок інтегрованого управління ризиками (IRM) покаже двократне зростання до 2024 року, поки зростаюча конкуренція не призведе до здешевлення інструментів та рішень [1].

Мета і задачі дослідження. Метою даної кваліфікаційної роботи освітнього рівня «Магістр» є виявлення вторгнень в хмарні платформи, які дозволять оцінити умови фактичного доступу і стан системи, для своєчасної реакції на загрози безпеці.

Для досягнення поставленої мети було потрібно виконати наступні завдання:

- розглянути еталонні архітектури;
- провести опис моделей та принципів побудови серверу;
- провести характеристику моделі надання хмарних послуг IaaS та сегмент її безпеки;
- розглянути варіанти використання описаних інструментів у організації публічного та локального трафіку хмарного серверу, віддаленого доступу до корпоративних ресурсів та віртуального робочого столу;
- розглянути можливості керування безпекою у налаштованій хмарі;
- провести експериментальні дослідження на час реакції вторгнень в хмарному сховищі;
- навести опис виявлення вторгнень за допомогою спеціальних агентів.

Об’єкт дослідження. Процеси захисту інформації у відомих хмарних платформах.

Предмет дослідження. Оперативна задача управління та адміністрування сервісами захисту інформації у хмарних платформах.

Наукова новизна одержаних результатів кваліфікаційної роботи полягає у тому, що отримано результати експериментального дослідження на час реакції вторгнень в хмарному сховищі, що дозволяє виявляти вторгнення за допомогою спеціальних агентів.

Практичне значення одержаних результатів. Описано розширену модель «спільної відповідальності» для публічного IaaS, структуру та політику безпеки узгодженої з її принципами моделі «надання доступу з нульовою довірою», що необхідна для мінімізації потенційних ризиків атаки.

Апробація результатів магістерської роботи. Основні результати проведених досліджень обговорювались на: Міжнародній науковій конференції „Іван Пулюй: життя в ім’я науки та України“ (до 175-ліття від дня народження) (м.Тернопіль), X науково-технічній конференції «Інформаційні моделі, системи та технології» (м.Тернопіль), XI Міжнародній науково-технічній конференції молодих учених та студентів «Актуальні задачі сучасних технологій» (м.Тернопіль).

Публікації. Основні результати кваліфікаційної роботи опубліковано у трьох працях конференції (див. Додаток А, Б, В).

Структура й обсяг кваліфікаційної роботи. Кваліфікаційна робота складається зі вступу, чотирьох розділів, висновків, списку літератури із 28 найменувань та 3 додатків. Загальний обсяг кваліфікаційної роботи складає 76 сторінки, з них 58 сторінок основного тексту, який містить 34 рисунки та 5 таблиць.

1 ІНСТРУМЕНТИ ОРГАНІЗАЦІЇ БЕЗПЕКИ ХМАРНИХ СЕРВЕРІВ

1.1 Розгляд моделей та принципів організації безпеки хмарного серверу

Перед аналізом безпосередньо архітектур для хмарного IaaS розглянемо, як відбувається міграція та організація хмарних систем.

Lift and Shift (підйом та переміщення) – виконує таку міграцію, коли системи, робочі навантаження та дані переміщуються з локальної мережі в хмару з незначними змінами або без них. Ресурси, розміщені в центрі обробки даних, копіюються та «піднімаються» з локальної інфраструктури, після чого вони «переносяться» на єдине, багаторазове або гібридне хмарне середовище [2]. Основна мета даної стратегії міграції полягає у збереженні архітектури, яку організація вже сформувала на сервері публічної хмари, без внесення будь-яких відчутних змін у її дизайн. Іншими словами, це процес переміщення ідентичної копії робочого навантаження (включно з операційною системою, програмами та даними), дизайну мережі та влаштованими елементами керування. Ця перевага робить «Lift and Shift» найбільш швидкою і найменш дорогою стратегією міграції. З точки зору безпеки, метод «підйому та переміщення» також зберігає ідентичні системи управління та політики безпеки як мінімум на перших етапах трансформації хмари.

У 2022 році, з урахуванням стрімкого розвитку та відчутних змін у сегменті хмарних технологій, попит на використання стратегії міграції «Lift and Shift» значною мірою знизився у порівнянні з іншими розробками. Однак, все ще існує достатньо багато сценаріїв, реалізація яких потребує використання саме цієї стратегії:

- Коли для власника інфраструктури важлива маневренність, масштабвання та швидкість процесу міграції.

- За необхідності розгортання динамічного типу інфраструктури, ZTNA, чи макросегментації.
- Коли здійснюється перехід від CAPEX до OPEX.
- Коли встановлені програми, які підприємство закупило у сторонніх розробників. Наприклад, існує немало випадків, коли відсутня можливість перекодувати або змінити будь-яким інструментом додаток, оскільки його розробник не надає дозвіл на такі дії.
- Це ж стосується і програм, розробка та реалізація яких відбувалась до створення чи поширення хмарних сервісів. Зазвичай, вони також не можуть бути змінені чи перекодовані для ефективнішої роботи в хмарній архітектурі. Але більшість із цих застарілих системних додатків можуть ефективно працювати, якщо вони розміщені в хмарі, якщо їх залишити як є, і саме тут вступає в дію оперативна міграція.
- Переміщення локальних ресурсів резервного копіювання та відновлення в хмару дозволяє підприємствам скористатися перевагами масштабованості та більшої економічності. Але оскільки рефакторинг або зміна платформи можуть вплинути на вміст резервних копій, «Shift and Lift» матиме більше сенсу.
- У випадках, якщо критично важливі програми запускаються на локальних віртуальних машинах (LVM). Перенесення робочих навантажень LVM на віртуальні машини (VM) в хмарі, які служать подібним цілям, досить просте. Навпаки, налаштування хмарних віртуальних машин з нуля є складним процесом.
- Компанії, які перший раз починають використовувати ХТ, оскільки «Lift and Shift» є інтуїтивно найпростішим варіантом для міграції систем [2].

Простота та висока швидкість переміщення програми або навантаження в хмарне середовище є одними з найбільш суттєвих та поширених переваг для використання саме «Lift and Shift». Міграція для

представленої стратегії не вимагає наймати команду спеціалістів чи інженерів з великим досвідом роботи з ХТ, витратних за часом процесів зміни кодування та архітектури і подібні складні речі, даючи, при цьому, можливість організаціям використовувати всі переваги ХТ.

Для більшої успішності та ефективності при виконанні стратегії «Lift and Shift» рекомендується використовувати нову оптимізовану модель міграції, яка надає організаціям більшу гнучкість, підвищену швидкість виконання, більшу масштабованість, динамічну безпеку та управління положеннями для покращеної моделі спільної відповідальності в стратегіях хмарних центрів обробки даних. Ця модель під назвою «Lift-and-Shift Optimized» забезпечує гармонізацію принципів «Hub and Spoke» та розширену структуру «Zero Trust» для забезпечення повної видимості, а також контролю безпеки та відповідності. В результаті, все це мінімізовує можливості кібер-атаки та захищає від уразливостей, виявляє перехоплення та втрату даних [5].

У традиційній індустрії IT будь-яка організація має у власності повний стек середовища, а спеціально сформована команда з безпеки вносить необхідні зміни в інфраструктуру. У публічній хмарі IaaS деякі обов’язки передаються постачальникам хмарних послуг, а деякі – власникам додатків

Постачальники хмарних послуг, зазвичай, самостійно несуть відповідальність за гарантії безпеки власного хмарного середовища, однак групи забезпечення IT-безпеки несуть відповідальність за контроль безпеки інфраструктури, за яку вони відповідають. Коли організація переходить на PaaS/FaaS і SaaS, деякі обов’язки будуть передані групам DevSecOps.

Тим не менш, провідна дослідницька та консультаційна компанія Gartner заявила, що «до 2020 року 99% збоїв хмарної безпеки [6] відбуваються з вини клієнта». Таким чином, можна зробити висновок, що персональна мережева безпека в хмарному середовищі та інструменти

керування безпекою для публічного IaaS забезпечують єдиний простір для правильного розгортання елементів керування Zero Trust [6].

Розглянути повну модель спільної відповідальності для загальнодоступного IaaS можна на рисунку 1.1.

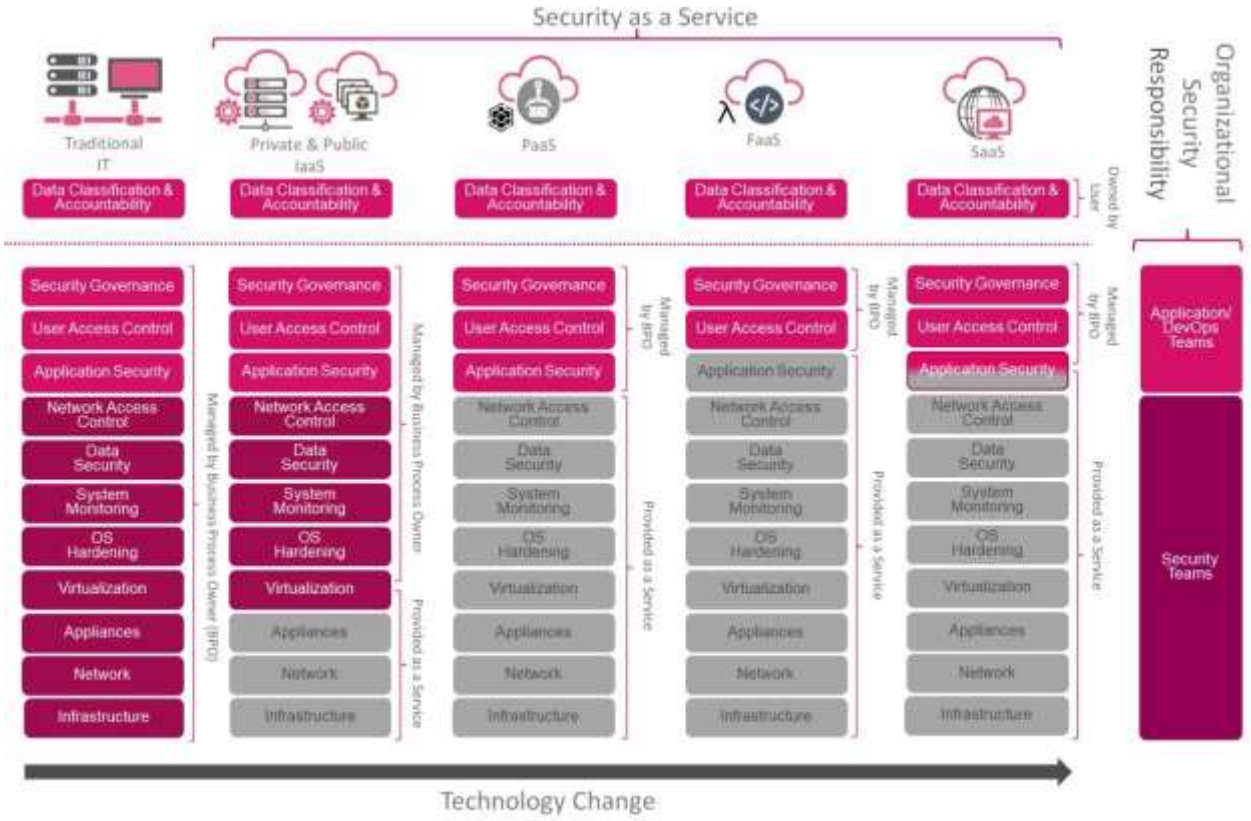


Рисунок 1.1 – Повна модель спільної відповідальності для загальнодоступного IaaS

Як показує практика, спільна відповідальність, синхронізована з принципами ZTNA (нульової довіри), здатна забезпечувати набагато більш якісну та стійку гармонізацію інструментів контролю безпеки, що допомагає максимально звести до мінімуму потенційні ризики під час міграції, особливо в регулярних операціях. Для більшого розуміння, продемонструємо архітектуру ZTNA-мережі (див. рис. 1.2).

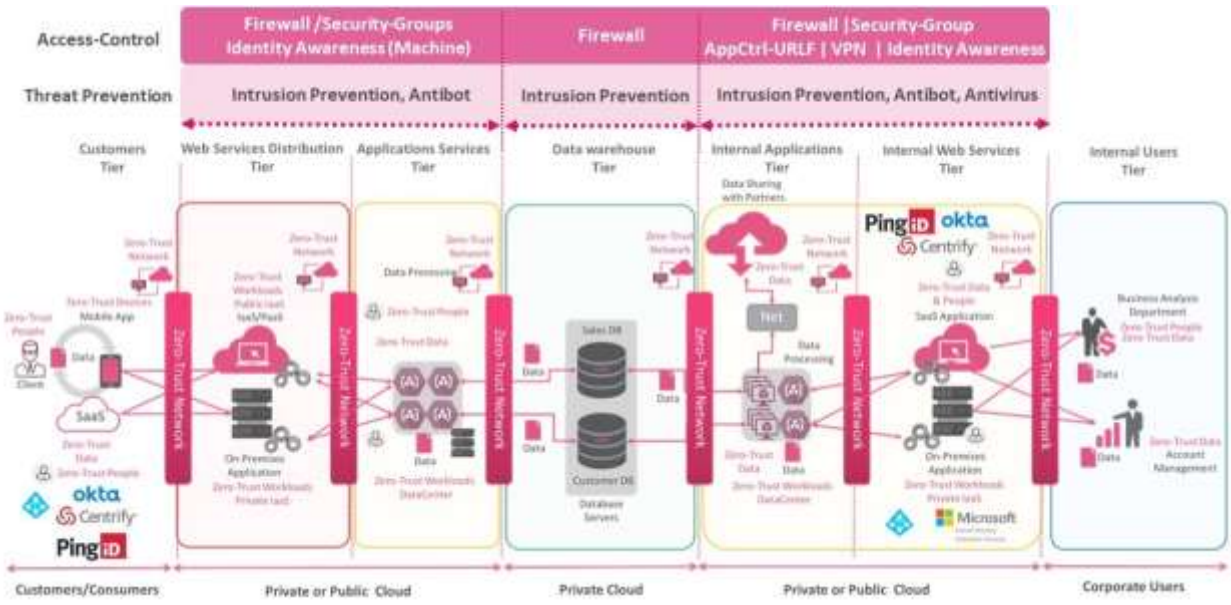


Рисунок 1.2 – Структурна схема архітектури нульової довіри для публічних і приватних IaaS

Структура ZTNA розглядає такі стовпи:

- Дані: ядро бізнесу.
- Робочі навантаження: «spokes», які перетворюють дані в інформацію.
- Мережі: «Hub», транспортний рівень, де дані та інформація переміщують за допомогою механізмів мікросегментації та наскрізного шифрування.
- Пристрої: Кінцеві точки або пристрої IOT, які завантажують дані або мають доступ до них у «Hub».
- Люди: взаємодіють з інформацією за допомогою додатків, наданих елементами «Spoke». Також включає адміністраторів для керування операціями безпеки хмари через систему безпеки.

Правильно вибудувана політика безпеки між веб-рівнем, SOA і рівнем БД дозволяє підприємству отримати набагато стійкішу позицію в хмарному середовищі з ціллю захисту своїх активів у загальнодоступному IaaS, таким чином значно знизивши потенційні ризики. Хоча SOA є традиційним підходом, якого дотримуються організації в процесі міграції, коли вони

починають перехід на мікросервіси, модель SOA також має бути трансформована. В такому випадку застосовується підхід сегментації безпеки.

Сегментація загальнодоступного та приватного IaaS ставить своєю цілю зменшити радіус враження системи та дозволити спеціалістам з безпеки посилити її контроль. Роботу в цьому напрямку значно легшою роблять дві опції: мікросегментація та макросегментація.

Макросегментація – інструмент, завдяки якому в загальній мережі, між основними сегментами сервера, створюються зони безпеки з метою запобігання атакам. Для цього використовуються кілька робочих навантажень з однаковою функціональністю та класифікацією безпеки.

Мікросегментація, в свою чергу, виконує логічний розділ vNET/VPC на окремі сегменти безпеки до окремих рівнів робочого навантаження. Такий детальний рівень, на якому мікросегментація контролює трафік робочого навантаження, мінімізує загрози безпеці та створює модель безпеки Zero Trust. Також, для загальнодоступної хмари на базі Check Point CPM забезпечує централізоване керування та може застосовуватися до окремих робочих навантажень, забезпечуючи більш безпечне середовище без додаткових витрат на конфігурацію для конкретного робочого навантаження.

До переваг мікросегментації можна віденсти застосування детальної сегментації на рівні однієї групи додатків, посилену безпеку критичних програм, а також застосування політики до сьомого рівня.

Що стосується макросегментації, то вона відзначається простішою реалізацією від вищезгаданої.

До недоліків мікросегментації відносяться високі вимоги до навиків спеціаліста, включаючи знання про видимі на рівні програми.

Щодо макросегментації, то її недоліками є вимоги розширених навичок роботи з мережами та безпекою для розгортання політик сегментації на основі мережі

Тепер давайте розглянемо відмінності між інструментами та їх практичне використання для сегментації IaaS у таблиці 1.1.

Таблиця 1.1 – Атрибути мікро- та макросегемнтацій

	Мікросегментація IaaS	**Макросегментація IaaS**
Варіант використання	Використовується для логічного поділу VPC/vNET на різні зони безпеки, включно з індивідуальним рівнем робочого навантаження.	Використовується для поділу між основними групами робочих навантажень зі схожою функціональністю та класифікацією безпеки, запобігаючи переміщенню зловмисників усередину системи та атаці на виробничі робочі навантаження
Область застосування	Широка через контроль бічного руху між хостами	На рівні периметру та через зони безпеки
Політики	Детальна політика «хост-хост»	Політики на рівні мережі/сегмента
Виконання політики	Обчислювальні екземпляри	Підмережа/VLAN
Управління та контроль	Політики безпеки між хостами для контролю доступу або запобігання загрозам	Функціональні політики безпеки vNET/VPC для контролю доступу або запобігання загрозам
Контроль зв'язку між хостами	Між навантаженнями в одному сегменті	Рівень мережі або зони безпеки
Контроль трафіку	«Схід-захід» або бічний рух	«Північ-південь» і «схід-захід»

Використання макро- та мікро-сегментації може допомогти організаціям зробити кращий вибір щодо елементів керування безпекою, які можна використовувати відповідно до потоків додатків. Крім того, контроль доступу можна розгортати за трьома різними сценаріями: на основі мережі, на основі агента або на основі хоста та API, використовуючи інструменти, вбудовані в хмару.

Щоб надати візуальне представлення всіх потоків, захищених у загальнодоступній IaaS, розглянемо діаграму на рисунку 1.3.

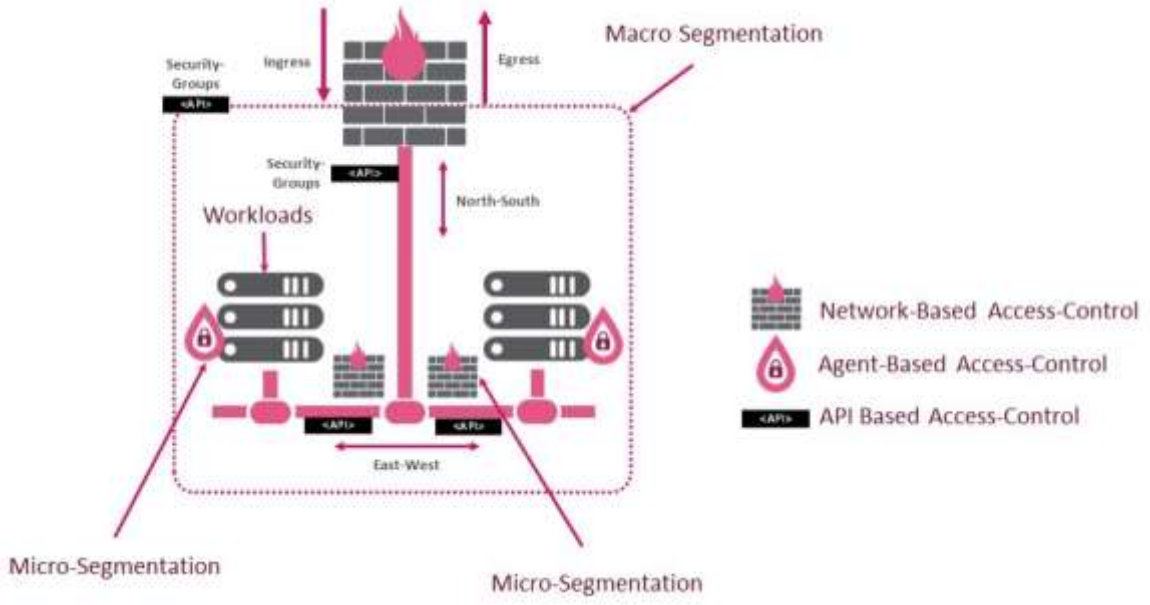


Рисунок 1.3 – Макро- та мікро-сегментації

З цієї точки зору проаналізуємо та підставимо різні сегменти безпеки відповідно до потоків, що дасть змогу точніше вибрати необхідні елементи керування. Результат дослідження описується у таблиці 1.2.

