ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕЧНОГО ДОСТУПУ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН AZURE»

Виконав студент 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бойко М. М.
(прізвище та ініціали)
Керівник Собчук А. В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** ……. 12

1.1 Дослідження проблеми управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ ……..…….……. 12

1.2 Аналіз підходів до управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ ……..……... 20

1.3 Аналіз існуючих рішень щодо управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ …….……..…..... 25

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ В AZURE** ……. 31

2.1 Мережеві сервіси хмарної платформи Azure …….. 31

2.2 Призначення та основні функції віртуальної мережі Azure …….. 36

2.3 Призначення та архітектура сервісу Azure Bastion …… 39

3 **ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** ……...…….……. 44

3.1 Порядок розгортання Azure Bastion з налаштуваннями по замовчанню ……..… 44

3.2 Порядок організації віддаленої роботи з використанням мережевих сервісів Azure …….. 52

3.3 Рекомендації щодо управління доступом користувачів до віртуальних машин при застосуванні хмарних платформ …… 57

ВИСНОВКИ …….. 61

ПЕРЕЛІК ПОСИЛАНЬ 63

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 65

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

AWS – Amazon Web Services

BGP – Border Gateway Protocol

CDN – Content Delivery Network

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

GRE – Generic Routing Encapsulation

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

OWASP – Open Web Application Security Project

RDP – Remote Desktop Protocol

TCP – Transmission Control Protocol

VPS – Virtual Private Server

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Сьогодні організації широко використовують можливості хмарних платформ для розміщення в них своїх віртуальних машин. Серверне обладнання, гіпервізори та віртуальні машини піддаються кібератакам зловмисників для досягнення ними різних злочинних цілей, що ще більш загострює проблему забезпечення безпеки інформаційних ресурсів організацій.

Особливістю Microsoft Azure є те, що цю технологію можна швидко масштабувати відповідно до вимог організації, тому клієнт платить лише за фактичне використання платформи. Платформа Microsoft Azure ґрунтується на зростаючій глобальній мережі центрів обробки даних під керуванням Microsoft. Завдяки цьому клієнтам відкриваються можливості запуску додатків із високою продуктивністю для користувачів із різних точок світу.

Мережеві сервіси в Azure надають різноманітні мережеві можливості, які можна використовувати разом або окремо. Серед них є сервіси захисту додатків, які захищають інформаційні ресурси за допомогою як окремо, так і в комбінації цих мережевих сервісів в Azure – балансування навантаження, приватне посилання, захист від DDoS-атак, брандмауер, групи безпеки мережі, брандмауер веб-додатків, управління та захист кінцевих точок віртуальної мережі.

Azure Bastion – це сервіс, який дозволяє підключатися до віртуальної машини за допомогою браузера та порталу Azure або через рідний клієнт SSH або RDP, уже встановлений на локальному комп’ютері. Сервіс Azure Bastion – це повністю керований платформою сервіс PaaS, який застосовується у корпоративній віртуальній мережі. Він забезпечує безпечне та безперебійне підключення RDP/SSH до корпоративних віртуальних машин безпосередньо з порталу Azure через TLS.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ на прикладі Azure.

Об’єкт дослідження – управління доступом користувачів до віртуальних

машин організації при застосуванні хмарних платформ.

Предмет дослідження – технологія управління доступом користувачів до віртуальних машин організації в Azure.

Мета роботи – розробити порядок застосування технології управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ;

проаналізувати підходи до управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ;

проаналізувати існуючі рішення із управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ;

проаналізувати методи та засоби управління доступом користувачів до віртуальних машин організації в Azure;

розкрити порядок реалізації технології управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ [12].

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

1.1. Дослідження проблеми управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ

Хмарні сервіси так чи інакше використовують усі користувачі всесвітньої мережі, а технологія віртуалізації та віртуальні машини є зручними та гнучкими інструментами побудови обчислювальної інфраструктури для різних організацій. До переваг таких рішень відносять високий рівень безпеки, доступність, гнучкість і масштабованість, економічну ефективність, надання можливості працювати віддалено з будь-якої точки світу.

