ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня магістра

зі спеціальності _____125_____

Кібербезпека_____

(код, найменування спеціальності)

освітньо-професійної програми Інформаційна та кібернетична безпека____

(назва)

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

_____ПРИБЛУДЮК Юрій

Виконав: здобувач вищої освіти групи БСДМ-61

ПРИБЛУДЮК Юрій
(ПРІЗВИЩЕ, ім'я)

Керівник
к.т.н, доцент СОБЧУК Андрій
(ПРІЗВИЩЕ, ім'я)

Рецензент
к.т.н, доцент _____
(ПРІЗВИЩЕ, ім'я)

КИЇВ – 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____Гайдур Г.І
«___»_____2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Приблудюку Юрію Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: «Технологія забезпечення кібербезпеки в хмарних сервісах організації»

керівник кваліфікаційної роботи Собчук А.В., к.т.н, доцент кафедри
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи

1) Моделі хмарних сервісів;
2) Рішення Barracuda CloudGen Firewall;
3) Наукова та технічна література.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1) Аналіз особливостей розгортання хмарних сервісів;
2) Дослідження методів та засобів протидії мережевим атакам при використанні хмарних сервісів;
3) Дослідження інтеграції рішень для забезпечення безпеки хмарних сервісів.

5. Перелік ілюстративного матеріалу:

1) Мета, об'єкт та предмет дослідження;

2) Моделі доставки хмарних сервісів;

3) Проблеми безпеки хмарних сервісів;

4) Система керування веб-доступом (WebAM)/система єдиного входу в Інтернет (WebSSO);

5) Варіанти інтеграції рішень Barracuda CloudGen Firewall;

6) Рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall;

7) Висновки.

6. Дата видачі завдання 19.10.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Аналіз науково-технічної літератури	28.10.2023 р.	виконано
2.	Аналіз особливостей розгортання хмарних сервісів	04.11.2023 р.	виконано
3.	Дослідження проблем забезпечення безпеки в хмарних сервісах	11.11.2023 р.	виконано
4.	Дослідження методів та засобів протидії мережевим атакам при використанні хмарних сервісів	21.11.2023 р.	виконано
5.	Інтеграція рішень для забезпечення безпеки хмарних сервісів	02.12.2023 р.	виконано
6.	Рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall	08.12.2023 р.	виконано
7.	Реферат, вступ, висновки	10.12.2023 р.	виконано
8.	Підготовка презентації	14.12.2023 р.	виконано

Здобувач вищої освіти _____ Юрій ПРИБЛУДЮК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 76 сторінок, 51 рисунок, 6 таблиць, 28 джерел.

Об'єкт дослідження – процес безпечного функціонування хмарних сервісів організації.

Предмет дослідження – механізми та засоби забезпечення безпеки даних в хмарних сервісах організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню інтегрованих рішень для забезпечення безпеки хмарних сервісів.

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

В роботі проаналізовано хмарні сервіси та основні моделі організації, що включають архітектури IaaS, PaaS, SaaS. Виокремлено проблеми безпеки в хмарних сервісах, зокрема ризики, пов'язані з незахищеними API, інсайдерськими загрозами, SQL-ін'єкціями, та загрозами автентифікації

Досліджено можливості файрволу Barracuda CloudGen для безшовної інтеграції з хмарною платформою AWS та оцінено різні моделі розгортання. Описано детальний алгоритм налаштування Barracuda CloudGen Firewall, включаючи створення файлів конфігурації, вибір обладнання та операційної системи, налаштування мережевих інтерфейсів та безпеки.

Розроблено рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall для захисту корпоративних віртуальних робочих столів, включаючи забезпечення безпеки в індустріях з високими вимогами до безпеки, еластичних робочих ресурсів для віддаленої роботи та тимчасових проектів.

Галузь використання – кібербезпека.

ХМАРНІ СЕРВІСИ, ХМАРА, ЗАХИСТ, ТРОЯНСЬКИЙ КІН, ВРАЗЛИВІСТЬ, ЗАГРОЗА, ФАЄРВОЛ, SQL, BARRACUDA CLOUDGEN FIREWALL, VPN, БЕЗПЕКА, ОРГАНІЗАЦІЯ, АУТЕНТИФІКАЦІЯ.

ABSTRACT

Qualification’s thesis: 76 pages, 51 figures, 6 tables, 28 sources.

The object of research – the process of secure operation of an organization's cloud services.

The subject of research – is the study is mechanisms and means of ensuring data security in an organization's cloud services

The aim of research is to increase the level of information security in the organization by implementing integrated solutions to ensure the security of cloud services.

Research methods – information theory, international and domestic standards in the field of cybersecurity, security policies.

The work analyzed cloud services and the main models of organization, including IaaS, PaaS, SaaS architectures. Identified security problems in cloud services, in particular risks associated with unprotected APIs, insider threats, SQL injections, and authentication threats.

Explored the capabilities of the Barracuda CloudGen firewall for seamless integration with the AWS cloud platform and assessed various deployment models. Described a detailed algorithm for configuring the Barracuda CloudGen Firewall, including creating configuration files, selecting hardware and operating system, configuring network interfaces and security.

Developed recommendations for scenarios of using Barracuda CloudGen Firewall to protect corporate virtual desktops, including ensuring security in industries with high security requirements, flexible working resources for remote work and temporary projects.

Field of use – cybersecurity.

CLOUD SERVICES, CLOUD, PROTECTION, TROJAN HORSE, VULNERABILITY, THREAT, FIREWALL, SQL, BARRACUDA CLOUDGEN FIREWALL, VPN, SECURITY, ORGANIZATION, AUTHENTICATION.

ЗМІСТ

ВСТУП

Актуальність дослідження. Дані становлять цінний ресурс для організацій і окремих людей, а управління ними є важливим завданням, що включає забезпечення їх цілісності та конфіденційності. Традиційно організації та особи використовували локальне комп'ютерне обладнання для зберігання даних. Однак, з розвитком технологій та мережевих систем, в тому числі мережі Інтернет, стали доступні нові моделі обчислень, включаючи грід-обчислення та комунальні обчислення.

Останні десятиліття зробили обробку інформації реальністю, коли дані можуть оброблятися ефективно на великих обчислювальних платформах і платформах зберігання, доступних через Інтернет.

Хмарні сервіси можна визначити як обчислювальні моделі, що забезпечують зручний мережевий доступ до спільного пулу конфігурованих ресурсів. Хмарні сервіси надають IT-інфраструктуру, платформи та програмні додатки у формі послуг через глобальну мережу. Кілька прикладів хмарних сервісів включають: онлайн-сховища файлів, соціальні мережі, веб-пошту, онлайн/бізнес-додатки тощо.

Оскільки організації прагнуть знайти нові методи для просування свого бізнесу (продукції), зростаючий попит перемістився на мережеву складові, які пропонують дешевші рішення для використання обчислювальних систем (як з точки зору доступу до обчислювальної інфраструктури, так і операційних витрат). Це призвело до експоненціального зростання популярності хмарних сервісів, які виявилися більш ефективними, ніж попередні реалізації. Тому питання забезпечення цілісності, безпеки та конфіденційності даних в хмарних сервісах стає ключовим пріоритетом для організацій.

Вищенаведені аргументи актуалізують тему даної кваліфікаційної роботи, зміст якої становлять дослідження щодо технології забезпечення кібербезпеки в хмарних сервісах організації.

Об'єкт дослідження – процес безпечного функціонування хмарних сервісів організації.

Предмет дослідження – механізми та засоби забезпечення безпеки даних в хмарних сервісах організації.

Мета роботи – підвищення рівня інформаційної безпеки в організації шляхом впровадженню інтегрованих рішень для забезпечення безпеки хмарних сервісів.

Наукові завдання:

- проаналізувати особливості розгортання хмарних сервісів;
- дослідити проблеми забезпечення безпеки в хмарних сервісах;
- дослідити методи та засоби протидії мережевим атакам при використанні хмарних сервісів;
- дослідити інтеграцію рішень для забезпечення безпеки хмарних сервісів;
- розробити рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall

Методи дослідження – теорія інформації, міжнародні та вітчизняні стандарти у сфері кібербезпеки, політики безпеки.

Практичне значення одержаних результатів полягає в підвищені рівня інформаційної безпеки в організації шляхом впровадженню інтегрованих рішень для забезпечення безпеки хмарних сервісів.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ОСОБЛИВОСТЕЙ РОЗГОРТАННЯ ХМАРНИХ СЕРВІСІВ

1.1. Еволюція хмарних сервісів та обчислень

Замість впровадження складних обчислювальних систем, сучасні компанії та організації все частіше користуються хмарними сервісами, звертаючись до віддалених обчислювальних потужностей. Більшість науковців наголошують на економічній вигоді такого підходу, однак часто пропускається важлива тема безпеки і конфіденційності, пов'язана зі стрімким переходом на хмарні сервіси. Саме ця проблематика стає все частіше предметом обговорення.

У контексті інформаційної безпеки, хмарні сервіси виявляються в двох основних аспектах:

- проблеми безпеки роблять хмарні сервіси дуже ризикованими;
- питання безпеки є більш сприйнятливими, але не надмірно ризикованими.

Обидві ці позиції мають свої переваги. Розвиток хмарних сервісів як нової моделі доставки обчислювальних ресурсів ставить перед федеральними IT-лідерами та архітекторами безпеки нові виклики та ризики, які потрібно розуміти та управляти. Краще розуміння цих ризиків може сприяти визначенню ефективних способів використання хмарних сервісів [1].

Розглядаючи хмарні сервіси з іншої точки зору, можна вбачати їх як логічну еволюцію у сфері обчислень. На рис.1.1 представлено хмарні сервіси та постачальників хмарних послуг (CSP) як розвиток моделі Інтернет-провайдера (ISP).

Розглядаючи постачальників послуг додатків і їх схожість з моделлю хмарних обчислень, зокрема програмним забезпеченням як послуги (SaaS), важливо відрізняти методи надання послуг та бізнес-моделі цих двох систем.

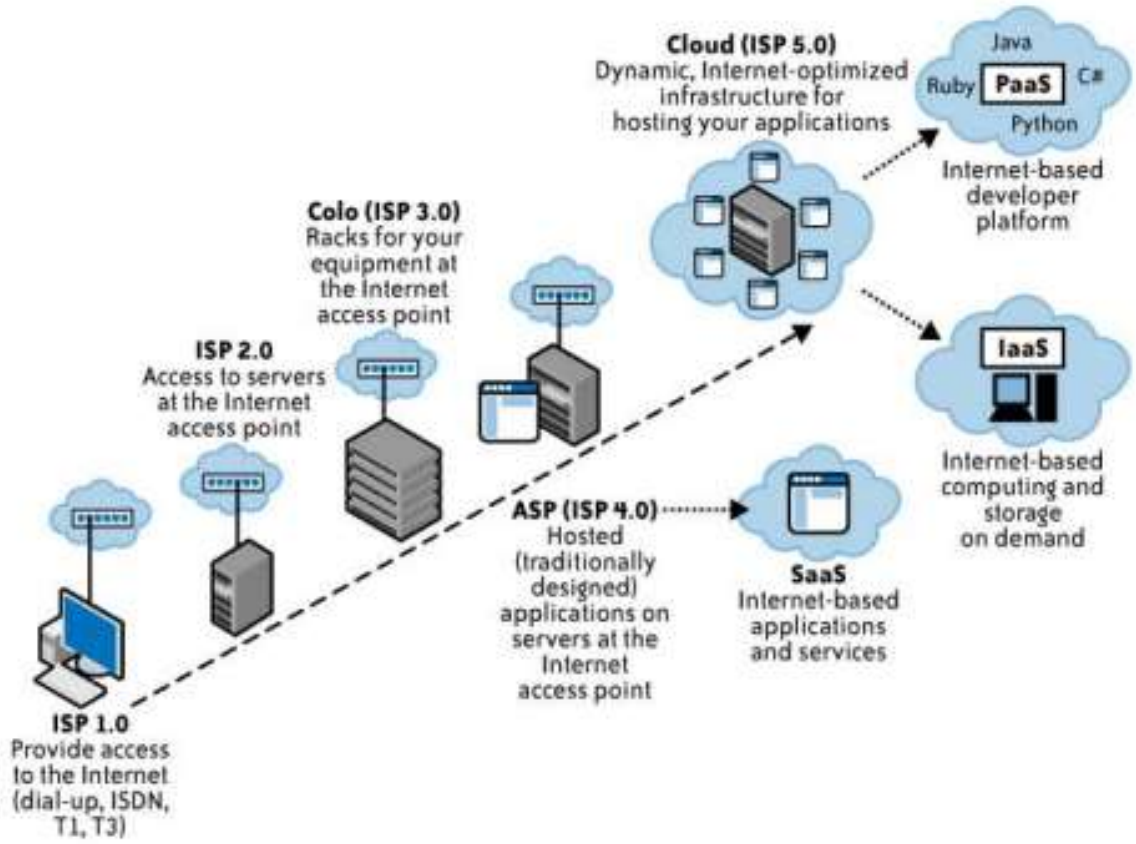


Рис.1.1. Еволюція хмарних сервісів та обчислень

Постачальники послуг традиційно надавали послуги різним клієнтам через виділені інфраструктури, де кожен клієнт мав власний екземпляр програми, запущений на окремому хості або сервері. Натомість, постачальники SaaS пропонують доступ до програм на спільній, не виділеній інфраструктурі, що становить ключову відмінність від постачальників послуг.

У контексті хмарних обчислень (ISP 5.0), виникає модель SPI, яка включає SaaS, «платформу як послуга» (PaaS) та «інфраструктуру як послуга» (IaaS). Ця модель описує комплексний підхід до надання обчислювальних ресурсів і послуг через хмару[2].

Сучасний етап розвитку хмарних сервісів та обчислень відзначається значною увагою та, як деякі стверджують, навіть ажіотажем. Численні компанії стверджують, що вони працюють «в хмарі», викликаючи розмивання чітких визначень хмарних послуг.

Разом з тим, багато організацій та груп оголосили про свої ініціативи щодо розвитку різних аспектів хмарних сервісів та обчислень. Наприклад, Національний інститут стандартів і технологій займається стандартизацією у сфері хмарних обчислень, а Cloud Security Alliance та Open Cloud Manifesto працюють над питаннями безпеки та сумісності в хмарних обчисленнях. Інші організації, такі як Distributed Management Task Force (DMTF), Американська асоціація інформаційних технологій, та Єрихонський форум, також активно займаються питаннями розвитку хмарних сервісів та обчислень. Аналіз даних і висновки були зібрані в результаті відкрито доступної дослідницької роботи, проведеної Cybersecurity Insiders у звіті Cloud Security Report, який публікує точну статистичну інформацію щодо безпеки хмар (рис.1.2).

Рис.1.2. Відсоток організацій, які стурбовані безпекою хмари

Хмарні сервіси та обчислення становлять собою швидкозростаючу та еволюційну модель, що постійно розширюється новими аспектами та можливостями.

Віртуалізація є однією з ключових технологій хмарних сервісів, включаючи засоби об’єднання кількох автономних систем в єдину апаратну платформу. Це досягається шляхом віртуалізації ресурсів, таких як мережі, процесори, пам'ять, та сховища даних. Віртуалізація, забезпечена апаратною абстракцією, приховує складність керування фізичною інфраструктурою, спрощуючи масштабування та управління ресурсами[3].

Гіпервізори грають ключову роль у цьому процесі, відповідаючи за ізоляцію віртуальних машин, щоб забезпечити безпеку та незалежність різних сервісів на одному фізичному хості. Віртуалізація сприяє масштабованості та мультитенантності, що є основними характеристиками хмарних сервісів, дозволяючи ефективно ділитися та об'єднувати ресурси, підвищуючи гнучкість та вартісну ефективність для бізнесу.

У практичному застосуванні хмарних сервісів, віртуалізація має свої особливості, пов'язані з конфігурацією, мережевими налаштуваннями та масштабуванням систем. Ініціалізація в хмарній віртуалізації є ключовим механізмом для розподілу ресурсів між клієнтами. Коли клієнт звертається до постачальника хмарних сервісів, останній ініціює створення відповідної кількості віртуальних машин та виділяє необхідні ресурси. Процеси такого виділення можуть бути попередньо заданими, динамічними або здійснюватися на основі самообслуговування користувачів. Постачальники хмарних сервісів стикаються з викликами, такими як оптимальне розподілення ресурсів, та працюють над забезпеченням безпеки віртуалізаційних механізмів для мінімізації потенційних загроз і вразливостей.

1.2. Основні характеристики, переваги та відмінності хмарних сервісів

Хмарні сервіси відрізняються від інших обчислювальних парадигм своїми унікальними характеристиками. Ось п'ять ключових характеристик хмарних сервісів:

- **Самообслуговування на вимогу.** Користувачі мають можливість

самостійно налаштовувати та керувати своїми хмарними ресурсами, такими як обчислювальні потужності та сховище даних, без необхідності взаємодії з постачальником послуг. Це забезпечує швидке та гнучке використання ресурсів відповідно до потреб користувачів.

- **Широкий доступ до мережі.** Хмарні сервіси доступні через мережу з будь-якого місця та на різноманітних пристроях, що забезпечує легкий доступ до ресурсів для користувачів, незалежно від їхнього місцезнаходження.
- **Об’єднання ресурсів.** Постачальники хмарних сервісів пулізують різні фізичні та віртуальні ресурси, щоб задовольнити потреби численних користувачів. Це сприяє оптимізації використання ресурсів та зменшенню витрат.
- **Швидка еластичність.** Хмарні сервіси можуть швидко масштабуватися вгору чи вниз в залежності від поточних потреб користувачів. Ця гнучкість дозволяє користувачам ефективно реагувати на зміни в навантаженні, оптимізуючи витрати та ресурси.
- **Вимірювана послуга.** Хмарні сервіси надають можливості для моніторингу, контролю та звітності використання ресурсів, що допомагає користувачам оптимізувати витрати та забезпечує прозорість використання послуг.

Хмарні сервіси проти комунальних послуг. У комунальних послугах ресурси програмного та апаратного забезпечення зосереджені в великих центрах обробки даних, і користувачі платять за використання послуг зберігання та зв'язку. Ці послуги часто залежать від хмарної інфраструктури, але їхня бізнес-модель базується на прямій оренді засобів для користувачів, які повністю контролюють ці ресурси.

Натомість, хмарні сервіси пропонують модель, де користувачі платять за використані ресурси та послуги, але не мають прямого контролю над фізичною інфраструктурою. Це означає, що хмарні сервіси надають більш гнучку та масштабовану модель використання, де інфраструктура та програмне забезпечення є повністю керованими власниками та операторами хмари.

Вони дозволяють користувачам легко масштабувати ресурси залежно від потреби, забезпечуючи більш ефективне та економічно вигідне використання обчислювальних ресурсів.

Хмарні сервіси проти мережевих (Ґрід) обчислень. Ґрід-обчислення — це мережа з розподіленими ресурсами, яка дозволяє спільно використовувати частини обладнання та програмного забезпечення між багатьма користувачами, які можуть належати різним організаціям. У цій моделі користувачі зобов'язані надавати свої ресурси іншим користувачам мережі відповідно до угоди, керованої менеджерами мережі.

На відміну від цього, хмарні сервіси надають більш гнучку та централізовану модель використання ресурсів. У хмарних сервісах ресурси, як правило, централізовано керуються однією організацією та розподіляються між користувачами згідно з їхніми потребами.

Хмарні сервіси комерційно пропонуються провайдерами, і користувачі платять за використання ресурсів за прозорою ціновою моделлю. Це дає організаціям можливість використовувати обчислювальні ресурси без необхідності вкладати значні кошти в розвиток та управління власними обчислювальними системами.

У хмарних сервісах використовується хмарне програмне забезпечення, яке забезпечує різноманітні послуги, такі як створення та управління віртуальними машинами, розгортання та налаштування програм, а також управління користувачами та облік. Це відрізняється від мережевих обчислень, де використовується спеціалізоване проміжне програмне забезпечення для координації ресурсів між різними організаціями.

Таким чином, хмарні сервіси та мережеві обчислення мають різні підходи до управління ресурсами, їхньої доступності та використання, з хмарними сервісами, що забезпечують більш централізований та комерційно орієнтований підхід.

Хмарні сервіси проти традиційних центрів обробки даних. Хмарні сервіси та традиційні центри обробки даних відрізняються за своїми підходами до обробки та зберігання даних. У традиційних центрах обробки даних кожне робоче

навантаження має власний рівень безпеки для своєї інфраструктури, з чітко визначеним фізичним розділенням компонентів, що запобігає взаємодії між різними мережевими, обчислювальними та компонентами зберігання даних різних користувачів.

Навпаки, хмарні сервіси використовують спільну інфраструктуру для обробки різних робочих навантажень. Вони не мають фізично ізольованих інфраструктур для кожного користувача, але використовують програмні методи для створення логічної ізоляції. Це означає, що всі користувачі використовують однакову серверну інфраструктуру, однакову інфраструктуру зберігання та мережеву інфраструктуру, але забезпечуються програмні механізми для ізоляції та безпеки їх даних.

Хмарні сервіси вважаються більш гнучким та економічно вигідним варіантом порівняно з традиційними центрами обробки даних. Вони надають всі необхідні функції та послуги за менші витрати, завдяки економії на масштабі.

Хмарні сервіси також забезпечують кращу гнучкість, оскільки не вимагають створення власної інфраструктури з нуля та забезпечення власного обслуговування та адміністрування. Вони легко масштабуються та адаптуються до змінних потреб користувачів, що робить їх ідеальним вибором для бізнесів, які потребують швидкої адаптації до змін на ринку або зростання обсягів даних [4].

1.3. Моделі доставки хмарних сервісів

У сфері хмарних сервісів існують три основні моделі доставки, кожна з яких пропонує різні рівні управління, гнучкості та контролю над технологічними ресурсами(рис.1.3).

Ці моделі включають:

- **Інфраструктура як послуга (IaaS).** Ця модель надає користувачам доступ до віртуальної інфраструктури, такої як віртуальні машини, мережі та сховища даних. IaaS дозволяє користувачам уникнути витрат та складнощів, пов'язаних з купівлею та управлінням власною фізичною інфраструктурою,

надаючи гнучкість у використанні обчислювальних ресурсів за потребою.

- **Платформа як послуга (PaaS).** PaaS забезпечує набір інструментів і сервісів, які дозволяють розробникам швидко створювати, тестувати та розгортати додатки у хмарному середовищі. Ця модель включає обчислювальні ресурси, бази даних, проміжне програмне забезпечення та інші інструменти для розробки, звільняючи розробників від необхідності управління підлеглою інфраструктурою.
- **Програмне забезпечення як послуга (SaaS).** У цій моделі користувачам надаються додатки, які працюють у хмарному середовищі та доступні через Інтернет, часто через веб-браузер. Користувачі не мають контролю над інфраструктурою або платформою, на якій функціонує програмне забезпечення, але можуть використовувати додатки для різних бізнес-потреб.

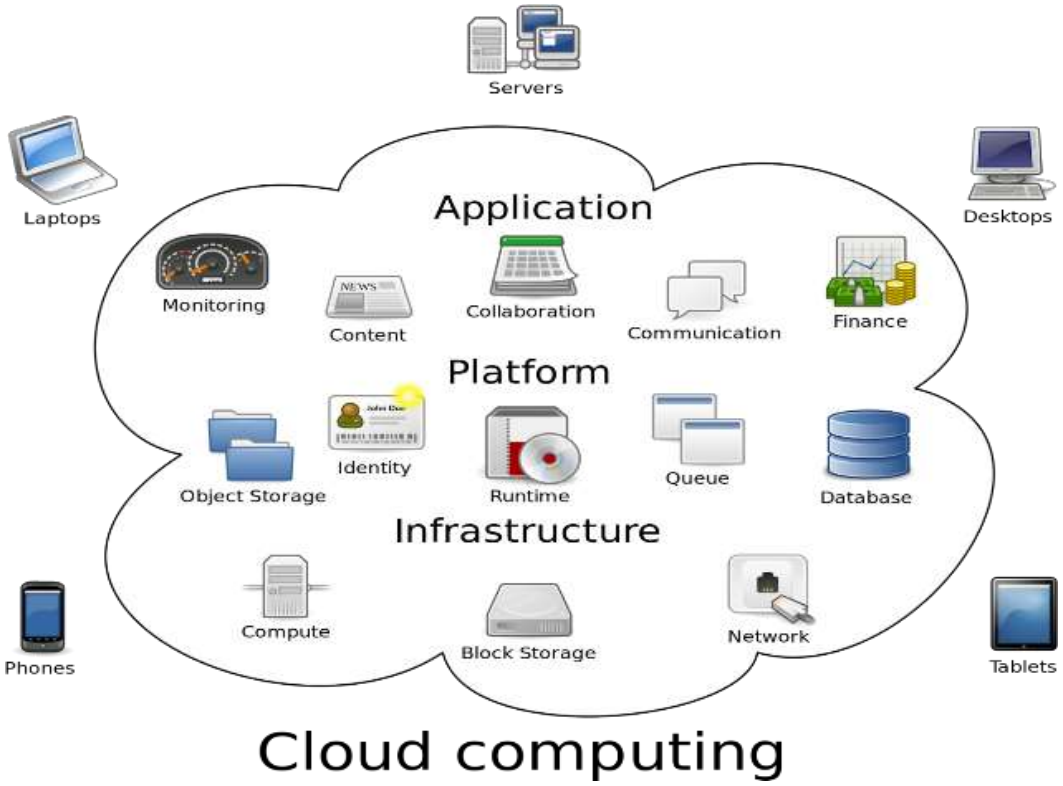


Рис.1.3. Моделі доставки хмарних сервісів

Кожна з цих моделей пропонує різні рівні гнучкості та контролю, дозволяючи організаціям вибирати найбільш підходящий варіант для своїх потреб у хмарних сервісах.