Таблиця 1.2 – Визначення блейдів безпеки згідно сегментів безпеки

Сегмент безпеки	**Потік**	**Блейд безпеки**
Вихідний трафік з Інтернету	Контроль пропуску «північ-південь» та перевірка руху	Брандмауер, IPS на основі правил, перевірка SSL
Вихідний трафік до Інтернету для обчислювальних екземплярів, віртуального робочого столу Azure або робочих просторів Amazon Web Services	Контроль пропуску «північ-південь» та перевірка руху	Брандмауер, контроль програм, URLF, антибот, антивірус, перевірка SSL або категоризація HTTP
Трафік між різними vNET/VPC і РН	Контроль доступу «схід-захід»	Групи безпеки мережі або брандмауер

Продовження таблиці 1.2

Сегмент безпеки	**Потік**	**Блейд безпеки**
Трафік між різними vNET/VPC і робочими навантаженнями	Інспекція руху «схід-захід»	Брандмауер, IPS на основі правил
Трафік від SD-WAN/MPLS (Backhaul)	«північ-південь»	Брандмауер, IPS на основі правил, Identity-Awareness
Трафік між локальним центром обробки даних (Backhaul)	«північ-південь»	Брандмауер, IPS на основі правил
Трафік між провайдерами мультихмарних послуг (backhaul)	«північ-південь»	Брандмауер, IPS на основі правил, VPN

За такого підходу модель спільної відповідальності є більш доступною для повсякденних операцій.

Тепер розглянемо метод налаштування хмарного середовища, який оптимізовує сегментацію при використанні стратегії «Lift and Shift», а саме метод «Hub and Spoke». Його особливість полягає у тому, що хмарне середовище перетворюється на систему з'єднань, у якій усі зв'язки під'єднані до транзитного вузла, через який проходить весь трафік.

Парадигма методу розподілу «Hub and Spoke» представляє форму оптимізації транспортної топології, згідно якої планувальники руху організовують маршрути в серії «Spoke», які, в свою чергу, з'єднують віддалені точки до центрального «Hub». Прості форми цієї моделі розподілу/з'єднання можна порівняти з транзитними системами «точка-точка», в яких кожна точка має прямий шлях до іншої будь-якої точки [3].

Основна мета цього принципу полягає в тому, щоб забезпечити більш практичну сегментацію стратегій «Lift and Shift», коли використовується vNET/VPC, щоб забезпечити простіше налаштування мережі «Zero Trust» у хмарі. Хоча ми можемо сегментувати всередині vNET/VPC, немає простого

способу забезпечити перевірку трафіку, оскільки постачальники хмарних послуг контролюють всю маршрутизацію всередині периметра vNET/VPC

Схема архітектури даного методу представлена на рисунку 1.4.

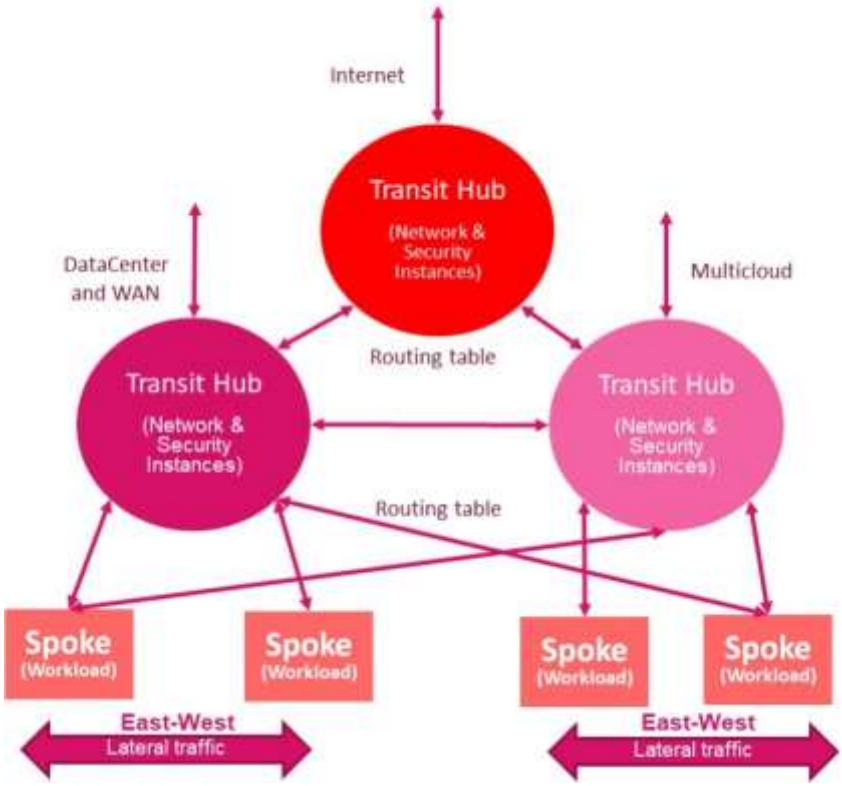


Рисунок 1.4 – Схема архітектури «Hub and Spoke»

Варто зауважити, що «spoke» є ізольованим мережевим середовищем, яке містить у собі набір однієї або кількох мережевих підмереж, з яких встановлюються та запускаються типові робочі навантаження. Прикладом його використання є система, яка містить кілька віртуальних серверів, що складають або частину, або цілий стек додатків (веб, додаток і база даних). Іншим варіантом використання може бути система, яка відіграє роль розширення існуючих локальних мереж, наприклад набір QA-серверів для тестування, або набір серверів обробки даних, які використовують хмарне забезпечення на вимогу для зниження витрат ресурів та покращеної гнучкості.

Однак, з точки зору безпеки, ми маємо цілий набір різноманітних «spokes», які можна розгорнути в загальнодоступній IaaS:

- Транзитні вузли.
- Обчислювальні екземпляри.
- Контейнер на вимогу або як послуга.
- Кластери Kubernetes.
- Кінцеві точки обслуговування або кінцеві точки VPC.
- Безсерверні або сервісні функції.

Більше прикладів різних «spoke» наведено на рисунку 1.5.

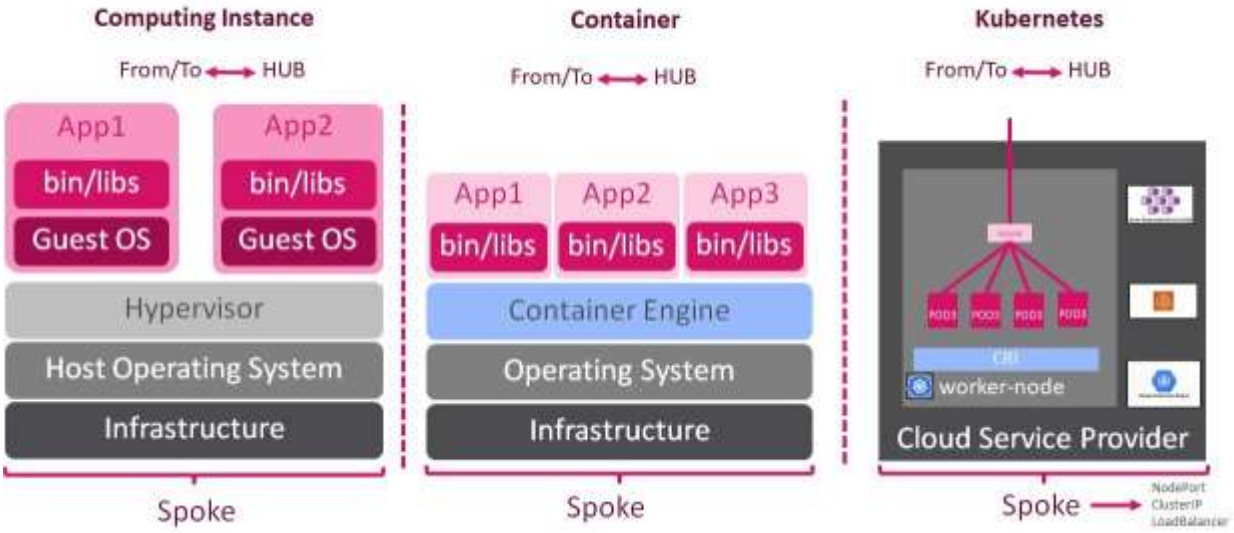


Рисунок 1.5 – Приклади різних «spoke» для публічного IaaS

Необхідно зауважити, що транзитний вузол забезпечує гнучкість і систематичне розділення комунікаційних потоків у середовищі. Він може бути призначений для вхідного трафіку, бічного трафіку між вузлами, або для вихідного трафіку до Інтернету чи інших хмарних середовищ. Трафік маршрутизації можна легко налаштувати відповідно до потоків трафіку в програмах.

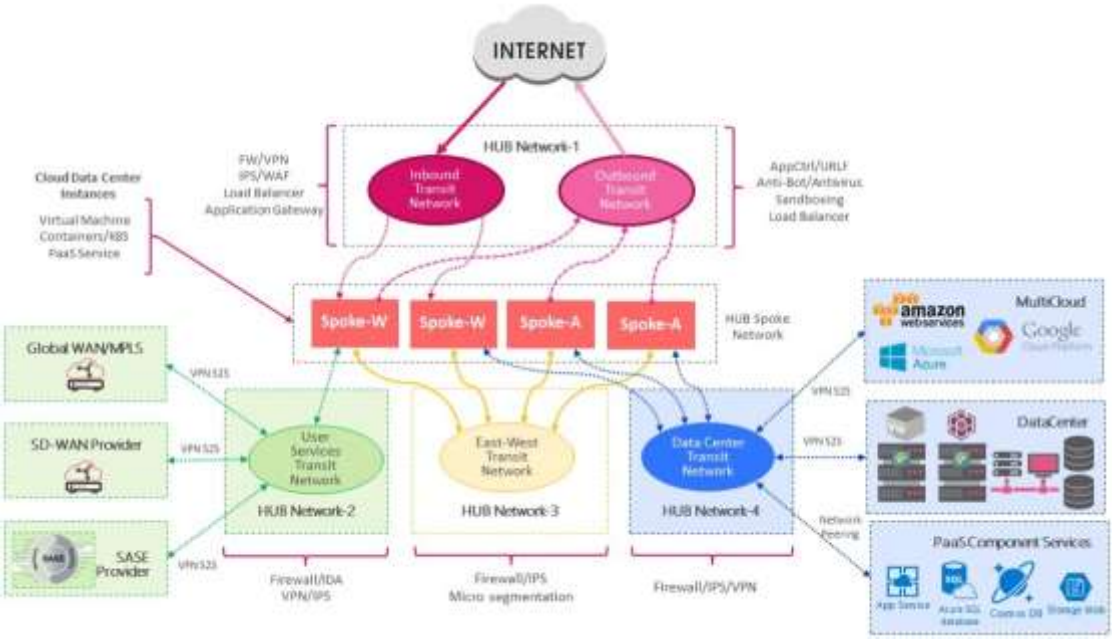


Рисунок 1.6 – Оптимізований метод для «Lift and Shift»

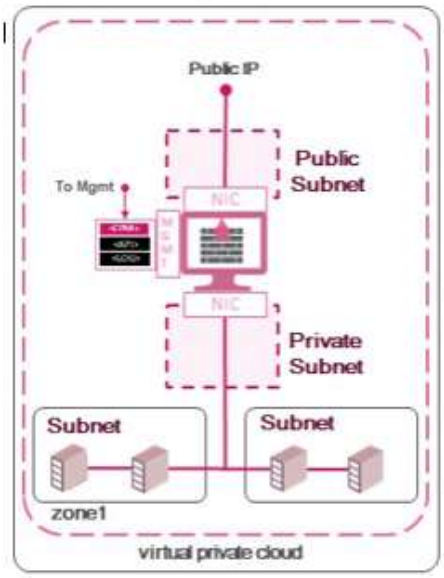
Розглянути схему роботи транзитної «Hubs and Spokes» в оптимізованій моделі «Lift and Shift Optimized» можна на рисунку 1.6.

1.2 Аналіз еталонних архітектур для IaaS

По завершенню аналізу основних стратегій переносу хмарного сервісу, моделей та принципів організації безпеки хмарної системи, а також їх оптимізацію для загальнодоступного IaaS, можна перейти до розгляду методів розгортання мережі «хмари» та еталонних архітектур.

Аналізуючи існуючі режими розгортання шлюзів безпеки, у результаті дослідження можна зазначити, що «єдиний шлюз VPC/vNET» – це метод найпростішого розгортання, який використовується з метою забезпечення розширеної безпеки для малих і середніх робочих навантажень. Цей сценарій не забезпечуватиме можливості високої доступності або масштабованості, тому його слід розглядати лише для середовищ, де стійкість системи не є основною проблемою, або з метою тестування.

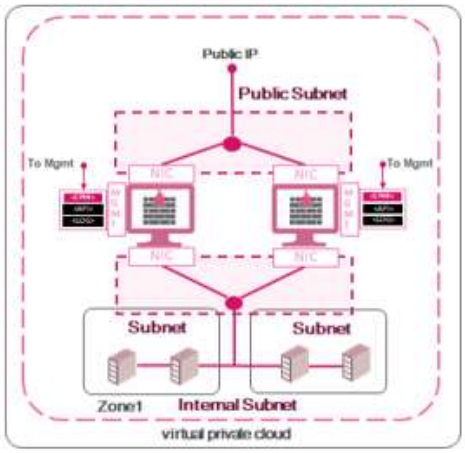
Схема методу «єдиного шлюзу» зображена на рисунку 1.7.



Постачальник хмарних послуг	Підтримуваний сценарій
Azure	Так, sk109360
Amazon Web Services	Так, sk120534
Google Cloud Platform	Так, sk114577
Oracle Cloud Infrastructure	Так,
Huawei	Так
Alibaba	Так

Рисунок 1.7 – Єдиний VPC з єдиним шлюзом безпеки

«Кластер високої доступності» представляє групу віртуальних машин, які працюють в єдиній системі, де один член кластера є активним, а другий – резервним. Приклад схеми кластеру високої доступності поданий на рисунку 1.8.



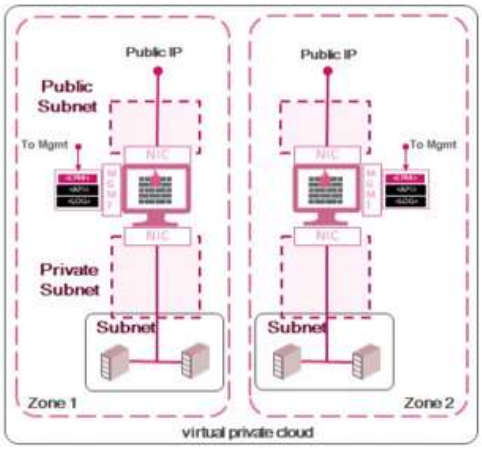
Постачальник хмарних послуг	Підтримуваний сценарій
Azure	Так, sk109360
Amazon Web Services	Так, sk120534
Google Cloud Platform	Так, sk114577
Oracle Cloud Infrastructure	Так, sk168202
Huawei	Hi
Alibaba	Hi

Рисунок 1.8 – Кластер високої доступності, розгорнутий в 1 зоні

Розгортання у вигляді двох шлюзів в двох зонах доступності з одним VPC/vNET є пропозицією високого рівня доступності, яка захищає програми

та дані від збоїв у центрі обробки даних. Зони доступності, в даному випадку, є унікальним фізичним простором в регіонах постачальників хмарних послуг. При цьому, розгорнуті обчислювальні екземпляри та шлюзи безпеки в різних службах із резервуванням зони дозволяють тиражувати програми та дані в зонах доступності, захищаючи від SPOF (єдиних точок відмови).

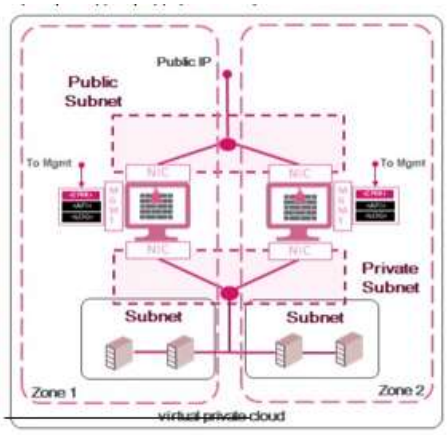
Приклад описаної системи зображено на рисунку 1.9.



Постачальник хмарних послуг	Підтримуваний сценарій
Azure	Так, sk109360
Amazon Web Services	Так, sk120534
Google Cloud Platform	Так, sk114577
Oracle Cloud Infrastructure	Так, sk168202
Huawei	Так
Alibaba	Так

Рисунок 1.9 – Приклад архітектури високого рівня доступності з розділенням на дві окремі зони

Автоматичне масштабування VPC/vNET ідеально підходить для робочих навантажень із змінною пропускною спроможністю, оскільки представляє процес групування обчислювальних ресурсів, які можна використовувати для розгортання системи ідентичних віртуальних машин із можливістю керування ними. Набори масштабу можуть в ході виконання завдань збільшувати або зменшувати кількість віртуальних машин, в залежності від рівня поточних потреб. Цей тип реалізації дуже рекомендується реалізовувати для служб публічного типу, або систем, через які користувачі отримують доступ до різних служб (див. рис. 1.10).

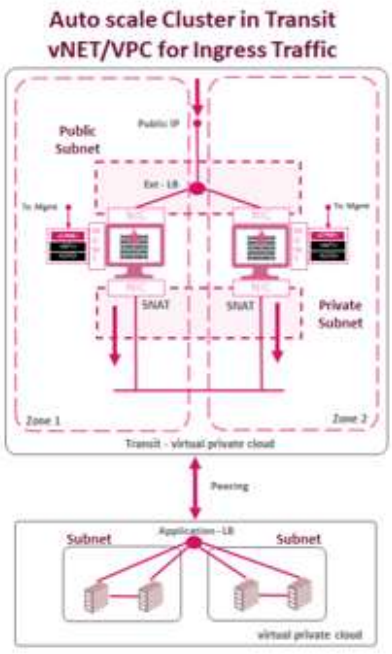


Постачальни хмарних поуг	Підтримуваний сценарій
Azure	Так, sk109360
Amazon Web Services	Так, sk120534
Google Cloud Platform	Так, sk114577
Oracle Cloud Infrastructure	Hi
Huawei	Hi
Alibaba	Hi

Рисунок 1.10 – Приклад автомасштабованого кластеру

Є і інший сценарій автоматичного масштабування, який виконується за допомогою Transit vNET або спільного VPC для вхідного трафіку.

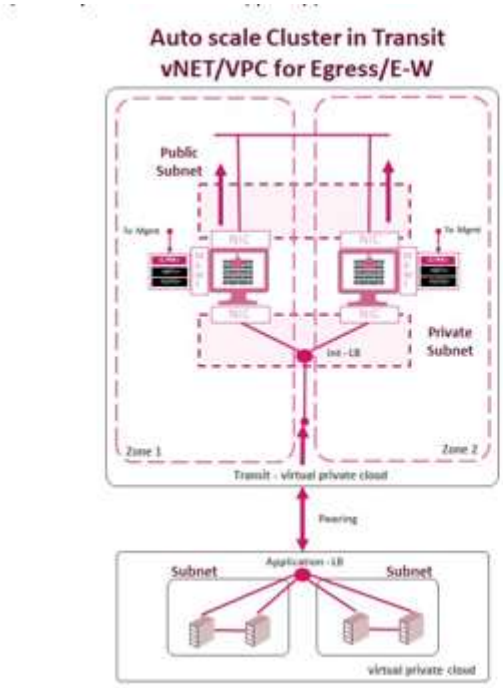
Схему автоматичного масштабування кластера для вхідного трафіку з використанням транзиту або спільних служб VPC/vNET можна розглянути на рисунку 1.11



Постачальни хмарних поуг	Підтримуваний сценарій
Azure	Так, sk109360
Amazon Web Services	Так, sk120534
Google Cloud Platform	Так, sk114577
Oracle Cloud Infrastructure	Hi
Huawei	Hi
Alibaba	Hi

Рисунок 1.11 – Другий сценарій автомасштабування кластеру

Окрім вищеописаного, існує і третій сценарій автоматичного масштабування кластеру з використанням Transit vNET або спільного VPC, тільки вже для вихідного трафіку (див. рис. 1.12).



Постачальник хмарних послуг	Підтримувані сценарії
Azure	Так
Amazon Web Services	Так, sk120534[11]- TGW[4] VPN with ECMP
Google Cloud Platform	Так
Oracle Cloud Infrastructure	Ні
Huawei	Ні
Alibaba	Ні

Рисунок 1.12 – Третій сценарій автомасштабування кластеру

Продемонстрована вище схема представляє сценарій, який проводить перевірку вихідного трафіку через транзитний або спільний сервіс VPC/vNET із можливостями автоматичного масштабування та змінною пропускною здатністю. Типовим варіантом його використання є розгортання внутрішнього балансувальника навантаження з метою підключення до мережі Інтернет, або обробка трафіку шлюзом безпеки та розміщення SNAT для публічної IP-адреси. Крім того, можна перевірити трафік «схід-захід» між різними vNET або VPC. Такий ВВ рекомендується використовувати, в основному, для малих або середніх середовищ, в яких вихідний трафік не має можливості спільно використовувати шлюз зі «схід-захід».

Для перевірки трафіку «схід-захід» (VPC), або vNET існує окремий сценарій автоматичного масштабування, який також здійснює обробку

коливаючої пропускної здатності, однак, дія такого методу направлена виключно на трафік «схід-захід».