Можливість віддаленої роботи з корпоративними сервісами та доступ до віртуальної інфраструктури забезпечують сервіс-провайдери. Завдяки гнучкості, надійності та необмеженій продуктивності IaaS у віртуальне середовище потрапляють як пробні проекти, так і додатки для ведення та управління бізнесом.

Розглянемо переваги віртуальної інфраструктури. На відміну від фізичного сервера віртуалізація дозволяє простіше ставитися до питання планування ресурсів, її масштабування більш швидке, гнучке та дешеве. Якщо обчислювальної потужності фізичного сервера не вистачає, то цьому випадку змінюють або додають певні комплектуючі: жорсткий диск, оперативну пам'ять, процесор та інші компоненти обчислювальної системи. Жорсткий диск можна замінити, не вимикаючи живлення, а для заміни інших елементів потрібно вимикати обладнання.

Це тягне за собою простий сервер, збої в його роботі, невдоволення з боку керівництва та користувачів, так як на розбирання та складання сервера знадобиться чимало часу. Іноді пошук потрібних комплектуючих займає більше одного тижня, протягом якого система працює в режимі неповної потужності, що

призводить до збитків у компанії та падіння репутації.

Збільшити продуктивність віртуальної машини простіше та швидше. Хмарний провайдер постійно надає потрібний запас продуктивності, завдяки чому розширюються можливості віртуального сервера. Всі зміни можна змінити за кілька хвилин. Цей процес здійснюється за допомогою панелі керування без вимкнення або перезавантаження сервера. Такий підхід дозволяє модернізувати дуже точно, виділяючи строго необхідні ресурси. Необов'язково замінювати процесор, якщо вам знадобляться, наприклад, два обчислювальні ядра. А для того, щоб збільшити об'єм диска, достатньо додати віртуальній машині необхідний об'єм та не витрачати гроші на дорогий фізичний диск.

Крім того, віртуальні ресурси не вимагають обслуговування з боку клієнта – ремонт апаратної платформи займається хмарний провайдер. Він надає резервування обчислювальних потужностей, тому якщо сервер, на якому функціонує віртуальна машина, дав збій, то вона автоматично переводиться на інший, безперебійно працюючий. Щодо фізичного обладнання, то його модернізація менш гнучка, тому адміністратори створюють запаси обчислювальних ресурсів, які часто простоюють. Хмарний провайдер спочатку купує обладнання з надмірною продуктивністю, щоб розміщувати безліч віртуальних машин, тому клієнту не потрібно створювати запаси - він отримує ресурси на вимогу будь-якої миті.

Під час будівництва фізичної інфраструктури компанія заздалегідь має спланувати її потужність, якої має вистачити задоволення всіх потреб бізнесу. Не варто забувати, що вони з кожним роком збільшуються, тому потужність розраховується на кілька років вперед. Це призводить до низької утилізації ресурсів та матеріальних витрат на самому початку реалізації проекту, коли інфраструктура працює не на повну силу і чекає збільшення потреб бізнесу в майбутньому. Інакше висловлюючись, корисність фізичної інфраструктури низька майже протягом усього життєвого циклу. Також існує проблема старіння обладнання до того моменту, коли навантаження вийде на потужність, що проектується.

Віртуальні машини дозволяють виділяти ресурси за поточною потребою, а підвищити продуктивність можна за лічені хвилини, при цьому не потрібно відключати системи та послуги організації. Клієнтам не доводиться витрачати гроші на мегагерці, що опинилися незатребуваними, і гігабайти.

Рівень навантаження VPS становить близько 70%, а фізичні сервери завантажуються лише на 20%, хоча їх купують за повною ціною. Якщо послуги іноді піддаються критичним навантаженням, наприклад, у святкові дні, то краще додати ресурси саме цієї пори, а інші періоди урізати потужність VPS до середньої за статистикою навантаження. Необхідно пам'ятати у тому, що менше споживає ресурсів віртуальна машина, тим простіше здійснити резервування даних.