1.3.1. Інфраструктура як послуга (IaaS) у хмарних сервісах

Інфраструктура як послуга (IaaS) у контексті хмарних сервісів передбачає надання користувачам віртуальних обчислювальних ресурсів, таких як процесори, пам'ять, зберігання даних, мережі та ресурси доставки контенту (рис.1.4).

Ці послуги дозволяють користувачам розгортати та запускати власне програмне забезпечення, включаючи операційні системи та застосунки, при цьому користувачі не мають контролю над базовою фізичною інфраструктурою, але мають повний контроль над вищими рівнями програмного забезпечення, ОС та мережевими компонентами, такими як брандмауери.

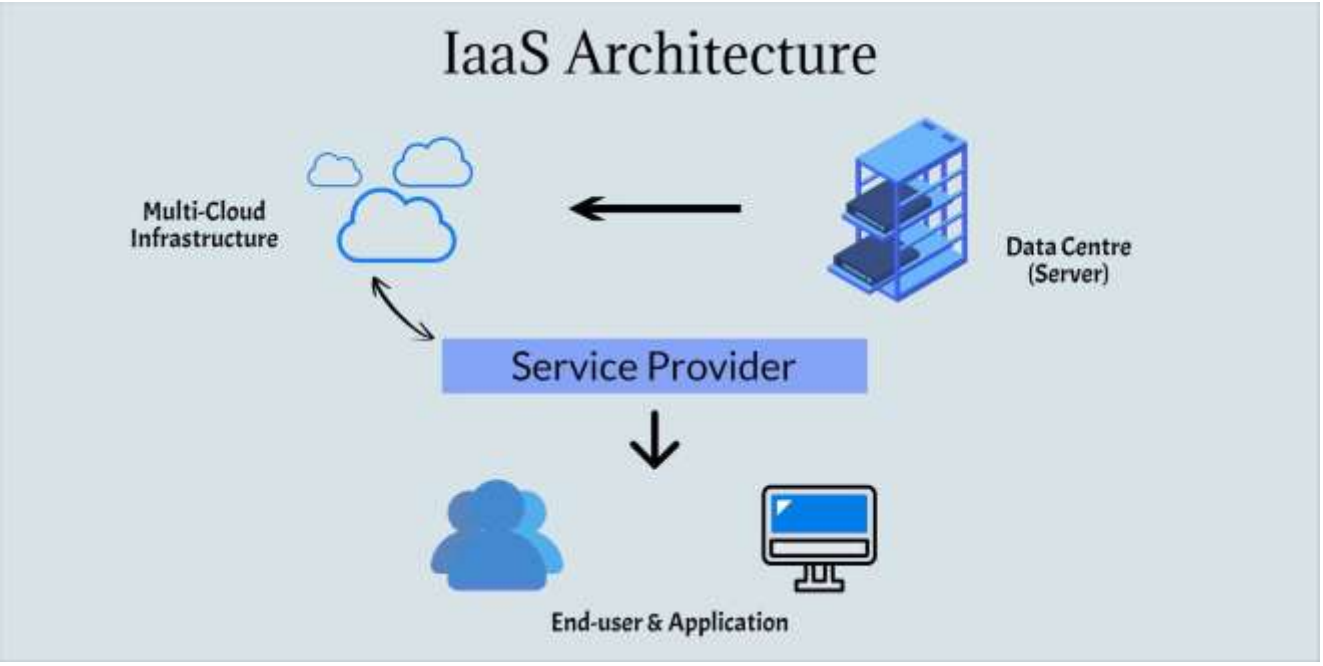


Рис.1.4. Платформа IaaS

Характеристики IaaS у хмарних сервісах включають:

- Можливість багатокористувацького доступу до спільного апаратного забезпечення.
- Доступ до ресурсів як послуги з можливістю оплати за використання.
- Динамічне масштабування ресурсів відповідно до потреб користувачів, з вартістю, заснованою на обраній інфраструктурі.
- Придатність IaaS для різних сценаріїв:

- Організації, що потребують повного контролю над своїм програмним забезпеченням, особливо для вимогливих застосунків.
- Стартапи та малі компанії, які шукають економію на придбанні та обслуговуванні апаратного забезпечення.
- Організації що розвиваються, які потребують гнучкості у виборі програмного забезпечення та інфраструктури.
- Сервіси з нестабільним попитом, де потрібна швидка адаптація до змін у трафіку.

Приклади провайдерів IaaS у хмарних сервісах включають Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE) та інші[5].

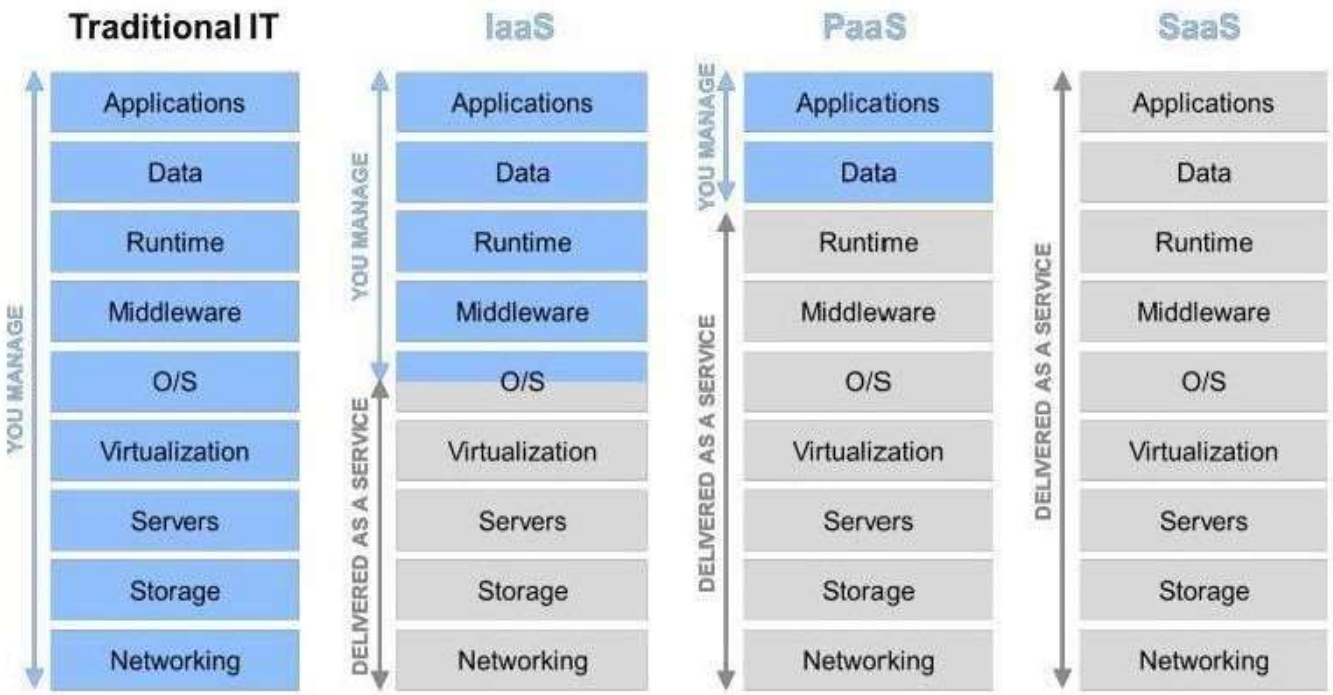


Рис.1.5. Розділена відповідальність моделей хмарних сервісів

1.3.2. Платформа як послуга (PaaS) у хмарних сервісах

PaaS у контексті хмарних сервісів дозволяє користувачам розгортати та управляти додатками, створеними з використанням мов програмування та інструментів, підтримуваних провайдером хмарних сервісів (рис.1.6).

Користувачам не надається контроль над базовою хмарною інфраструктурою, але вони мають повний контроль над розгорнутими програмами та середовищем їх розміщення, що сприяє швидкому запуску та ефективному управлінню програмами.

Характеристики PaaS у хмарних сервісах включають:

- Використання технології віртуалізації, що дозволяє легко отримувати ресурси за вимогою та масштабувати їх залежно від потреби.
- Набір послуг для розробки, тестування, розгортання та розміщення додатків у інтегрованому середовищі, що сприяє ефективності процесу розробки.
- Можливість спільного використання середовища розробки між різними користувачами.
- Інтеграція з веб-сервісами та базами даних.
- Система виставлення рахунків і підписки, що забезпечує гнучкість у використанні та оплаті ресурсів.

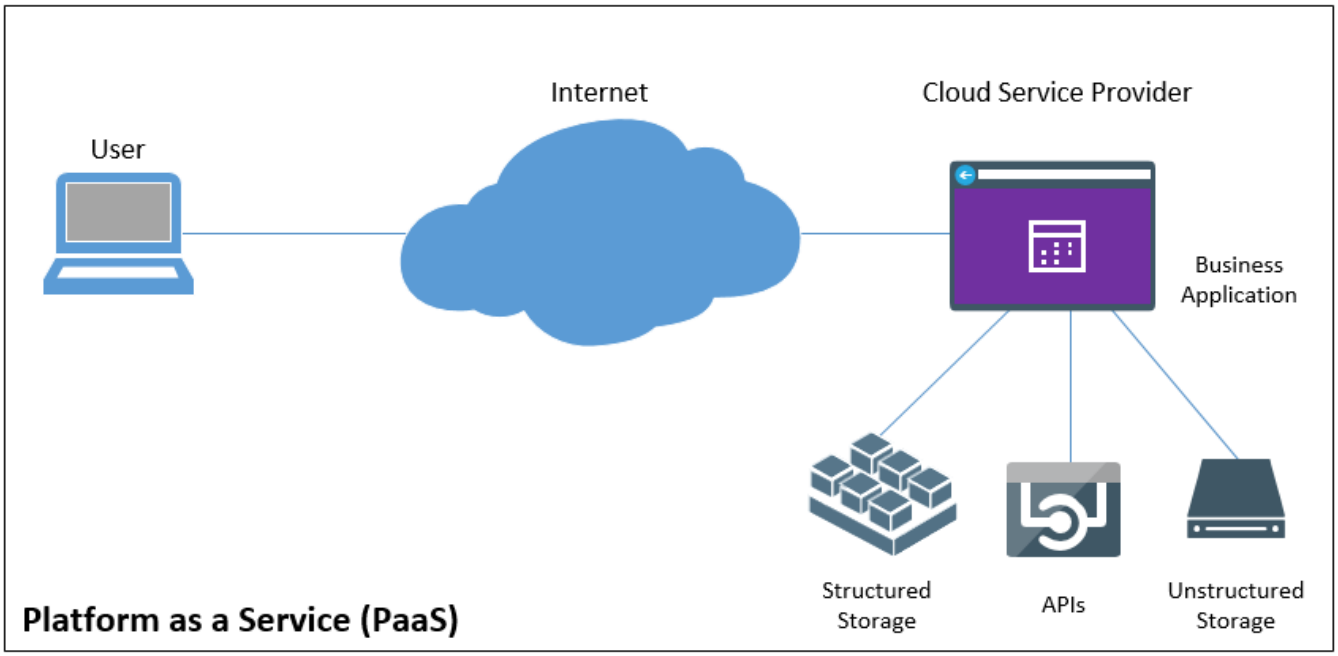


Рис.1.6. Платформа PaaS

Придатність PaaS:

- Розробники, які працюють над спільними проектами, отримують вигоду від швидкості та гнучкості, яку пропонує PaaS.

- Організації, які використовують гнучкі методології розробки, можуть скористатися PaaS для швидкої ітерації та розробки додатків.
- Організації, що прагнуть оптимізувати свої капіталовкладення, можуть скористатися PaaS для зменшення витрат на інфраструктуру та розробку додатків.

Приклади провайдерів PaaS для підприємств включають Apprenda та інші популярні платформи, які надають необхідні інструменти та сервіси для розробки та управління додатками в хмарному середовищі[6].

1.3.3. Програмне забезпечення як послуга (SaaS) у хмарних сервісах

У моделі SaaS, що є частиною хмарних сервісів, споживачам надається доступ до додатків, які працюють на хмарній інфраструктурі провайдера. На відміну від PaaS, користувачі не розгортають свої власні програми, а використовують готові рішення від провайдера (рис.1.7).

У моделі SaaS користувачі не мають контролю над хмарною інфраструктурою або деталями реалізації програм, але мають доступ до налаштувань програмних додатків, що може бути обмеженим.

Характеристики SaaS у хмарних сервісах включають:

- Програмне забезпечення, доступне через Інтернет, зазвичай через веб-браузер.
- Централізоване керування програмним забезпеченням, що забезпечує постійні оновлення та технічну підтримку.
- Звільнення користувачів від необхідності турбуватися про апаратне забезпечення, оновлення програмного забезпечення тощо.
- Інтеграція з іншими додатками за допомогою API.

Рис.1.7. Платформа SaaS

Придатність SaaS:

- Для програм, які відчувають сезонні сплески попиту.
- Для програм, що потребують як Інтернет, так і мобільного доступу.
- Для короткострокових проектів, які вимагають співпраці.
- Для стартапів, які шукають швидкі та ефективні рішення для запуску онлайн-бізнесу.

Приклади SaaS включають Google Apps, Salesforce, Workday, Concur, Citrix GoToMeeting, Cisco WebEx, які надають широкий спектр послуг від електронної пошти та офісних додатків до управління відносинами з клієнтами та інструментів для проведення онлайн-зустрічей[7].

1.4. Огляд перешкод, що заважають впровадженю хмарних сервісів

При впровадженні хмарних сервісів організаціями існують деякі загальні перешкоди:

Внутрішній опір. Інтеграція хмарних сервісів може зменшити потребу в деяких внутрішніх IT-завданнях, що може викликати опір серед IT-персоналу через страх втрати контролю над ключовими системами або навіть робочих місць.

Проблеми безпеки та конфіденційності. Безпека та конфіденційність даних є ключовими занепокоєннями для багатьох організацій, які розглядають перехід до хмарних сервісів. Деякі організації можуть вважати, що не існує ефективних рішень для повністю вирішення цих проблем.

Надійність і довіра. Публічні випадки збоїв у хмарних сервісах відомих постачальників можуть викликати занепокоєння щодо надійності та довіри до цих технологій серед потенційних користувачів.

Інтеграція та сумісність. Відсутність узгоджених стандартів для API та хмарних інтерфейсів створює труднощі для інтеграції з існуючими приватними та громадськими хмарними системами.

Управління, угоди про рівень обслуговування (SLA) і якість обслуговування (QoS): Управління IT-ресурсами та послугами в хмарі може бути складним, особливо коли мова йде про забезпечення високої якості обслуговування та дотримання угод SLA.

При впровадженні хмарних сервісів існують певні фактори, які можуть впливати на їхню продуктивність та вартість:

- Угода про рівень обслуговування (SLA). Важливим фактором є чітко визначені SLA, які описують обсяг послуг, якість обслуговування, штрафи та збори, що допомагає управляти очікуваннями та відповідальністю.
- Пропускна здатність мережі. Висока пропускна здатність мережі критично важлива для забезпечення високої продуктивності хмарних сервісів, особливо при великих обсягах даних.
- Кількість користувачів. Збільшення числа користувачів може впливати на продуктивність, особливо якщо інфраструктура сервісу не масштабована відповідно.
- Відмовостійкість. Здатність хмарних сервісів продовжувати функціонувати навіть у разі технічних проблем є важливою для забезпечення

стабільності та продуктивності.

- Безпека. Наявність надійних заходів безпеки збільшує ефективність хмарних сервісів та забезпечує кращу продуктивність, водночас захищаючи дані користувачів.
- Відновлення даних. Можливість швидкого відновлення даних після збоїв або втрат є критично важливою для підтримки продуктивності хмарних сервісів.
- Інші фактори: До інших важливих факторів належать масштабованість, затримки, резервування, робоче навантаження та потужність процесора.

Загальна вартість володіння (TCO) для хмарних сервісів включає всі витрати, пов'язані з їх використанням протягом усього терміну експлуатації. Прямі витрати включають плату за ліцензування, витрати на ресурси та управління послугами. Непрямі витрати охоплюють витрати на персонал, координацію між хмарними та локальними додатками та управління хмарними контрактами.

1.5. Інформаційна безпека та конфіденційність у хмарах

Безпека в контексті хмарних сервісів — це забезпечення захисту діяльності користувачів в хмарному середовищі від небажаного втручання чи доступу. Конфіденційність у цьому аспекті можна визначити як право користувачів хмарних сервісів мати свою інформацію в безпеці та недоступну для сторонніх. Це включає вибірковий контроль доступу до своїх даних та інформації. Користувачі хмарних сервісів можуть контролювати, як і з ким вони діляться своєю інформацією, вибираючи ступінь своєї відкритості.

Класична тріада безпеки у хмарних сервісах, також відома як модель «CIA», включає:

- *Конфіденційність* – означає захист від несанкціонованого доступу до даних, які зберігаються чи обробляються в хмарі (тобто дані в хмарі є недоступними для невповноважених осіб);
- *Цілісність* – гарантія, що дані в хмарі залишаються незмінними та

надійними, відображаючи їхню вихідну форму без несанкціонованих модифікацій;

- *Доступність* – забезпечення, що користувачі мають надійний доступ до своїх ресурсів у хмарі, коли це потрібно, без непередбачуваних затримок чи перебоїв.

Протягом багатьох років дослідження безпеки та конфіденційності у сфері хмарних сервісів займали центральне місце в наукових роботах. Для кращого розуміння цих питань, дослідники та експерти з технологій використовували різноманітні критерії, щоб створити комплексне розуміння цих проблем. Вони рекомендують розглядати екосистему безпеки хмарних сервісів через призму трьох ключових учасників:

- сервісу;
- користувача сервісу;
- провайдера хмарних послуг.

Також вони визначають різні категорії потенційних атак, які можуть бути здійснені користувачем проти сервісу, сервісу проти користувача, користувачем проти хмарного провайдера, провайдером проти користувача, сервісом проти провайдера, а також провайдером проти сервісу. Незважаючи на численні виклики в області безпеки та конфіденційності, хмарні сервіси можуть бути ефективно захищені шляхом впровадження відповідних заходів безпеки.

Хмарні сервіси стали популярними завдяки зростаючій потребі в гнучкій IT-інфраструктурі, поширенню аналітики великих даних та збільшенню використання мобільних пристроїв. Ця технологія відіграє ключову роль у сучасному цифровому світі, надаючи користувачам можливість доступу до ресурсів та обробки даних через Інтернет без необхідності володіння фізичною інфраструктурою[8].

Висновки до першого розділу

Досліджено хмарні сервіси та основні моделі організації, що включають архітектури IaaS, PaaS, SaaS. Зазначено особливості та переваги розгортання кожної.

Підкреслено важливість гнучкості та масштабованості у хмарних сервісах, особливо в контексті швидкої адаптації до змінних потреб бізнесу та різних обсягів даних.

Виокремлено питання безпеки та конфіденційності в хмарних сервісах, та підкреслено необхідність захисту не лише кінцевого користувача, але і даних, що ним передаються.

Зазначено роль та значення управління відмовостійкістю та надійності хмарних сервісів, що включає забезпечення стабільного доступу до сервісів навіть у разі технічних збоїв чи інших непередбачуваних обставин.

2 ДОСЛІДЖЕННЯ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ

2.1. Категорії безпеки в хмарних сервісах

Хмарні сервіси вирізняються своєю гнучкістю та економічною ефективністю. Конфіденційна інформація клієнтів зберігається на розподілених хмарних платформах, що знаходяться під контролем провайдера хмарних сервісів, а не клієнтів.

Захист даних у хмарі є одним із ключових завдань, оскільки хмарні сервіси, включаючи програмне забезпечення, платформи та інфраструктуру, вразливі до різних загроз, таких як незаконне розповсюдження, шкода або компрометація.

Таблиця 2.1.

Вимоги до безпеки в хмарних сервісах порівняно з механізмами та функціями, що їх забезпечують

Характеристика / Вимога	**Аутентифікація**	**Авторизація**	**Шифрування даних**	**Конфіденційність даних**	**Багатокористувацьке середовище**
API	Ні	Ні	Ні	Так	Так
Хмарне ПЗ	Так	Ні	Так	Ні	Так
Захист даних	Так	Ні	Так	Ні	Ні
Апаратна віртуалізація	Ні	Ні	Ні	Так	Так
Програмна віртуалізація	Ні	Так	Ні	Ні	Так
Комунальні обчислення	Ні	Так	Ні	Ні	Так
Віртуалізація	Ні	Так	Ні	Ні	Так
Веб-портали	Ні	Ні	Ні	Так	Так

Безпека в хмарних сервісах є вирішальною, оскільки вона становить помітну перешкоду для їх впровадження та ефективного використання. Постачальник хмарних сервісів несе основну відповідальність за управління та захист даних. Ефективне забезпечення безпеки передбачає створення безпечного обчислювального середовища, що включає контроль за зберіганням та використанням даних, та знижує ризики від фізичного або програмного пошкодження.

Використання хмарних сервісів стає більш економічно ефективним у безпечному середовищі. Високий рівень безпеки сприяє збільшенню продуктивності, зменшуючи ймовірність пошкодження даних, програмного та апаратного забезпечення.

Модель безпеки в хмарних сервісах - це гарантія довіри та масштабованості. Ефективна модель безпеки є критичною для хмарних сервісів, щоб забезпечити довіру користувачів та управління ризиками у масштабованих та багатокористувацьких середовищах. Через об’єднання ресурсів у хмарних сервісах, де численні користувачі мають доступ до спільних даних та інфраструктури, виникає необхідність у суворих заходах безпеки.

Організації, які мігрують до хмарних сервісів, часто повинні відмовитися від певного рівня контролю над своєю інфраструктурою та даними. Важливо встановити довіру до систем та провайдерів хмарних сервісів, забезпечуючи при цьому можливість моніторингу та перевірки хмарних процесів та подій. Ключові аспекти такої довіри та перевірки включають контроль доступу, безпеку даних, відповідність нормативним вимогам і управління подіями.

Хмарні сервіси включають різні механізми безпеки, такі як автентифікація, авторизація, шифрування даних, забезпечення конфіденційності даних та багатокористувацькість. Такі механізми гарантують цілісність і узгодженість хмарних систем, як показано в таблиці 1, що демонструє зв'язок між вимогами безпеки хмарних сервісів і відповідними механізмами та функціями, які їх забезпечують[9].

Категорії безпеки хмарних сервісів, показані на рис.2.1, включають: ідентифікаційну, інформаційну, інфраструктурну, мережеву та програмну безпеку.

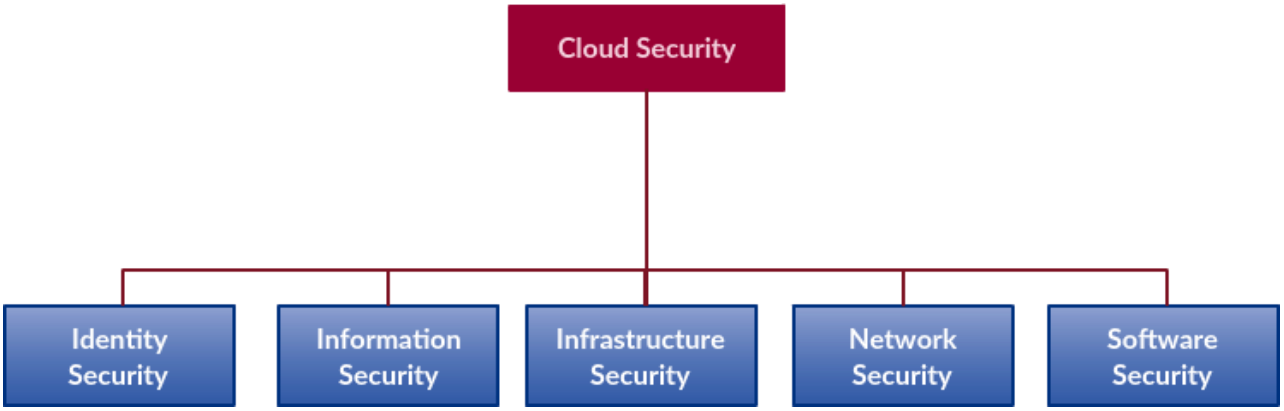


Рис.2.1. Категорії безпеки хмарних сервісів

Безпека ідентифікації у хмарних сервісах. Безпека ідентифікації є важливою частиною хмарних сервісів, що дозволяє користувачам безпечно отримувати доступ до необхідних ресурсів. Це сприяє забезпеченню цілісності та конфіденційності даних і програм, а також підвищує їх доступність для уповноважених користувачів. Наскрізне керування ідентифікацією, сторонні служби автентифікації та сильна ідентифікація є ключовими для забезпечення безпеки ідентифікації у хмарних сервісах.