Будь-яке середовище може бути розгорнуто в якості функціонального вузла для підтримки ізоляції. Наприклад, робочі навантаження, розташовані у зовнішній, або back-end vNET використовуватимуть різні служби безпеки, тому надати доступ до спільних служб забезпечить відчутну гнучкість, масштабованість і кращий розподіл обов'язків між командами. На практиці роботи публічних IaaS виходить, що виробничі робочі навантаження обмежені зв'язком один з одним (мікросегмент), що забезпечується групами безпеки мережі (NSG), і вимагають доступу до спільних служб через транзитний вузол (макросегмент). Відповідно до цього підходу центри безпеки забезпечують централізований контроль у транзитному центрі, пропонуючи кращу ізоляцію відповідно до потоків трафіку між робочими навантаженнями та перевіркою трафіку.

Схему еталонної архітектури для Azure подано на рисунку 1.13.

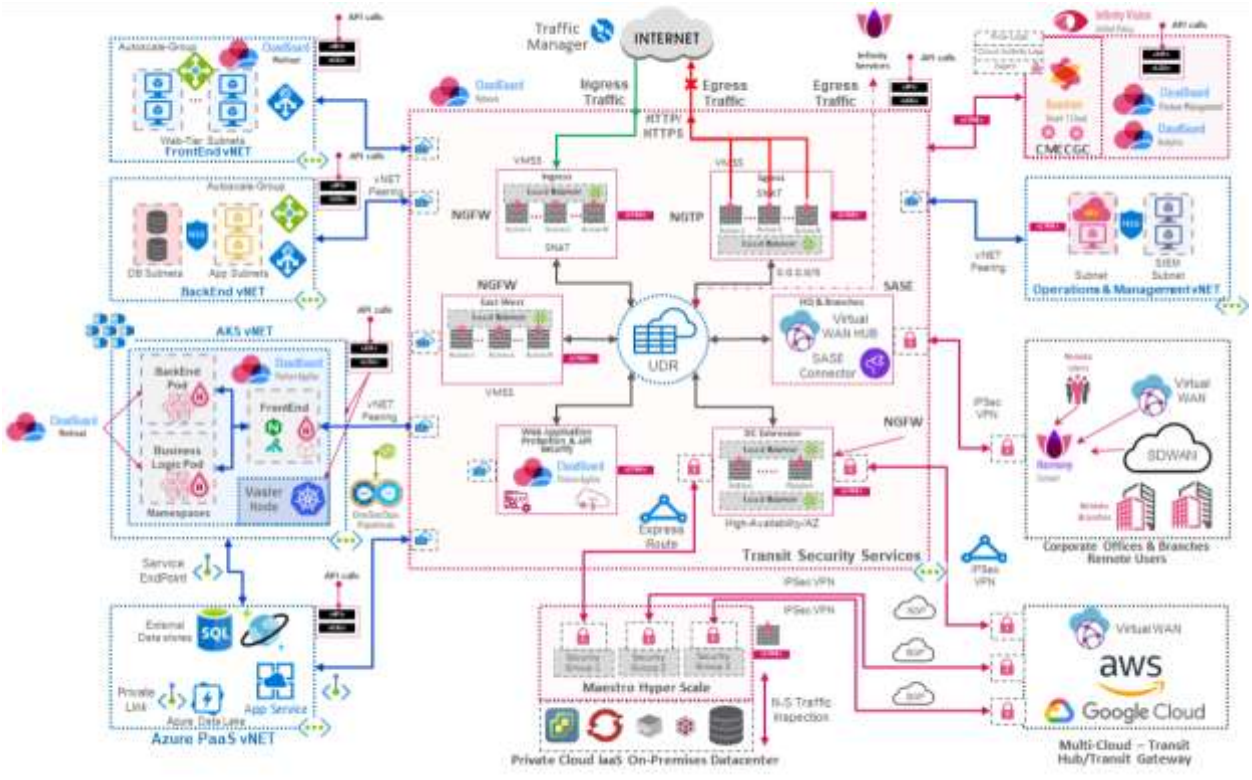


Рисунок 1.13 – Еталонна архітектура для Microsoft Azure

Публічна хмара IaaS на базі Microsoft Azure може використовуватися в кількох випадках:

- В якості хостингу для складних веб-сайтів.
- Як сервер з високою обчислювальною продуктивністю.
- Для тестування та розробки ПО.
- В якості інструменту резервного копіювання та аварійного відновлення.
- За необхідності проведення аналізу великих даних.

Подібно до Azure, Check Point CloudGuard для Google Cloud Platform (GCP) легко розширює комплексну безпеку запобігання загрозам, щоб захистити активи в хмарі від атак, водночас забезпечуючи безпечне підключення.

Еталонна архітектура GCP подана на рисунку 1.14.

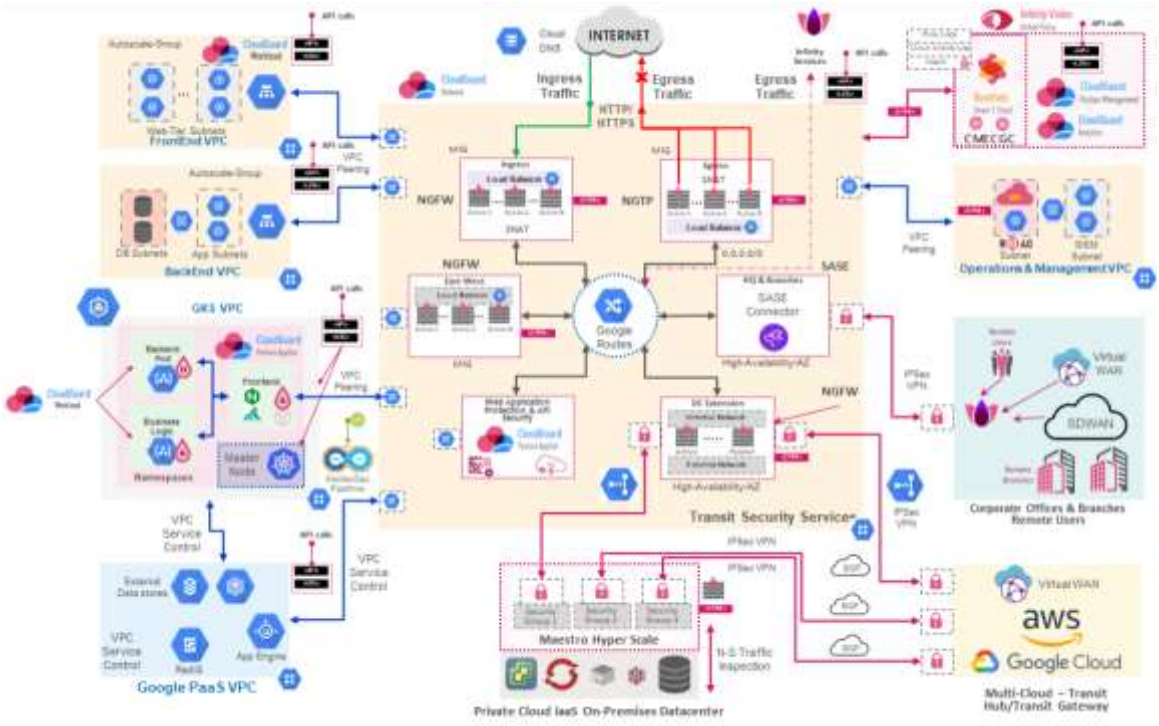


Рисунок 1.14 – Еталонна архітектура для GCP

Від Azure дану платформу відрізняють лише варіанти її використання, більш детально які будуть розглянуті у наступному розділі роботи.

Однак, важливо відзначити, що для всіх сценаріїв існує пряма кореляція між одночасними з'єднаннями, з'єднаннями за секунду і пакетами за секунду, оскільки кожен постачальник хмарних послуг дотримується правила «rate-limits», визначені для кожного обчислювального екземпляра. Тому аналіз потоку трафіку слід виконати перед процесом міграції, щоб переконатися, що варіанти використання та правильні конфігурації застосовані належним чином.

Щоб запобігти атакам і зменшити втрату або витік даних, сервіс також перевіряє дані, які отримує і надсилає приватна підмережа в VPC. Таким чином, CloudGuard NS може захистити служби в загальнодоступній хмарі від найскладніших загроз, несанкціонованого доступу, а також запобігти атакам типу «Відмова в обслуговуванні» (DoS) на прикладному рівні.

Схему еталонної архітектури для Amazon Web Services відображено на рисунку 1.15.

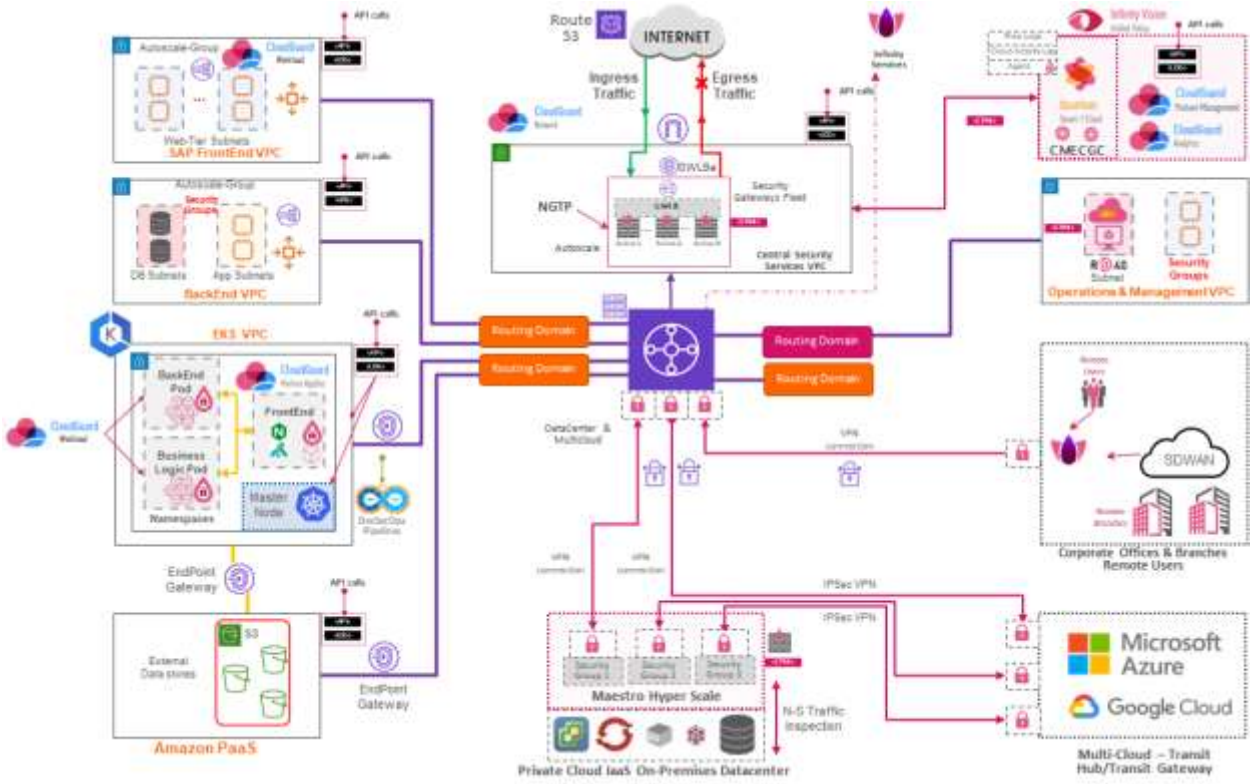
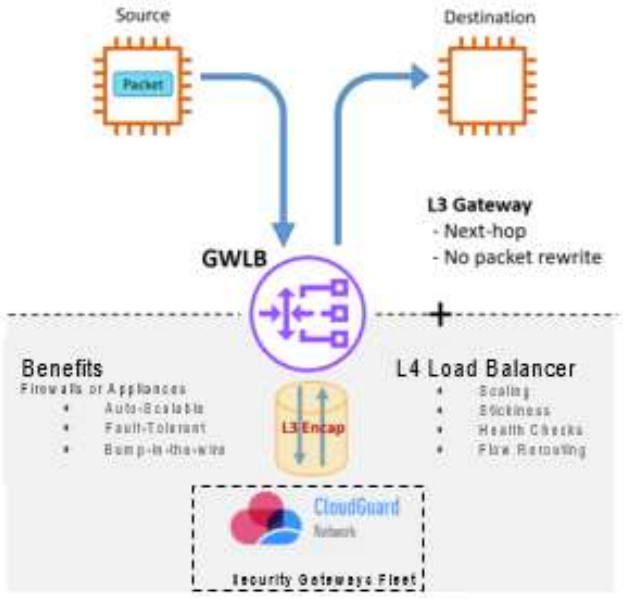


Рисунок 1.15 – Еталонна архітектура для AWS

За необхідності підвищення вимог до трафіку та забезпечення більш централізованого доступу до спільних служб, подібно до транзитного центру в Azure, TGW має можливість налаштувати пристрій (наприклад, пристрій безпеки) у спільній службі VPC. Цей сценарій забезпечує масштабованість і гнучкість, необхідні, коли потреба в трафіку зростає.

В напрямку покращення та оновлення архітектури, у 2020 році AWS запустила у роботу GWLB (Gateway Load Balancer), який поєднав функціональність шлюзу L3 і балансувальника навантаження L4. Це дало змогу організаціям «прозоро» підключати віртуальні мережеві пристрої до шлюзів безпеки з метою глибокої перевірки пакетів. На продемонстрованій нижче діаграмі зрбражено принцип роботи, наявні потоки та функціональні можливості GWLB і парку шлюзів безпеки (див. рис. 1.16).



Рисуно 1.16 – Потік і функціональність AWS Gateway Load Balancer

На схемі рисунку 1.17 продемонстровано приклад архітектури з використанням GWLBE.

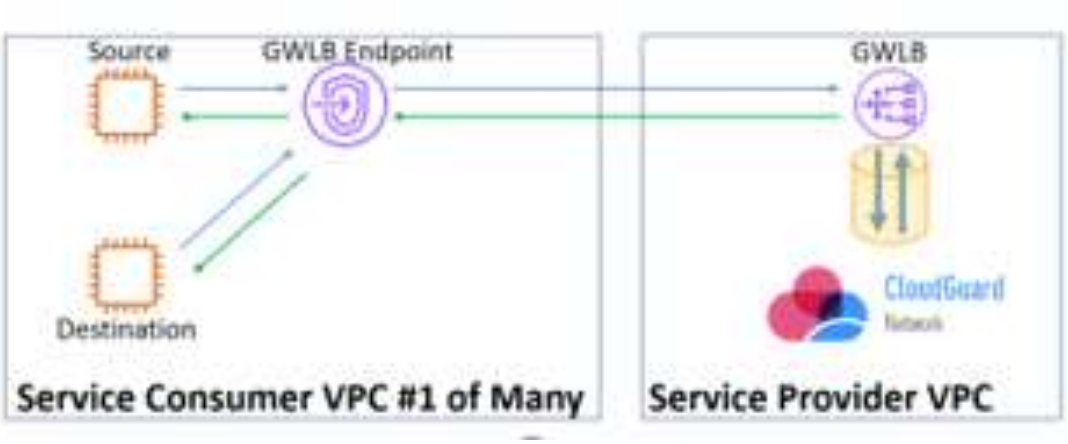


Рисунок 1.17 – Проста архітектура GWLBE

Feature	aws	Microsoft Azure	Google Cloud Platform
Geography	Geography	Geography	Geography
Availability Zone	Availability Zone	Availability Zone	Availability Zone
Network	VPC	VNET	VPC-Cloud Virtual Network
Subnet	Subnet	Subnet	Subnet Network
Resources Management	Across Specific Account	Across Specific Subscription	Global, Regional, and Zone Specific Resources
Virtual Machine (VM)	Instance	Virtual Machine	Virtual Machine Instance
Image Type Format	AMI	VM Images	Public / Private / Custom Image
Public IP Addresses	Public / Elastic IP	Basic / Standard IP	Ephemeral / Static external IP
Load Balancing	Application / Network / Classic Load Balancer / ELB	Azure Load Balancer, Application Gateway	External Network and HTTP Load Balancing, Internal Load Balancing
Native Security / Security Groups	Security Groups / NACL	Network Security Group (NSG)	Computer Engine Firewall Rules
Scalable Computer Instances (Servers)	Elastic Computer Cloud (EC2)	Azure VM	Computer Engine
Domain Name System (DNS)	Route 53	Azure DNS or Traffic Manager	Cloud DNS
Network Address Translation (NAT)	NAT Gateways	NAT Gateways	Cloud NAT
Network Peering	VPC Peering Connections	Virtual Network Peering	VPC Network Peering
Network Routes / Routing	Route Tables	Azure Virtual Network Routing	Routes
Region	Region	Region	Region
Virtual Private Cloud (VPC)	Virtual Private Cloud (VPC)	Virtual Network (VNET)	Virtual Private Cloud (VPC)
VPC Endpoints	VPC Endpoints	Virtual Network Service Endpoint	Private Services, Private Google Access and/or Shared VPC
VPN Gateway	Virtual Private Gateway	Azure VPN Gateway	Cloud VPN
Object Storage	S3 Buckets	Blob Storage	Cloud Storage
Identity and Access Management (IAM)	Identity Access Management (IAM)	Azure Role-Based ACL (RBAC) or Azure AD	Cloud IAM
Content Delivery Network (CDN)	Cloudfront	Azure CDN	Cloud CDN or CDN Interconnect
Autoscaling	Auto-scaling group	VM Scale Sets	Computer Engine Autoscaler
API Endpoints	API Gateway	API Management	Cloud Endpoints

Рисунок 1.18 – Різниця термінологій різних хмарних сервісів

Враховуючи принципи нульової довіри, GWLB дозволяє організаціям розробляти відмовостійку архітектуру простішим та інтуїтивно зрозумілішим способом; зокрема додавання кількох віртуальних пристроїв і функціональних VPC постачальників послуг. Такий підхід дозволяє організації, особливо IT-командам і мережевим командам, підтримувати узгоджену практику безпеки між хмарними та локальними розгортаннями. Це забезпечує величезну перевагу можливості використовувати наявний набір навичок інженерів із безпеки, які розуміють і довіряють віртуальним пристроям Cloud Guard Network Security із NGFW або NGTP.

Варто звернути увагу на той факт, що кожен постачальних хмарних послуг використовує власну термінологію у організації хмарної системи. Приклад цього наведено на рисунку 1.18.

1.3 Висновок до першого розділу

В ході написання першого розділу роботи було охарактеризовано стратегію міграції хмарного середовища зі збереженням його структури «Lift and Shift», розглянуті її основні переваги та практичні методи оптимізації для архітектур безпеки публічної IaaS.

Досліджено розширену модель «спільної відповідальності» для публічного IaaS, структуру та політики безпеки узгодженої з її принципами моделі «надання доступу з нульовою довірою», що необхідна для мінімізації потенційних ризиків атаки. Також були розглянуті види сегментації: мікро- та макросегментації; їх роль в забезпеченні безпеки публічної IaaS, що відповідає використанню першої для логічного поділу VPC/vNET на різні зони безпеки та поділу робочих навантажень між основними групами зі схожою функціональністю та класифікацією безпеки, запобігаючи проникненню зловмисників всередину системи та атаці на виробничі робочі навантаження для другої [4].

Охарактеризовано призначення та варіанти використання моделі «Hub and Spoke», різновиди та призначення елементів («Hubs» і «Spokes») цієї моделі в різних еталонних архітектурах. Продемонстровано використання цього принципу в дизайні високого рівня безпеки.

Детально розкрито та проаналізовано еталонні архітектури безпеки для публічного IaaS: Microsoft Azure (Azure), Google Cloud Platform (GCP), Amazon Web Services (AWS), інструменти їх покращення (GWLB, GWLE для AWS), а також можливі методи розгортання та варіанти реалізації автоматичного масштабування.

2 ВАРІАНТИ ВИКОРИСТАННЯ МОДЕЛЕЙ АРХІТЕКТУРИ

2.1 Потік вхідного трафіку у публічній хмарі

Після аналізу основних принципів роботи та побудови еталонних архітектур, можемо більш детально розглянути варіанти їх використання. Першим проаналізуємо вхідний потік трафіку в еталонних архітектурах.

Представимо діаграму віртуальної мережі vNET, яка побудована на базі інфраструктури «Lift and Shift» (див. рис. 2.1).