Хмарний провайдер проводить регулярне планове оновлення свого обладнання, а отже віртуальна машина завжди матиме найбільшу продуктивність. Також надання віртуальних ресурсів має не тільки високий ступінь масштабованості, а й варіативність – клієнт може замовити дискову підсистему сервера із звичайними магнітними дисками, а у разі недостатньої продуктивності виконати міграцію на твердотілі SSD. Використовуючи власну фізичну інфраструктуру, така заміна спричинить значні фінансові витрати.

Отже, переносячи свою IT-інфраструктуру в хмару провайдера, організаціям слід подумати лише про резервування конкретних сервісів, а не обчислювальних ресурсів. Наприклад, можна запустити паралельно на різних віртуальних машинах екземпляри баз даних, щоб у разі критичної зупинки одного з них робота сервісів тривала, але створювати запас обчислювальної потужності, як у випадку з фізичним обладнанням, не потрібно. Провайдер сам відповідає за надмірність та необмежену масштабованість, клієнту достатньо лише вчасно додавати своїм віртуальним серверам віртуальні ядра, віртуальну оперативну пам'ять та віртуальні диски.

Віртуальна машина (ВМ) – це програмний комп'ютер, який існує в операційній системі іншого комп'ютера і часто використовується для тестування, резервного копіювання даних або запуску додатків SaaS.

Хмарне середовище відноситься до серверів, доступ до яких здійснюється через Інтернет, а також до програмного забезпечення та баз даних, які працюють на цих серверах. Хмарні сервери розташовані у дата центрах по всьому світу. Користуючись хмарними обчисленнями, користувачі та компанії не повинні самі керувати фізичними серверами або запускати програмні засоби на своїх комп'ютерах.

Хмара дозволяє користувачам отримувати доступ до тих самих файлів і програм практично з будь-якого пристрою, оскільки обчислення та зберігання відбуваються на серверах у центрі обробки даних, а не локально на пристрої. Ось чому користувач може увійти до свого облікового запису Instagram на новому телефоні після перерви в роботі старого телефону і, як і раніше, знаходити свій старий обліковий запис з усіма своїми фотографіями, відео та історією розмов. Він працює також із постачальниками хмарної електронної пошти, такими як Gmail або Microsoft Office 365, та з постачальниками хмарних сховищ, такими як Dropbox або Google Drive.

Для організацій перехід на хмарні обчислення усуває деякі витрати на IT та накладні витрати: наприклад, їм більше не потрібно оновлювати та обслуговувати власні сервери, оскільки постачальник хмарних обчислень зробить це. Це особливо позначається на малих підприємствах, які, можливо, не змогли дозволити собі власну внутрішню інфраструктуру, але за доступними цінами можуть передати свої потреби в інфраструктурі через хмару. Хмара також може спростити роботу компаній на міжнародному рівні, оскільки співробітники та клієнти можуть отримувати доступ до тих самих файлів і додатків з будь-якого місця.

Декілька хмарних провайдерів пропонують віртуальні машини своїм клієнтам. Ці віртуальні машини зазвичай функціонують на потужних серверах, які можуть виступати як хост для кількох віртуальних машин і можуть використовуватися з різних причин, які не будуть практичними з локальною віртуальною машиною. Це включає:

запуск програм SaaS. Програмне забезпечення як послуга є хмарним

методом надання програмного забезпечення користувачам. Користувачі SaaS підписуються на додаток, а не купують її один раз і встановлюють. Ці додатки зазвичай надаються користувачеві через Інтернет. Часто саме віртуальні машини в хмарі виконують обчислення для SaaS, а також доставляють їх користувачам. Якщо хмарний провайдер має географічно розподілений кордон мережі, то додаток буде працювати ближче до користувача, що призведе до більш високої продуктивності;

резервне копіювання даних. Хмарні послуги віртуальних машин дуже популярні для резервного копіювання даних, оскільки до них можна отримати доступ з будь-якого місця. Крім того, хмарні віртуальні машини забезпечують кращу надмірність, вимагають меншого обслуговування та в цілому масштабуються краще, ніж фізичні центри обробки даних. Наприклад, зазвичай досить просто купити додатковий гігабайт дискового простору у постачальника віртуальних хмарних машин, але набагато складніше побудувати новий локальний сервер даних для цього додаткового гігабайта даних;

послуги хостингу, такі як електронна пошта та керування доступом. Розміщення цих сервісів на хмарних віртуальних машинах зазвичай швидше і економічніше, а також допомагає мінімізувати проблеми, пов'язані з обслуговуванням і безпекою.