Безпека ідентифікації вимагає надійної автентифікації та авторизації, що перевищує традиційне використання імен користувачів та паролів. Це може включати більш складні механізми, як-от двофакторна автентифікація, автентифікація на основі ризиків, моніторинг поведінки та інші стратегії, які допомагають оцінити рівень ризику запиту користувача. Надійні можливості авторизації особливо важливі для обробки конфіденційних даних та дотримання вимог у хмарному середовищі.

Інформаційна безпека у хмарних сервісах. Інформаційна безпека у хмарних сервісах охоплює стратегії управління процесами, інструментами та політиками для запобігання, виявлення, документування та протидії загрозам цифрової та нецифрової інформації. Вона включає встановлення бізнес-процесів для захисту інформаційних активів.

Контроль фізичного доступу, доступу до апаратного та програмного забезпечення, а також ідентифікація та автентифікація користувачів, є ключовими для захисту даних у хмарі. Ізоляція даних, включаючи шифрування та контроль доступу, є важливою для забезпечення безпеки даних у загальнодоступних хмарних середовищах. Це особливо важливо в мультитенантних хмарних середовищах, де різні користувачі та організації можуть використовувати спільні ресурси без обміну даними між собою.

Технології Trusted Computing у хмарних сервісах. Технології Trusted Computing використовуються в хмарних сервісах для забезпечення довіри в середовищі з кількома клієнтами. Вони дозволяють створити безпечне середовище, в якому можна впевнено обробляти конфіденційну інформацію та виконувати критичні для бізнесу операції. Ключовими елементами безпеки в таких системах є зменшення довіреної обчислювальної бази, окремі компоненти управління, відокремлення політик від застосування та застосування політики від простору додатків.

Безпека інфраструктури хмарних сервісів. Безпека інфраструктури хмарних сервісів вимагає демонстрації того, що як віртуальна, так і фізична інфраструктура надійні та безпечні. Критично важливо, щоб організації могли перевіряти безпеку базової інфраструктури, щоб відповідати бізнес-вимогам. Сервіси та механізми безпеки повинні включати відокремлення критичних системних компонентів та політик, забезпечення мінімального необхідного набору сервісів для управління віртуальними машинами та видалення надлишкових стеків керування.

Безпека мережі у хмарних сервісах. Безпека мережі є ключовою вимогою для хмарних сервісів. Це включає застосування фізичних та програмних заходів для захисту основної мережевої інфраструктури від несанкціонованого доступу та інших загроз. Задача полягає в створенні безпечної платформи для комп’ютерів, користувачів та програм (табл.2.2).

Таблиця 2.2.

Короткий перелік проблем безпеки мережі та їх вирішення

Тема	**Проблеми**	**Рішення**
Периметральна безпека	Нерухома мережева інфраструктура	Мережева безпека для віртуальної машини
	Обмеження брандмауерів, обмежений мобільний зв'язок	Мережева безпека за допомогою брандмауера на основі дерева-правила
	Прослуховування мережі та спуфінг в vmm	Аутентифікація на основі обміну ключами в мережі
Мобільні платформи	Генерація мобільного шкідливого ПЗ	Не визначено рішень
	Розширення вразливостей мобільних платформ	Система виявлення вторгнень для захисту мобільних платформ
	Вразливості мобільних додатків з синхронізацією в хмарі	Не визначено рішень

Проблеми безпеки мережі можуть безпосередньо впливати на хмарну систему, збільшуючи перевантаження та впливаючи на пропускну здатність. У контексті мобільного доступу до хмарних сервісів, безпека мережі також повинна враховувати вразливості, пов'язані з мобільними пристроями та програмами.

Розробка ефективних рішень для мережевої безпеки включає в себе ряд викликів, включаючи управління мережевими з'єднаннями, захист від зловмисного програмного забезпечення та забезпечення безпеки при міграції віртуальних машин у межах хмари.

Безпека програмного забезпечення у хмарних сервісах. Безпека програмного забезпечення є ключовою для хмарних сервісів, де широкий спектр програмного забезпечення має бути розроблений з врахуванням безпеки як основного принципу,

а не як додаткової функції, що враховується пізніше. Це дозволяє створювати програми з високим рівнем захисту від потенційних атак.

Таблиця 2.3.

Короткий перелік проблем безпеки програмного забезпечення та їх вирішення

Теми	**Проблеми безпеки**	**Рішення безпеки**
Платформи та фреймворки	Ізоляція між платформами, безпечне завершення потоків, моніторинг ресурсів	Безпека багатокористувацької програмної платформи
	Невизначені системні виклики та недосконала ізоляція пам'яті	Не визначено рішень
	Недосконалий механізм SDLC	Не визначено рішень
Користувацький інтерфейс	Витік інтерфейсів користувача	Не визначено рішень
	Недосконалі конфігурації, несанкціонований доступ, недоліки програмного застосунку, масковане впровадження коду	Легка система виявлення вторгнень
	Витік консолі управління vmm	Не визначено рішень
	Довіра до програмістів, відкрите програмне забезпечення, процедура зворотного інженірингу	Впровадження рішень проти шкідливого пз

Розробка безпечного програмного забезпечення для хмарних сервісів має включати процес безпеки від самого початку ідеї і протягом усіх етапів проектування та реалізації, формуючи цикл аналізу безпеки. Кожен етап процесу повинен сприяти забезпеченню найвищого рівня безпеки програмного забезпечення(табл.2.3).

Розробники хмарних сервісів повинні слідувати процедурам безпечної розробки, які охоплюють створення захищеної архітектури, належний моніторинг, ізоляцію, а також аналіз дизайну та реалізації з точки зору безпеки. Важливо, щоб команди розробників впроваджували ефективні системи журналювання, які можуть виявляти та фіксувати події безпеки, забезпечуючи при цьому більш

детальний запис важливих подій, що впливають на безпеку. Таке журналювання може бути інтегроване з зовнішніми системами моніторингу для комплексного аналізу безпеки в хмарних сервісах[10].

2.2. Проблеми безпеки хмарних сервісів

Хмарні сервіси вносять різні ризики для організацій, які їх використовують. Безпека хмарних сервісів визначається їх моделлю надання та розгортання. Наприклад, приватні хмари можуть надати вищий рівень безпеки порівняно з публічними хмарними сервісами(рис.2.2).

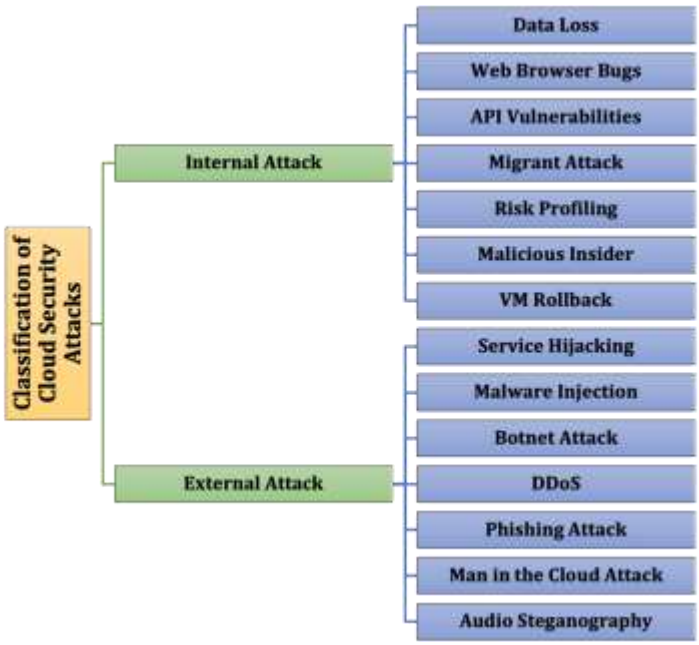


Рис.2.2. Класифікація проблем безпеки в хмарі

Проблеми безпеки можуть включати незахищені інтерфейси та API, загрозу від внутрішніх співробітників, викрадення облікових записів або служб, а також проблеми з спільним використанням технологій.

Переповнення буфера у хмарних сервісах. Переповнення буфера - це вразливість, що виникає, коли програма дозволяє введенню даних перевищити ємність відведеної пам'яті, що може призвести до зміни даних у пам'яті або виконання шкідливого коду.

У хмарних сервісах це може бути особливо критично, оскільки успішна атака може призвести до повного контролю над хостом або сервісом. Тому важливо виявляти та запобігати таким вразливостям на ранніх етапах розробки та впровадження хмарних сервісів.

Атаки на хмарну автентифікацію. Автентифікація в хмарних сервісах важлива для забезпечення того, що тільки уповноважені користувачі мають доступ до ресурсів та даних. Проблеми з автентифікацією, такі як використання слабких або викрадених облікових даних, можуть призвести до несанкціонованого доступу до хмарних сервісів.

Важливо використовувати сильні механізми автентифікації, такі як багатофакторна автентифікація, для підвищення безпеки хмарних сервісів та запобігання несанкціонованому доступу(рис.2.3).

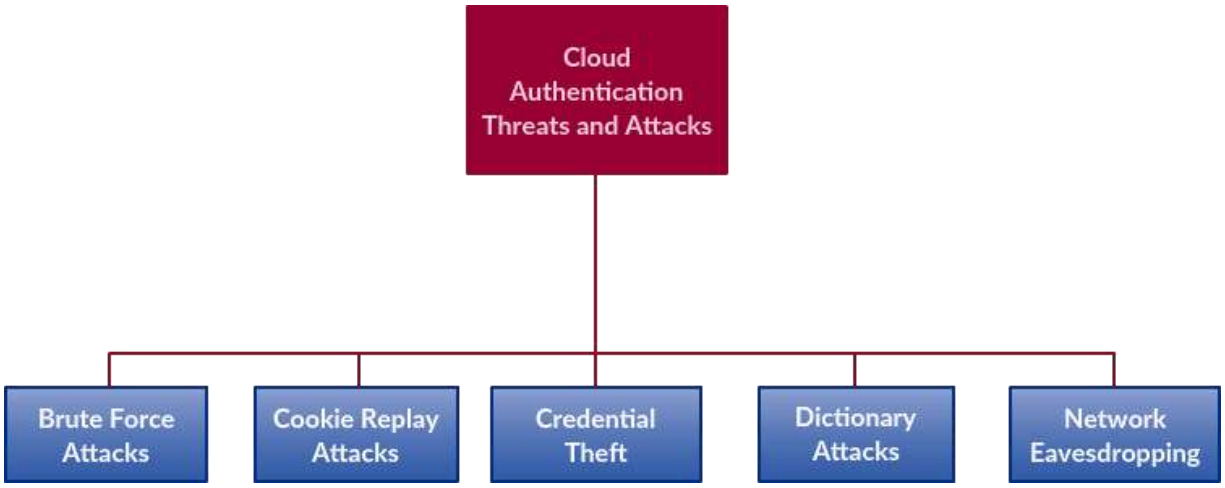


Рис.2.3. Загрози та атаки хмарної автентифікації

Загрози та атаки на автентифікацію в хмарних сервісах. Хмарні сервіси можуть бути вразливими до різних типів атак на автентифікацію, що ставлять під загрозу безпеку даних і доступу до системи.

Найпоширеніші типи атак включають:

- Атаки грубою силою - зловмисники намагаються вгадати облікові дані користувача шляхом випробувань численних комбінацій.
- Атаки на повторне відтворення файлів cookie - зловмисники отримують доступ до системи користувача, повторно використовуючи викрадені файли cookie.

- Крадіжка облікових даних - зловмисники отримують доступ до системи та крадуть облікові дані користувачів, наприклад, через фішинг.
- Атаки на словник - зловмисники вгадують облікові дані, використовуючи спроби зі списку загальновживаних паролів.
- Прослуховування мережі - зловмисники викрадають облікові дані, зчитуючи мережевий трафік.

Існували підходи до захисту від таких атак, такі як Microsoft Passport і MS Cardspace, які були призначені для поліпшення безпеки автентифікації у хмарних сервісах. Microsoft Passport був прикладом протоколу з довіреною третьою стороною, який дозволяв користувачам вводити свої облікові дані для доступу до хмарних сервісів, тоді як MS Cardspace був ініціативою для заміни ідентифікаторів користувачів і паролів на цифрову або віртуальну ідентифікацію[11].

Атаки впровадження зловмисного ПЗ у хмарні сервіси. Атаки впровадження зловмисного програмного забезпечення у хмарні сервіси можуть мати різні форми, включаючи створення та впровадження шкідливих віртуальних машин або сервісів у хмарну інфраструктуру. Такі атаки можуть завдати шкоди, змінюючи дані або блокуючи послуги. Щоб запобігти цьому, хмарні сервіси повинні включати розширені механізми безпеки та моніторингу для виявлення та блокування спроб впровадження зловмисного програмного забезпечення[12].

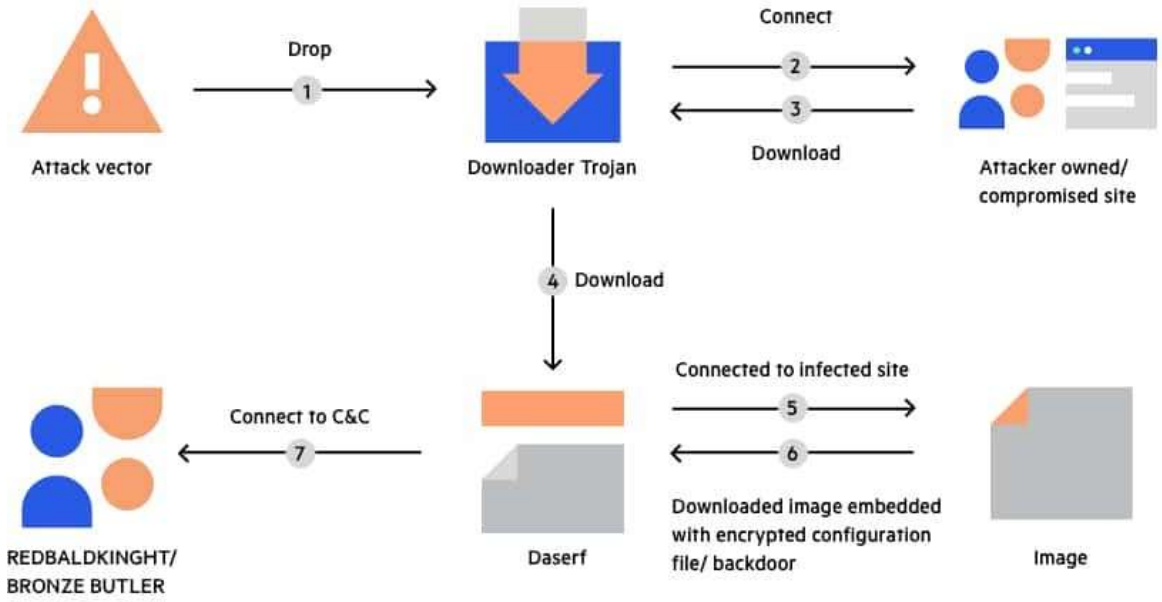


Рис.2.4. Зловмисне програмне забезпечення Trojan Horse

DOS-атаки та безпека мобільних хмарних сервісів. В хмарних сервісах DOS-атаки (Відмова в обслуговуванні) та DDOS-атаки (Розподілена відмова в обслуговуванні) є важливими загрозами безпеки. DOS-атаки відбуваються, коли зловмисник намагається перешкодити доступу авторизованих користувачів до хмарних сервісів. DDOS-атаки включають використання кількох компрометованих систем для атакування певної хмарної системи. Особливо небезпечні DDOS-атаки на прикладному рівні, які можуть використовувати неефективності веб-додатків і бути важко виявленими на мережевому рівні. Операторам веб-сайтів слід вдаватися до комбінації хмарних та проксі-рішень, а також до кращих практик розробки програм та управління їх підтримуючою архітектурою для захисту від таких атак.

Безпека мобільних терміналів в хмарних сервісах також є важливою проблемою. Користувачі мобільних телефонів часто не інформовані про питання безпеки та конфіденційності, що робить їх вразливими до атак. Зловмисники можуть використовувати слабкий захист для монтування DOS-атак, заважаючи користувачам отримувати доступ до хмарних сервісів.

Незахищені API в хмарних сервісах. Незахищені інтерфейси прикладного програмування (API) є критичною проблемою безпеки в хмарних сервісах. API є основними каналами для взаємодії з хмарними сервісами та використовуються як для збору журналів, так і для інтеграції з базами даних та компонентами зберігання. Вони також важливі для автентифікації користувачів у мобільних додатках. Недостатня автентифікація, авторизація та шифрування в API можуть створити вразливості, які зловмисники можуть використовувати для атак на хмарні сервіси.

Зловмисні інсайдери у хмарних сервісах. Зловмисним інсайдером у контексті хмарних сервісів може бути нинішній або колишній співробітник, підрядник або діловий партнер, який має авторизований доступ до мережі, систем або даних і використовує свої привілеї в зловмисних цілях. Інсайдери можуть завдати значної шкоди хмарним сервісам, особливо в масштабах, коли вони впливають на багатьох клієнтів хмарних послуг, а не лише на одну організацію. Вони можуть отримати доступ до конфіденційних даних або навіть контролювати хмарні сервіси.

Для зменшення загрози від зловмисних інсайдерів, існують контрзаходи, які можуть включати обмеження доступу до хмарних сервісів і даних, підвищення прозорості в процесах безпеки та управління, а також застосування систем виявлення вторгнень та багатофакторної автентифікації.

Дві основні категорії внутрішніх загроз у хмарних сервісах:

- Інсайдерські загрози в хмарному постачальнику: Інсайдер, який працює на хмарного провайдера, може завдати шкоди як провайдеру, так і його клієнтам. Контрзаходи включають моделі виявлення шкідливих інсайдерів, журналювання та встановлення юридичних обов'язків.
- Внутрішні загрози в хмарі. Аутсорсер: Інсайдер, який є співробітником організації, що використовує хмарні сервіси. Такі інсайдери можуть використовувати свій доступ для викрадення інформації або інших зловмисних дій. Засоби контролю включають застосування систем виявлення вторгнень та багатофакторної автентифікації для забезпечення захисту даних та систем.

Атаки SQL-ін'єкцій у хмарних сервісах. Атака SQL-ін'єкції у хмарних сервісах відбувається, коли зловмисник вводить шкідливий код у запити до баз даних, які використовуються хмарними сервісами, з метою отримання несанкціонованого доступу до даних або їх фальсифікації. Це може статися, наприклад, на веб-сайті, який використовує хмарну базу даних для зберігання інформації.

Для захисту від атак SQL-ін'єкцій важливо використовувати належні практики безпечного програмування, включаючи перевірку та очищення вхідних даних, використання параметризованих запитів та розробку з дотриманням принципів захисту від відомих уразливостей.

Крім того, ефективним заходом захисту є використання систем виявлення веб-вторгнень (IDS), які можуть виявляти спроби SQL-ін'єкцій та інші шкідливі дії у хмарних сервісах. Ці системи допомагають розрізняти легітимні запити від шкідливих, знижуючи ризик пошкодження даних або компрометації систем.

Загрози конфіденційності в хмарних сервісах. Конфіденційність є важливим аспектом використання хмарних сервісів, оскільки клієнтська

інформація та бізнес-логіка зберігаються на серверах, керованих хмарними провайдерами, а не клієнтами. Забезпечення конфіденційності даних користувачів є ключовим фактором, що підвищує довіру клієнтів до хмарних сервісів і сприяє їх ширшому використанню.

Конфіденційність та приватність часто плутають, хоча це різні поняття. Конфіденційність стосується захисту інформації від доступу неавторизованих осіб, тоді як приватність включає контроль над розкриттям особистої інформації.

Для забезпечення конфіденційності в хмарних сервісах необхідно впровадити заходи, які захищають дані від несанкціонованого доступу або викрадення. Це може включати шифрування даних, використання надійних систем автентифікації та контроль доступу. Крім того, провайдери хмарних послуг повинні впровадити політики та процедури, які забезпечують захист конфіденційності інформації користувача.

Забезпечення конфіденційності не тільки захищає користувачів, але й збільшує довіру до хмарних провайдерів, сприяючи зростанню їхнього бізнесу. Важливо, щоб користувачі розуміли, які заходи безпеки вживаються провайдерами для захисту їхніх даних.

Конфіденційність і приватність в хмарах вимагають від користувачів та постачальників послуг встановлення чітких правил і політик щодо доступу та обробки даних. Особливу увагу слід приділити захисту персональних даних, що обмінюються або зберігаються у хмарі.

Конфіденційність може бути порушена, якщо хмарний провайдер не забезпечує належних заходів безпеки або ділиться інформацією без дозволу користувача. Також існує ризик, що уряди або інші структури можуть вимагати від провайдера доступу до даних користувачів.

Для мінімізації ризиків порушення конфіденційності, постачальники хмарних сервісів повинні впровадити ефективні стратегії та технології для захисту даних. Користувачі також повинні бути усвідомлені щодо потенційних ризиків та вжити заходів для захисту своєї конфіденційності, контролюючи свою поведінку та дії у хмарі.

Загрози автентифікації в хмарних сервісах. Однією з ключових проблем у сфері хмарних сервісів є порушена автентифікація та скомпрометовані облікові дані. Це включає в себе ситуації, де механізми перевірки легітимності користувачів є неадекватними або ненадійними. Наприклад, коли сертифікати користувачів не можуть гарантувати їхню особу або коли системи автентифікації не здатні ефективно перевіряти облікові дані користувачів.

Такі випадки можуть призвести до несанкціонованого доступу до даних, збережених в хмарі, що становить серйозний ризик для конфіденційності користувачів хмарних сервісів. Ефективність автентифікації та контролю доступу є критичною для забезпечення безпеки в хмарних середовищах.

Недостатність або відсутність засобів контролю безпеки може призвести до скомпрометованих облікових даних. Такі прогалини в безпеці створюють вразливі місця, які можуть бути використані зловмисниками. Тому, роль провайдерів хмарних сервісів полягає в тому, щоб забезпечити наявність надійних і ефективних систем автентифікації. Це допоможе забезпечити, що доступ до даних у хмарі здійснюється лише авторизованими користувачами, мінімізуючи ризики порушення конфіденційності.

Загрози цілісності даних в хмарних сервісах Цілісність даних у хмарних сервісах передбачає надійне зберігання інформації користувача. Всі порушення даних, такі як втрата, зміна або несанкціонований доступ, повинні бути негайно виявлені. Однак, дані залишаються вразливими до зовнішніх загроз, таких як зловмисне програмне забезпечення або недбалість з боку провайдера послуг.

Сервери, які надають хмарні послуги, зазвичай зберігають значні обсяги даних, що вимагає високого рівня безпеки та надійності для запобігання втраті або компрометації даних. Наявність помилок у резервному копіюванні, відновленні та міграції даних може призвести до втрати даних.

Наслідки порушення даних для організацій можуть включати втрату доходу, додаткові витрати на реагування на інциденти, втрату репутації та довіри клієнтів. Особливо небезпечні випадки, коли порушення даних є наслідком умисного зловживання, недбалості або технічних проблем.

Для запобігання порушенню даних важливо забезпечити належні заходи безпеки та конфіденційності на рівні хмарної інфраструктури. Це включає в себе ефективні механізми контролю, які дозволяють швидко виявляти та блокувати можливі порушення, а також обмежують доступ до даних тільки для авторизованих осіб[13].

Проблеми з розташуванням даних у хмарних сервісах. Проблема розташування даних є значною для організацій, які використовують хмарні сервіси. У випадку хмарних сервісів, дані організації можуть зберігатися у різних фізичних локаціях, і часто організації не мають детальної інформації про місцезнаходження своїх даних. Це ускладнює визначення, чи вжито адекватних заходів для захисту даних.

Підприємства, що використовують хмарні сервіси, повинні знати, де зберігаються та обробляються їхні дані, а також забезпечити, щоб постачальники хмарних сервісів дотримувалися відповідних законодавчих та нормативних вимог. Зберігання даних за кордоном може створити додаткові юридичні та технічні виклики, оскільки законодавство з конфіденційності може істотно відрізнятися між країнами.

Транскордонний транзит конфіденційних даних та заходи їх захисту є важливою проблемою національної та регіональної безпеки та конфіденційності. Різні юрисдикції мають різні закони, що стосуються транскордонного потоку даних, і це може породити правові проблеми та ризики для безпеки даних.