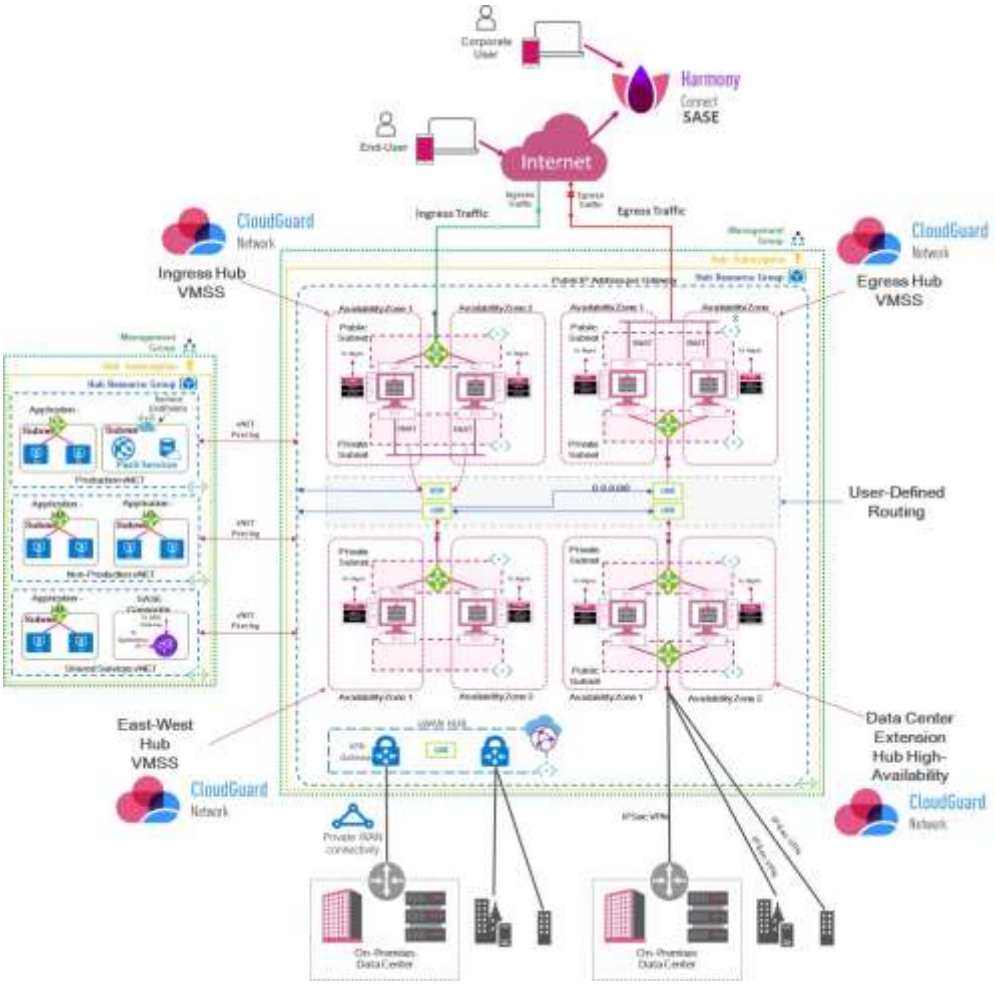


Рисунок 2.1 – Еталонна архітектура для Microsoft Azure

У нас є еталонна архітектура GCP, яка відображає систему CloudGuard NS захисту ресурсів, розгорнутих в GCP. Стандартним сценарієм

застосування є середовище веб-додатків, розгорнуте у віртуальній мережі в Google Compute Engine. До їх складу можуть входити декілька рівнів, включаючи веб-рівень, рівень додатків, рівні БД і контейнери.

Трафік у цьому середовищі, стандартно, має ряд наступних атрибутів:

- Вхідний трафік (з мережі Інтернет на веб-рівень).
- Трафік «схід-захід» (обмін між веб- і прикладним рівнями).
- Розширення центру обробки даних або транзитний зв’язок (трафік, що проходить між середовищем і локальною мережею, призначений для адміністрування та серверних служб).
- Вихідні підключення (від середовища до мережі Інтернет, призначений для оновлення ПЗ та доступу до зовнішніх веб-служб).

Еталонна архітектура для Google Cloud Platform буде виглядати наступним чином (див. рис. 2.2).

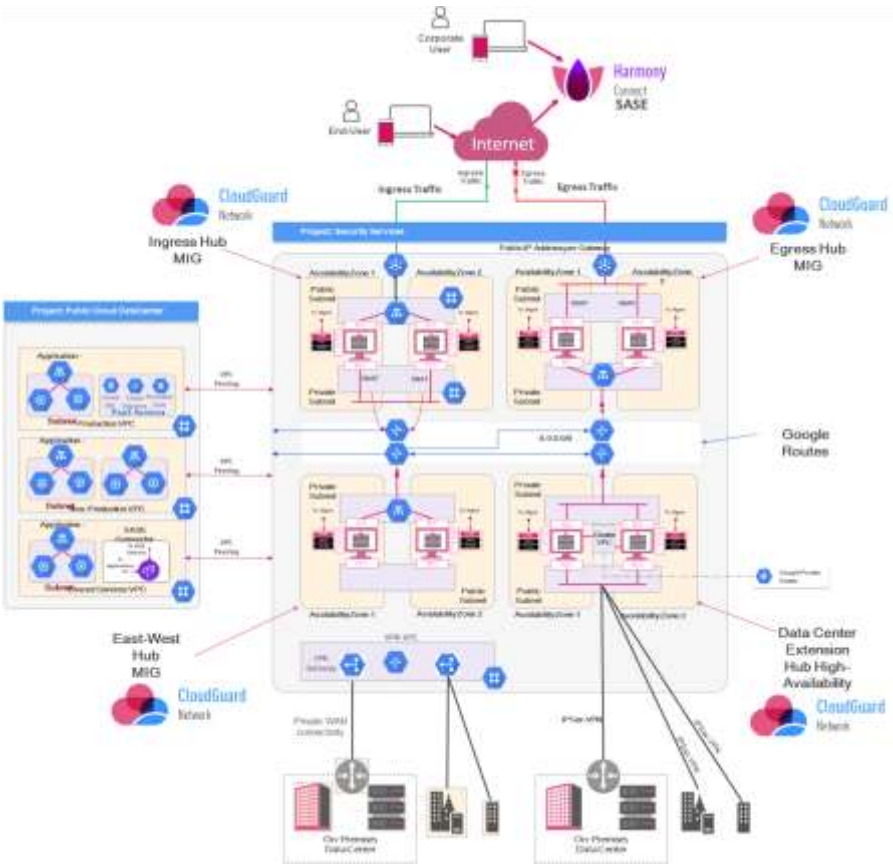


Рисунок 2.2 – Еталонна архітектура для Google Cloud Platform

Еталонна архітектура для AWS, аналогічно представленій схемі, має «Hubs» вхідного та вихідного типу для публічних служб, що означає наявність відповідних шлюзів безпеки та їх політику безпеки, а також «схід-захід», або центр обробки даних і транспортні центри. TGW розташований посередині діаграми, що відображає домени маршрутизації.

Використовуючи поданий підхід, у системі AWS отримуємо відмінну архітектуру, яка може забезпечувати високомасштабовану, гнучку та розподілену архітектуру з інтеграцією балансувальників навантаження шлюзу, як зображено на рисунку 2.3.

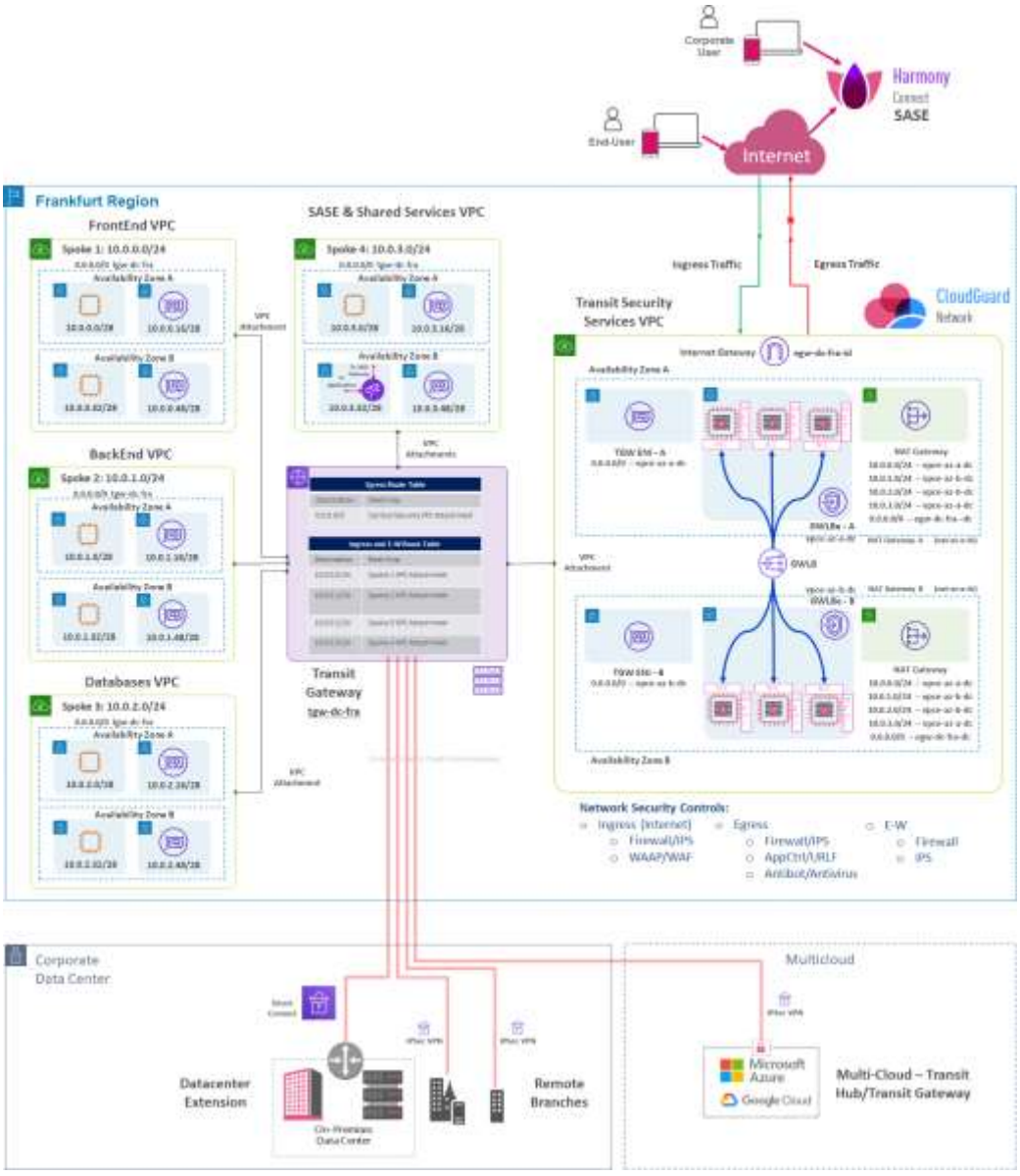


Рисунок 2.3 – Еталонна архітектура для AWS

Якщо розглядати систему зі сторони вхідного трафіку, то він пов’язаний із загальним сценарієм публікації веб-серверу, виробничими системами та службами. Нижче перелічимо шляхи, через які це досягається:

- Вхідний трафік для робочих навантажень із використанням традиційного трирівневого підходу.
- Вхідний трафік для веб-додатків, наданий PaaS.
- Вхідний трафік для контейнерів, які діють в якості веб-серверів та виконують функцію надання високодинамічних послуг.

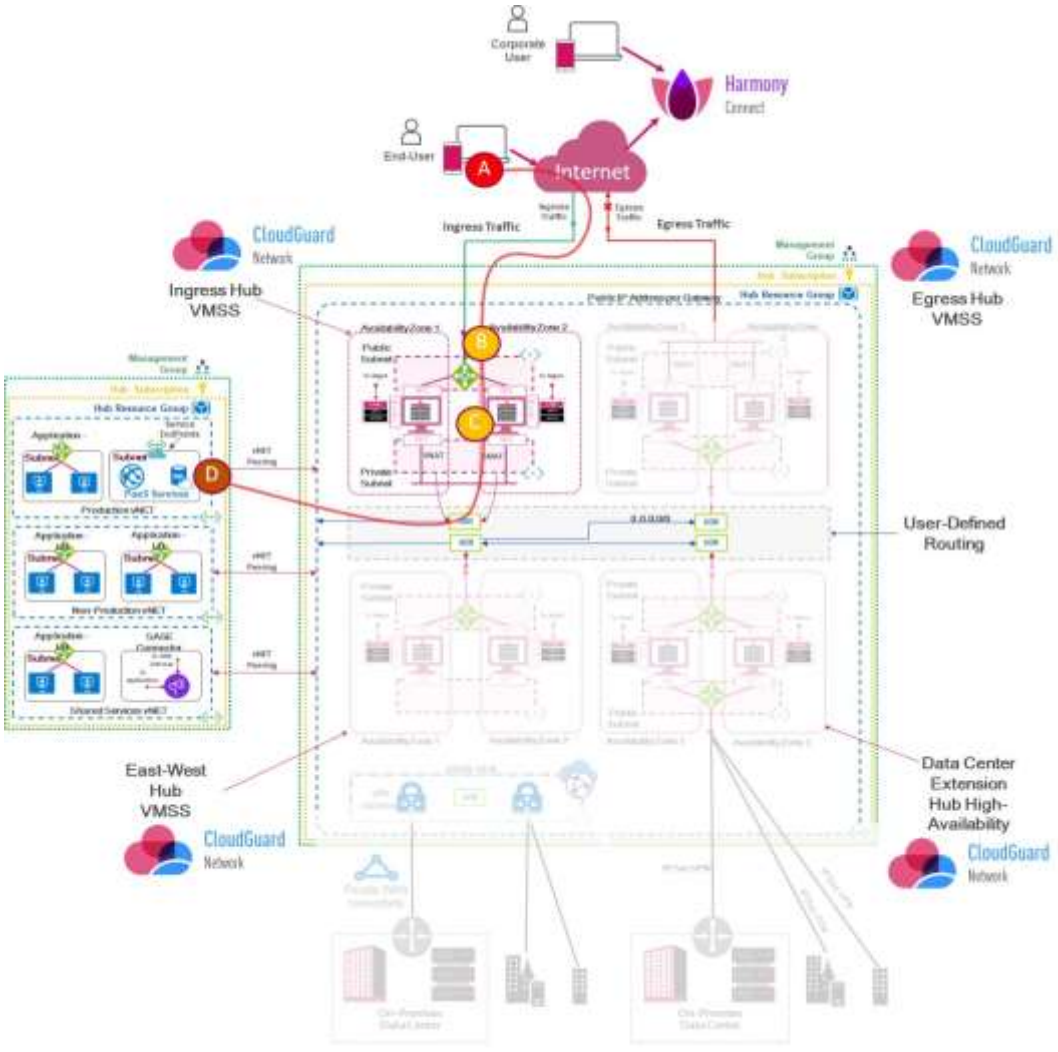


Рисунок 2.4 – Потік вхідного трафіку між Transit Security Services Hub і Production Hub – Microsoft Azure

Для Microsoft Azure діаграма еталонної ерхітектури з потоком вхідного трафіку між Transit Security Services Hub і Production Hub виглядатиме наступним чином (див. рис. 2.4).

В попередньому розділі відзначалось, що в Azure центр транзитного сервісу безпеки є віртуальною мережею (vNET), що виконує функцію центральної точки підключення для всіх хмарних центрів обробки даних. Нижче описано принцип роботи вхідного трафіку у представленій на рисунку вище системі.

Трафік, який отримується з мережі Інтернет:

- Трафік для WebApp1 («D») надходить до загальнодоступної IP-адреси («B»), призначеної для цієї веб-програми.
- Зовнішній балансувальник навантаження Azure («C») налаштовується з використанням правила вхідного NAT, яке пересилає весь трафік HTTP (порт 80), що надходить на цю публічну адресу, на зовнішню приватну адресу шлюзу «Check Point» (наприклад, 10.0.1.10) на порт 8081.
- Трафік для WebApp2 («B») надсилається на загальнодоступну IP-адресу, призначену для цієї веб-програми.
- Зовнішній балансувальник навантаження Azure («C») налаштовано за допомогою правила вхідного NAT, яке пересилає весь трафік HTTP (порт 80), що надходить на цю публічну адресу, на зовнішню приватну адресу шлюзу Check Point (10.0.1.10) на порт 8082. WebApp2 розташований подібно до служби PaaS, де потрібно налаштувати кінцеву точку служби.
- Шлюз безпеки «Check Point» використовує SNAT для таких потоків (від A до D).
- Від «A» до «D-WebApp1» перенаправляється трафік, що надходить на TCP-порт 8081, на порт 80 Web1.
- Так само, від «A» до «D-WebApp2» перенаправляється трафік, що надходить на TCP-порт 8082, на порт 80 Web2.

Подія масштабування виникає в результаті зменшення струмового навантаження. Коли запускається подія масштабування, функція автоматичного масштабування Azure визначає один або кілька шлюзів в якості варіантів на завершення. Після цього зовнішній балансувальник навантаження припиняє транспортування нових з'єднань до цих шлюзів, а автомасштабування завершує їх роботу. Далі сервер керування безпекою «Check Point» виявляє зупинку шлюзів безпеки CloudGuard NS та автоматично видаляє шлюзи зі своєї БД.

З метою резервування та доступності рекомендується мати як мінімум 2 шлюзи безпеки.

Що стосується події масштабування, то вона відбувається за умови, якщо поточне навантаження зростає. Після запуску події масштабування, Azure запускає один або декілька нових екземплярів шлюзів безпеки «Check Point» CloudGuard NS. Нові екземпляри шлюзів безпеки CloudGuard NS автоматично запускають майстра першого налаштування «Check Point», а потім перезавантажуються.

Під час масштабування сервер керування «Check Point Security» визначає запуск нових екземплярів шлюзів безпеки CloudGuard NS, після чого сервер керування безпекою очікує завершення розгортання шлюзів безпеки CloudGuard NS. Після цього сервер керування безпекою автоматично: ініціалізує канал безпечного внутрішнього зв'язку (SIC) із шлюзами безпеки CloudGuard NS та встановлює політику безпеки на шлюзах безпеки CloudGuard NS.

По завершенню цих дій, шлюзи безпеки CloudGuard NS починають реагувати на перевірки працездатності, а балансувальник навантаження починає пересилати їм нові підключення. В кінці, тільки що створені шлюзи безпеки CloudGuard NS повідомляють про свій статус і надсилають журнали на сервер керування безпекою «Check Point».

Подібний підхід застосовується і у GCP через використання групи керованих екземплярів автоматичного масштабування (MIG). MIG представляє ресурс обчислювальної системи Google Cloud Platform, який є набором екземплярів віртуальних машин, керування якими відбувається, як єдиним об’єктом. У такій системі зовнішній балансувальник навантаження надсилає вхідний трафік до MIG автоматичного масштабування «Check Point», що знаходиться на зовнішньому VPC. Далі шлюзи в групі перевіряють трафік і, якщо політики дають таку можливість, перенаправляють трафік до внутрішнього балансувальника навантаження.

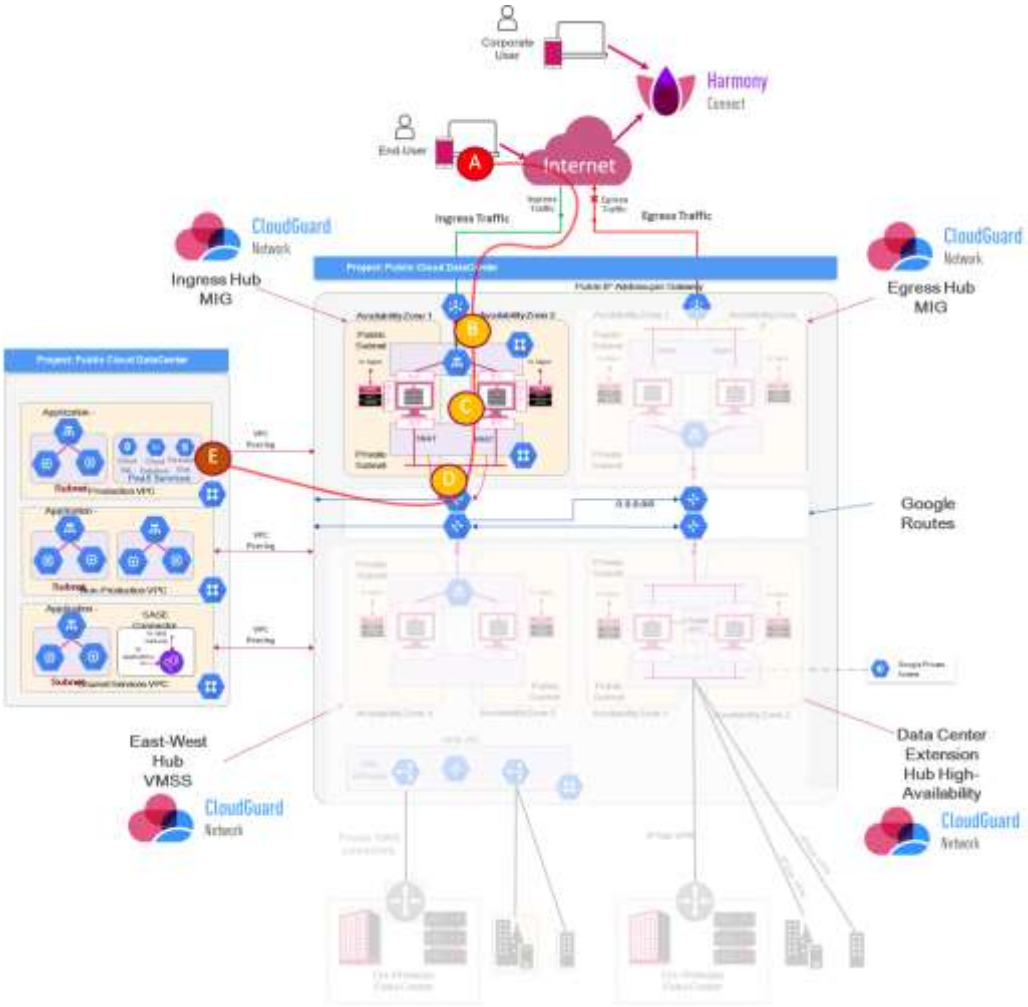


Рисунок 2.5 – Потік вхідного трафіку між Transit Security Services Hub і Production Hub – Google Cloud Platform

Після цього внутрішній балансувальник навантаження відправляє вхідний трафік групі серверів, які розміщені у ще більшій внутрішній мережі. В кінці, автоматичне масштабування GCP налаштовується на збільшення або зменшення кількості шлюзів безпеки «Check Point» CloudGuard у MIG.