За даними Fortinet [7] більшість організацій продовжують використовувати гібридну (39%, порівняно з 36% минулого року) або багатохмарну стратегію (33%) для інтеграції кількох служб для масштабування або для забезпечення безперервності бізнесу. Сімдесят шість відсотків використовують два або більше хмарних провайдерів.

Організації продовжують швидкими темпами переносити робочі навантаження в хмару. Сьогодні 39% респондентів мають більше половини робочого навантаження в хмарі, а 58% планують вийти на цей рівень у найближчі 12-18 місяців [7].

Користувачі хмари підтверджують, що хмара забезпечує гнучку пропускну здатність і масштабованість (53%), підвищену гнучкість (50%) і покращену

доступність і безперервність бізнесу (45%) [7].

Необхідно зауважити, що фахівці з безпеки відзначають недостатню видимість (49%), високу вартість (43%), відсутність контролю (42%) і відсутність безпеки (22%) як найбільші непередбачені фактори, які сповільнюють або зупиняють впровадження хмари. Хмарна безпека продовжує бути серйозною проблемою для фахівців з кібербезпеки. Зі збільшенням на два відсоткові пункти порівняно з минулим роком 95% організацій помірно або надзвичайно стурбовані станом безпеки в публічному хмарному середовищі [7].

Понад три чверті (78%) респондентів вважають дуже чи надзвичайно корисним мати *єдину хмарну платформу безпеки* з єдиною інформаційною панеллю для постійного та всебічного захисту даних у всій хмарі.

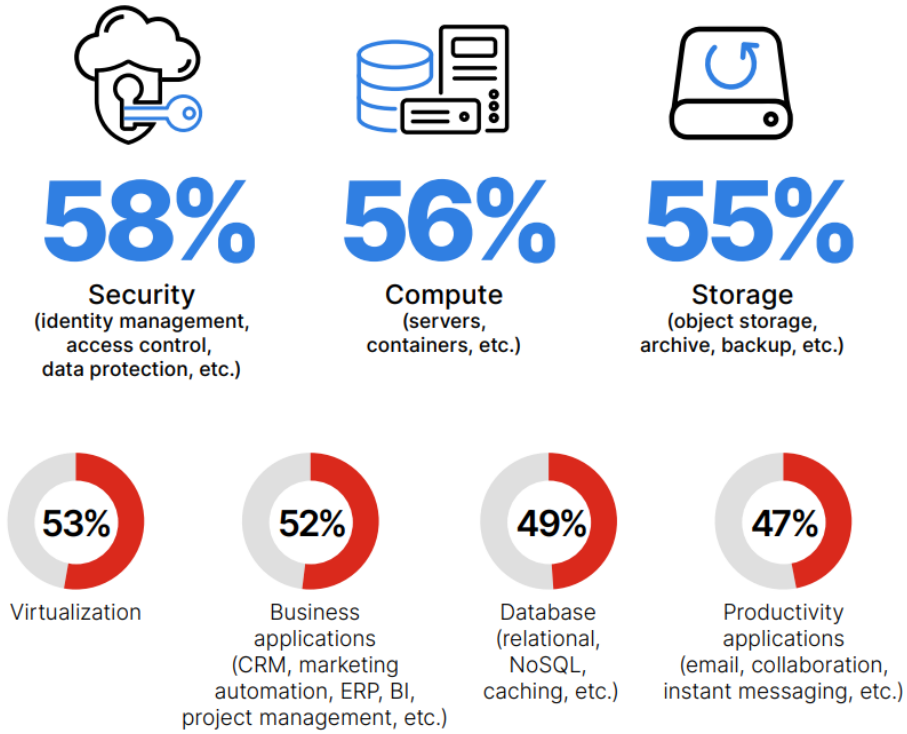

Рис. 1.1. Сервіси та робочі навантаження, які організації розгортають в хмарі [7]