З огляду на ці виклики, організації повинні ретельно обирати провайдерів хмарних сервісів, враховуючи їх політику та практики щодо розташування даних, а також розуміючи правові наслідки розміщення даних у певних юрисдикціях. Організації повинні також розробляти стратегії та механізми для управління та захисту своїх даних у хмарному середовищі.

Проблеми, пов'язані з правом власності на дані та розкриттям вмісту в хмарних сервісах. Право власності на дані та розкриття інформації є ключовими питаннями у контексті хмарних сервісів. Коли користувачі передають свої дані в хмарні сервіси, виникає ризик втрати контролю над конфіденційністю цих даних.

Це може призвести до невизначеності щодо права власності на дані, а також права на їх розкриття.

У хмарних сервісах постачальники послуг часто стають власниками та зберігачами даних, що може порушувати традиційну парадигму розділення обов'язків, де різні організації володіють та зберігають дані. Така практика може порушувати принципи найкращих практик безпеки даних, що передбачають розподіл обов'язків та ротацію посад.

Проблеми віртуалізації в хмарних сервісах. Віртуалізація, яка використовується для ефективного спільного використання ресурсів у хмарних сервісах, створює додаткові виклики для конфіденційності. Гіпервізори в хмарних системах дозволяють розподіляти ресурси між віртуальними машинами, але це також відкриває можливості для порушень конфіденційності.

Дані, які передаються в хмару, можуть бути зашифровані, але вони повинні бути розшифровані для обробки, створюючи потенційні вразливості. Це особливо стосується ситуацій, коли віртуалізація дозволяє несанкціонований доступ до даних з боку хмарного провайдера або інших користувачів хмари. Тому важливо, щоб постачальники хмарних сервісів впроваджували ефективні механізми безпеки та конфіденційності, щоб захистити дані користувачів від несанкціонованого доступу або витоку[14].

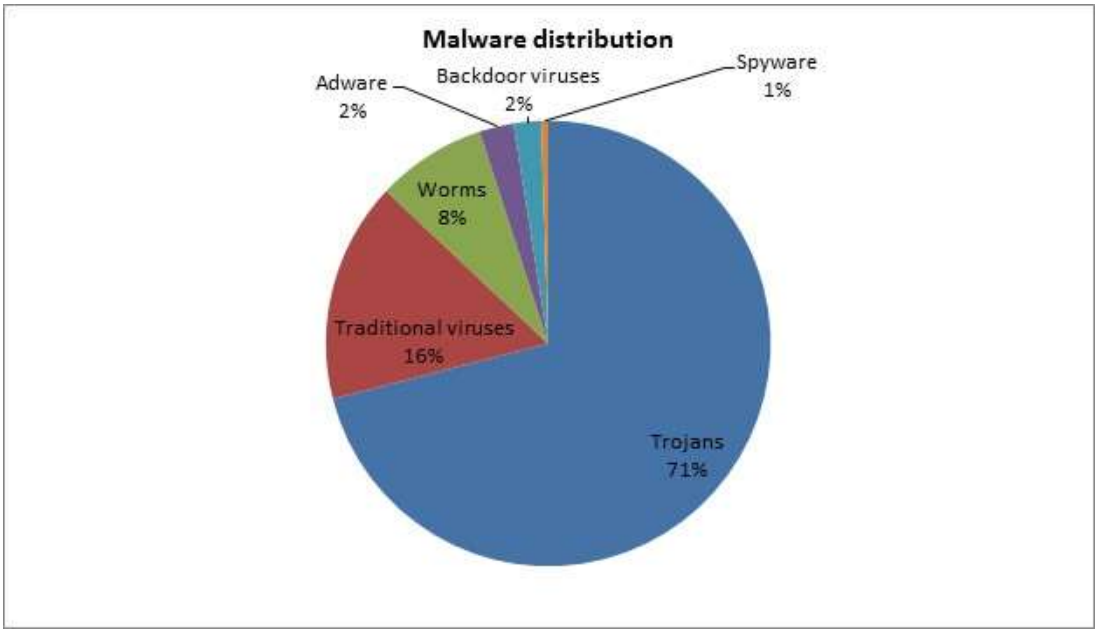


Рис.2.5. Розповсюдження шкідливих програм

Таблиця 2.4.

Аналіз проблем безпеки віртуалізації та їх вирішення

Теми	**Проблеми безпеки**	**Рішення безпеки**
Шкідливе ПЗ	Вразливість програмного забезпечення	Не визначено рішень
	Переміщення ВМ	Покращений протокол міграції на основі довірчого каналу
	Відкат ВМ	Не визначено рішень
	Уникнення шкідливого пз	Система запобігання вторгненням
Мобільність	Прослуховування пакетів і спуфінг	Не визначено рішень
Мережева віртуалізація	Двоїстий трафік, обмежений доступ до мережі, непридатність стандартних механізмів безпеки.	Не визначено рішень
Управління зображеннями вм	Крадіжка вм і впровадження шкідливого коду, недооцінення репозиторію зображень	Система управління зображеннями вм
	Розширення віртуальних машин	Не визначено рішень
Монітор віртуальних машин	Несправність гіпервізора, недовіра до компонентів, прозорість, відсутність GUI монітора	

2.3. Дослідження заходів протидії проблемам безпеки в хмарних сервісах

Існують різні заходи та елементи керування для захисту хмарних сервісів.

Рис.2.6. Методи зменшення та запобігання ризикам хмарних обчислень

Контроль проти апаратних атак у хмарних сервісах. У контексті хмарних сервісів, фізична безпека даних центрів та криптографія є ключовими заходами проти апаратних атак. Атаки по бічному каналу, які виникають через неналежну реалізацію алгоритмів шифрування або неадекватний контроль доступу, можуть призвести до втрати конфіденційної інформації. Криптографія, включаючи технології, як криптографія на основі ідентифікації та ієрархічна криптографія на основі ідентифікації, допомагає забезпечувати безпеку даних у хмарному середовищі.

Унікальні ідентифікатори користувачів та серверів у хмарному середовищі сприяють ефективній автентифікації та контролю доступу. Підходи до безпеки, які застосовуються для захисту від апаратних атак, включають ізоляцію рядків кешу, що містять критичні дані, використання криптографії для захисту даних під час передачі, а також вимкнення доступу до критичних частин пам'яті, як кешу S-Box.

Такі засоби безпеки, як поділ кешу, блокування кешу, вимкнення доступу до кешу S-Box, уникнення таблиць пошуку та вставлення фіктивних операцій, є важливими для забезпечення захисту від апаратних атак у хмарних сервісах. Ці методи допомагають запобігти несанкціонованому доступу та витоку інформації, забезпечуючи більш безпечне середовище для зберігання та обробки даних у хмарі.

Контроль проти атак на основі гіпервізора в хмарних сервісах. Важливим аспектом безпеки хмарних сервісів є захист від атак, що спрямовані на гіпервізор, який є центральним елементом віртуалізації в хмарних технологіях. Використання віртуалізації з апаратною підтримкою (HaV) допомагає захистити гіпервізор від атак, поліпшуючи ізоляцію апаратних ресурсів системи. HaV дозволяє безпечно транслювати адреси пам'яті і забезпечувати безпечний блок керування пам’яттю введення-виведення (IOMMU), що запобігає атакам зловмисних пристроїв.

Технології безпеки на основі програмного забезпечення важливі для захисту віртуальних машин, які використовуються в хмарних сервісах, зокрема під час міграції віртуальних машин. Ці методи включають ізоляцію пам’яті, ізоляцію пристрою та ізоляцію мережі для забезпечення безпеки гіпервізора та запобігання атакам на основі гіпервізора[15].

Рис.2.7. Фактори для посилення контролю доступу

Контроль через хмарний аудит. Аудит безпеки є ключовим елементом для забезпечення безпеки хмарних сервісів. Регулярні аудити допомагають оцінювати політику, операції, практику та технічний контроль, а також відповідність вимогам безпеки. Вони повинні включати як реактивні аудити на випадок інцидентів, так і профілактичні аудити для оцінки адекватності заходів безпеки.

Постачальники хмарних послуг повинні забезпечити прозорість своїх процедур аудиту безпеки для клієнтів. Крім того, обсяг використовуваного охоплення безпеки повинен відповідати юридичним та регулятивним вимогам. Завдяки аудитам безпеки хмарних сервісів, можна ефективно виявляти та усувати вразливості, а також підтримувати високий рівень довіри та надійності серед користувачів хмарних сервісів.

Прозорість аудиту безпеки є ключовою для забезпечення, що клієнти, як фізичні особи, так і корпорації, розуміють, як здійснюється захист їх даних. Це включає інформування клієнтів про різні аспекти аудиту, включаючи політику, операції, практики та технічний контроль.

Існують певні виклики, пов'язані з аудитом безпеки у хмарних сервісах, зокрема, управління великим обсягом даних та забезпечення їх захисту від кіберзлочинів та шахрайства. Це може ускладнювати роботу криміналістичних команд, особливо коли необхідно отримати доступ до хмарних даних для судових розглядів.

Ефективне управління аудитом в хмарних сервісах вимагає не тільки прозорості, але й детального планування та реалізації різних елементів контролю. Це може включати засоби керування доступом, процеси моніторингу, використання шифрування, а також регулярну оцінку вразливостей та загроз безпеці. Все це допомагає забезпечити, що хмарні сервіси здатні ефективно реагувати на потенційні ризики, а також відповідати на змінні вимоги безпеки та конфіденційності.

Таблиця 2.5.

Проблеми аудиту, характерні для хмари

Виклик	**Практика аудиту безпеки хмарних сервісів**	**Специфічні виклики для хмарних сервісів**	**Можливе рішення аудиту безпеки хмарних сервісів**
Колокація	Рідко відбувається	CSPS сильно залежать від цього.	Стандартизація та посилення нагляду
Шифрування	Власник даних контролює	Постачальники хмарних сервісів можуть бути відповідальними за шифрування.	Використання сторонніх служб та гомоморфне шифрування
Масштаб, сфера та складність	Відносно менше	Аудитори мають бути обізнаними та свідомими цих відмінностей	Впровадження постійної освіти та нових програм сертифікації
Прозорість	Системи управління даними та інформаційною безпекою більш доступні	Дані та їх безпека керуються третіми сторонами	Угоди про рівень послуг (SLA) повинні окреслювати політики безпеки контенту (CSP) та гарантії, тоді як csp надають клієнту результати аудиту

Ефективне шифрування в хмарних сервісах. Використання ефективних методів шифрування є ключовим для забезпечення безпеки даних у хмарних сервісах. Існують різні алгоритми та підходи, які можуть бути впроваджені для посилення захисту даних, включаючи:

- **Шифрування на основі атрибутів (ABE).** ABE дозволяє

контролювати доступ до зашифрованих даних через атрибути. У шифруванні з політикою цифрування текстів (CP-ABE), шифрувальник визначає політику доступу, а у шифруванні з політикою ключів (KP-ABE), атрибути використовуються для визначення ключів та зашифрованих текстів, що дозволяє більш гнучке управління доступом.

- **Повністю гомоморфне шифрування (FHE).** FHE дозволяє проводити обчислення безпосередньо на зашифрованих даних. Це розширює можливості захисту даних у хмарі, дозволяючи проводити обчислення, не розкриваючи вміст даних. Однак ця технологія має обмеження у використанні через свою складність та обмежену обробку даних.
- **Симетричне шифрування (SE).** SE використовує однаковий ключ для шифрування та розшифровки, що робить його ефективним для безпечного пошуку в зашифрованих даних. Використання індексів ключових слів може підвищити ефективність пошуку, дозволяючи користувачам швидко знаходити необхідну інформацію[16].

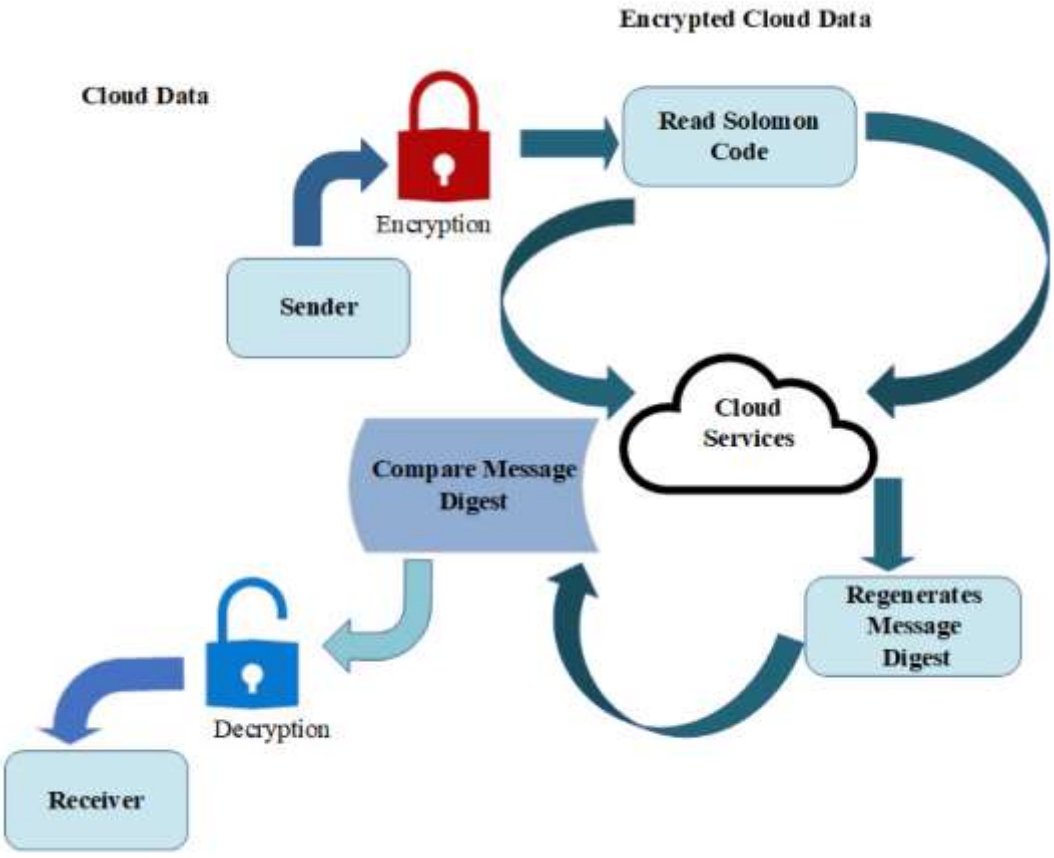


Рис.2.8. Приклад шифрування в хмарних сервісах

Методи шифрування можуть бути доповнені іншими заходами, наприклад, використанням активних пакетів, для забезпечення більшого захисту даних у хмарному середовищі. Впровадження зазначених методів шифрування в хмарних сервісах допомагає забезпечити конфіденційність, цілісність та доступність даних, які обробляються та зберігаються у хмарі.

Контроль конфіденційності даних. Особисті та конфіденційні дані часто виявляються вразливими перед загрозами злому, особливо у випадку використання публічних хмарних сервісів. Коли користувачі передають свої дані хмарним постачальникам, виникає питання про право власності та управління цією інформацією.

Занепокоєння з приводу безпеки привели деякі організації, зокрема державні установи, до створення власних приватних хмарних рішень. Це підкреслює необхідність більшої уваги до захисту даних, особливо для користувачів, які мало обізнані у питаннях конфіденційності, таких як користувачі мобільних пристроїв.

Зловмисники часто використовують цю необізнаність, здійснюючи шахрайські дії, такі як крадіжка даних, їх фальсифікація або блокування доступу користувачів до їх особистих даних.

Для протидії цим загрозам рекомендуються різні методи:

- Орієнтоване на користувача управління ідентифікацією. Підхід, який дозволяє користувачам більш ефективно керувати своїми обліковими записами і автентифікаційними даними.
- Одноразовий вхід (SSO). Метод, що дозволяє використовувати єдині облікові дані для доступу до різних послуг без необхідності повторного входу.
- Двофакторна автентифікація. Забезпечує додатковий рівень безпеки шляхом вимоги двох різних форм підтвердження ідентичності перед наданням доступу до рахунку або даних.
- Методи на основі доказів із нульовим знанням. Підхід, що дозволяє довести ідентичність або право доступу без розкриття інших конфіденційних даних.

Впровадження перерахованих заходів може значно підвищити захист даних користувачів хмарних сервісів, знижуючи ризики, пов'язані з несанкціонованим доступом та порушенням конфіденційності.

Методи та засоби керування автентифікацією та ідентифікацією в хмарних сервісах. Хмарні сервіси, забезпечуючи організаціям місце для зберігання інформації, стикаються з ризиками, такими як маніпуляції даними та порушення цілісності даних. Проблеми з автентифікацією сприяють загрозам безпеки, включаючи DoS-атаки, підроблення ідентифікаційних даних, перехоплення пакетів і атаки «людина посередині».

- Орієнтоване на користувача управління ідентифікацією (IdM). Ідентифікатори та атрибути використовуються для допомоги в ідентифікації та визначенні хмарних користувачів. Цей підхід дозволяє користувачам контролювати свою цифрову ідентифікацію.
- Мобільність цифрових ідентифікаційних даних. Важливо, щоб користувачі могли експортувати та безпечно передавати свої цифрові ідентифікаційні дані на різні цифрові пристрої.
- Підзвітність. Хмарна система повинна генерувати незаперечні докази неправильної діяльності та здатна виявляти зловживання.
- SAML (Мова розмітки безпеки). Використовується в хмарних сервісах для безпечного обміну ідентифікаційними даними між організаціями, що дозволяє SSO (одноразовий вхід) в Інтернеті. SAML допомагає зменшити потребу в багаторазовому вході, збільшуючи безпеку та зручність користувачів.

Зазначені методи дозволяють забезпечити більш надійну та безпечну передачу даних в хмарному середовищі, а також контролювати доступ до інформації, мінімізуючи ризики порушення конфіденційності[17].

Система керування веб-доступом (WebAM)/система єдиного входу в Інтернет (WebSSO). WebSSO/WebAM у хмарних сервісах використовуються для керування автентифікацією та авторизацією користувачів, які отримують доступ до хмарних додатків та сервісів. Ці системи спрощують процес входу користувачів, дозволяючи їм використовувати один набір облікових даних для доступу до різних

сервісів і додатків. WebSSO перехоплює початковий контакт користувача з веб-додатком і перевіряє, чи користувач вже пройшов автентифікацію, або перенаправляє користувача на сторінку автентифікації. Після автентифікації користувача, WebAM контролює доступ до функцій і даних програми. Це може включати фільтрацію вмісту, до якого користувач може отримати доступ, або надання API для прийняття рішень під час виконання.

Продукти WebSSO/WebAM зазвичай інтегровані з серверним сховищем LDAP, яке ідентифікує всіх користувачів, і часто пов'язані з програмою «керування ідентифікацією та доступом», що дозволяє ефективне управління обліковими записами. Наприклад, обліковий запис Google може використовуватися для входу в різні хмарні послуги, такі як Gmail, Google Drive, YouTube тощо (рис.2.9).

Рис.2.9. Вхід до Amazon Console за допомогою ідентифікатора користувача

Ці системи єдиного входу значно підвищують зручність і безпеку користувачів, дозволяючи їм мати єдиний доступ до різноманітних хмарних

ресурсів без потреби утримувати численні облікові записи або паролі (рис.2.10-рис.2.11) [18].

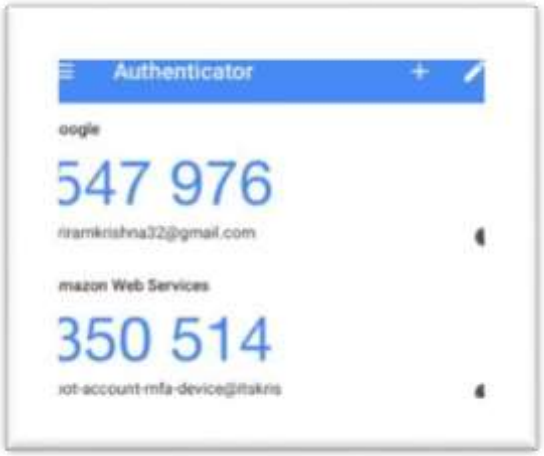


Рис.2.10. Отримання коду автентифікатора з пристрою [19]

Рис.2.11. Використання коду для входу в Cloud Console

Двофакторна автентифікація в хмарних сервісах. Двофакторна автентифікація (2FA) є ефективним засобом захисту в хмарних сервісах. Ця система вимагає від користувачів надати два різні типи підтвердження своєї особи перед наданням доступу до хмарного сервісу. Це забезпечує додатковий рівень безпеки порівняно з традиційними логіном та паролем[20].

Двофакторна автентифікація включає в себе щось, що користувач знає (наприклад, пароль), та щось, що користувач має (наприклад, фізичний токен або смартфон для отримання одноразового пароля). 2FA ускладнює зловмисникам доступ до користувацьких облікових записів, оскільки потребує фізичного доступу

до другого фактора автентифікації, наприклад, до мобільного телефону користувача.

Основним недоліком може бути необхідність управління фізичними пристроями або токенами, що може призвести до затримок або додаткових витрат. Крім того, існує ризик втрати або крадіжки цих фізичних пристроїв.

Завдяки вимозі фізичного компоненту, 2FA значно знижує ризик віддалених атак, таких як фішинг. Це також підвищує ймовірність того, що спроба несанкціонованого доступу буде виявлена користувачем.

Використання 2FA стає все більш популярним в хмарних сервісах для захисту користувацьких облікових записів, особливо в середовищах, де зберігаються конфіденційні або критично важливі дані.

Застосування 2FA в хмарних сервісах значно підвищує рівень безпеки, зменшуючи ймовірність несанкціонованого доступу до даних та аккаунтів користувачів.

Управління довірою в хмарних сервісах. Управління довірою в хмарних сервісах є ключовим аспектом для забезпечення безпеки та конфіденційності даних. Це особливо важливо у середовищах, де різні хмарні провайдери співпрацюють для надання послуг, і кожен може мати свої підходи до безпеки та конфіденційності.

- Довіра в хмарних сервісах включає здатність провайдерів і користувачів довіряти один одному щодо безпечного зберігання та обробки даних.
- Інтеграція політик включає створення інтегрованих політик між різними провайдерами, що дозволяє встановити довіру і сприяє безпечній співпраці.
- Оскільки поведінка користувачів і вимоги до послуг можуть швидко змінюватися, системи управління довірою повинні бути гнучкими та адаптованими до цих змін.
- Керування довірою повинно враховувати різні підходи до безпеки, що існують у різних хмарних сервісах, та забезпечувати їх сумісність.
- Користувачі повинні бути активно втягнуті у процес управління

довірою, не ігноруючи своїх провайдерів та проводячи належну перевірку.

- Провайдери хмарних сервісів повинні забезпечувати прозорість своїх процедур та політик безпеки для своїх клієнтів.
- Хмарні системи повинні бути здатні адаптуватися до змінних вимог до довіри, встановлюючи і модифікуючи політики у відповідності до цих потреб.
- Ефективне управління довірою в хмарних сервісах забезпечує захист даних від несанкціонованого доступу та використання.

Управління довірою в хмарних сервісах вимагає постійного аналізу, оцінки ризиків та адаптації до змінюваних умов і потреб користувачів. Воно є критично важливим для підтримки безпеки та конфіденційності в динамічному середовищі хмарних технологій[21].

2.4. Методи та засоби протидії мережевим атакам при використанні хмарних сервісів

Для забезпечення безпеки в хмарних сервісах, провайдери повинні ретельно захищати не тільки внутрішній трафік між віртуальними машинами у своїй хмарній інфраструктурі, але й трафік, що надходить ззовні.

Ефективними методами захисту є використання брандмауерів, систем виявлення вторгнень та антивірусних шлюзів, а також моніторинг вхідного та вихідного трафіку. Ці контрзаходи спрямовані на забезпечення доступності, конфіденційності та цілісності даних у хмарних системах.

Атаки DoS і DDoS. Для протидії атакам DoS і DDoS, хмарні постачальники повинні мати комплексний план захисту, що включає як превентивні заходи, так і реактивні стратегії. Це може означати використання систем, які постійно активні, а також тих, що активуються відповідно до виявлення потенційних атак. Такий підхід дозволяє забезпечити надійність та безперервність роботи хмарних сервісів, незважаючи на спроби зовнішнього втручання.

Атаки «флуд». У контексті хмарних сервісів, для протидії атакам типу «флуд», постачальники хмарних послуг впроваджують стратегії, спрямовані на оптимізацію обробки запитів та запобігання перевантаженням. Одним із ефективних підходів є розподіл ресурсів за допомогою згрупування серверів у різні групи, призначені для обробки специфічних типів завдань. Така організація дозволяє ізолювати ресурси і запобігти впливу надмірних або недоречних запитів на продуктивність всієї системи. Ця методика допомагає підвищити ефективність обробки запитів і знижує ризики, пов'язані з атаками DoS, які можуть завдати шкоди доступності та функціонуванню хмарних сервісів. Однак, слід враховувати, що ця стратегія може мати обмеження у випадках, коли окремі сервери або групи серверів перевантажені великою кількістю легітимних завдань. В таких ситуаціях, розподіл навантаження між різними групами може бути ускладнений через обмеження доступних ресурсів.