Схема потоку вхідного трафіку між «Hub» транзитного сервісу безпеки і «Hub» виробництва у Google Cloud Platform зображена на рисунку 2.5.

Якщо описувати підхід AWS до розгортання GWLB, то він значно відрізняється від описаних вище (див. рис. 2.6).

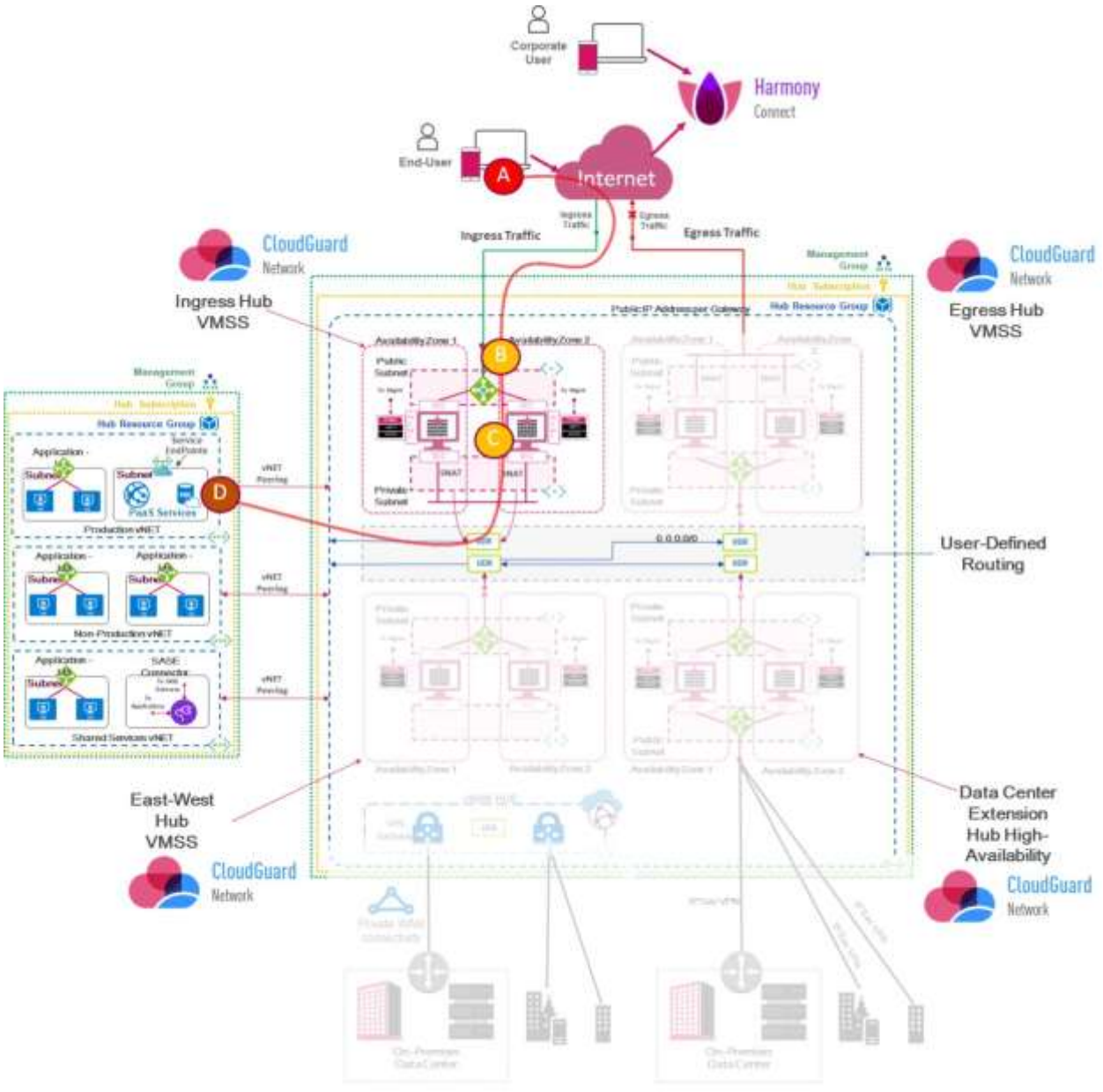


Рисунок 2.6 – Приклад вхідного трафіку AWS

На схемі вище продемонстровано перевірку потоку трафіку «північ-південь» за допомогою централізованого пристрою VPC.

Потік «A» є трафіком кінцевого користувача, що йде до інтернет-шлюзу. Шлюз NAT транслюється за IP-адресою джерела. Інтернет-шлюз направляє трафік назад до NAT-шлюзу «A».

В потоці «B» шлюз NAT «A» використовує маршрут мережевої адреси інтерфейсу VPC у таблиці маршрутів «A» шлюзу NAT і направляє трафік до GWLBE (кінцевої точки балансування навантаження шлюзу) «A».

Потік «C»: GWLBE «A» за допомогою AWS PrivateLink безпечно направляє трафік на GWLB (балансувальник навантаження шлюзу) через мережу Amazon.

В потоці «D», оскільки цей зворотний пакет пов’язаний з існуючим потоком, GWLB інкапсулює вихідний IP-трафік із заголовком GENEVE і пересилає його на шлюз безпеки R80.40 або R81, обраний для цього потоку.

Шлюз безпеки R80.40 або R81 за GWLB декапсулює заголовок GENEVE, перевіряє трафік і вирішує, як його обробити в залежності від того, як налаштовані політики безпеки. У R80.x діє перевірка трафіку на основі правил для IPS, Antibot і Antivirus. Відповідно до цього підходу з’являється можливість створювати політики відповідно до потоків і точніше вибирати потреби перевірки для різних програм.

Припускаючи, що трафік дозволено та перевірено політикою безпеки, шлюз безпеки R80.40 або R81 повторно інкапсулює заголовки GENEVE та пересилає трафік до GWLB.

GWLB на основі GENEVE TLV вибирає GWLBE «A», видаляє заголовок GENEVE та перенаправляє трафік до GWLBE «A».

Той, в свою чергу, використовує маршрут мережевої адреси інтерфейсу VPC у таблиці маршрутів «A» пристрою та направляє трафік транзитного шлюзу.

Оскільки VPC шлюзу безпеки R80.40 або R81 пов’язано з таблицею транзитних маршрутів, транзитний шлюз використовує маршрут мережевої адреси зовнішнього VPC у таблиці транзитних маршрутів, щоб надсилати трафік до зовнішнього VPC.

В кінці, коли трафік потрапляє на інтерфейсний VPC, адресат пакета знаходиться в межах діапазону VPC CIDR, де локальний маршрут використовується для доставки трафіку до екземпляра програми, який отримав трафік.

Описаний вище шлях потоків дозволяє шлюзам безпеки підтримувати з’єднання без SNAT. Здатність GWLB використовувати 5 кортежів або 3 кортежі IP-пакетів для вибору певного пристрою за ним протягом усього життя цього потоку в поєднанні з режимом пристрою транзитного шлюзу також забезпечує постійність сеансу незалежно від джерела та призначення AZ. Це включає AZ, у яких розгорнуто підключення транзитного шлюзу та GWLB, але все ще забезпечує автомасштабування та автоматичні перевірки працездатності.

Політики безпеки мають бути зосереджені на кожному потоку, що означає, що важливо визначити захист відповідно до зазначених робочих навантажень і політик із джерелом, одержувачем, послугами та відповідними підписами для IPS. Наприклад, робоче навантаження з використанням сервера Windows/Linux і сервера Microsoft IIS/Apache має бути захищене лише спеціальним контролем доступу, дозволяючи трафік HTTP/HTTPS і ввімкнувши перевірку трафіку відповідні підписи для робочого навантаження.

2.2 Потік вихідного трафіку у еталонних архітектурах для публічного IaaS

Тепер розглянемо шлях та обробку вихідних потоків трафіку. Цей тип трафіку у безпечний спосіб реалізовує процес надання доступу до обчислювальних екземплярів. Вихідний трафік не повинен націлюватись на кінцевих користувачів, а його застосування здійснюється лише для цілей обслуговування. Варто зазначити, що фільтрація виходу контролює трафік, який намагається вийти через транзитний центр безпеки або транзитний шлюз від vNET або VPC. Таким чином, фільтрація є важливим процесом, який охоплює забезпечення безпечного доступу до мережі Інтернет; обчислювальних примірників, розташованих у vNET або VPC, а також запобігає вихідним з'єднанням із небезпечними та небажаними хостами. Останнє реалізовується в наступних сценаріях.

Нехай, одна із наявних у підмережах vNET/VPC віртуальних машин заражена шкідливим програмним забезпеченням. У цьому випадку вибрані політики запобігання вихідним загрозам запобігають підключенню до командного сервера зловмисного програмного забезпечення. Якщо атакуюче програмне забезпечення намагається експортувати дані комп'ютера, вихідний фільтр може завадити йому під'єднатися до пункту призначення.

У хмарних центрах обробки даних вихідний трафік не орієнтований на корпоративних користувачів. В результаті, у користувачів немає дозволу на вихід до мережі Інтернет або спілкування в чаті за допомогою сайтів соціальних мереж. Політика безпеки виходу також може блокувати порти, протоколи, програми та URL-адреси, які використовуються для надання певних служб з метою обслуговування, або будь-яких інших сайтів, до яких вони не мають доступу. Виконання блокування певних типів трафіку запобігає використанню обчислювальних елементів vNET/VPC для реалізації

DDoS-атак, інтеграції вірусного програмного забезпечення, спаму та ботнетів.

Сучасні методи запобігання та попередження вихідних загроз пропонує багаторівневий підхід захисту з використанням інструментів для запобігання зараження та протидії шкідливим програмам, якщо воно вже відбулось:

- Anti-Bot – являє собою систему виявлення ботів на хостах після зараження. Здатний виявляти інфекції за допомогою кількох методів виявлення та блокувати комунікації C&C (командування та керування) під час зараження.
- Антивірус – спеціалізована програма для виявлення комп'ютерних вірусів, небажаних (шкідливих) програм загалом. Також використовується для відновлення заражених (модифікованих) такими програмами файлів [7].
- SandBlast – захист від зараження невиявленими експлойтами, «атак нульового дня» та цілеспрямованих атак. Виконує емуляцію загроз, тобто швидку перевірку файлів та запуск їх у віртуальному середовищі з метою виявлення шкідливих програм, а також їх видалення.

Тепер відобразимо вихідні потоки на еталонних архітектурах для публічного IaaS. Традиційно, спершу розглянемо для Azure (див. рис. 2.7).

Внутрішній трафік (точка «A») проходить маршрутизацію через шлюз «Check Point» за допомогою UDR (вивчених користувачем маршрутів), що вказують на внутрішній балансир навантаження (точка «B»). Потім трафік перенаправляється до шлюзу безпеки для проходження обробки та перевірки за допомогою політик запобігання загрозам на основі правил (точка «C»).

Шлюз використовує SNAT (точка «D»), щоб приховати цей тип трафіку за своєю зовнішньою приватною адресою (10.0.1.10). Коли трафік залишає віртуальну мережу, Azure замінює приватну адресу публічною адресою шлюзу для доступу до мережі Інтернет (точка «E»).

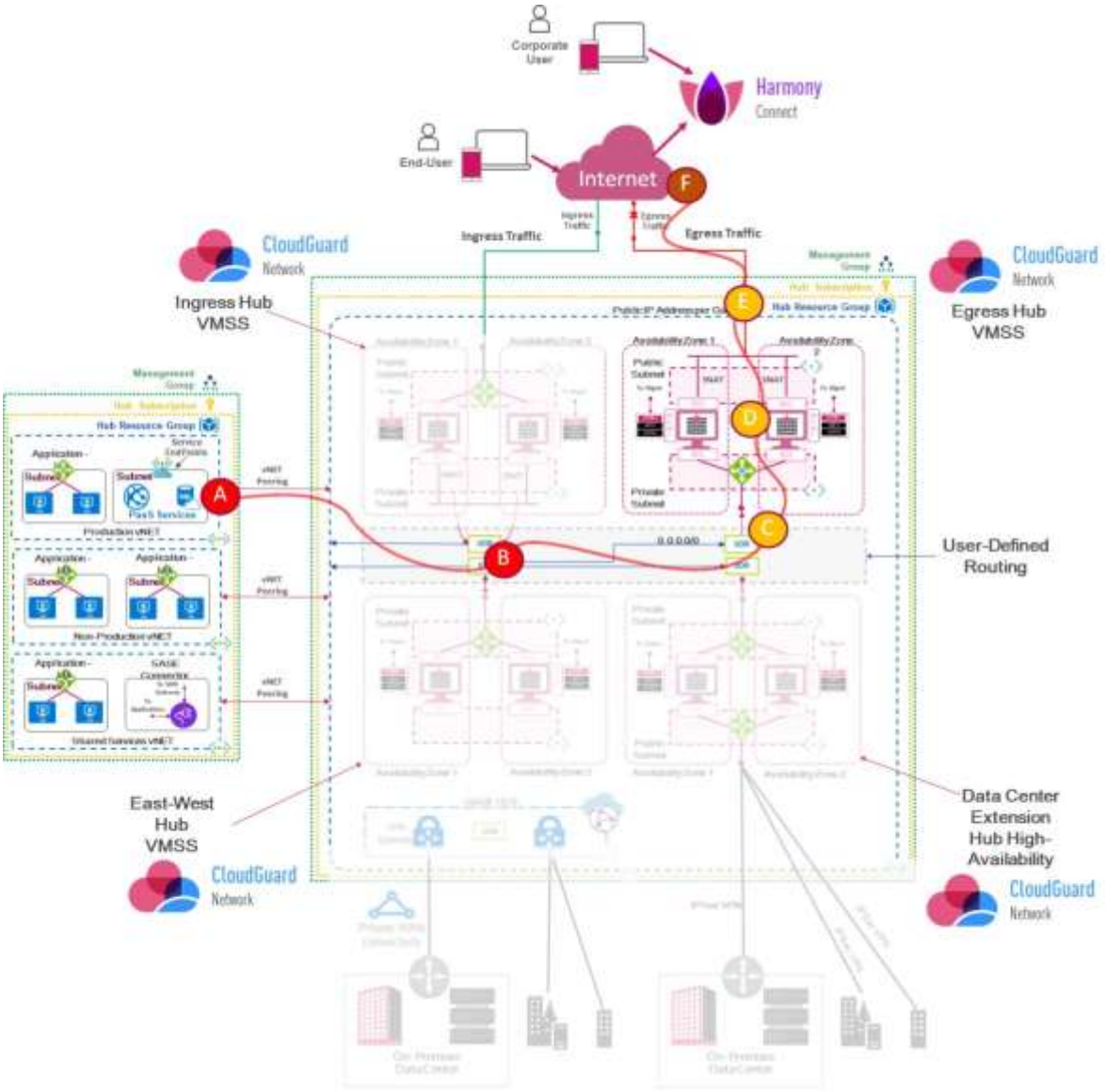


Рисунок 2.7 – Вихідний трафік для обчислювальних модулів Azure

Подібний підхід використовується і для виходу на платформу GCP, що зображено на рисунку 2.8.

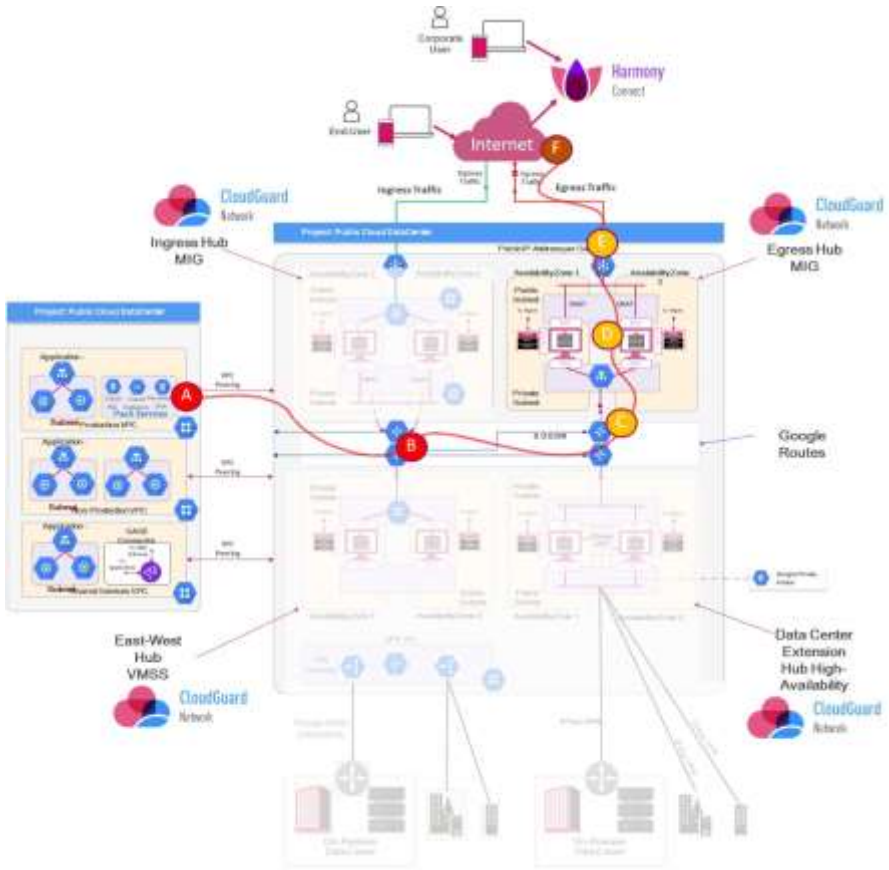


Рисунок 2.8 – Вихідний трафік для обчислювальних модулів GCP

На продемонстрованій вище діаграмі зображено, як, на основі маршруту, балансувальник навантаження розподіляє вихідні запити на з'єднання між шлюзами безпеки «Check Point» CloudGuard. Потім одиниця шлюзу безпеки CloudGuard отримує запит, перевіряє його та, якщо є дозвіл, пересилає в мережу Інтернет.

Обчислювальний екземпляр (потік «A») намагається підключитися до Інтернету, використовуючи (потік «B») кілька маршрутів до 0.0.0.0/0 із наступним переходом (потік «C») до шлюзу безпеки в групі керованих примірників (потік «D»). Однак GCP не дає можливості встановити балансувальник навантаження в якості наступної дії. Тоді необхідно вказати маршрут для кожної одиниці шлюзу безпеки. Для цієї дії рекомендується вимкнути автомасштабування на вихідній MIG, щоб уникнути випадків, коли після виконання автоматичного завершення роботи визначеного екземпляра шлюзу безпеки шлях (потік «E») стає недоступним.

З іншого боку, у AWS використовується відмінний підхід із GWLB для вихідного трафіку, як зображено на рисунку 2.9.

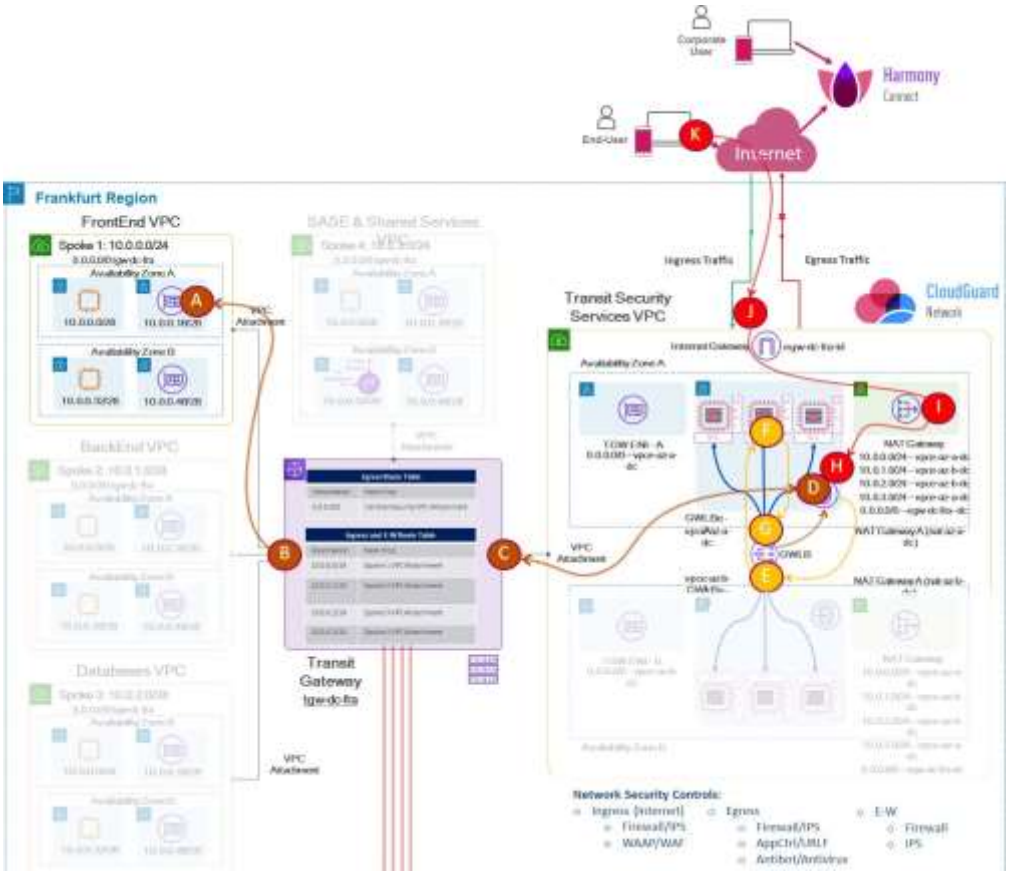


Рисунок 2.9 – Вихідний трафік AWS

Програма у інтерфейсі VPC (потік «A») хоче отримати доступ до Інтернету, зазвичай завантажуючи патчі або виправлення. Програма використовує маршрут за замовчуванням (0.0.0.0/0) у інтерфейсній таблиці маршрутів VPC A для надсилання трафіку до транзитного шлюзу. Оскільки Fronend VPC (потік «B») пов’язано з таблицею вихідних маршрутів, транзитний шлюз використовує маршрут за замовчуванням у таблиці вихідних маршрутів для надсилання трафіку до VPC служб безпеки транзиту.

У транзитних службах безпеки VPC (потік «C») підмережа транзитного шлюзу «A» використовує маршрут за замовчуванням у таблиці маршрутів транзитного шлюзу «A» для надсилання трафіку до GWLBE «A», який знаходиться в тій самій зоні доступності (AZ).

GWLBE «A» за допомогою AWS PrivateLink направляє трафік до GWLB (потік «D»). Трафік безпечно маршрутизується через мережу Amazon без додаткового налаштування.

GWLB (потік «E») використовує 5 кортежів або 3 кортежі IP-пакетів, щоб вибрати пристрій для життя цього потоку. Це створює прив'язаність сеансу до пристрою протягом усього терміну дії потоку, необхідного для шлюзів безпеки R80.40/R81. GWLB інкапсулює оригінальний IP-трафік із заголовком GENEVE [8] і пересилає його на пристрій через UDP-порт 6081. Ця інкапсуляція дозволяє доставляти весь IP-трафік на шлюзи безпеки R80.40/R81 для перевірки, не вказуючи слухачів для кожного порту та протоколу.

У потоці «F» шлюз безпеки R80.40/R81 декапсулює заголовок GENEVE і вирішує дозволити трафік на основі налаштованої політики безпеки. Для вихідного трафіку слід увімкнути відповідні блейд-сервери: антивірус, антибот і піскоструй. Потім, у потоці «G», шлюз безпеки R80.40/R81 повторно інкапсулює трафік і пересилає його до GWLB.

GWLB (потік «H») на основі значення довжини типу GENEVE (TLV) [9] вибирає GWLBE «A», видаляє заголовок GENEVE та перенаправляє трафік до GWLBE «A».

У потоці I GWLBE «A» використовує маршрут за замовчуванням у таблиці маршрутів «A» пристрою та направляє трафік до шлюзу NAT «A».

На етапі «J» NAT «A» використовує маршрут за замовчуванням у таблиці маршрутів «A» шлюзу NAT, виконує трансляцію IP-адреси джерела та направляє трафік до інтернет-шлюзу (igw-id). Звідти трафік виходить в мережу Інтернет.

2.3 Потік трафіку «схід-захід» у публічному хмарному IaaS

Трафік «схід-захід» пов’язаний із зв’язком між виробничими системами в рамках 3-рівневої архітектури додатків (веб-сервери, сервери додатків і бази даних). Трафік може надходити від віртуальної машини, служби PaaS або контейнера та спрямовуватися до іншої віртуальної машини, служби PaaS або контейнера.

Для трафіку «схід-захід» існують два різних призначення:

- Контроль доступу.
- Запобігання загрозам.

CloudGuard покращує власну мікросегментацію та еластичну мережу хмарних середовищ, щоб динамічно забезпечувати розширену безпеку та узгоджене застосування політики, яка автоматично зростає та масштабується разом із вашим хмарним середовищем. Він може легко захистити робочі навантаження та програми, що працюють у гібридних і загальнодоступних хмарних середовищах, таким чином зменшуючи ризики від проникнення шкідливого ПО або вірусів, витоку даних і загроз «нульового дня».

Групи безпеки забезпечують надійний захист і дозволяють мікросегментацію, оскільки вони можуть бути пов’язані з мережевим інтерфейсом хмарного об’єкта. Однак вони обмежені традиційним контролем доступу рівня 3-4 і не підходять для «запобігання загрозам». Групи безпеки також не можуть розпізнати, чи заборонений протокол тунелюється всередину дозволеного, чи трафік є справді чистим SQL чи чимось зловмисним (наприклад, атака SQL-ін’єкцій) через відомий порт SQL. Крім того, групи безпеки не можуть дозволити або заборонити доступ на основі призначених тегів метаданих із такими значеннями, як «сервери бази даних» або «веб-сервери».

Важливо відзначити, що макросегментація, зазвичай, відноситься до трафіку, що виходить з нашої мережі або зони, а мікросегментація стосується трафіку, що перетікає між ресурсами всередині них.

2.4 Висновок до другого розділу

В ході написання другого розділу роботи було продемонстровано варіанти використання безпеки еталонних архітектур на прикладі організації роботи потоків у хмарному середовищі для загальнодоступного IaaS.

Досліджено властивості вхідних та вихідних потоків відправки пакетів даних. Також було розглянуто структуру та призначення потіку «схід-захід».

Охарактеризовано та описано схеми організації перевірки безпеки, запобіганню вірусним загрозам та методи запобіжних заходів при проникненні шкідливого ПЗ в систему.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ

3.1 Проведення експериментального дослідження на час реакції вторгнень в хмарному сховищі

Експериментальні дослідження проводились за допомогою розподіленої комп'ютерної системи з розгорнутим засобом хмарних обчислень за допомогою файлового середовища. Досліджувана система була реалізована за допомогою 7-ми комп'ютерів (файлові сервера) і одного комп'ютера, як головного серверу, зокрема на кожному комп'ютері було проістальовано програмне забезпечення, що дає змогу реалізувати хмарне сховище даних. Всі файлові сервера мають спеціальні агенти безпеки, за допомогою яких проводиться визначання вторгнень на перших стадіях, щоб провести швидке реагування.

Наступним кроком експерименту було внесення частини шкідливого коду до файлів з різними типами розширення, зокрема текстового, відео, аудіо та графічного, з подальшою передачею на файлові сервери. Після ідентифікації зараженого файлу, агент безпеки проводить процедуру зупинки передачі даних, і за допомогою зібраної інформації відносно мережі, визначає швидкий шлях передачі повідомлень про встановлену загрозу до блоку управління безпеки у розподіленій мережі (адміністративний комп'ютер), для подальшого визначення процедури безпеки. Зокрема проводиться відслідковування швидкості передачі файлів до модуля адміністрування безпеки по збору статистики, а зокрема для обчислення середньої швидкості реакції на вторгнення.

Даний метод, який має за основу ієрархію агентів, дає змогу підвищити ефект управлінням безпеки мережі, за допомогою повідомлень про загрозу всім агентам ієрархії. Що дозволяє зменшувати час реакції на вторгнення і в свою чергу зберегти всі сервера нашої мережі від загроз.

Розглянемо метод моніторингу сусідніх вузлів, для того щоб підвищити ефективність адміністрування безпеки.

Наведемо етапи процесу збору результатів. З самого початку була змодельована класична модель агентів з зв’язками по вертикалі, що наведено на рисунку 3.2, в свою чергу дає можливість на реалізацію послідовності дій під час виявлення атак [26]:

- За допомогою агента нижнього рівня відбувається виявлення загрози на своєму вузлі, після цього проводиться відправка повідомлення про виявлену атаку на агент вищого рівня.
- Агент вищого рівня, після отримання повідомлення про небезпеку, в свою чергу проводить передачу агенту 1 рівня (головний агент системи).
- Аналіз повідомлення проводиться після того, як головний агент системи отримує повідомлення про атаку.
- Після того, як завершиться аналіз, всі агенти верхнього рівня системи получають один з можливих результатів: так, виявлена загроза; ні, помилкова загроза.
- Агенти другого рівня (верхнього), реагують і відсилають повідомлення про небезпеку агентам третього рівня (нижнього).
- Агенти третього рівня після отримання повідомлення про небезпеку від агентів другого рівня, виконують наперед встановлені правила.

Проведені експерименти, які в свою чергу складаються з атак на сервери сховищ даних. Проводиться також збір статистики відносно швидкості реагування на виникаючі небезпеки, а зокрема на загальний час реакції на виявлену небезпеку.

Наведено модель агентів ієрархії з зв’язками по горизонталі, що реалізують наступні дії:

- Агенти рівня вузла (нижній рівень) виявляючи небезпеку на своєму вузлі, проводить виконання відповідного правила з бази правил,

відправляючи повідомлення про небезпеку на агент верхнього рівня, і на агенти які є сусідами даного рівня.

- Агент рівня сегменту (верхній рівень) виконує відповідне правило з бази, тоді коли виявить небезпеку в своєму сегменті, після того відправляє повідомлення агенту координатору (агент 1 рівня) і на агенти свого рівня.
- В свою чергу головний агент 1 рівня аналізує отримані повідомлення про небезпеку, і активовує мобільний агент при потребі на потрібному вузлі.

В таблиці 3.1 наведено час реакції класичної моделі агентів, які в свою чергу змінюються за результатами експериментів, в діапазоні значень від 2 секунд до 6 секунд.

Таблиця 3.1 – Час реакції класичної моделі агентів

	Час реакції, сек						
№ Експеримента	вузол 1	вузол 2	вузол 3	вузол 4	вузол 5	вузол 6	вузол 7
1	3,795	2,53	2,498	2,985	3,561	2,739	3,671
2	2,389	3,468	2,671	3,428	4,17	3,789	4,304
3	4,148	2,815	3,873	2,81	3,841	2,644	2,49
4	2,85	3,719	2,856	2,605	2,489	3,41	2,508
5	2,771	2,511	4,287	4,301	2,883	4,209	3,71
6	4,091	3,349	2,691	2,722	3,424	2,489	2,782
7	3,689	2,964	2,507	2,981	2,901	3,378	2,816
8	2,457	2,584	3,049	3,549	3,748	2,941	3,284
9	3,089	4,197	2,486	3,97	2,647	3,079	2,478
10	2,988	2,623	3,852	2,78	3,821	2,671	2,876

Таблиця 3.2 – Час реакції ієрархічної моделі агентів

	Час реакції, сек						
№ Експеримента	вузол 1	вузол 2	вузол 3	вузол 4	вузол 5	вузол 6	вузол 7
1	4,01	4,31	4,201	4,174	3,955	5,37	3,783
2	4,579	5,344	3,668	3,271	4,799	4,904	3,92
3	2,109	4,063	4,015	3,553	5,904	5,824	5,421
4	5,204	3,321	3,303	4,264	4,382	6,069	4,781
5	4,312	3,49	4,534	4,285	5,2	5,246	4,021
6	3,878	4,746	5,201	5,171	4,865	4,187	3,892
7	4,844	3,124	4,421	4,078	4,382	3,47	5,904
8	3,947	4,96	3,993	3,004	3,651	3,796	4,187
9	4,79	5,567	4,41	4,452	3,314	3,944	4,48
10	4,984	4,742	4,634	3,231	4,622	5,713	4,783

В таблиці 3.2 наведено час реакції ієрархічної моделі агентів, що коливаються від 2,5 секунд до 4,3 секунди, це дає змогу зрозуміти наявність попереджувального регулювання на виявлену загрозу за допомогою горизонтальної передачі.

Таблиця 3.3 – Порівняння сумарної часу реакції Класичних і Ієрархічних агентів

	вузол 1	вузол 2	вузол 3	вузол 4	вузол 5	вузол 6	вузол 7
Класична	4,2657	4,3667	4,238	3,9483	4,5074	4,8523	4,5172
Ієрархічна	3,2267	3,076	3,077	3,2131	3,3485	3,1349	3,0919

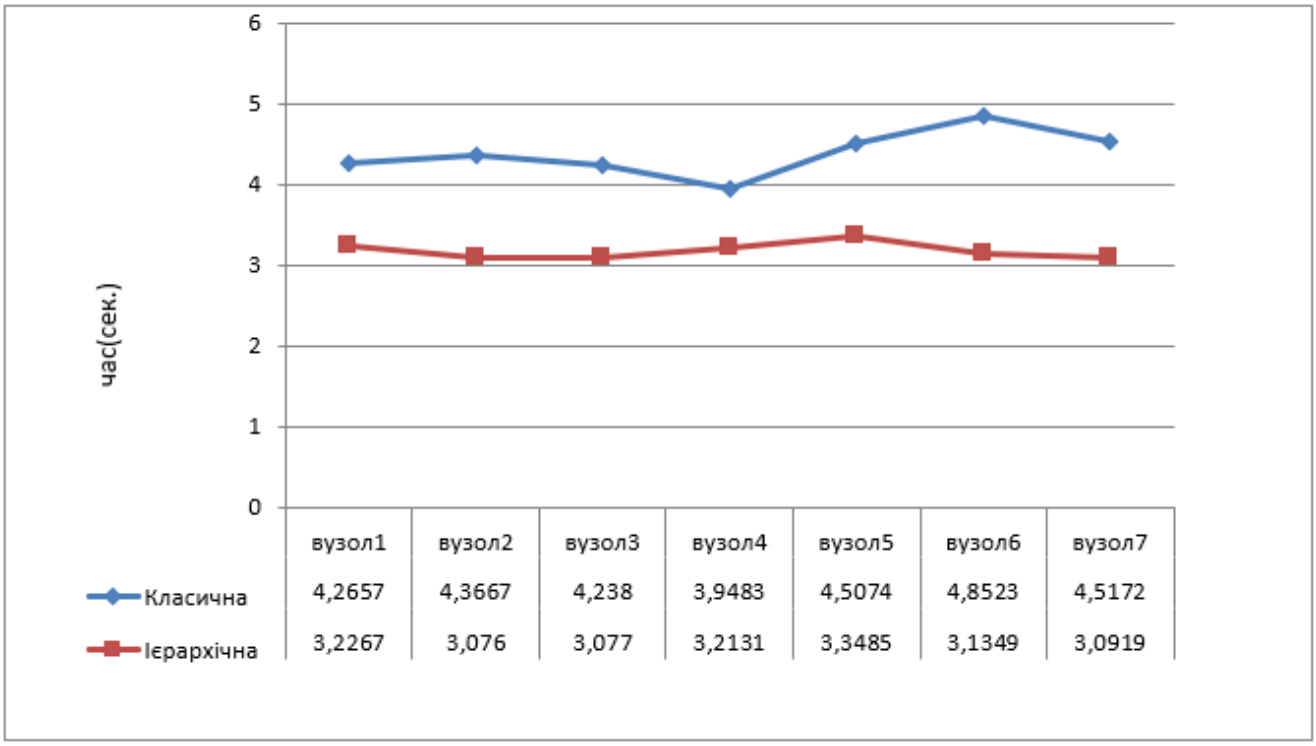


Рисунок 3.1 – Порівняння середнього часу для двох моделей

На рисунку 3.1 видно середній час реакції всіх вузлів на небезпеку, що в свою чергу для класичної моделі становить від 4-5 секунд, а для горизонтальних зв’язків реакція на загрози в рамках від 3-3,35 с.

Згідно графіків, ми бачимо, що даний метод позволить підвищити ефективність рівня безпеки хмарних систем за допомогою збільшення швидкодії реакції на вторгнення, що не знижує швидкість запису файлів до хмарного середовища.

3.2 Виявлення вторгнень за допомогою спеціальних агентів

Для статистичного збору використаємо комплекс із чотирьох локальних об’єктів і 1-го сервера безпеки, в свою чергу 2-ва з 4-х локальних агентів будуть розташовані на 1-й робочій станції, що зображено на рисунку 3.2.

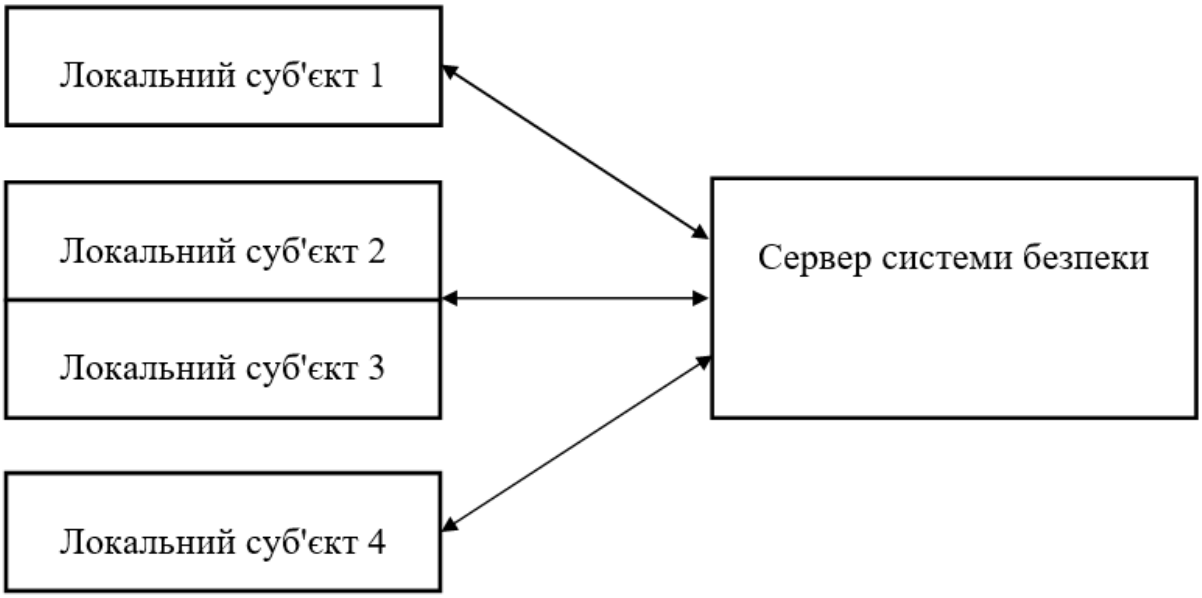


Рисунок 3.2 – Структурна схема системи для проведення експериментів

В свою чергу в процесі збору статистики, буде сформовано сеансовий вектор $X=\{x1, x2,..., xn\}$, містить фактори за допомогою, яких вони можуть бути зв'язані з порушенням системи. Зокрема, елементами вектора X є такі чинники: Чинники вектора X наведено на рисунку 3.3.

Вектор	Чинники
x1	запущені системні процеси;
x2	інтегральний час недоступності агента (у хв);
x3	відкриті порти;
x4	питомий обсяг використаної пам'яті (у %);
x5	показник співвідношення часу доступу до файлу і його розміру (мс/ Кб);
x6	показник завантаженості каналу передачі даних (у %);
x7	потенційно небезпечні програми, в т.ч. на сусідніх вузлах.

Рисунок 3.3 – Чинники вектора X

Вводиться ваговий коефіцієнт вектора X відповідно до впливу безпеки системи. В таблиці 3.3 наведено значення коефіцієнтів.

Після цього формується сам пороговий вектор, який в собі має максимально допустимі значення, що в свою чергу не класифікується, як вторгнення.

Проведемо наступний експеримент де будуть задіяні 10 локальних суб’єктів для імітації різних події, в тому числі і несанкціонованих. Також наведено результати дій користувачів, що були напрямлені на перевищення максимальних значень вектора X.

Як видно, що кількість наведених атак у випадку не задіяння підсистеми виходить більше ніж в 4 рази в порівнянні з використаною нами підсистеми, через те, що за допомогою рішення ПЛВ відбувалось вимкнення локальних суб’єктів.

3.3 Висновок до третього розділу

В даному розділі наведено проведення експериментального дослідження на час реакції вторгнень в хмарному сховищі, а також на прикладах проведено опис виявлення вторгнень за допомогою спеціальних агентів.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1 Охорона праці

Метою кваліфікаційної роботи магістра є дослідження методів захисту відомих хмарних платформ. Оскільки, проведення робіт з розробки та використання системи передбачає використання комп'ютерної техніки, зокрема ПК та периферійних пристроїв, то обов'язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників, в тому числі і фахівців з підвищення ефективності контролю доступу в приміщення, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [27]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Згідно вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог:

- переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

- Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, ДБН В.2.5-56:2010, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі

перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним. Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у

НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги». Відстань від екрана до ока фахівців, які працюють за комп'ютером визначається згідно з вимогами ДСанПіН 3.3.2.007-98.

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації в зоні досяжності моторного поля згідно з вимогами ДСанПіН 3.3.2.007-98.