Фільтрація. Фільтрація даних є ключовою технікою для запобігання DDOS-атакам. Ця методика дозволяє ідентифікувати та блокувати небажаний трафік до того, як він досягне хмарного середовища. Фільтрація може бути застосована на різних етапах передачі даних, включаючи маршрутизатори та інші точки доступу до мережі. Однією з передових технік фільтрації є фільтрація на основі довіри (CBF), яка відрізняється високою швидкістю обробки, мінімальними вимогами до обсягу пам'яті та високою точністю фільтрації. Цей метод є особливо корисним у хмарному середовищі, оскільки він здатен задовольняти вимоги фільтрації в реальному часі. CBF може бути активовано як до, так і під час атаки, забезпечуючи надійний захист від небажаного трафіку. Під час періодів без атак CBF збирає легітимні пакети даних для створення номінального профілю, що дозволяє системі точніше ідентифікувати та блокувати шкідливий трафік. Такий підхід забезпечує ефективний захист хмарних ресурсів від потенційних загроз та підтримує стабільність та надійність хмарних сервісів.

Механізм захисту рухомої цілі DDoS. Механізм є інноваційним способом захисту від атак DDoS. Цей механізм працює шляхом використання динамічної групи прихованих проксі-серверів, які служать для ретрансляції трафіку між

авторизованими користувачами хмари та хмарними серверами. Основна ідея полягає у створенні додаткового рівня ізоляції, який відокремлює легітимних користувачів від потенційних зловмисників, включаючи зловмисних інсайдерів.

У процесі ретрансляції трафіку, проксі-сервери, які можуть бути об'єктами атаки, постійно замінюються на резервні проксі-сервери. Це забезпечує перемішування трафіку та робить атаки на конкретні проксі менш ефективними. Таким чином, легітимні користувачі хмари залишаються захищеними та відокремленими від можливих загроз.

Використання жадібного алгоритму дозволяє оптимізувати цей процес, збільшуючи ефективність відокремлення потенційно зловмисних користувачів та підвищуючи можливості для їх карантину. Такий підхід є важливим елементом у стратегії безпеки хмарних сервісів, забезпечуючи високий рівень захисту від складних DDoS атак.

Алгоритм також дозволяє оцінити ресурси, необхідні хмарним сервісам для запобігання DDoS-атакам. Захист від рухомої цілі досягає кількох цілей:

1) Подолання цілеспрямованих атак за допомогою динамічних IP-адрес у величезному діапазоні адрес IPv6;

2) Усунення втрати пакетів через колізію адрес;

3) Перевірка кожним вузлом того, що його нова IP-адреса вільна (уникнення колізії адрес); необхідний механізм для інформування вузлів-кореспондентів про цю перевірену нову IP-адресу (механізм обов’язкового оновлення);

4) Уникнення додавання нових вимог, таких як синхронізація часу;

5) Додавання можливості динамічного інтервалу чергування адрес;

6) Уникнення обміну оновленнями IP з вузлом-кореспондентом, відомим як зловмисник;

7) Уникайте використання постійно доступних домашніх агентів, оскільки постійні домашні адреси доступні лише через домашніх агентів.

Стратегії проти витоку та втрати даних. Шифрування в хмарних сервісах є основним методом запобігання неавторизованому доступу та втручанню в дані користувачів. Одним з ефективних підходів є повторне шифрування проксі-

сервера, що забезпечує вищий рівень конфіденційності та приватності даних у хмарі.

Цей механізм використовує асиметричну схему шифрування, яка дозволяє проксі перетворювати зашифровані тексти під одним відкритим ключем у зашифровані тексти за іншим відкритим ключем. Це означає, що користувачі хмари надають проксі-серверу ключ повторного шифрування, що дозволяє процесу трансформації відбуватися без необхідності взаємодії з основними відкритими текстами та закритим ключем. Така схема повторного шифрування визначає відповідні функції шифрування, дешифрування та перетворення, полегшуючи безпечний обмін даними в хмарній мережі.

За допомогою цієї схеми, зашифровані тексти, що зберігаються у хмарі, можуть бути перетворені так, що лише авторизовані особи можуть розшифрувати їх, забезпечуючи, що навіть мережеві сервери не можуть прочитати ці дані. Це захищає дані від несанкціонованого доступу та можливої втрати.

Техніки, такі як шифрування на основі атрибутів (ABE) і повторне шифрування проксі (PRE), можуть бути використані для розширення можливостей цієї системи. Ці методи дозволяють точно керувати доступом до зашифрованих даних та ефективно відкликати користувачів, що мають доступ. Поєднання ABE та PRE вимагає, щоб користувачі хмари були активними в онлайн-режимі для своєчасної передачі ключів PRE постачальникам послуг.

Крім того, повторне шифрування проксі на основі часу є ефективним у забезпеченні тимчасового доступу до даних, обмежуючи права доступу користувачів після певного періоду часу. Цей підхід поєднує шифрування на основі атрибутів (ABE), шифрування закритого ключа (PKE) та часові обмеження, забезпечуючи структурований доступ до даних на основі визначених атрибутів користувачів і встановлених термінів дії їхніх прав доступу.

Інші методи забезпечення конфіденційності та цілісності даних включають:

1) Управління ключами: генерація, обмін, використання зберігання та заміна ключів;

2) Токенізація даних;

3) Резервне копіювання та реплікація даних;

4) Моніторинг цілісності даних;

5) Методи автентифікації та авторизації.

Контроль загроз у моделях доставки хмарних сервісів. Різні моделі доставки хмарних сервісів, такі як інфраструктура як сервіс (IaaS), платформа як сервіс (PaaS) та програмне забезпечення як сервіс (SaaS), стикаються з унікальними переплетеними викликами у сфері безпеки та конфіденційності.

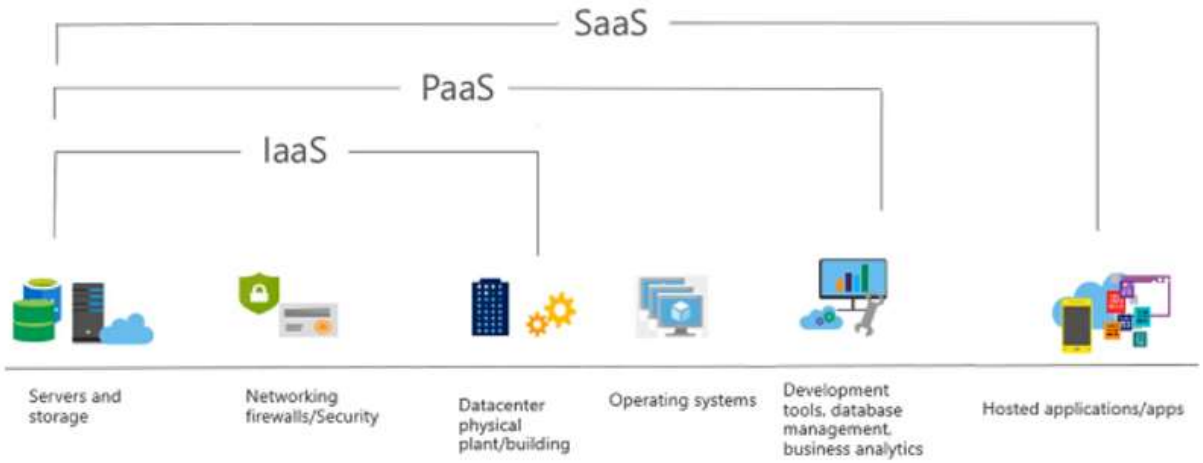


Рис.2.12. Безпека в моделях доставки хмарних сервісів

Ці проблеми вимагають комплексного підходу до їх вирішення, включаючи заходи, такі як надійне наскрізне шифрування та ефективна схема довірчого керування.

У таблиці 2.6. надано детальний огляд специфічних проблем безпеки для кожної з моделей доставки хмарних сервісів та рекомендації щодо їх вирішення. Цей аналіз допомагає зрозуміти, які конкретні заходи безпеки найкраще підходять для кожної моделі, забезпечуючи комплексний захист даних та операцій у хмарному середовищі.

У контексті загальнодоступних хмар, авторизація є критичною для всіх трьох моделей (IaaS, PaaS, SaaS), щоб запобігти неавторизованому доступу до ресурсів.

Таблиця 2.6.

Аналіз проблем безпеки для моделей доставки хмарних сервісів та рекомендації щодо їх вирішення

Проблема	**Ефекти**	**Залучені хмарні сервіси**	**Рішення**
Втрата та витік даних	Чутливі особисті дані можуть бути видалені, знищені, пошкоджені або змінені	PaaS, SaaS, IaaS	Аудит конфігурації та вразливості, використання сильної аутентифікації та механізмів контролю доступу для адміністративних завдань.
Різні моделі надання/отримання послуг	Втрата контролю над інфраструктурою хмари	PaaS, SaaS, IaaS	Надання послуг під контролем та з моніторингом
Небезпечний інтерфейс та API	Неправильна аутентифікація та авторизація, неправильна передача вмісту	PaaS, SaaS, IaaS	Спостереження за станом мережі, надання надійних методів реєстрації та аутентифікації
Зловмисники зсередини	Проникнення в ресурси організації, шкода активам, втрата продуктивності, вплив на операції	PaaS, SaaS, IaaS	Передача даних в зашифрованій формі, сильний контроль доступу та механізми аутентифікації
Захоплення сервісу/акаунту	Крадіжка облікових даних користувача, доступ до критичних даних хмари, що дозволяє зловмисникам компрометувати безпеку сервісів	PaaS, SaaS, IaaS	Використання сильної аутентифікації

Цілісність даних також є ключовою вимогою, оскільки вона забезпечує перевірку правильності та незмінності інформації. Крім того, висока доступність та

надійність послуг вимагають впровадження міцних механізмів безпеки на базовому мережевому рівні.

Контроль оцінки ризиків. Оцінка ризиків стає ключовим елементом у забезпеченні безпеки та конфіденційності. Вона дозволяє визначити потенційні проблеми та розробляти стратегії для їх превентивного усунення або зменшення впливу. Ця оцінка ризиків включає аналіз активів, загроз та уразливостей, що допомагає визначити потенційні ризики у хмарному середовищі.

Оцінка ризику для хмарного провайдера є важливою частиною цього процесу, оскільки безпека та конфіденційність послуг часто залежать від постачальника хмарних сервісів. Ризик можна кількісно визначити як поєднання кількості активів (NrAssets), уразливостей (NrVulnerabilities) та загроз (NrThreats). Такий підхід дозволяє комплексно оцінити потенційні ризики, а також розробити ефективні стратегії захисту, що враховують усі аспекти хмарного середовища.

Таким чином, оцінка ризиків стає невід'ємною частиною процесу управління хмарними сервісами, забезпечуючи вищий рівень безпеки для користувачів та їхніх даних.

Оцінка ризику складається з наступних кроків:

1) Ідентифікація активів у хмарному середовищі;

2) Огляд технічних, правових і бізнес-вимог, що стосуються ідентифікованих активів;

3) Оцінка ідентифікованих активів з урахуванням визначених технічних, юридичних і бізнес-вимог і наслідків втрати конфіденційності та довіри, цілісності, конфіденційності та доступності;

4) Визначення потенційних загроз і вразливостей для ідентифікованих активів;

5) Оцінка ймовірності виникнення загроз і вразливостей;

6) Розрахунок ризиків і порівняння із заздалегідь визначеною шкалою ризиків.

Після завершення оцінки ризиків організація повинна розробити відповідні заходи щодо потенційних загроз безпеці та конфіденційності[22].

Висновки до другого розділу

Досліджено проблеми безпеки в хмарних сервісах, зокрема ризики, пов'язані з незахищеними API, інсайдерськими загрозами, SQL-ін'єкціями, та загрозами автентифікації.

Розглянуто ключові аспекти ідентифікаційної, інформаційної, інфраструктурної, мережевої та програмної безпеки в хмарних сервісах. Проаналізовано значення та важливість застосування криптографії, фізичної безпеки даних центрів, та контролю доступу для забезпечення безпеки хмарних сервісів.

Виявлено потенційні ризики, пов'язані з віртуалізацією в хмарних сервісах, та важливість захисту від атак на гіпервізор.

Зазначено важливість забезпечення конфіденційності та приватності в хмарних сервісах, в тому числі захисту даних від несанкціонованого доступу.

3 ІНТЕГРАЦІЯ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

3.1. Варіанти інтеграції рішень Barracuda CloudGen Firewall

Файрвол Barracuda CloudGen - це файрвол нового покоління, створений для безшовної інтеграції з хмарною платформою AWS. Гнучкість файрволу CloudGen дозволяє архітекторам хмар розробляти референсну архітектуру, виходячи з призначеного випадку використання та розміру навантаження. Для кожної референсної архітектури надається шаблон CloudFormation, що полегшує її розгортання або інтеграцію з поточними хмарними ресурсами.

CloudGen додає мережеві контролі безпеки, видимість і з'єднання до хмарної мережі. Залежно від випадку використання, вибирається розгортання файрволу CloudGen, щоб задовольнити правильний баланс серед наступних критеріїв:

- Підтримка необхідних функцій файрволу, таких як фаєрволінг або VPN: висока доступність, масштабованість, оптимізація витрат та час відновлення.
- Основні випадки використання файрволу Barracuda CloudGen: крайовий файрвол., захищений віддалений доступ, офіс до хмари/гібридна хмара, сегментація

Звичайні випадки використання:

- Забезпечення безпеки мережі за допомогою файрволу та IPS;
- За замовчуванням (вихідний) шлюз для хмарних ресурсів у тій самій VPC (рис.3.1)

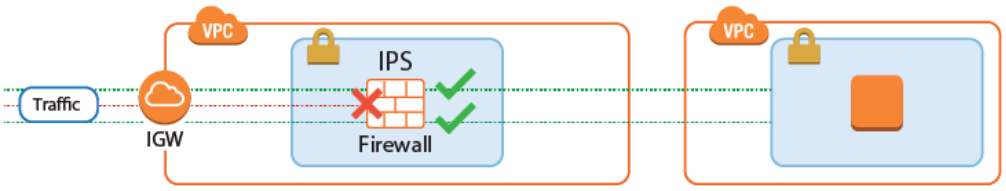


Рис.3.1. Приклад реалізації вихідного шлюзу для хмарних ресурсів у VPC

CloudGen забезпечує захист доступу до хмарних ресурсів AWS з Інтернету, застосовуючи детальні політики доступу файрволу та скануючи вхідний трафік на наявність шкідливих програм та експлойтів. Функції файрволу нового покоління замінюють або розширюють рідні групи безпеки AWS та NACLs за допомогою:

- Захисту від мережевих атак та експлойтів із вбудованим IPS;
- Сканування вірусів та захисту від передових загроз (ATP);
- Контролю доступу на основі геолокації;
- Формування трафіку (QoS) для захисту бізнес-критичного трафіку.

Кластер високої доступності файрволу CloudGen зі зміною маршруту. Кластер високої доступності файрволу CloudGen підтримує всі функції файрволінгу та шлюзу за замовчуванням, необхідні для функціонування як крайового файрволу.

Файрволи працюють у активно-пасивному кластері, який синхронізує інформацію про сесії та конфігурації. Весь вихідний трафік з приватних підмереж направляється через активний файрвол (рис.3.2).

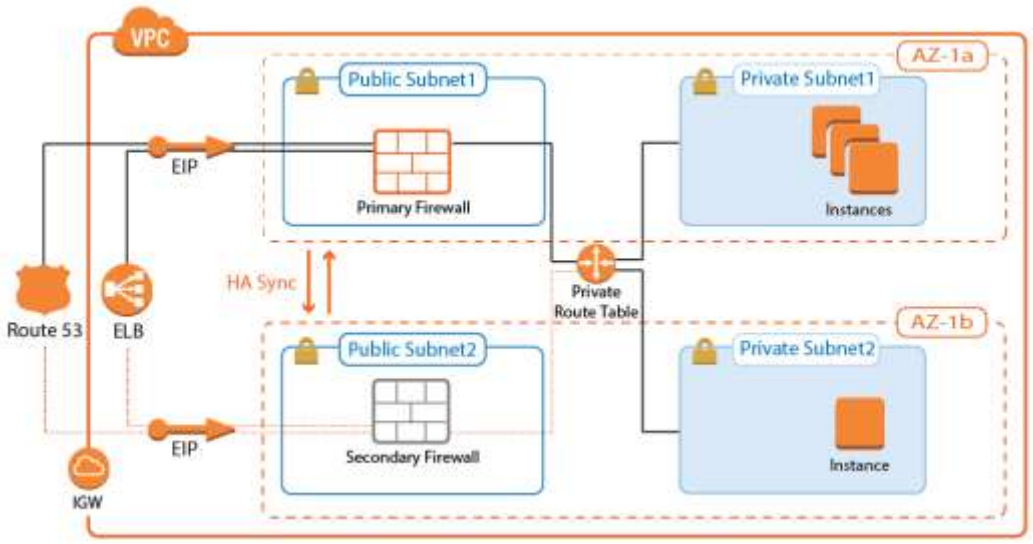


Рис.3.2. Кластер високої доступності файрволу CloudGen зі зміною маршруту

У разі відмови, пасивний файрвол бере на себе управління та підключається до хмарної інфраструктури для переписування всіх маршрутів на використання тепер активного файрволу у кластері високої доступності як цілі[23].

Маршрути, додані після розгортання, які використовують файрвол як шлюз, автоматично виявляються і, у разі відмови, також переписуються.

Кластер холодного резервування файрволу CloudGen. Кластер холодного резервування є економічно ефективним рішенням, яке пропонує повний спектр функцій файрволу нового покоління. У разі, якщо інстанс файрволу не відповідає, він автоматично замінюється. Маршрути для приватних підмереж переписуються, але їх потрібно вручну налаштувати в шаблоні CloudFormation, щоб вони відповідали архітектурі (рис.3.3).

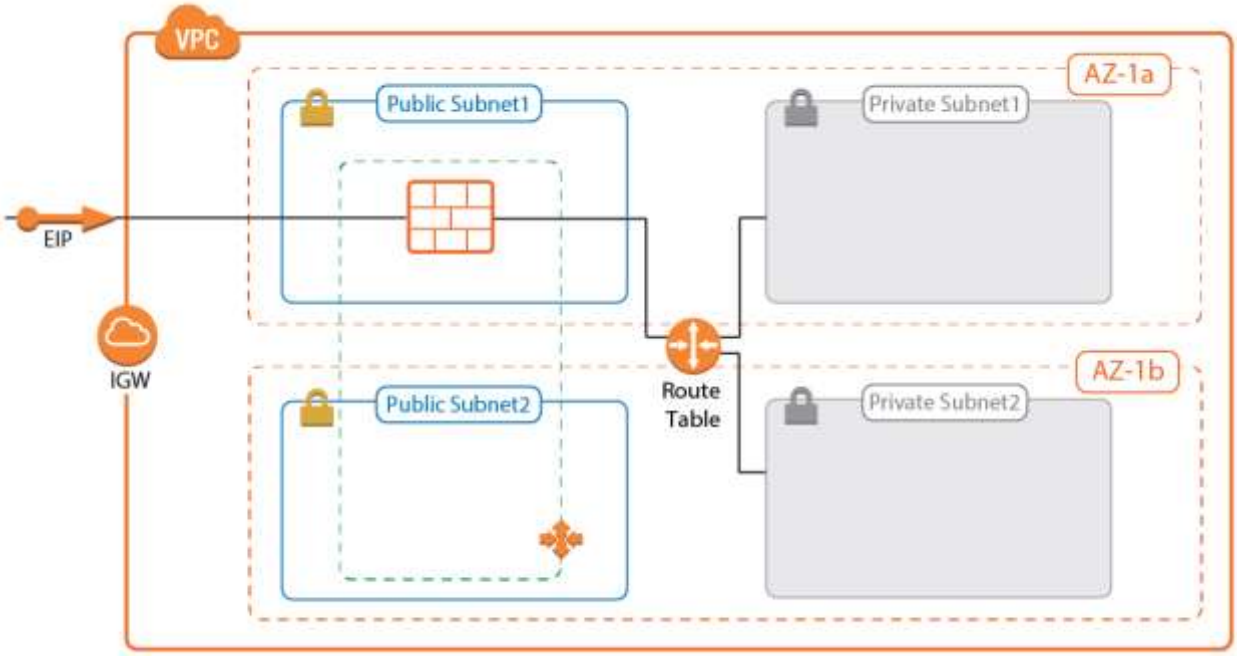


Рис.3.3. Кластер холодного резервування файрволу CloudGen

Таблиці маршрутизації не моніторяться автоматично; додаткові маршрути або зміни до існуючих маршрутів повинні бути виконані шляхом спочатку оновлення шаблону, а потім оновлення стеку CloudFormation.

Кластер автомасштабування файрволу CloudGen. Підбір розміру файрволу для високодинамічного трафіку може бути складним. Легко можна витратити зайві кошти на занадто великі інстанси, або ж ризикувати створенням «вузьких місць» у архітектурі організації, якщо файрвол не встигає за поточним попитом. Кластер автомасштабування файрволу CloudGen автоматично масштабується відповідно до навантаження організації. Один або декілька

балансувальників навантаження Elastic Load Balancer розподіляють трафік між інстансами файрволу в групі Auto Scaling (рис.3.4).

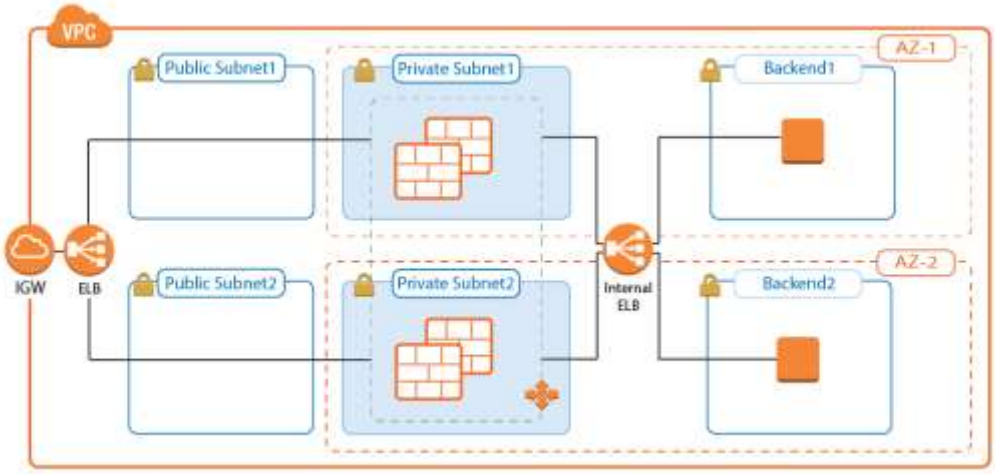


Рис.3.4. Кластер автомасштабування файрволу CloudGen

Власні метрики файрволу, зібрані CloudWatch, дозволяють налаштувати політики масштабування, які відповідають хмарним додаткам організації. Оскільки IP-адреса джерела повинна бути переписана на файрволі, кластер автомасштабування файрволу CloudGen не може бути використаний як шлюз за замовчуванням для вихідного трафіку інстансів у приватних мережах[24].

Кластер автомасштабування файрволу CloudGen. Функції віддаленого доступу надають користувачам безпечний доступ до хмарних додатків та ресурсів їхньої організації з практично будь-якого пристрою.

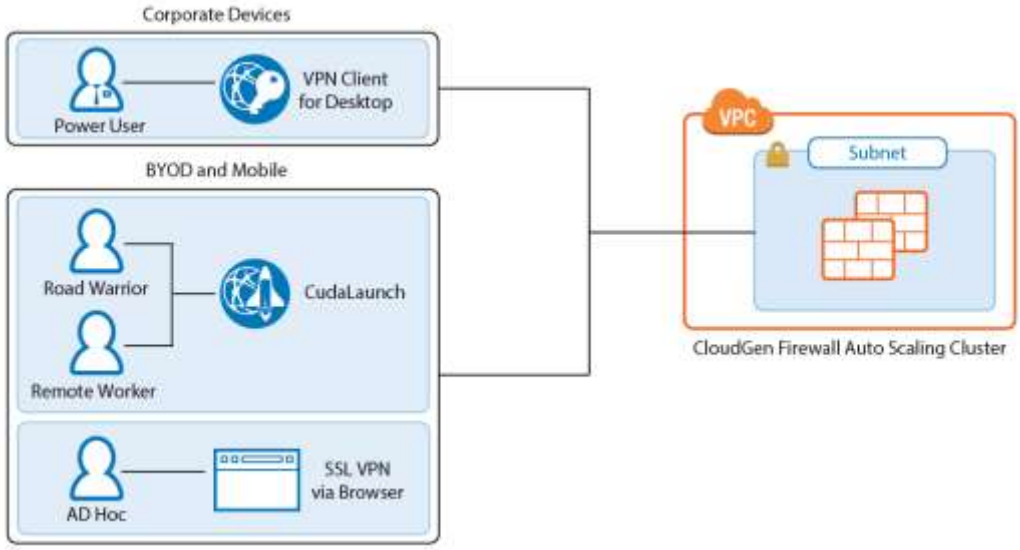


Рис.3.5. Кластер автомасштабування файрволу CloudGen

Залежно від навантаження, доступні повні VPN клієнт-до-сайту або SSL VPN, причому CudaLaunch пропонує більш широкий рівень віддаленого доступу, що охоплює як VPN клієнт-до-сайту, так і SSL VPN.

Для досвідчених користувачів або користувачів з централізовано керованими корпоративними пристроями VPN клієнт-до-сайту пропонує прозорий доступ до корпоративної мережі. Клієнт VPN Barracuda використовує протокол VPN TINA, спеціально розроблений для міцних VPN-з'єднань. VPN-клієнти можуть бути аутентифіковані через клієнтські сертифікати, зовнішні та внутрішні схеми аутентифікації або їх комбінацію.

SSL VPN сервіс забезпечує безшовну інтеграцію без необхідності встановлення клієнтського додатку. CudaLaunch працює з сервісом SSL VPN, щоб надати більш передові функції SSL VPN, такі як SSL тунелювання або підтримка нативних додатків. Кількість одночасних користувачів, які використовують SSL VPN, обмежена лише продуктивністю інстансів AWS.

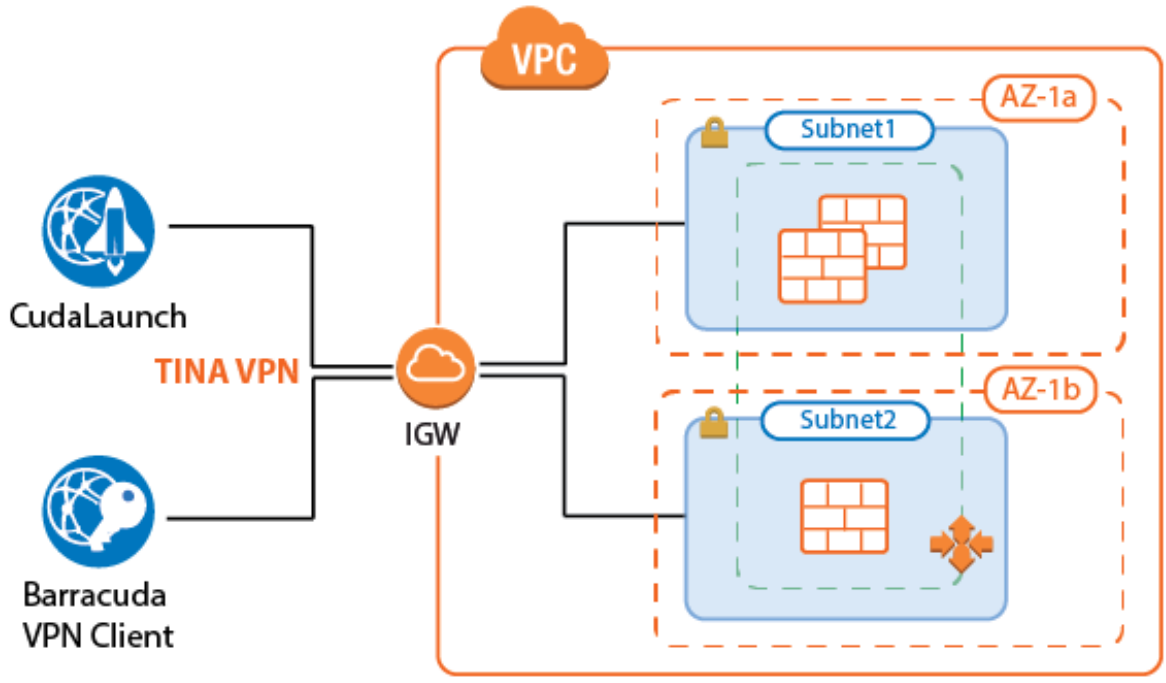


Рис.3.6. Варіант реалізації автомасштабування файрволу CloudGen

Навантаження на роботу з віддаленим доступом мають тенденцію бути циклічними за природою. Віддалені працівники підключаються до своїх VPN-

клієнтів вранці та відключаються в кінці робочого дня. Використовуючи кластер автомасштабування файрволу CloudGen, кількість файрволів автоматично масштабується для задоволення поточного попиту. Кластер також може бути масштабований відповідно до розкладу, залежно від передбачуваності навантаження. Інстанси файрволу автоматично розгортаються у двох або більше зонах доступності.

Власні метрики файрволу та VPN, зібрані AWS CloudWatch, дозволяють адміністратору налаштувати індивідуальні політики масштабування. Автомасштабування обмежене PAYG-образами файрволу Barracuda CloudGen.

Кластер холодного резервування файрволу CloudGen. Для невеликої кількості віддалених користувачів з передбачуваними моделями трафіку кластер холодного резервування є дуже економічно ефективним рішенням для віддаленого доступу організації.

Єдиний працюючий файрвол автоматично замінюється протягом декількох хвилин після збою. Конфігурація зберігається в бакеті S3 і за бажанням може бути завантажена з CloudGen Control Center.

Використання Control Center дозволяє використовувати ліцензії BYOL pool для інстансу. Для окремих файрволів використовується образ PAYG. Кластери холодного резервування потрібно масштабувати вручну для задоволення збільшеного попиту.

Створення з'єднання VPN між сайтами, щоб прозоро з'єднати мережі на місцях з додатками та сервісами, які розміщені в хмарі організації. Для тунелів VPN, які використовують власний протокол VPN TINA, SD-WAN дозволяє розділити VPN-тунель на до 24 VPN-транспортів, кожен з яких використовує різне з'єднання WAN з файрволом у хмарі[25].

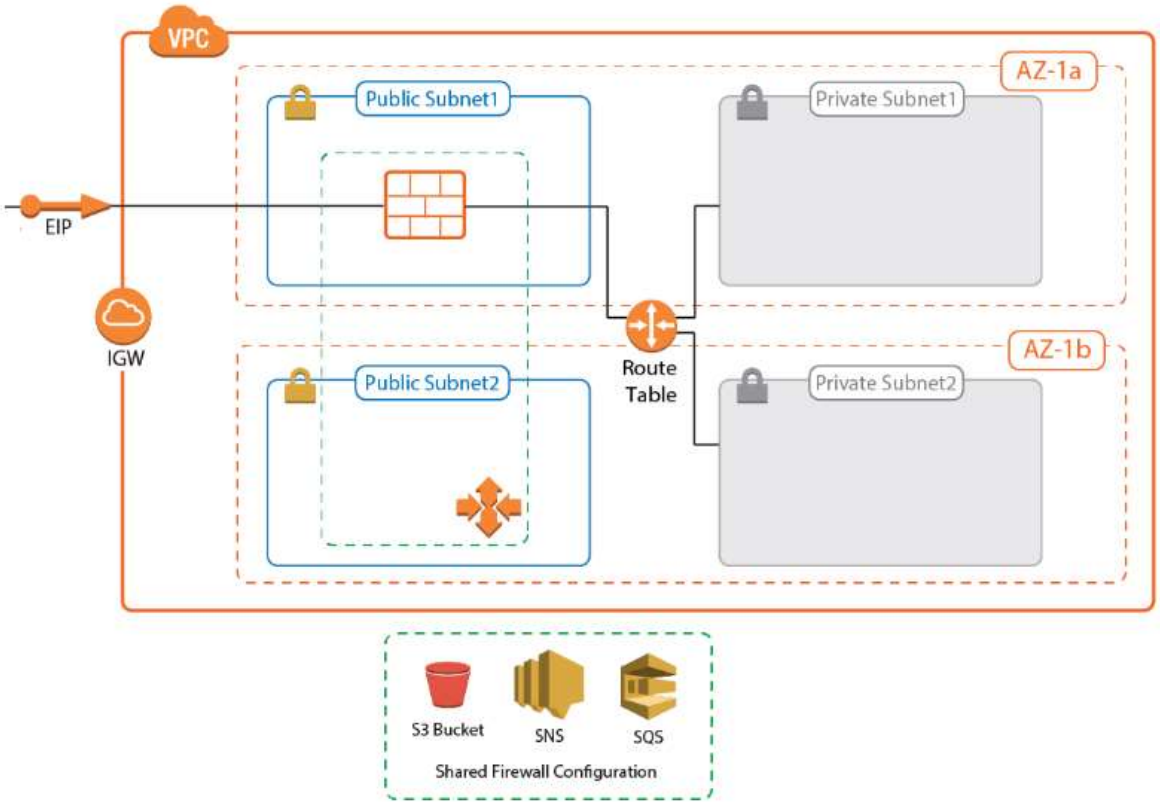


Рис.3.7. Кластер холодного резервування файрволу CloudGen

Для користувача це відбувається абсолютно прозоро. Крім того, SD-WAN також дозволяє динамічно маршрутизувати трафік залежно від вимог до пропускної здатності або затримки. Перенаправлення трафіку на дешевші з'єднання дозволяє використовувати з'єднання Direct Connect з меншою пропускною здатністю або підвищити якість для бізнес-критичної або чутливої до затримок інформації.

Звичайні випадки використання:

- Гібридна хмара за допомогою VPN між сайтами;
- За замовчуванням (вихідний) шлюз для хмарних ресурсів;
- Захист трафіку на лінії Direct Connect MPLS.

Створюйте з'єднання VPN між сайтами, щоб прозоро з'єднати мережі на місцях з додатками та сервісами, які розміщені в хмарі. Для тунелів VPN, які використовують власний протокол VPN TINA, SD-WAN дозволяє розділити VPN-

тунель на до 24 VPN-транспортів, кожен з яких використовує різне з'єднання WAN з файрволом у хмарі.

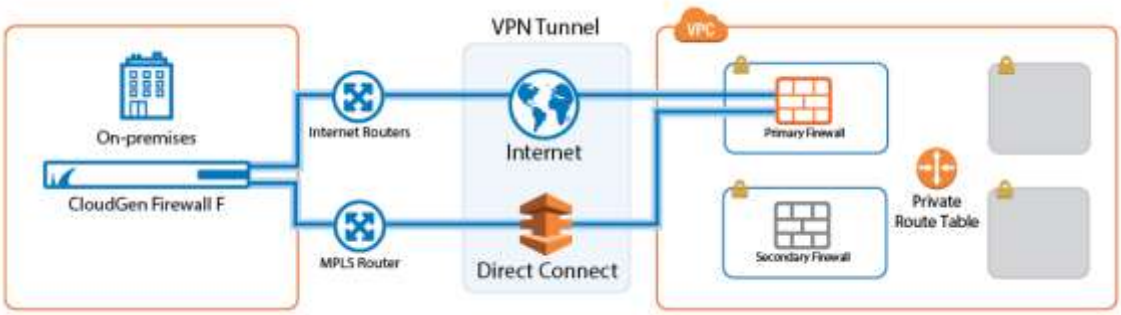


Рис.3.8. Створення з'єднання VPN між сайтами

Для користувача це відбувається абсолютно прозоро. Крім того, SD-WAN також дозволяє динамічно маршрутизувати трафік залежно від вимог до пропускної здатності або затримки. Перенаправлення трафіку на дешевші з'єднання дозволяє використовувати з'єднання Direct Connect з меншою пропускною здатністю або підвищити якість для бізнес-критичної або чутливої до затримок інформації.

Кластер високої доступності файрволу CloudGen. Кластер високої доступності файрволу CloudGen підтримує як TINA, так і IPsec IKEv1 та IKEv2 VPN тунелі між сайтами. Для IPsec тунелів для вхідного трафіку потрібно використовувати Route 53, оскільки балансувальник навантаження Elastic Load Balancer не підтримує UDP.

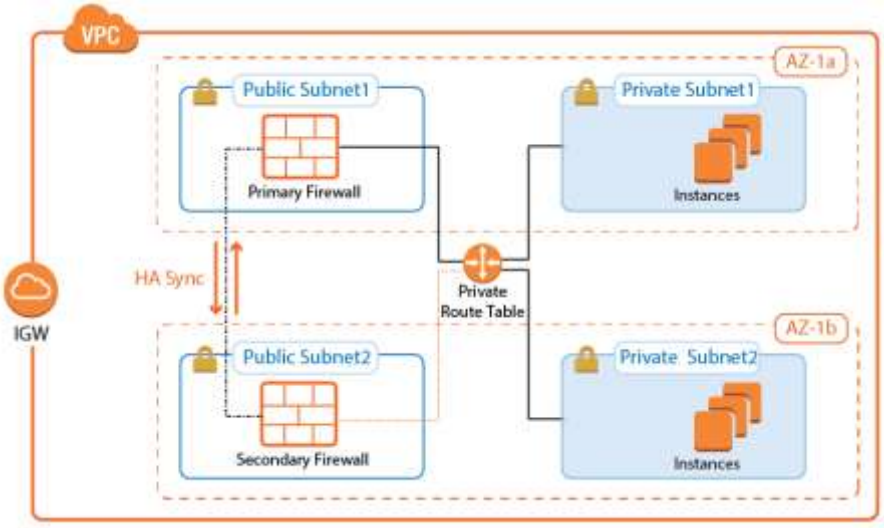


Рис.3.9. Кластер високої доступності файрволу CloudGen

За бажанням можна використовувати CloudGen Control Center для отримання та управління конфігурацією файрволу та для моніторингу віддалених файрволів в одному центральному місці. Якщо використовуються лише TINA VPN тунелі, балансування вхідного навантаження не потрібне, оскільки TINA VPN тунелі можуть бути налаштовані на використання двох публічних IP-адрес як VPN-кінцевих точок. Кластери високої доступності файрволу CloudGen потрібно масштабувати вручну, якщо навантаження збільшується.

Кластер холодного резервування файрволу CloudGen. Кластер холодного резервування файрволу CloudGen підтримує ті ж VPN-функції, що й кластер високої доступності. Окремий інстанс файрволу працює в групі автомасштабування з одним інстансом, конфігурація файрволу зберігається в бакеті S3.

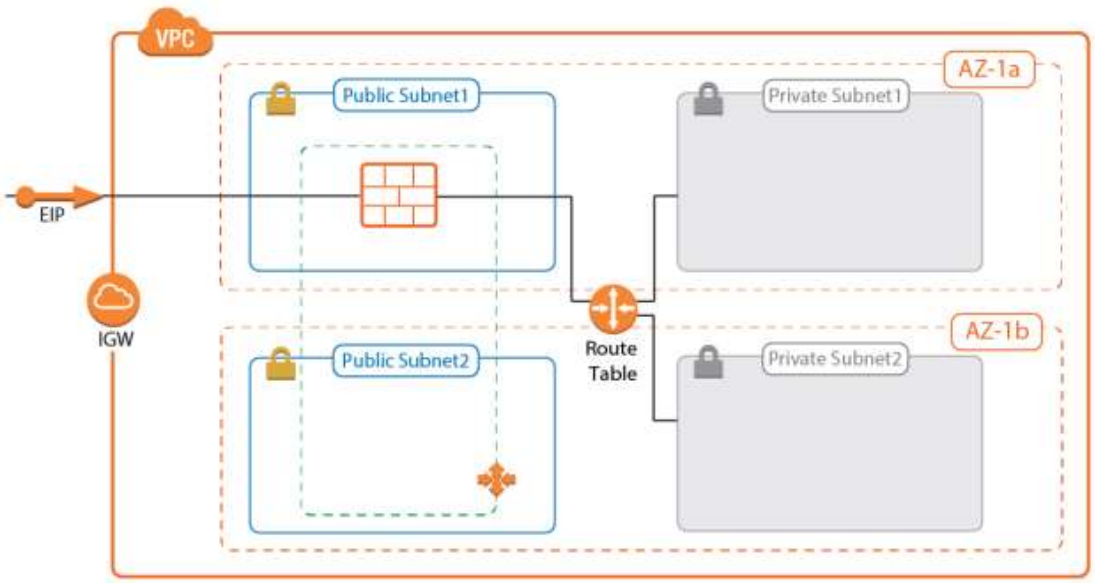


Рис.3.10. Кластер холодного резервування файрволу CloudGen

У разі, якщо файрвол стає недоступним, він автоматично замінюється. За замовчуванням підтримуються лише ліцензії PAYG. Однак можливо використовувати Центр управління файрволами для управління файрволом, що дозволяє використовувати пулові ліцензії BYOL. Кластер холодного резервування повинен бути розмірений так, щоб задовольнити піковий попит, оскільки він не масштабується динамічно.

Транзитний VPC. Для того, щоб хмарні нативні додатки повною мірою використовували можливості хмарної платформи AWS, кожен додаток розміщується у спеціалізованому VPC. Це дозволяє додатку бути логічним контекстом для сегментації.

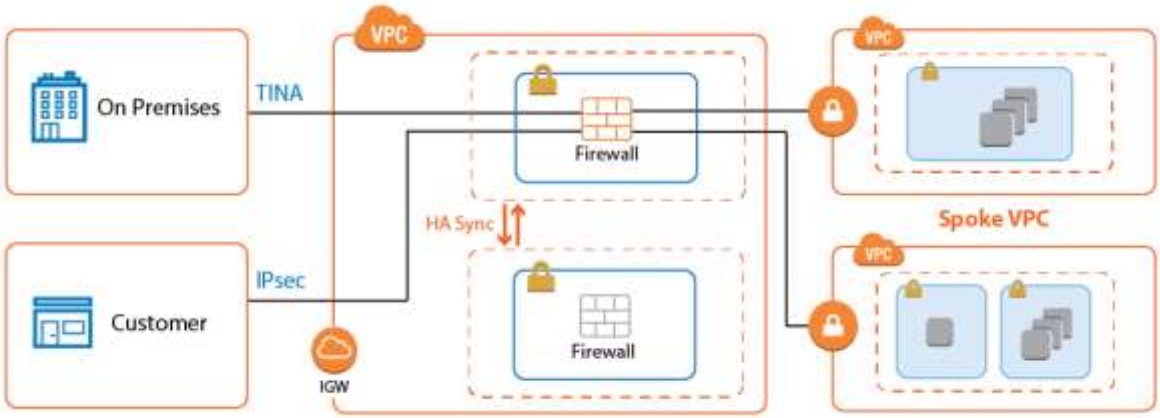


Рис.3.11. Транзитний VPC

Щоб організувати та забезпечити безпеку цих високодинамічних VPC, необхідно з'єднати їх у архітектурі хаба з кластером файрволу у центральному транзитному VPC. Архітектура транзитного VPC є дуже гнучкою: її можна комбінувати з кластерами високої доступності, кластерами холодного резервування або автомасштабувальними кластерами, залежно від навантаження та переважаючого випадку використання.

Стандартна конфігурація пакету OVA може бути недоречною для специфіки розгортання організації. У разі необхідності використання декількох мережевих інтерфейсів, іншого типу мережевого адаптера чи збільшення розміру віртуального диска, слід звернутися до інструмента Barracuda Firewall Install для створення спеціалізованих файлів конфігурації, щоб розгорнути файрвол Barracuda CloudGen Firewall Vx з індивідуальними налаштуваннями[26].

3.2. Алгоритм налаштування Barracuda CloudGen Firewall

Перед початком необхідно завантажити з порталу Barracuda наступні компоненти:

- ISO-образ файрволу Barracuda CloudGen Firewall Vx обраної версії. Існує лише один ISO для файрволу Barracuda CloudGen і Barracuda Firewall Control Center.
- Інструмент Barracuda Firewall Install для версії прошивки, яку необхідно встановити.
- Завантажити та встановити WinImage або аналогічний утиліта для створення образів гнучких дисків (flp).
- На ПК має бути встановлено Visual C++ Redistributable для Visual Studio 2012 для використання Barracuda Firewall Install.

Крок 1. Створення файлів конфігурації за допомогою Barracuda Firewall Install

Необхідно створити файли конфігурації за допомогою Barracuda Firewall Install. Запустити Barracuda Firewall Install, та обрати режим «Повний майстер» та натиснути «Далі» (рис.3.12).

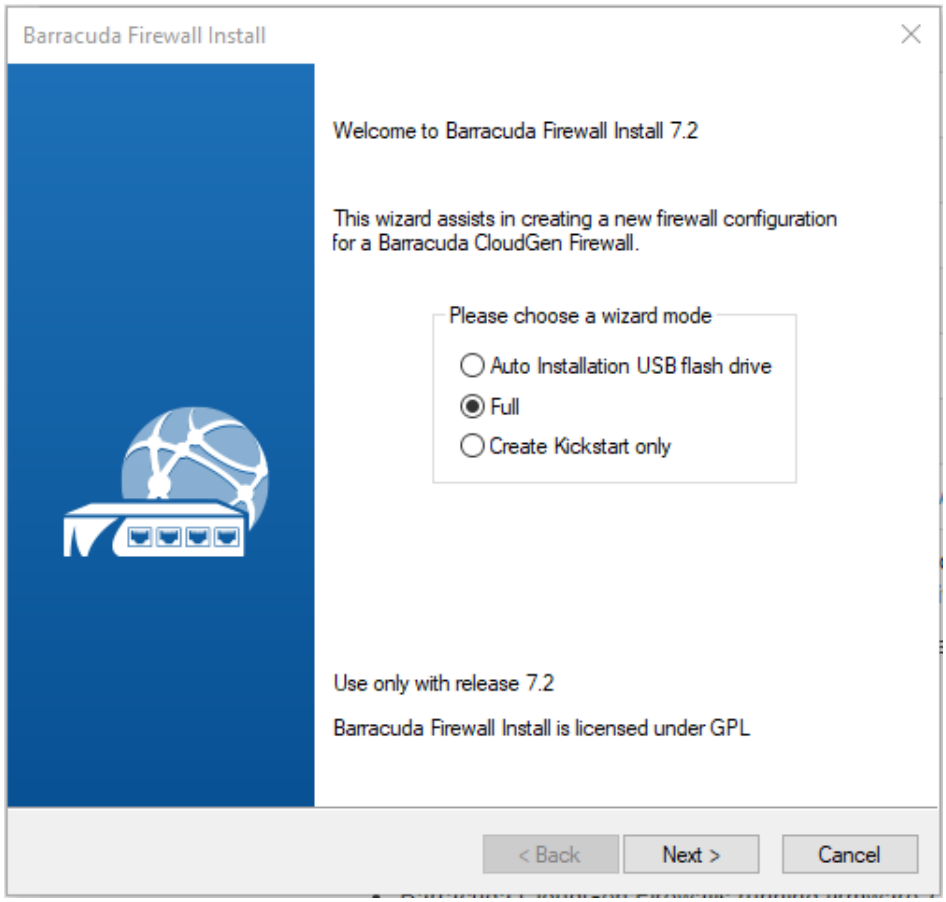


Рис.3.12. Перший крок налаштування Barracuda Firewall

Крок 2. На сторінці налаштувань типу пристрою необхідно обрати тип продукту та модель для віртуального обладнання. Можна налаштувати віртуальні складові Barracuda CloudGen та центри управління файрволом Barracuda. Після вибору необхідно натиснути «Далі» (рис.3.13).

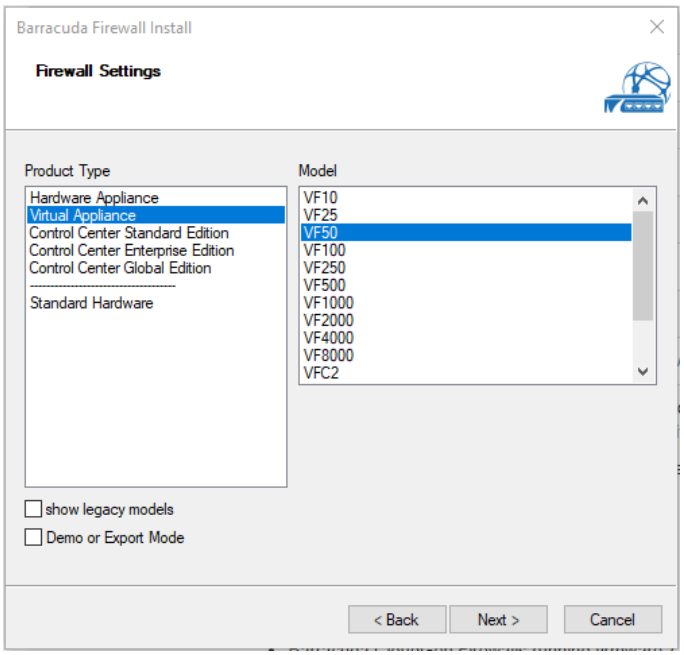


Рис.3.13. Вибір віртуальних компонентів

Крок 3. На сторінці налаштувань системи необхідно виконати наступні кроки:

- ввести ім'я хоста (наприклад, CloudGen Firewall VF50),
- обрати часовий пояс, в якому знаходиться обладнання,
- вибрати розкладку клавіатури для консолі файрволу Barracuda CloudGen Firewall Vx,
- ввести DNS-сервери мережі та домен, до якого належить обладнання,
- активувати NTP та ввести IP-адресу сервера NTP.