4.2 Безпека в надзвичайних ситуаціях

4.2.1 Міжнародний тероризм

Терор (лат. terror – страх, жах) – має ознаку «усувати», «закривати». Ця обставина і визначає терор як особливу форму політичного насильства, що характеризується жорстокістю, цілеспрямованістю й уявленою ефективністю. Ці особливості визначили широке використання терору упродовж людської історії як засобу політичної боротьби в інтересах держави, організацій чи окремих угруповань. Безпосередньо сам факт привселюдної страти кримінальних чи політичних злодіїв, чи процес «аутодафе» в період середньовікової інквізиції, є класичною формою терору в інтересах держави чи католицької церкви.

Правовою основою боротьби з міжнародним тероризмом є «Декларація про заходи для ліквідації міжнародного тероризму», що затверджена на 49-й сесії Генеральної асамблеї ООН (резолюція 49/60 від 9 грудня 1994 р.)

Цей документ встановлює принципи відносин світової спільноти і програму заходів з метою ліквідації такого огидного суспільного явища, як

міжнародний тероризм, а також встановлює подальше співробітництво між державами для невідкла-деної ліквідації будь-яких форм і проявів терористичної діяльності. Характерним для розвитку світової спільноти є те, що наявність лідера (провідної країни чи провідної сили) народжує відповідну реакцію – формування нижчого за рангом (рівнем) іншого лідера (іншої країни чи іншої провідної сили). Має місце формування біполярності, виникають реалії антагонізму на різних рівнях світового суспільства, в т.ч. суперечності на рівні «держава»↔«держава», «держава»↔«внутрішня організація» (організація зовнішня), «держава»↔«партія» та ін. Крім того, у світовій практиці мають місце комбіновані види із вищезгаданих «пар», з яких формуються інші групи (сили), в т.ч. політичні, злочинні та ін. відповідні сили чи угруповання. На другому етапі формування ці сили (групи) шукають собі відповідні «ніші» існування; економічну, політичну, наукову та інші види підтримок; формують свої озброєні сили, відповідні професійні кадри, джерела озброєння, територію знаходження тощо. При цьому використовуються всі «блага» цивілізації особистого розвитку і поширення впливу на світову спільноту.

Міжнародний тероризм, створюючи свій плацдарм, може викликати кризи (системні) в світовій, моральній, політичній, економічній системі відносин і зруйнувати та усунути всі передумови розвитку світової спільноти.

В Україні, за даними служби безпеки, за останні два роки скоєно понад 560 злочинів терористичного характеру, внаслідок цього 90 осіб (із них 15 представників владних структур) загинуло. В Україні зростає активність міжнародних терористичних організацій, насамперед із країн Ближнього Сходу («Хезболах», «Абу Ніджаль», «Хамас», «Брати мусульмани»), які прагнуть використати територію України для транзиту своїх бойовиків до країн західної Європи, підготовки терористичних акцій.

Головними принципами попередження та боротьби з міжнародним тероризмом має стати постійне удосконалення відповідної законодавчої бази, співробітництво з правоохоронними організаціями, консолідація з іншими країнами й організація напрямів запобігань поширенню будь-яких терористичних організацій і угруповань.

Терористичний акт не має безпосередніх можливостей досягнення оголошеної кінцевої мети і звичайно складається з таких елементів: насильницька дія у різноманітних її формах, політичний мотив в основі здійснення самого терористичного акту; сам акт спрямовано проти осіб, організацій, націй, національностей і меншин, державних інститутів чи їх представників з метою їх залякування чи виконання окремих вимог. Терор щодо націй, етнічної, расової чи релігійної групи, що здійснюється для її повного чи часткового усунення, розглядається світовою спільнотою вже як акт геноциду.

Варіанти комбінацій за спрямованістю суб'єкт—об'єкт здійснення терористичного акту багатоспрямовані, тому важко дати універсальне визначення «терору». Проте деякі критерії певної класифікації можна встановити:

- індивідуальний, організований терор і терор як політика держави;
- терор як метод внутрішньополітичної боротьби і терористичні акти міжнародного характеру.

4.2.2 Структура системи БЖД

Поняття «життєдіяльність» стосується тільки людини. Людина живе і працює в безпосередньому зв’язку з навколишнім середовищем.

Життєдіяльність (ЖД) – це складна фізіологічна система, яка має назву «система ЖД».

Системою називають сукупність взаємозв’язаних елементів, функціонування яких спрямоване на досягнення певної загальної мети.

Система ЖД складається із взаємопов’язаних елементів: життя, діяльності людини, навколишнього середовища, – і має підтримувати комфортне та безпечне існування людини, забезпечити сталий розвиток людства.

Розглянемо характеристики елементів системи ЖД.

Життя – це форма існування матерії, яка характеризується обміном речовин, здатністю до розмноження і розвитку, вмінням пристосовуватись до навколишнього середовища.

Людина – вища форма розвитку живої матерії, і її існування – дуже складний процес, що не тільки підтримує її фізіологічний стан, але й задовольняє духовні потреби. Крім того, на життя людини суттєво впливають умови проживання та праці, медичний догляд і багато інших факторів, що виникають завдяки діяльності самих людей.

Діяльність – це специфічна форма ставлення людей до навколишнього середовища та одне до одного, яка має задовольняти потреби та інтереси людини. Це соціальна категорія, нерозривно зв’язана із суспільством. Тільки завдяки діяльності людини створено всі блага, які має людство.

Основні види діяльності такі:

- виробнича;
- наукова;
- мистецька;
- освітня.

Однією із специфічних форм діяльності людини є праця – перша й основна умова існування людини (людства).

Праця – цілеспрямована діяльність людини, у процесі якої вона впливає на природу і використовує її з метою виробництва матеріальних та інших благ, необхідних для задоволення своїх потреб.

Потреби – це необхідність для людини того, що забезпечує її існування і самозабезпечення (фізіологічне, матеріальне, соціальне, духовне та ін.).

Навколишнє середовище (довкілля) або середовище існування – це все, що оточує людину впродовж її життя. Навколишнє середовище, у свою чергу, поділяють на такі види:

- природне середовище;
- штучне середовище.

Природне середовище (біосфера) – це частина Землі і простору навколо неї, де зосереджено все живе. Біосфера включає:

- атмосферу (газоподібна частина);
- гідросферу (рідка водна частина);
- літосферу (тверда частина).

На ЖД людей найбільше впливає частина біосфери від поверхні Землі вглиб на 15–20 км і до висоти 20–22 км, де починається озоновий шар. Природне середовище є джерелом природних ресурсів для існування людини: повітря, води, деревини, корисних копалин, ґрунту та ін.

Штучне середовище – це складова довкілля, створена людством за тривалий час його існування. Штучне середовище умовно можна поділити на два види:

- виробниче середовище;
- побутове середовище.

Виробничим називають середовище, в якому людина реалізує свою трудову діяльність (підприємства, установи, навчальні заклади тощо).

Побутовим є середовище, де люди мешкають або проводять вільний час. Воно охоплює сукупність житлових будинків, комунально-побутових об’єктів, місця відпочинку та ін.

Організм людини може нормально функціонувати тільки тоді, коли умови (параметри) зовнішнього середовища відповідають оптимальним. Якщо умови середовища змінюються, стають несприятливими, то на протидію їм організм людини включає спеціальні механізми, які зберігають

постійність параметрів внутрішнього середовища (всередині організму) чи змінюють їх у межах допустимого.

Можливість функціонування організму в середовищі, параметри якого постійно змінюються, забезпечується завдяки механізму, який називають адаптацією.

Адаптація (лат. adapto – пристосування) – динамічний процес пристосування організму до мінливих умов зовнішнього середовища, який спостерігається в будь-якому виді діяльності щоразу, коли виникають значні зміни в системі «людина – середовище». Адаптація може бути фізіологічною, психологічною, соціальною.

Отже, для функціонування системи ЖД середовище має обов'язково відповідати природним параметрам. Відхилення можливі в межах допустимого, коли організм людини здатний адаптуватися, захистити себе, підтримувати існування. Усе, що існує за цими межами, становить загрозу життю, тому виникає потреба захисту ЖД людей. Отже, безпека – важлива складова системи ЖД.

Розглядаючи систему ЖД як взаємодію людей з навколишнім середовищем, слід зауважити, що вона завжди підпорядкована певним принципам, правилам, умовам життя, природним умовам, традиціям тощо.

Система ЖД має такі характерні ознаки:

- її функціонування підпорядковане об'єктивним законам природи;
- це динамічна система, яка розвивається, удосконалюється, пристосовується до змін умов існування;
- тяжіє до сталого розвитку, вживаючи заходів захисту від упливу негативних факторів.

Основні принципи забезпечення ЖД такі:

- своєчасність, достатність, якість забезпечення людей необхідними для життя засобами високої якості і заходами в потрібний час у належній кількості;

- безпека ЖД (захист ЖД від упливу негативних факторів, що виникають унаслідок як природних явищ, так і діяльності людей).

Рівень реалізації цих принципів значною мірою залежить від способів забезпечення ЖД. Виходячи із сказаного, можна визначити такі головні способи забезпечення ЖД:

1. Організація ефективної трудової діяльності людей в суспільстві з максимальним залученням усіх ресурсів (створення робочих місць, упровадження високопродуктивного виробництва і технологій, нормування праці тощо).

2. Організація та удосконалення освіти і підготовка кадрів, розвиток науки відповідно до вимог часу.

3. Розвиток сфери послуг (комунальних, транспортних, торговельних, побутових і т. ін.).

4. Розширення мережі культурних, спортивних, розважальних установ.

5. Проведення заходів щодо збереження здоров’я людей (диспансеризація, оздоровлення, кваліфіковане медичне обслуговування і лікування, санітарно-епідеміологічний стан).

6. Розроблення законодавчих і нормативно-правових актів із забезпечення прав, свобод і захисту людей і суспільства в цілому.

Залежно від того, якою мірою реалізуються принципи та способи забезпечення ЖД, визначається рівень життя людей окремих країн і загальний розвиток людства.

4.2.3 Елементи теорії, що відповідають моделі безпеки життєдіяльності

Модель у широкому розумінні – це предмет, явище, система (опис, схема, знак, графік, план, макет та ін.), які за певних умов відіграють роль замінника або представника будь-якого іншого предмета, явища чи системи.

З точки зору науки модель – це матеріальна чи уявна система, що відображає чи імітує принципи внутрішньої організації, функціонування, певні властивості чи характеристики об'єкта дослідження, безпосереднє вивчення якого неможливе. Модель може замінити цей об'єкт у пізнавальному процесі з метою отримання нових знань про нього. Таким чином, відношення «модель—оригінал» не природне, а зумовлене процесом пізнання, і питання про їх співвідношення, ступінь їх подібності, адекватності – одне з найважливіших і найскладніших у процесі використання моделей у науковому пізнанні.

Сам процес моделювання – це непрямий, опосередкований метод наукового дослідження об'єктів пізнання на їх моделях, коли з певних причин безпосереднє їх вивчення неможливе.

Моделі в дисципліні «Безпека життєдіяльності» можна систематизувати за об'єктом зв'язків. Усі моделі можна умовно поділити на дві множини залежно від обсягу зв'язків, які вони демонструють.

Перша множина об'єднує моделі, що характеризуються структурою зв'язків.

Друга множина об'єднує моделі парних зв'язків. Певна умовність щодо цієї множини пов'язана з тим, що запровадження глибокого аналізу дозволяє уявити механізми реалізації цих зв'язків діючих великих систем.

Для характеристики довкілля на глобальному, державному і регіональному рівні використовують поняття структури зв'язків (на світовому рівні – навіть загальної). Відповідно до визначеної послідовності рівнів (за територією, від світового до регіонального) зменшується кількість таких зв'язків – з одного боку, а з іншого – збільшується рівень їх деталізації.

Під державним рівнем у цьому випадку розуміють сукупність діючих галузей виробництва як джерел забруднення і географічні чинники території, що одержує це забруднення. Відповідно до двох визначених рівнів подано моделі, що формують уявлення про стан світового довкілля і держави (на

прикладі сільськогосподарської галузі). На регіональному рівні модель, що формує стан довкілля, може бути представлена у вигляді взаємодій комплексу діючих (діючого) підприємств із середовищем виробництва.

Для визначення умов роботи підприємства найбільшу увагу для застосування привертають моделі, що відображають зв'язки:

- «регіональний природно-виробничий комплекс – середовище виробництва»;
- «виробниче підприємство – довкілля»;
- «виробниче середовище виробничого підприємства (середовище робочого місця) – людина».

Здобуття найбільш деталізованої інформації за взаємодії можливе на рівні парних (взаємодій) у вигляді: забруднювач середовища (джерелом є підприємство) – елемент довкілля. Таким чином, необхідно розробити відповідні моделі парної взаємодії.

До таких моделей (як зразок) належать:

- модель розповсюдження елемента забруднення в середовищі (елементи довкілля – атмосфера, гідросфера, літосфера);
- моделі обігу елемента забруднення в елементах довкілля;
- моделі обігу елементів середовища;
- моделі взаємних впливів на елементи довкілля;
- моделі взаємодій екологічних компонентів і організації екосистем;
- моделі впливів небезпечних і шкідливих чинників;
- моделі ієрархії екосистем та ін.

У рамках пари «виробниче середовище – людина» певний зміст взаємодій реалізується на базі спрощення уявлення «виробниче середовище» і представлення його як «технологічний процес, обладнання, види господарських робіт тощо».

В період виконання «технологічного процесу...» виникають небезпеки. Це може бути ініційовано як з боку «технологічного процесу, обладнання, видів господарських робіт», так і з боку – «людини». Виходячи з цього, у схемі розгляду нещасного випадку необхідно йти двома шляхами відносно:

- технологічного процесу, обладнання, видів господарських робіт та ін.;
- «людини» як джерела небезпек.

Розвиток подій вивчають за допомогою ступеневих логіко-імітаційних моделей. Характер ступеневої суті моделі визначає перехід від події до події. Події і переходи за змістом формуються трьома складовими: 1) технологічний процес, його операції й елементи; 2) конструкція обладнання; 3) стан охорони праці при їх взаємодії.

За наявності небезпечних обставин під час виконання будь-яких робіт людина сприяє, усвідомлює, приймає і реалізує відповідні рішення в послідовності.

Обидві моделі в межах поєднання свого змісту дають змогу усвідомити комплексний розвиток подій, причини аварій та ін., сприяють створенню безпечних умов праці і запобіганню травматизму.

4.3 Висновки до 4 розділу

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи.

Також розглянуто питання міжнародного тероризму, структури системи БЖД, елементів теорії, що відповідають моделі безпеки життєдіяльності.

ВИСНОВКИ

В ході виконанні кваліфікаційної робота освітнього рівня «Магістр» було охарактеризовано стратегію міграції хмарного середовища зі збереженням його структури «Lift and Shift», розглянуті її основні переваги та практичні методи оптимізації для архітектур безпеки публічної IaaS.

Досліджено розширену модель «спільної відповідальності» для публічного IaaS, структуру та політики безпеки узгодженої з її принципами моделі «надання доступу з нульовою довірою», що необхідна для мінімізації потенційних ризиків атаки. Також були розглянуті види сегментації: мікро- та макросегментації; їх роль в забезпеченні безпеки публічної IaaS, що відповідає використанню першої для логічного поділу VPC/vNET на різні зони безпеки та поділу робочих навантажень між основними групами зі схожою функціональністю та класифікацією безпеки, запобігаючи проникненню зловмисників всередину системи та атаці на виробничі робочі навантаження для другої [4].

Охарактеризовано призначення та варіанти використання моделі «Hub and Spoke», різновиди та призначення елементів («Hubs» і «Spokes») цієї моделі в різних еталонних архітектурах. Продемонстровано використання цього принципу в дизайні високого рівня безпеки.

Детально розкрито та проаналізовано еталонні архітектури безпеки для публічного IaaS: Microsoft Azure (Azure), Google Cloud Platform (GCP), Amazon Web Services (AWS), інструменти їх покращення (GWLB, GWLE для AWS), а також можливі методи розгортання та варіанти реалізації автоматичного масштабування.

Було продемонстровано варіанти використання безпеки еталонних архітектур на прикладі організації роботи потоків у хмарному середовищі для загальнодоступного IaaS.

Досліджено властивості вхідних та вихідних потоків відправки пакетів даних. Також було розглянуто структуру та призначення потіку «схід-захід».

Охарактеризовано та описано схеми організації перевірки безпеки, запобіганню вірусним загрозам та методи запобіжних заходів при проникненні шкідливого ПЗ в систему.

Наведено експериментальне дослідження на час реакції вторгнень в хмарному сховищі, а також на прикладах проведено опис виявлення вторгнень за допомогою спеціальних агентів.

Також були розглянуті питання з охорони праці і безпеки в надзвичайних ситуаціях.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Gartner визначає три фактори, що впливають на зростання витрат на безпеку. [Електронний ресурс]. URL: https://www.gartner.com/en/newsroom/press-releases/2022-10-13-gartner-identifies-three-factors-influencing-growth-i.

2. Міграція хмари з використанням методу підйому та переміщення. [Електронний ресурс]. URL: https://www.teradata.com/Trends/Cloud/Lift-and-Shift-Migration1.

3. Парадигма розподілу Spoke-Hub. [Електронний ресурс]. URL: https://hmn.wiki/ru/Hub_and_spoke.

4. Matrix таблиця мікро-сегментації та макро-сегментації. URL: https://networkinterview.com/micro-segmentation-vs-network-segmentation/

5. Що ZTX означає для постачальників послуг та користувачів. [Електронний ресурс]. URL: https://go.forrester.com/blogs/what-ztx-means-for-vendors-and-users/

6. Безпека хмари. [Електронний ресурс]. URL: https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

7. Антивірусна програма. Вікіпедіа. Вільна енциклопедія. [Електронний ресурс]. URL: https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%BD%D0%B0_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0

8. Geneve: Загальна віртуалізація інкапсуляції мережі. [Електронний ресурс]. URL: https://tools.ietf.org/html/rfc8926

9. TLV vs Bit Fields. [Електронний ресурс]. URL: https://tools.ietf.org/html/draft-ietf-nvo3-encap-05#section-6.6

10. Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

11. Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl 75:200–222

12. Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35

13. Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88

14. Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res Comput Commun Eng 2(10):6245–6253

15. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11

16. A. Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy, "Security Threats and Challenges in Cloud Computing," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 46-51, doi: 10.1109/CSCloud.2017.59.

17. Pavan Muraidhara, "Security issues in cloud computing and its countermeasures", International Journal of Scientific & Engineering Research, vol. 4, no. 10, October 2013.

18. M. Zeller, R. Grossman, C. Lingenfelder, M. Berthold, E. Marcade, R. Pechter, et al., "Open standards and cloud computing: KDD-2009 panel report" in , Paris, France:KDD, pp. 11-18, 2009.

19. Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020). https://doi.org/10.1007/s11227-020-03213-1

20. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42

21. Mell P, Grance T (2018) SP 800-145, The NIST Definition of cloud computing CSRC (online)

Csrc.nist.gov. https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed 11 Dec 2018

22. Ramachandra G, Iftikhar M, Khan FA (2017) A comprehensive survey on security in cloud computing. Proc Comput Sci 110:465–472

23. Kaur M, Singh H (2015) A review of cloud computing security issues. Int J Adv Eng Technol 8(3):397–403

24. Kumar PR, Raj PH, Jelciana P (2018) Exploring data security issues and solutions in cloud computing. Proc Comput Sci 125:691–697

25. Огляд моделей хмарних послуг / Н. А. Шевченко, М. В. Валігула, Т. О. Маєвський, Г. В. Шимчук // Матеріали міжнародної наукової конференції „Іван Пулюй: життя в ім’я науки та України“ (до 175-ліття від дня народження), 28-30 вересня 2020 року. — Т. : ФОП Паляниця В. А., 2020. — С. 109–110. — (Важливі аспекти практичного застосування здобутків сучасної науки і новітніх технологій).

26. Радченко Г.И. Распределенные вычислительные системы / Г.И. Радченко. – Челябинск: Фотохудожник, 2012, 184 с. ISBN 978-5-89879-198-8

27. 26. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень. [Електронний ресурс]. URL: https://zakon.rada.gov.ua/rada/show/va042282-99#Text.

28. 27. ГОСТ 12.1.005-88. ССБТ. Загальні санітарно-гігієнічні вимоги до повітря робочої зони. [Електронний ресурс]. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=6264.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національна академія наук України
Тернопільський національний технічний університет імені Івана Пулюя
Західний науковий центр НАН України і МОН України
Тернопільська державна обласна адміністрація
Тернопільська обласна рада
Тернопільська міська рада
Наукове товариство імені Шевченка
Віденський університет (Австрія)
Чеський технічний університет (Чехія)
Університет імені П'єра і Марії Кюрі Сорбона Париж (Франція)
Університет прикладних наук Шмалькайдена (Німеччина)
Технічний університет у Кошице (Словаччина)
Опольський технологічний університет (Польща)
Науково-технічне товариство (Тернопіль)

Матеріали міжнародної наукової конференції «ІВАН ПУЛЮЙ: ЖИТТЯ В ІМ'Я НАУКИ ТА УКРАЇНИ»

(до 175-ліття від дня народження)

28–30 вересня 2020 року

ТЕРНОПІЛЬ, 2020

Матеріали Міжнародної наукової конференції
«Іван Пулюй: життя в ім'я науки та України», Тернопіль, 2020

УДК 004.056

Н.А. Шевченко, М.В. Валігула, Т.О. Маєвський, Г.В. Шимчук
Тернопільський державний технічний університет імені Івана Пулюя

ОГЛЯД МОДЕЛЕЙ ХМАРНИХ ПОСЛУГ

N. Shevchenko, M. Valihula, T. Mayevs'kyy, H. Shymchuk

OVERVIEW OF CLOUD SERVICE MODELS

Сучасні організації залежать від можливостей обробки даних, витрат і накладних витрат на управління своїми обчислювальними ресурсами. Концепція хмарних обчислень призначена звільнити організації та їх співробітників від додаткових витрат пов'язаних з IT. Клієнт може перенести зберігання даних, обробку інформації або навіть всю інформаційну інфраструктуру до провайдера послуг, що дозволяє сфокусуватися на своїй основній діяльності і залишити IT професіоналам [1].

У той час як концепція хмарних обчислень надає новий підхід до обробки інформації, проблеми безпеки виходять на перший план. Вимоги безпеки є ключовим чинником для прийняття рішення про використання інформаційно-технічних послуг і, зокрема, для вирішення про перехід до середовища публічних хмарних обчислень [2].

Виходячи з даних Morgan Stanley Research [3], перше місце серед всього списку проблем хмарних обчислень займає проблема забезпечення безпеки. У рамках даного дослідження, відсутність достатніх гарантій безпеки зберігання даних було названо найбільшою перешкодою при переході в «хмару» (24 % респондентів), це вдвічі більше, ніж наступна проблема - неочевидність економічної вигоди (12 % респондентів).

Основна ідея хмарних обчислень - надання ресурсів високої надійності, масштабованості та доступності в розподіленому середовищі на вимогу. Незважаючи на простоту ідеї, термін Cloud Computing розуміється і подається по-різному [4], загальноприйнятого визначення немає. Компанія Cisco Systems визначає Cloud Computing як IT-ресурси та послуги, які абстраговані від інфраструктури та надаються на вимогу «в необхідному масштабі» в середовищі множинної оренди. У свою чергу Лабораторія інформаційних технологій Національного інституту стандартів і технологій США (NIST) опублікувала наступне визначення хмарних обчислень [5]: «Хмарні обчислення - це модель, що забезпечує зручний мережевий доступ на вимогу до загальних конфігурованих обчислювальних ресурсів (мереж, серверів, сховищ даних, додатків і сервісів), який оперативно надається з мінімальними зусиллями з управління та взаємодії з сервіс-провайдером». Визначення хмарних обчислень описує п'ять основних характеристик (самообслуговування на вимогу, широкий мережевий доступ, оперативна еластичність, пул ресурсів, розрахунок вартості послуги), три сервісні моделі (SaaS, PaaS, IaaS) і чотири моделі розгортання (приватні хмари, публічні хмари, групові хмари, гібридні хмари). Концептуально, хмарні послуги класифікуються як сервіси (XaaS): TaaS (тестування як послуга), SaaS (програмне забезпечення як послуга), PaaS (платформа як послуга), HAAS (апаратне забезпечення як послуга).

На даний момент існує безліч сервіс провайдерів, які надають різні сервіси (Amazon EC2, Google App Engine (GAE), SalesForce.com (SFDC), Microsoft Azure, IBM Blue Cloud, 3Tera). Поточний етап еволюції хмарних обчислень характеризується наявністю різнорідних пропозицій від сервіс-провайдерів. Важливо зауважити, що концепція хмарних обчислень не нова, а являє собою наступний етап еволюції декількох ініціатив останніх років, включаючи розподілені обчислення, грід обчислення, комунальні (utility) обчислення, віртуалізацію, кластерізацію [6].

Хмарні обчислення працюють на основі сервісно-орієнтованої бізнес-моделі. Іншими словами, апаратні ресурси і ресурси платформи надаються як сервіс та на

вимогу. Варіанти хмари систематизуються за моделями служб та залучення ресурсів: пропоновані послуги можуть бути згруповані у три категорії: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) і інфраструктура як послуга (IaaS) [7].

Інфраструктура як послуга (IaaS) абстрагує обладнання (сервер, сховище і мережеву інфраструктуру) і об'єднує його у вигляді можливостей обчислення, зберігання та підключення, які поставляються як послуги з ціною, встановленою за фактичним використанням. Її мета полягає в наданні гнучкого стандартного віртуального операційного середовища, що стає основною для PaaS і SaaS. [8]

IaaS, як правило, забезпечує стандартизований віртуальний сервер. Споживач бере на себе відповідальність за конфігурацію і операції гостьової ОС, ПО і бази даних (БД). Обчислювальні можливості (такі як швидкодія, смуга пропускання та доступ до сховища) також стандартизовані. Рівні обслуговування охоплюють швидкодію і доступність інфраструктури, яка віртуалізується. Споживач бере на себе операційні ризики, які існують крім інфраструктури.

Платформа як послуга (PaaS) надає служби виконання додатків, такі як час виконання, зберігання та інтеграція, для додатків, створених для заздалегідь зазначеної архітектури. Ця модель забезпечує ефективний і гнучкий підхід до передбачуваної економічно ефективної роботи горизонтально масштабованих додатків. PaaS відноситься до надання ресурсів рівня платформи, включаючи операційні системи та підтримку фреймворку розробки програмного забезпечення. Приклади PaaS провайдерів включають Google App Engine, Microsoft Windows Azure і Force.com.

Програмне забезпечення як послуга (SaaS) забезпечує бізнес-процеси і додатки, такі як управління відносинами з клієнтами, спільна робота і електронна пошта, у вигляді стандартизованих можливостей, вартість яких визначається за фактичним використанням відповідно до встановленого рівня обслуговування, відповідного бізнес-потребам. Ця модель відрізняється великою ефективністю витрат та доставки при мінімальних налаштуваннях і знімає операційні ризики зі споживача, покладаючи на постачальника. Вся інфраструктура і функції експлуатації IT абстраговані від споживача.

Література:

3. W. Wang, R. Owens, Z. Li, B. Bhargava. Secure and Efficient Access to Outsourced Data. Proceedings of the 2009 ACM workshop on Cloud computing security. Pages 55-65, 2009.
4. W. Jansen, T.Grance. Guidelines on Security and Privacy in Public Cloud Computing. National Institute of Standards and Technology Draft Special Publication 800-144. 60 pages, Jan. 2011.
5. Adam Holt, Keith Weiss, CFA1, Katy Huberty, CFA1, Ehud Gelblum. Cloud Computing Takes Off. Market Set to Boom as Migration Accelerates. //Morgan Stanley Research. - May 23, 2011.
6. Cloud Computing and Grid Computing 360-Degree Compared / Foster I., Zhao Y., Raicu I., Lu S.: Grid Computing Environments Workshop, 2008. GCE '08.
7. National Institute of Standards and Technology. [Електронний ресурс]. Режим доступу: http://www.nist.gov/index.html.
8. Eric Brewer. Towards Robust Distributed Systems. – Brewer E. : Principles of Distributed Computing, Portland, Oregon, 2000.
9. Tharam Dillon. Cloud Computing: Issues and Challenges. / Dillon T., Wu C., Chang E.: 2010 24th IEEE International Conference on Advanced Information Networking and Applications.
10. Что такое инфраструктура как услуга. [Електронний ресурс]: Documentation – Режим доступу: https://technet.microsoft.com/ru-ru/cloud/hh744751.aspx

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей

XI Міжнародної науково-практичної конференції молодих учених та студентів
7-8 грудня 2022 року

УКРАЇНА
ТЕРНОПІЛЬ – 2022

Матеріали XI Міжнародної науково-практичної конференції молодих учених та студентів «АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль, 7-8 грудня 2022 року

УДК 004.56

Г.В. Шимчук, О.С. Голотенко, к.т.н., доцент, Р.З. Золотий, к.т.н., доцент
Тернопільський державний технічний університет імені Івана Пулюя

ПРОБЛЕМИ БЕЗПЕКИ ХМАРНИХ СЕРЕДОВИЩ

G.V. Shymchuk, O.S. Holotenko. Ph. D., Assoc. Prof., R.Z. Zoloty, Ph. D., Assoc. Prof.

SECURITY PROBLEMS OF CLOUD ENVIRONMENTS

Сучасний бізнес хоче всього: безпечні дані та програми, доступні будь-де з будь-якого пристрою. Це можливо завдяки хмарним середовищам, але є невід'ємні проблеми безпеки хмарних обчислень, щоб втілити це в реальність.

Хмарні середовища дозволяють легко обмінюватися даними, що зберігаються в них. Ці середовища доступні безпосередньо з загальнодоступного Інтернету та включають можливість легко обмінюватися даними з іншими сторонами через прямі запрошення електронною поштою або шляхом спільного використання загальнодоступного посилання на дані.

Простота обміну даними в хмарі – хоча це головний актив і ключ до співпраці в хмарі – викликає серйозні занепокоєння щодо втрати або витоку даних. Насправді 69% організацій вказують на це як на найбільшу проблему безпеки хмарних технологій. Обмін даними за допомогою загальнодоступних посилань або налаштування хмарного сховища на загальнодоступне робить їх доступними для будь-кого, хто знає про посилання, і існують спеціальні інструменти для пошуку в Інтернеті цих незахищених хмарних розгортань.

Конфіденційність і конфіденційність даних є основною проблемою для багатьох організацій. Положення про захист даних, як-от Загальний регламент ЄС щодо захисту даних (GDPR), Закон про мобільність і доступність медичного страхування (HIPAA), Стандарт безпеки даних індустрії платіжних карток (PCI DSS) та багато інших зобов'язують захистити дані клієнтів і накладають суворі штрафи за збої безпеки. Крім того, організації мають велику кількість внутрішніх даних, необхідних для збереження конкурентної переваги.

Розміщення цих даних у хмарі має свої переваги, але також створює серйозні проблеми з безпекою для 66% організацій. Багато організацій запровадили хмарні обчислення, але їм не вистачає знань, щоб переконатися, що вони та їхні співробітники використовують їх безпечно. У результаті конфіденційні дані знаходяться під загрозою розголошення, про що свідчить величезна кількість порушень хмарних даних.

Фішери зазвичай використовують хмарні програми та середовища як привід для своїх фішингових атак. Зі зростанням використання хмарної електронної пошти (G-Suite, Microsoft 365 тощо) і служб обміну документами (Google Drive, Dropbox, OneDrive) співробітники звикли отримувати електронні листи з посиланнями, які можуть попросити їх підтвердити обліковий запис. облікові дані, перш ніж отримати доступ до певного документа або веб-сайту.

Це дозволяє кіберзлочинцям легко дізнатися облікові дані співробітника для хмарних сервісів. У результаті випадкове відкриття хмарних облікових даних викликає серйозне занепокоєння для 44% організацій, оскільки це потенційно ставить під загрозу конфіденційність і безпеку їхніх хмарних даних та інших ресурсів.

Багато організацій мають стратегії реагування на внутрішні інциденти кібербезпеки. Оскільки організація володіє всією внутрішньою мережевою інфраструктурою, а персонал служби безпеки працює на місці, можна заблокувати інцидент. Крім того, це право власності на їх інфраструктуру означає, що компанія, ймовірно, має видимість, необхідну для визначення масштабу інциденту та виконання відповідних дій з усунення.

Завдяки хмарній інфраструктурі компанія має лише часткову видимість і право власності на свою інфраструктуру, що робить традиційні процеси та інструменти безпеки неефективними. У результаті 44% компаній стурбовані своєю здатністю ефективно реагувати на інциденти в хмарі.

Правила захисту даних, такі як PCI DSS і HIPAA, вимагають від організацій продемонструвати, що вони обмежують доступ до захищеної інформації (даних кредитних карток, медичних записів пацієнтів тощо). Це може вимагати створення фізично або логічно ізольованої частини мережі організації, яка буде доступна лише для працівників, які мають законну потребу в доступі до цих даних.

Під час переміщення даних, захищених цими та подібними правилами, у хмару досягти та продемонструвати відповідність нормативним вимогам може бути складніше. Завдяки хмарному розгортанню організації мають можливість переглядати та контролювати лише деякі рівні своєї інфраструктури. Як наслідок, 42% організацій вважають відповідність законодавству та нормативним вимогам основною проблемою безпеки хмари та потребують спеціалізованих рішень відповідності хмарі.

Більшість хмарних провайдерів мають кілька територіально розподілених центрів обробки даних. Це допомагає підвищити доступність і продуктивність хмарних ресурсів і полегшує для постачальників послуг гарантування того, що вони здатні підтримувати угоди про рівень обслуговування в умовах руйнівних подій, таких як стихійні лиха, відключення електроенергії тощо.

Організації, які зберігають свої дані в хмарі, часто не знають, де насправді зберігаються їхні дані в масиві центрів обробки даних CSP. Це викликає серйозні занепокоєння щодо суверенітету даних, місця розміщення та контролю для 37% організацій. З нормативними актами щодо захисту даних, такими як GDPR, які обмежують, куди можна надсилати дані громадян ЄС, використання хмарної платформи з центрами обробки даних за межами затверджених зон може привести організацію до стану невідповідності нормативним вимогам. Крім того, різні юрисдикції мають різні закони щодо доступу до даних для правоохоронних органів і національної безпеки, що може вплинути на конфіденційність даних і безпеку клієнтів організації.

Хмара надає організаціям ряд переваг; однак вона також має свої власні загрози безпеці та проблеми. Хмарна інфраструктура дуже відрізняється від локального центру обробки даних, і традиційні інструменти та стратегії безпеки не завжди здатні ефективно захистити її.

Література

1. A. Alshammari, S. Alhaidari, A. Alharbi and M. Zohdy, "Security Threats and Challenges in Cloud Computing," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 46-51, doi: 10.1109/CSCloud.2017.59.

2. Pavan Muraidhara, "Security issues in cloud computing and its countermeasures", International Journal of Scientific & Engineering Research, vol. 4, no. 10, October 2013.

3. M. Zeller, R. Grossman, C. Lingenfelder, M. Berthold, E. Marcade, R. Pechter, et al., "Open standards and cloud computing: KDD-2009 panel report" in , Paris, France:KDD, pp. 11-18, 2009.

4. Tabrizchi, H., Kuchaki Rafsanjani, M. A survey on security challenges in cloud computing: issues, threats, and solutions. J Supercomput 76, 9493–9532 (2020). https://doi.org/10.1007/s11227-020-03213-1

5. Subramanian N, Jeyaraj A (2018) Recent security challenges in cloud computing. Comput Electr Eng 71:28–42

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

X НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

7–8 грудня 2022 року

ТЕРНОПІЛЬ
2022

УДК 004.56
Г. Шимчук, О. Голотенко, Р. Золотий,
(Тернопільський державний технічний університет імені Івана Пулюя, Україна)

ОСНОВНІ ПРОБЛЕМИ ТА ЗАГРОЗИ ХМАРНОЇ БЕЗПЕКИ

УДК 004.56
G. Shymchuk, O. Holotenko, R. Zoloty

USE THE MAIN PROBLEMS AND THREATS OF CLOUD SECURITY

Майже кожна організація різною мірою використовує хмарні обчислення у своєму бізнесі. Однак із запровадженням хмари виникає необхідність переконатися, що стратегія хмарної безпеки організації здатна захистити від найпоширеніших загроз безпеці хмари.

Неправильна конфігурація параметрів безпеки хмари є основною причиною витоку хмарних даних. Стратегії керування хмарною безпекою багатьох організацій недостатні для захисту їхньої хмарної інфраструктури.

Цьому сприяє кілька факторів. Хмарна інфраструктура розроблена таким чином, щоб її можна було легко використовувати та надавати можливість легкого обміну даними, що ускладнює організаціям забезпечення доступу до даних лише авторизованим сторонам. Крім того, організації, які використовують хмарну інфраструктуру, також не мають повної видимості та контролю над своєю інфраструктурою, а це означає, що вони повинні покладатися на елементи керування безпекою, які надає їхній постачальник хмарних послуг (CSP), щоб налаштувати та захистити свої хмарні розгортання. Оскільки багато організацій не знайомі з захистом хмарної інфраструктури та часто мають багатохмарні розгортання – кожне з різним набором засобів безпеки, наданих постачальником, неправильна конфігурація або недогляд у безпеці можуть легко залишити хмарні ресурси організації відкритими для зловмисників.

На відміну від локальної інфраструктури організації, їх хмарні розгортання знаходяться поза периметром мережі та доступні безпосередньо з загальнодоступного Інтернету. Хоча це є активом для доступності цієї інфраструктури для співробітників і клієнтів, це також полегшує зловмиснику отримання неавторизованого доступу до хмарних ресурсів організації. Неправильно налаштований захист або скомпрометовані облікові дані можуть дозволити зловмиснику отримати прямий доступ, можливо, без відома організації.

CSP часто надають своїм клієнтам низку інтерфейсів прикладного програмування (API) та інтерфейсів. Загалом, ці інтерфейси добре задокументовані, щоб зробити їх зручними для використання клієнтами CSP.

Однак це створює потенційні проблеми, якщо клієнт належним чином не захистив інтерфейси своєї хмарної інфраструктури. Документація, розроблена для замовника, також може бути використана кіберзлочинцем для виявлення та використання потенційних методів доступу та викрадання конфіденційних даних із хмарного середовища організації.

Багато людей мають надзвичайно слабкий захист паролів, включаючи повторне використання паролів і використання слабких паролів. Ця проблема посилює вплив фішингових атак і витоку даних, оскільки дає змогу використовувати один викрадений пароль для кількох різних облікових записів.

Викрадення облікових записів є однією з найсерйозніших проблем безпеки в хмарі, оскільки організації все більше покладаються на хмарну інфраструктуру та програми для основних бізнес-функцій. Зловмисник, маючи облікові дані співробітника, може отримати доступ до конфіденційних даних або функцій, а скомпрометовані облікові дані клієнта дають повний контроль над їхнім обліковим записом в Інтернеті. Крім того, у хмарі організаціям часто не вистачає можливості ідентифікувати ці загрози та реагувати на них так само ефективно, як у локальній інфраструктурі.

Хмарні ресурси організації розташовані за межами корпоративної мережі та працюють на інфраструктурі, якою компанія не володіє. Як наслідок, багато традиційних інструментів для

досягнення видимості мережі неефективні для хмарних середовищ, а деяким організаціям бракує інструментів безпеки, орієнтованих на хмару. Це може обмежити можливості організації контролювати свої хмарні ресурси та захищати їх від атак.

Хмара створена для полегшення обміну даними. Багато хмар надають можливість явно запросити співавтора електронною поштою або надіслати посилання, яке дає змогу будь-кому, хто має URL-адресу, отримати доступ до спільного ресурсу.

Хоча цей простий обмін даними є перевагою, він також може бути серйозною проблемою безпеки хмари. Використання спільного доступу на основі посилань – популярного варіанту, оскільки це простіше, ніж явно запросити кожного співавтора – ускладнює контроль доступу до спільного ресурсу. Спільне посилання може бути перенаправлено комусь іншому, викрадене під час кібератаки або здогадане кіберзлочинцем, забезпечуючи несанкціонований доступ до спільного ресурсу. Крім того, обмін на основі посилань унеможливлює скасування доступу лише до одного одержувача спільного посилання.

Внутрішні загрози є серйозною проблемою безпеки для будь-якої організації. Зловмисник уже має авторизований доступ до мережі організації та деяких конфіденційних ресурсів, які вона містить. Спроби отримати такий рівень доступу – це те, що відкриває більшість зловмисників до їхньої цілі, що ускладнює для непідготовленої організації виявлення зловмисного інсайдера.

У хмарі виявити зловмисника ще складніше. Завдяки хмарному розгортанню компаніям не вистачає контролю над базовою інфраструктурою, що робить багато традиційних рішень безпеки менш ефективними. Це, а також той факт, що хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету та часто страждає від неправильних конфігурацій безпеки, ще більше ускладнює виявлення зловмисників.

Кіберзлочинність – це бізнес, і кіберзлочинці обирають свої цілі на основі очікуваної прибутковості своїх атак. Хмарна інфраструктура доступна безпосередньо з загальнодоступного Інтернету, часто неналежним чином захищена та містить велику кількість конфіденційних і цінних даних. Крім того, хмара використовується багатьма різними компаніями, а це означає, що успішна атака може бути повторена багато разів з високою ймовірністю успіху. Як наслідок, хмарні розгортання організацій є звичайним об'єктом кібератак.

Хмара необхідна для ведення бізнесу багатьма організаціями. Вони використовують хмару для зберігання важливих бізнес-даних і запуску важливих внутрішніх і клієнтських програм.

Це означає, що успішна атака типу «відмова в обслуговуванні» (DoS) проти хмарної інфраструктури, швидше за все, матиме серйозний вплив на низку різних компаній. У результаті DoS-атаки, коли зловмисник вимагає викуп, щоб зупинити атаку, становлять значну загрозу для хмарних ресурсів організації.

Література

1. Khalil I, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
2. Singh S, Jeong Y-S, Park JH (2016) A survey on cloud computing security: issues, threats, and solutions. J Netw Comput Appl 75:200–222
3. Khalil IM, Khreishah A, Azeem M (2014) Cloud computing security: a survey. Computers 3(1):1–35
4. Ahmed M, Litchfield AT (2018) Taxonomy for identification of security issues in cloud computing environments. J Comput Inf Syst 58(1):79–88
6. Sumitra B, Pethuru C, Misbahuddin M (2014) A survey of cloud authentication attacks and solution approaches. Int J Innov Res Comput Commun Eng 2(10):6245–6253
7. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11