Натиснути «Далі».

Крок 4. На сторінці налаштувань розділів:

- для типу диска - необхідно обрати відповідний тип диска;
- для параметра «Зашифровано» - обрати чи потрібно щоб вміст жорсткого диска зберігався повністю зашифрованим чи ні (рис.3.14). Варіанти

будуть запропоновані наступні:

Зашифровано = Ні – Вся інформація на диску буде зберігатися незашифрованою.

Зашифровано = Так – Вся інформація на диску буде зберігатися у зашифрованому вигляді.

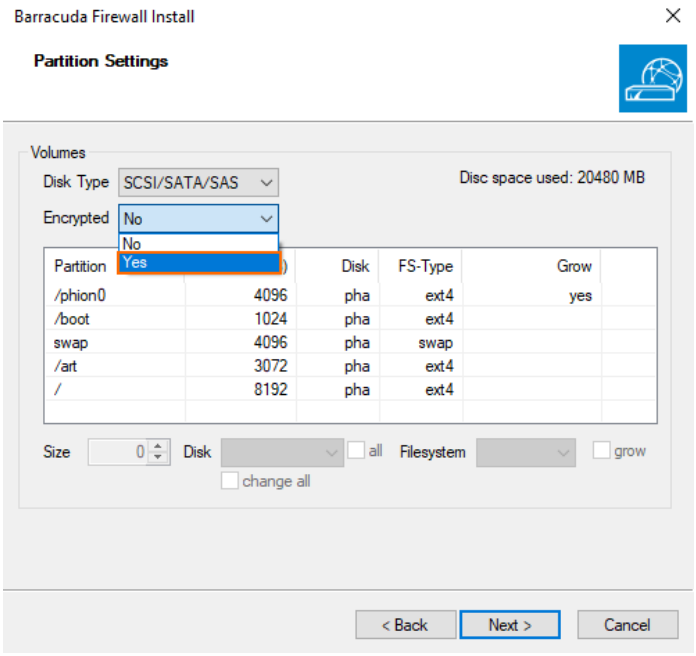


Рис.3.14. Вибір параметрів шифрування

Натиснути «Далі».

Крок 5. На сторінці налаштувань мережевого пристрою (рис.3.15):

Необхідно натиснути «Додати», а потім вказати наступні параметри у вікні списку NIC реселерів:

- Реселер – обрати «Віртуальний»;
- Мережевий адаптер – обрати автоматичний вибір драйвера.
- Кількість – обрати кількість мережевих інтерфейсів.

Процедура додає нові мережеві інтерфейси до віртуального обладнання. Вибір «Віртуальний» як реселера гарантує, що налаштування будуть оптимізовані для віртуального середовища.

Автоматичний вибір драйвера мережевого адаптера дозволяє системі самостійно визначити найкращий драйвер для використання. Вибір кількості

мережевих інтерфейсів дозволить налаштувати мережеве підключення відповідно до специфічних потреб системи організації. Після налаштувань необхідно натиснути «ОК».

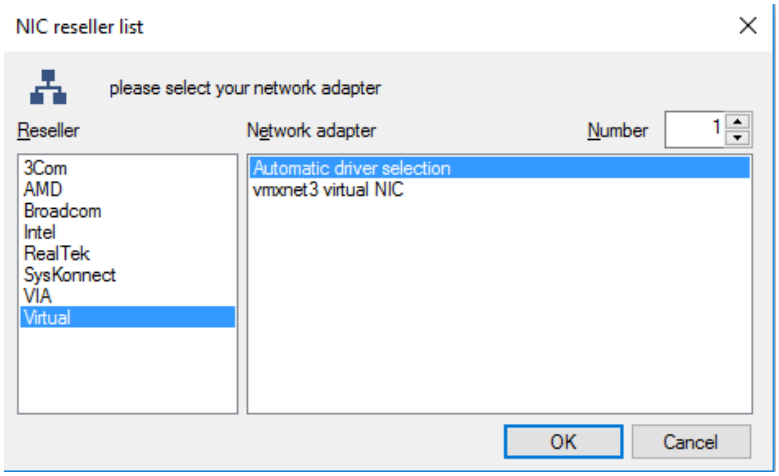


Рис.3.15. Налаштування мережевого пристрою

Крок 6. Необхідно обрати мережевий інтерфейс eth0 у таблиці мережевих адаптерів, а потім вказати наступні параметри у вікні конфігурації NIC адаптера (рис.3.16):

- Управлінська IP-адреса – необхідно ввести IP-адресу, яку потрібно використовувати як управлінську IP-адресу.
- Маска підмережі – необхідно ввести значення маски підмережі.
- Налаштувати додатковий маршрут до шлюзу (Необов'язково).

Ці кроки дозволяють встановити управлінську IP-адресу для первинного мережевого інтерфейсу eth0, яка буде використовуватися для керування апаратурою.

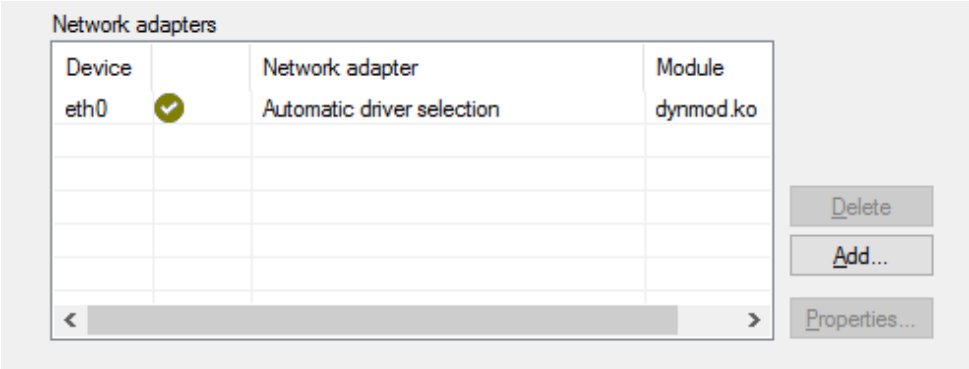


Рис.3.16. Вибір мережевого інтерфейсу eth0

Введення маски підмережі важливе для визначення мережі, до якої належить IP-адреса. Налаштування додаткового маршруту до шлюзу є необов'язковим, але це може бути корисним для забезпечення з'єднання обладнання з іншими мережами або мережею Інтернет(рис.3.17).

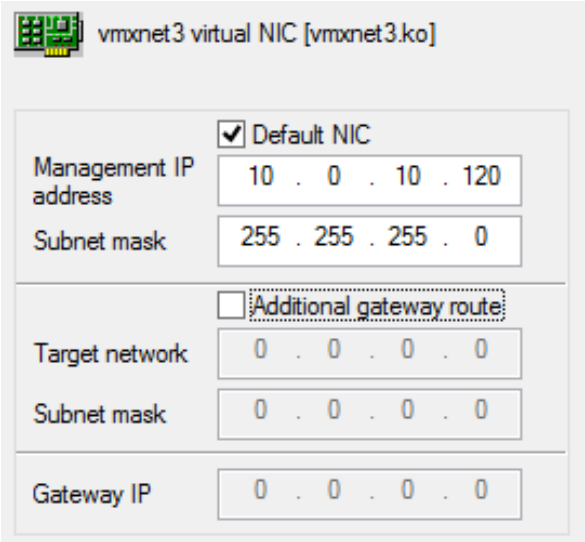


Рис.3.17. Введення маски підмережі

Крок 7. На сторінці налаштувань безпеки необхідно ввести пароль користувача та пароль для входу в сервіс (рис.3.18). Натиснути «Далі». З’явиться сторінка програмних пакетів. Залиите все без змін, та натиснути «Далі». На сторінці налаштувань скриптів необхідно ввести місце зберігання для файлів конфігурації у поле «Зберегти до». Цей процес включає встановлення основних параметрів безпеки для системи, зокрема створення надійного пароля, що є критично важливим для захисту мережевих ресурсів.

Вибір місця зберігання для файлів конфігурації дозволяє зберегти ці важливі дані у безпечному та доступному місці для майбутнього використання або оновлень. Натиснути «Далі» та «Завершити».

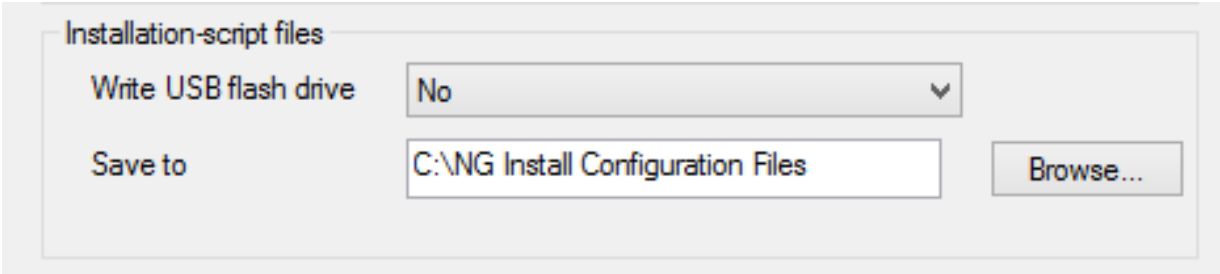


Рис.3.18. Нелаштування безпеки

Після створення файлів конфігурації з'явиться повідомлення, що підтверджує успішне записування файлів конфігурації (рис.3.19). Наступні файли конфігурації будуть створені в місці, яке було обрано.

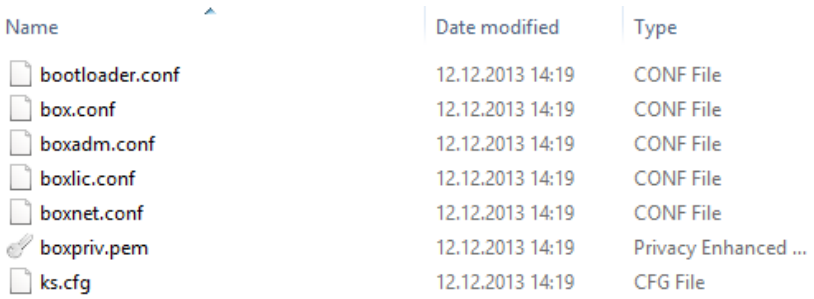


Рис.3.19. Збережені файли конфігурації

Крок 8. Створення образу гнучкого диска за допомогою WinImage.

Для цього, необхідно додати файли конфігурації, створені за допомогою Barracuda Firewall Install, до образу FLP-файлу гнучкого диска. Цей образ буде прикріплено до віртуальної машини VMware під час встановлення.

Запустити WinImage. Знайти файли конфігурації, які були створені за допомогою Barracuda Firewall Install. Обрати усі файли конфігурації Barracuda Firewall Install та перенести їх у вікно WinImage.

У вікні вибору формату необхідно зазначити «1.44 MB» зі списку стандартних форматів, та натиснути «OK» (рис.3.20).

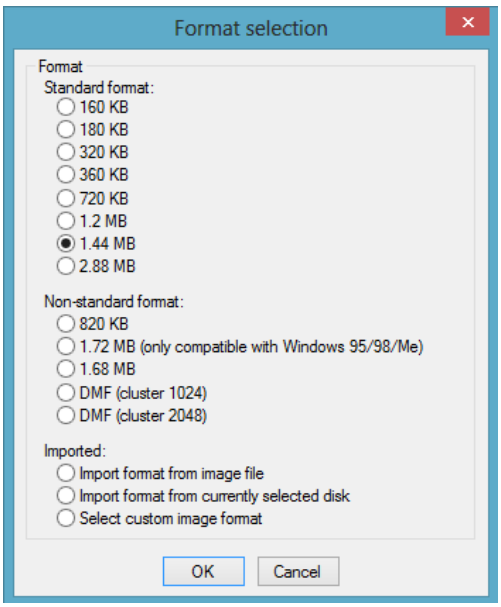


Рис.3.20. Список стандартних форматів

Ці дії дозволяють створити образ гнучкого диска з файлами конфігурації, необхідними для інсталяції файрволу на віртуальній машині. Образ гнучкого диска забезпечить необхідне середовище для запуску та налаштування віртуальної апаратури у VMware. У вікні «Inject» натиснути «Так» (рис.3.21). Натиснути на значок збереження, та «Зберегти як».

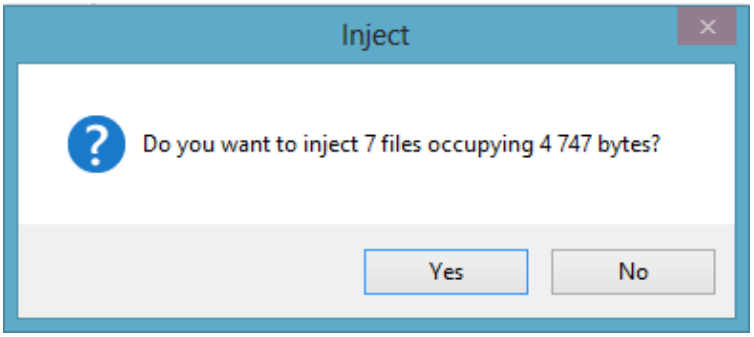


Рис.3.21. Внесення змін у вікно «Inject»

Крок 9. Обрати «Віртуальний образ гнучкого диска (.vfd,.flp)» у списку «Зберегти як тип», ввести назву файлу з розширенням .flp (наприклад, NGInstallFloppy.flp).

В іншому випадку WinImage збереже образ гнучкого диска з розширенням .vfd, яке не може бути використане гіпервізором VMware. Після чого, «Зберегти» (рис.3.22).

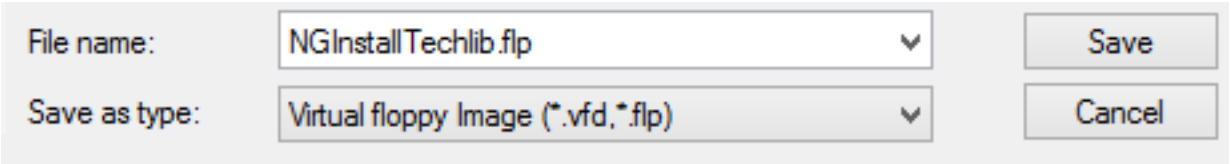


Рис.3.22. Збереження типу віртуального образу гнучкого диска

Крок 10. Створення нової віртуальної машини

На сервері VMware необхідно створити нову віртуальну машину для файрволу Barracuda CloudGen Firewall Vx. Використовуючи VMware vSphere Client, необхідно увійти у гіпервізор VMware та обрати «Нова віртуальна машина». Відкриється вікно «Створення нової віртуальної машини». У вікні «Конфігурація» бажано обрати «Типова» та натиснути «Далі» (рис.3.23).

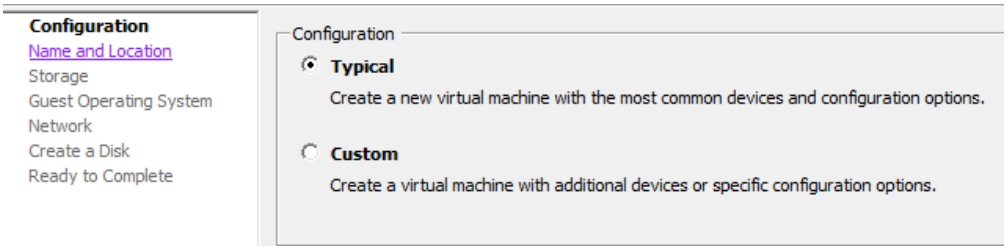


Рис.3.23. Створення нової віртуальної машини

На сторінці «Назва та місце розташування» необхідно ввести назву віртуальної машини (наприклад, BarracudaNGFirewallVF50) та натиснути «Далі».

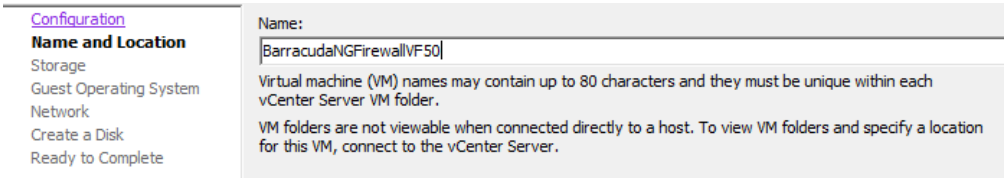


Рис.3.24. Сторінка «Назва та місце розташування»

На сторінці «Зберігання» необхідно обрати сховище даних, де має бути створений віртуальний диск. На сторінці «Операційна система гостя» необхідно обрати:

- Зі списку «Операційна система гостя» - «Linux».
- Зі списку «Версія» - «Інші 2.6.x Linux (64-біт)».

Натиснути «Далі».

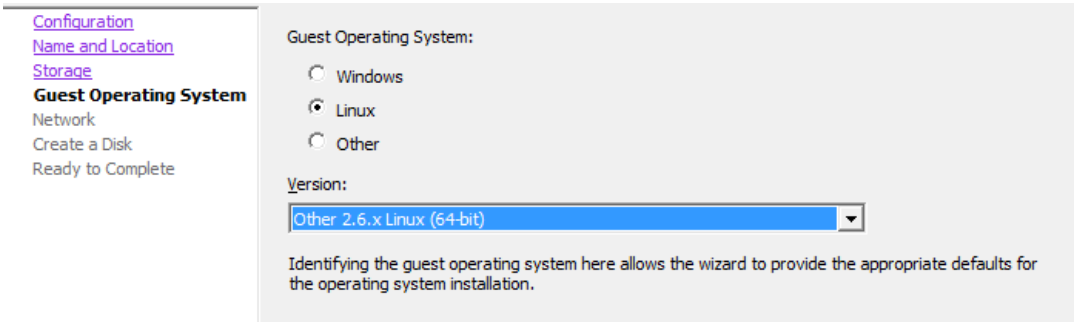


Рис.3.25. Вибір значень для ОС гостя

На сторінці «Мережа» необхідно обрати кількість мережевих інтерфейсів зі списку «Скільки NIC ви хочете підключити». Кількість має відповідати кількості

мережевих інтерфейсів, яку було обрано при створені файлів конфігурації за допомогою Barracuda Firewall Install.

У майстру «Створення нової віртуальної машини» можна додати лише чотири мережеві інтерфейси. Якщо потрібно більше чотирьох віртуальних мережевих інтерфейсів, можна додати додаткові NIC, редагуючи конфігурацію завершеної віртуальної машини. VMware обмежує кількість віртуальних мережевих інтерфейсів на гостьову ОС до 10[27].

Для кожного NIC необхідно вказати наступні параметри:

- Обрати віртуальну мережу, до якої підключатиметься віртуальний інтерфейс.
- Обрати VMXNET 3. Адаптер має відповідати конфігурації Barracuda Firewall Install. Barracuda Networks рекомендує використовувати драйвер VMXNET3.
- Необхыдно обрати пункт «Підключитися при включенні», щоб підключити NIC до віртуальної машини.

Рис.3.26. Налаштування мережі

На сторінці «Створення диска» необхідно: ввести розмір віртуального диска та обрати «Thick Provision Eager Zeroed». Натиснути «Далі».

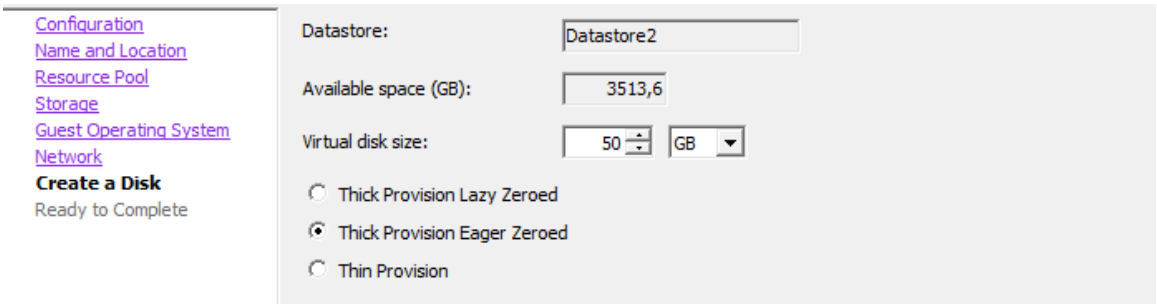


Рис.3.27. Налаштування для створення диску

На сторінці «Готово до завершення» необхідно натиснути «Завершити». Залежно від розміру віртуального диска, створення віртуальної машини може зайняти кілька хвилин. Спостерігати за статусом завдання можна в «Створення віртуальної машини» на панелі «Останні завдання» внизу вікна клієнта vSphere.

У вікні «Властивості віртуальної машини» необхідно налаштувати пам'ять та процесори відповідно до моделі файрволу Barracuda CloudGen Firewall Vx. Не бажано призначати віртуальній машині більше віртуальних процесорів, ніж дозволено в ліцензії.

Після цього, віртуальна машина відображатиметься в лівій панелі під сервером VMware, на якому її створили.

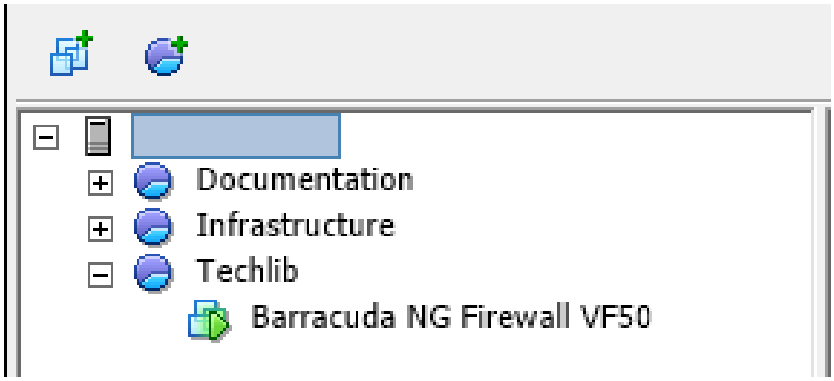


Рис.3.28. Відображенн віртуальної машини

Крок 11. Запуск віртуальної машини

ISO-образ файрволу Barracuda CloudGen Firewall Vx та образ гнучкого диска необхідно підключити до віртуальної машини для автоматизованої установки. Використовуючи VMware vSphere Client, необхідно увійти у гіпервізор VMware. Увімкнути віртуальну машину файрволу Barracuda CloudGen Firewall Vx.

У панелі задач натиснути на іконку CD ( ), обрати «CD/DVD Drive 1» та обрати «Підключитися до ISO-образу на локальному диску». Обрати файл ISO файрволу Barracuda CloudGen Firewall Vx на локальному жорсткому диску та натиснути «Відкрити». Натискаючи Ctrl + Alt + Ins ВМ буде перезавантажено.

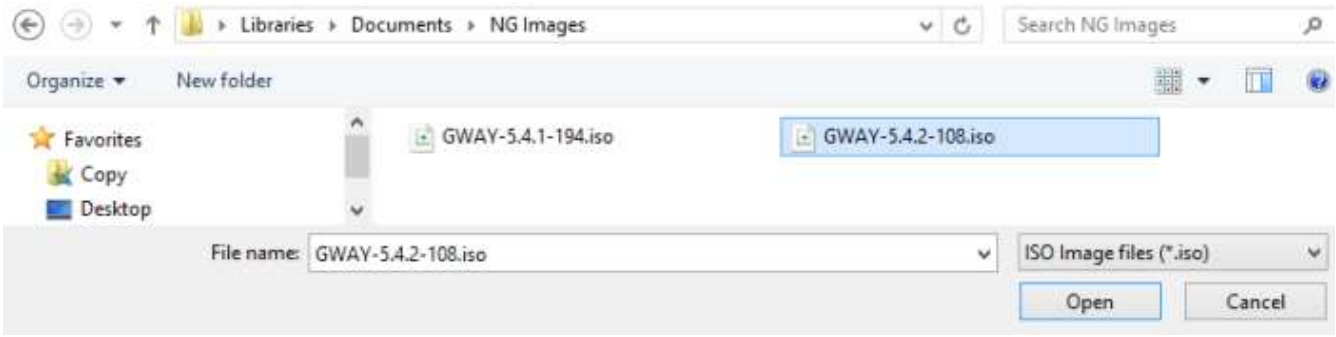


Рис.3.29. Відкриття файрволу Barracuda CloudGen Firewall

На вітальному екрані завантаження файрволу Barracuda CloudGen Firewall необхідно натиснути на будь-яку клавішу, крім <Enter>, щоб зупинити 10-секундний відлік.

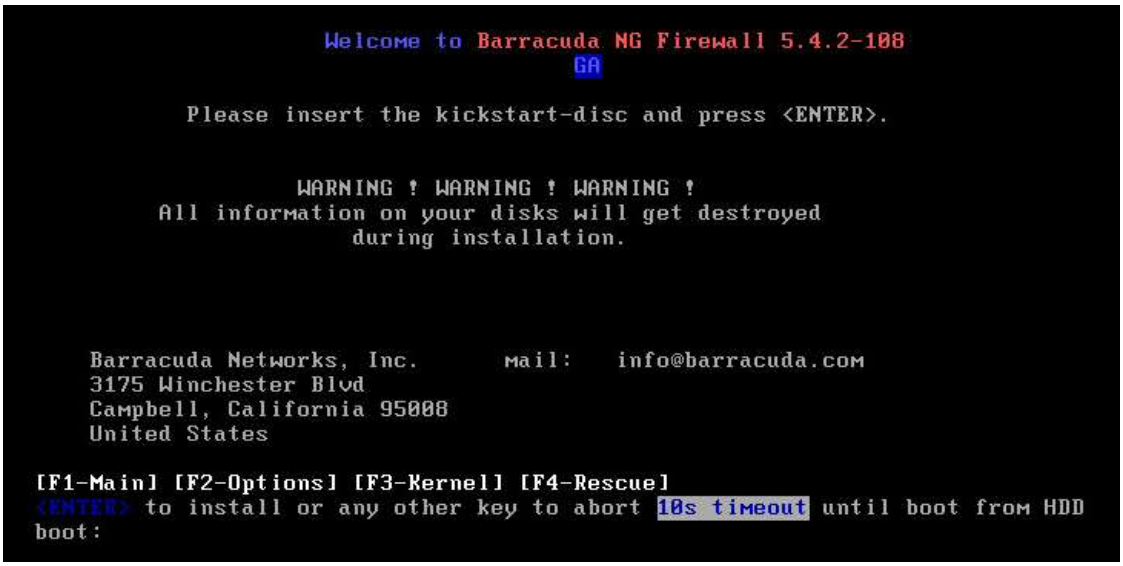


Рис.3.30. Вітальна сторінка завантаження файрволу Barracuda CloudGen Firewall

Ці дії дозволяють підготувати віртуальну машину до процесу установки файрволу, включаючи підключення необхідних медіа-ресурсів та перезавантаження системи для запуску установки. Зупинка відліку часу на екрані завантаження забезпечує можливість ручного втручання перед автоматичним запуском установки.

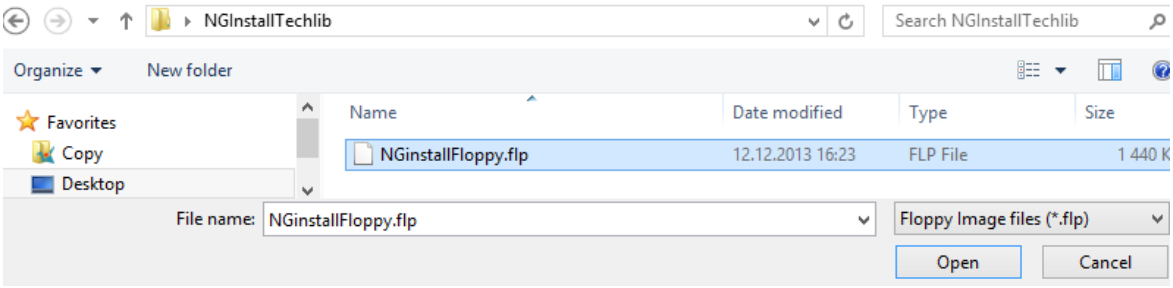


Рис.3.31. Збережений образ файрволу Barracuda CloudGen Firewall

Після натискання Enter, розпочнеться установку. Після завершення установки необхідно натиснути Enter для перезавантаження. Це дозволить запустити процес установки файрволу Barracuda CloudGen Firewall Vx на віртуальній машині. Після завершення установки, перезавантаження системи є важливим для того, щоб усі зміни та оновлення набули чинності та віртуальна машина готова була до використання[28].

Рис.3.32. Завершення налаштувань Barracuda CloudGen Firewall

3.3. Рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall

Для Barracuda CloudGen Firewall, який є ефективним рішенням для захисту корпоративних віртуальних робочих столів, доцільні наступні сценарії використання:

1. Застосування в індустріях з високими вимогами до безпеки - включає фінансові послуги, охорону здоров'я та урядові організації. Barracuda CloudGen Firewall забезпечує високий рівень безпеки для захисту конфіденційних даних і відповідає вимогам регулювання;

2. Еластичні робочі ресурси для віддаленої роботи та тимчасових проектів – забезпечує безпечний доступ до корпоративних ресурсів для підрядників, партнерів, та короткострокових співробітників.

3. Barracuda CloudGen Firewall може ефективно захищати дані, коли співробітники використовують особисті пристрої для доступу до корпоративних ресурсів (BYOD та мобільні користувачі).

4. Програми для проектування та розробки, застарілі програми, та тестування програмного забезпечення можуть отримати вигоду від високої безпеки та здібності Barracuda CloudGen Firewall до налаштування.

5. Персональні та загальні робочі столи:

- Barracuda CloudGen Firewall може забезпечити безпеку для персональних робочих столів, дозволяючи користувачам налаштовувати середовище та зберігати файли у безпечному класичному середовищі. Рішення може також призначити виділені ресурси для певних варіантів використання, наприклад, виробничих або розробницьких сценаріїв.

- Для не постійних робочих столів, Barracuda CloudGen Firewall забезпечує захист, управляючи алгоритмами балансування навантаження та обмежуючи доступ до адміністративних функцій, щоб запобігти несанкціонованому доступу або змінам у середовищі робочого столу.

6. Використання UTM може посилити безпеку, забезпечуючи функції, такі як антивірус, антишпигунське програмне забезпечення, фільтрація контенту та запобігання вторгненню (IPS).

7. Забезпечення динамічного контролю доступу залежно від ролі користувача, локації, і типу пристрою для підвищення безпеки.

8. Забезпечення шифрування всього трафіку між віртуальними робочими столами та серверами для захисту передачі даних.

Barracuda CloudGen Firewall забезпечує гнучкість та масштабованість, необхідні для підтримки різноманітних сценаріїв використання віртуальних

робочих столів, водночас підтримуючи високий рівень безпеки та конфіденційності.

Висновки до третього розділу

Досліджено можливості файрволу Barracuda CloudGen для безшовної інтеграції з хмарною платформою AWS, включаючи варіанти використання для крайового файрволу, захищеного віддаленого доступу, офісу до хмари, та гібридної хмари.

Проаналізовано різні сценарії використання файрволу Barracuda CloudGen, у тому числі забезпечення безпеки мережі, встановлення вихідного шлюзу для хмарних ресурсів та інтеграцію з системами VPN.

Розглянуто ключові функції файрволу нового покоління, які замінюють або розширюють рідні групи безпеки AWS та NACLs, включаючи захист від мережевих атак, сканування вірусів, контроль доступу на основі геолокації, формування трафіку для захисту бізнес-критичного трафіку.

Оцінено різні моделі розгортання файрволу Barracuda CloudGen, включаючи кластери високої доступності, холодного резервування та автомасштабування, з огляду на їхні переваги та обмеження.

Досліджено функціонал віддаленого доступу файрволу, що надає користувачам безпечний доступ до хмарних додатків та ресурсів організації з різних пристроїв.

Описано детальний алгоритм налаштування Barracuda CloudGen Firewall, включаючи створення файлів конфігурації, вибір обладнання та операційної системи, налаштування мережевих інтерфейсів та безпеки.

Розроблено рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall для захисту корпоративних віртуальних робочих столів, включаючи забезпечення безпеки в індустріях з високими вимогами до безпеки, еластичних робочих ресурсів для віддаленої роботи та тимчасових проектів.

ВИСНОВКИ

В кваліфікаційній роботі отримано наступні наукові та науково-практичні результати:

1. Досліджено хмарні сервіси та основні моделі організації, що включають архітектури IaaS, PaaS, SaaS.

2. Виокремлено проблеми безпеки в хмарних сервісах, зокрема ризики, пов'язані з незахищеними API, інсайдерськими загрозами, SQL-ін'єкціями, та загрозами автентифікації. Виявлено потенційні ризики, пов'язані з віртуалізацією в хмарних сервісах, та важливість захисту від атак на гіпервізор.

3. Досліджено можливості файрволу Barracuda CloudGen для безшовної інтеграції з хмарною платформою AWS.

4. Розглянуто ключові функції файрволу нового покоління, які замінюють або розширюють рідні групи безпеки AWS та NACLs, включаючи захист від мережевих атак, сканування вірусів, контроль доступу на основі геолокації, формування трафіку для захисту бізнес-критичного трафіку.

5. Оцінено різні моделі розгортання файрволу Barracuda CloudGen, включаючи кластери високої доступності, холодного резервування та автомасштабування, з огляду на їхні переваги та обмеження.

6. Досліджено функціонал віддаленого доступу файрволу, що надає користувачам безпечний доступ до хмарних додатків та ресурсів організації з різних пристроїв.

7. Описано детальний алгоритм налаштування Barracuda CloudGen Firewall, включаючи створення файлів конфігурації, вибір обладнання та операційної системи, налаштування мережевих інтерфейсів та безпеки.

8. Розроблено рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall для захисту корпоративних віртуальних робочих столів, включаючи забезпечення безпеки в індустріях з високими вимогами до безпеки, еластичних робочих ресурсів для віддаленої роботи та тимчасових проектів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cloud security. [Електронний ресурс] - Режим доступу: http://www.cloudsecurityandprivacy.com.

2. SaaS Vs. PaaS Vs. IaaS – An Ultimate Guide on When to Use What. [Електронний ресурс] - Режим доступу: https://www.linkedin.com/pulse/saas-vs-paas-iaas-ultimate-guide-when-use-what-sonia-patel

3. Cloud Security Report. Cybersecurity Insiders. [Електронний ресурс] - Режим доступу: https://www.isc2.org/Resource-Center/Reports/Cloud-Security-Report//media/44A81ED54571463997B1DDACE905665F.ashx

4. Aljumah A., Ahanger T.A. Cyber security threats, challenges and defence mechanisms in cloud computing. IET Communications. № 14(7). Pp.1185-1191. 2020.

5. U. Hoyer, H. Obel. Guide on SaaS vs PaaS and IaaS. [Електронний ресурс] - Режим доступу: https://www.linkedin.com/pulse/guide-saas-vs-paas-iaas-ulrik-hoyer-hansen-obel

6. L. Rodero-Merino, L.Vaquero, E.Caron, F.Desprez, A.Muresan. Building Safe PaaS Clouds: a Survey on Security in Multitenant Software Platforms. Computers and Security. vol. 31 (1). 2020.

7. Aljahdali H., Townend P., Xu J. Enhancing multi-tenancy security in the cloud IaaS model over public deployment. 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering. Pp. 385- 390. IEEE. 2013.

8. The CIA Principle. [Електронний ресурс] - Режим доступу: http://www.doc.ic.ac.uk/~ajs300/security/CIA.htm

9. D. Daniels. Identity Management Practices and Concerns in Enterprise Cloud Infrastructures. J- Gate Acad. J. Database.vol. II, no. 14. Pp. 2321–5518. 2013.

10. Amara N., Zhiqui H., Ali A. Cloud computing security threats and attacks with their mitigation techniques. 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). Pp.244-251. IEEE. 2017.

11. A Study on Secure File Storage in Cloud Computing using Cryptography. [Електронний ресурс] - Режим доступу: https://www.researchgate.net/profile/Thilina-Dharmakeerthi/publication/341508689_A_Study_on_Secure_File_Storage_in_Cloud_Computing_using_Cryptography_April_2020/links/5ec4d77e92851c11a877966c/A-Study-on-Secure-File-Storage-in-Cloud-Computing-using- Cryptography-April-2020.pdf

12. What is a Trojan Virus. [Електронний ресурс] - Режим доступу: www.imperva.com/learn/application-security/Trojans

13. Khalil S., Fernandez V., Fautrero V. Cloud impact on IT governance. 2016 IEEE 18th Conference on Business Informatics (CBI). Vol.1. Pp. 255-261. IEEE. 2016.

14. Buck K., D. Hanf. Cloud SLA Considerations for the Government Consumer. Cloud Computing. The MITRE Corporation. 2010

15. Duncan A. J., Creese S., Goldsmith, M. Insider attacks in cloud computing. 2012 IEEE 11th international conference on trust, security and privacy in computing and communications. Pp.857-862. IEEE. 2012.

16. Assets, Threats and Vulnerabilities: Discovery and Analysis. [Електронний ресурс] - Режим доступу: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/assets- threats-vulnerabilities-01-en.pdf.

17. BullGuard. A definition of malware. [Електронний ресурс] - Режим доступу: https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats

18. Amazon.com. Amazon Elastic Compute Cloud (Amazon EC2). [Електронний ресурс] - Режим доступу: http://aws.amazon.com/ec2.

19. Google. Security Whitepaper Google Apps Messaging and Collaboration Products.

20. What is Two Factor Authentication. [Електронний ресурс] - Режим доступу: https://www.securenvoy.com/two-factor-authentication/what-is-2fa.shtm

21. Megouache L., Zitouni A., Djoudi M. Ensuring user authentication and data integrity in multi-cloud environment. Human-centric Computing and Information Sciences. №10. Pp.1-20. 2020

22. B. Panja, B. Bhargava, S. Pati, D. Paul, L.T. Lilien, P. Meharia. Monitoring and Managing Cloud Computing Security using Denial of Service Bandwidth Allowance. Recent Patents on Computer Science, Vol. 6 (1).Pp. 73-81.2021.

23. Barracuda CloudGen Firewall. [Електронний ресурс] - Режим доступу: https://www.barracuda.com/products/network-protection/cloudgen-firewall

24. Chandrakala N., Rao B.T. Migration of Virtual Machine to improve the Security of Cloud Computing. International Journal of Electrical and Computer Engineering. №8(1). P.210. 2018.

25. G. Ateniese. Provable data possession at untrusted stores. 14th ACM Conf. on Computer and communications security. P. 598. 2017

26. O. Harfoushi, B. Alfawwaz, N.A.Ghatasheh, R.Obiedat, M.M.Abu-Faraj, H.Faris, Data Security Issues and Challenges in Cloud Computing: A Conceptual Analysis and Review. Commun. Netw. vol. 6 (1). Pp. 15–21. 2014.

27. Barracuda CloudGen Firewall [Електронний ресурс] - Режим доступу: https://softprom.com/ua/barracuda-cloudgen-firewall-ua

28. Web protection. [Електронний ресурс] - Режим доступу: https://www.barracuda.com/products/email-protection/web-security

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА
НА ТЕМУ:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ХМАРНИХ СЕРВІСАХ ОРГАНІЗАЦІЇ»

Виконав:
здобувач вищої освіти
групи БСДМ-61
ПРИБЛУДЮК Юрій

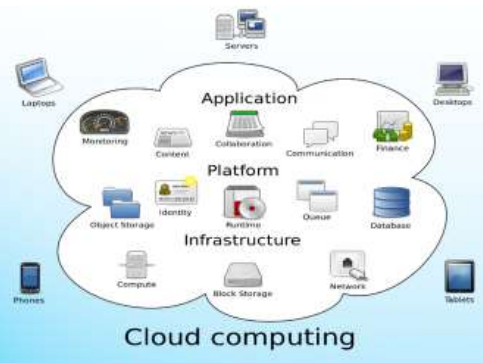
Керівник:
к.т.н, доцент кафедри
СОБЧУК Андрій

Київ 2024

- *Об'єкт дослідження* – процес безпечного функціонування хмарних сервісів організації.
- *Предмет дослідження* – механізми та засоби забезпечення безпеки даних в хмарних сервісах організації.
- *Мета роботи* – підвищення рівня інформаційної безпеки в організації шляхом впровадженню інтегрованих рішень для забезпечення безпеки хмарних сервісів.

Наукові завдання:
- проаналізувати особливості розгортання сучасних корпоративних мереж;
- проаналізувати підходи до забезпечення безпеки корпоративної мережі;
- дослідити мережеве обладнання для проєктування корпоративної мережі;
- дослідити налаштування рішень для безпечної роботи віддалених працівників в корпоративній мережі;
- розробити комплексне рішення для забезпечення безпеки підключення віддалених користувачів до ресурсів корпоративної мережі.

2



Моделі включають:
- **Інфраструктура як послуга (IaaS).**
- **Платформа як послуга (PaaS).**
- **Програмне забезпечення як послуга (SaaS).**

Рис.1. Моделі доставки хмарних сервісів

3

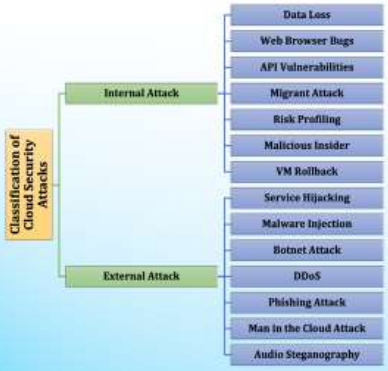


Рис.2.Класифікація проблем безпеки в хмарі

Рис.3. Методи зменшення та запобігання ризикам хмарних обчислень

Рис.4. Вхід до Amazon Console за допомогою ідентифікатора користувача

Рис.5. Використання коду для входу в Cloud Console

Варіанти інтеграції рішень Barracuda CloudGen Firewall

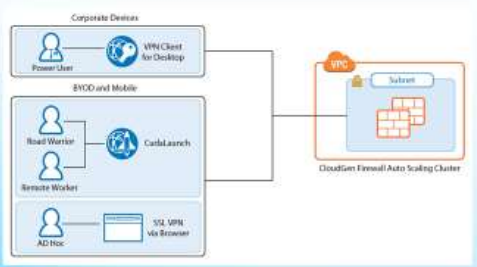


Рис.6. Кластер автомасштабування файрволу CloudGen

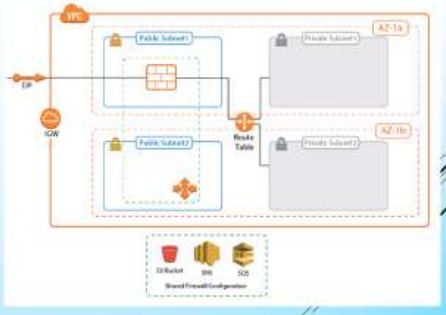


Рис.7. Кластер холодного резервування файрволу CloudGen

Варіанти інтеграції рішень Barracuda CloudGen Firewall

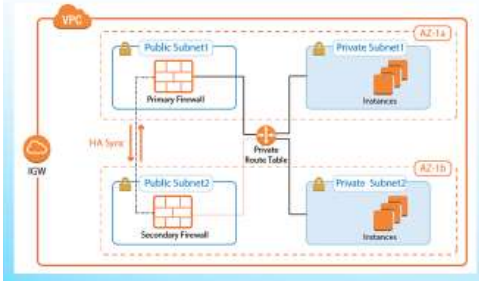


Рис.8. Кластер високої доступності файрволу CloudGen

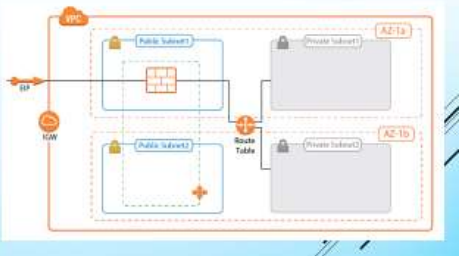


Рис.9. Кластер холодного резервування файрволу CloudGen

АЛГОРИТМ НАЛАШТУВАННЯ BARRACUDA CLOUDGEN FIREWALL

Рис.10. Перший крок налаштування Barracuda Firewall

Рис.11. Вибір віртуальних компонентів

АЛГОРИТМ НАЛАШТУВАННЯ BARRACUDA CLOUDGEN FIREWALL

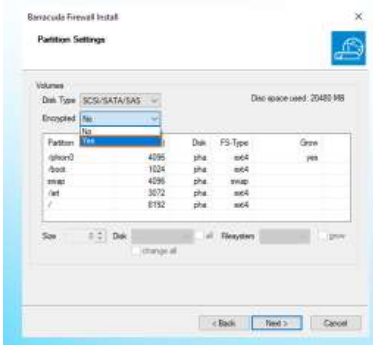


Рис.12. Вибір параметрів шифрування

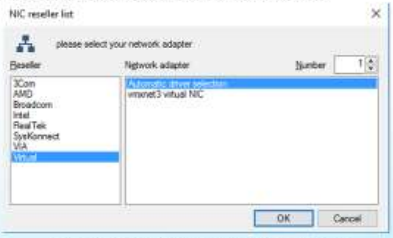


Рис.13. Налаштування мережевого пристрою

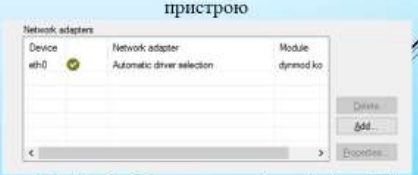


Рис.14. Вибір мережевого інтерфейсу eth0

АЛГОРИТМ НАЛАШТУВАННЯ BARRACUDA CLOUDGEN FIREWALL

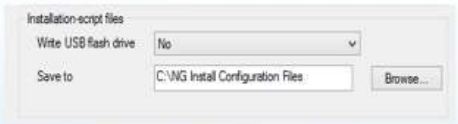


Рис.15. Нелаштування безпеки

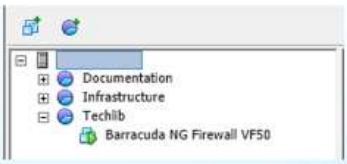


Рис.17. Відображення віртуальної машини

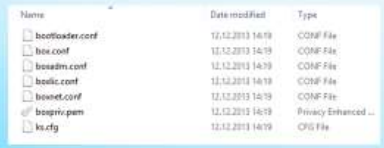


Рис.16. Збережені файли конфігурації

Рис.18. Вітальна сторінка завантаження файрволу Barracuda CloudGen Firewall

Рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall

1. Застосування в індустріях з високими вимогами до безпеки;
2. Еластичні робочі ресурси для віддаленої роботи та тимчасових проектів;
3. Barracuda CloudGen Firewall може ефективно захищати дані, коли співробітники використовують особисті пристрої для доступу до корпоративних ресурсів (BYOD та мобільні користувачі);
4. Програми для проектування та розробки, застарілі програми, та тестування програмного забезпечення можуть отримати вигоду від високої безпеки та здібності Barracuda CloudGen Firewall до налаштування;
5. Персональні та загальні робочі столи:

- Barracuda CloudGen Firewall може забезпечити безпеку для персональних робочих столів;
- Для не постійних робочих столів, Barracuda CloudGen Firewall забезпечує захист, управляючи алгоритмами балансування навантаження та обмежуючи доступ до адміністративних функцій;

6. Використання UTM може посилити безпеку, забезпечуючи функції, такі як антивірус, антишпигунське програмне забезпечення, фільтрація контенту та запобігання вторгненню (IPS);
7. Забезпечення динамічного контролю доступу залежно від ролі користувача, локації, і типу пристрою для підвищення безпеки;
8. Забезпечення шифрування всього трафіку між віртуальними робочими столами та серверами для захисту передачі даних.

Висновки:

- Досліджено хмарні сервіси та основні моделі організації, що включають архітектури IaaS, PaaS, SaaS.
- Виокремлено проблеми безпеки в хмарних сервісах, зокрема ризики, пов'язані з незахищеними API, інсайдерськими загрозами, SQL-ін'єкціями, та загрозами автентифікації. Виявлено потенційні ризики, пов'язані з віртуалізацією в хмарних сервісах, та важливість захисту від атак на гіпервізор.
- Досліджено можливості файрволу Barracuda CloudGen для безшовної інтеграції з хмарною платформою AWS.
- Розглянуто ключові функції файрволу нового покоління, які замінюють або розширюють рідні групи безпеки AWS та NACLs, включаючи захист від мережевих атак, сканування вірусів, контроль доступу на основі геолокації, формування трафіку для захисту бізнес-критичного трафіку.
- Оцінено різні моделі розгортання файрволу Barracuda CloudGen, включаючи кластери високої доступності, холодного резервування та автомасштабування, з огляду на їхні переваги та обмеження.
- Досліджено функціонал віддаленого доступу файрволу, що надає користувачам безпечний доступ до хмарних додатків та ресурсів організації з різних пристроїв.
- Описано детальний алгоритм налаштування Barracuda CloudGen Firewall, включаючи створення файлів конфігурації, вибір обладнання та операційної системи, налаштування мережевих інтерфейсів та безпеки.
- Розроблено рекомендації щодо сценаріїв використання Barracuda CloudGen Firewall для захисту корпоративних віртуальних робочих столів, включаючи забезпечення безпеки в індустріях з високими вимогами до безпеки, еластичних робочих ресурсів для віддаленої роботи та тимчасових проектів.