Найпопулярніші хмарні провайдери, Microsoft Azure та Amazon Web Services (AWS), мають однакові показники (73%), оскільки AWS набрала три відсоткові пункти з минулорічного опитування. Далі йде Google Cloud Platform (38%). З року в рік найбільше зросло використання Oracle Cloud (з 15% до 21%) (рис. 1.1) [7].

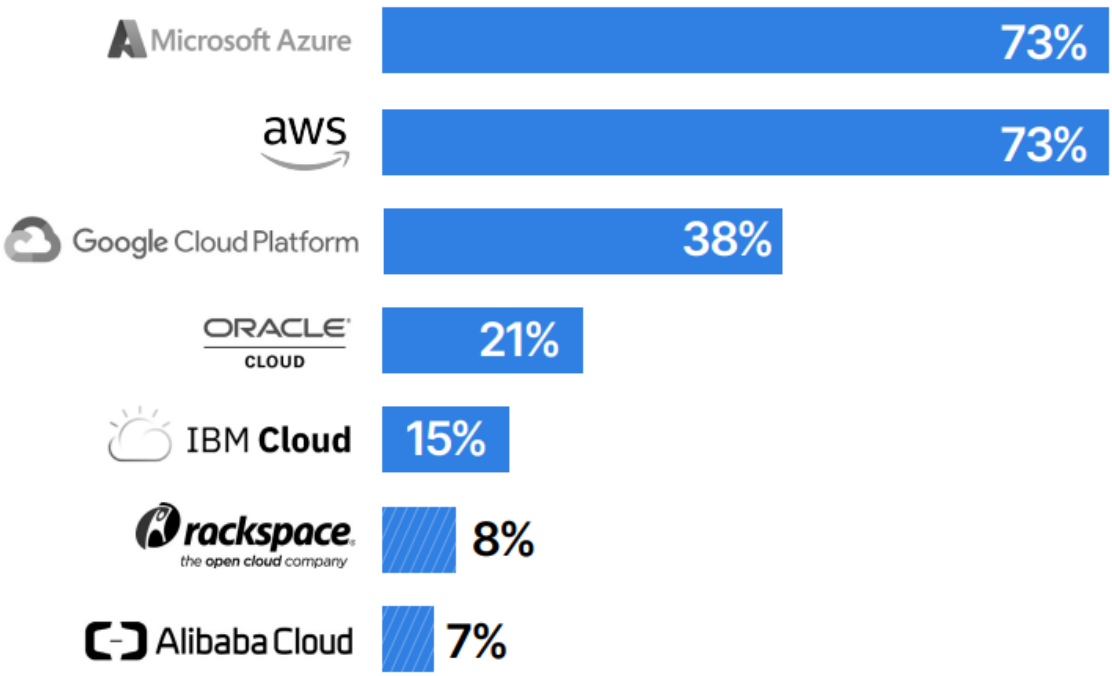

Рис. 1.2. Найпопулярніші хмарні провайдери [7]

Хмарна безпека продовжує бути серйозною проблемою для фахівців з кібербезпеки. Зі збільшенням на два відсоткові пункти порівняно з минулим роком 95% організацій помірно або надзвичайно стурбовані станом безпеки в публічному хмарному середовищі [7].

Фахівці з кібербезпеки визначили загрози хмарній безпеці, які їх найбільше хвилюють. Неправильна конфігурація хмарної платформи залишається найбільшим ризиком безпеки хмари, згідно з 62% фахівців з кібербезпеки в нашому опитуванні. Далі йдуть незахищені інтерфейси/API (52%, порівняно з 49% минулого року), викрадання конфіденційних даних (51%) і неавторизований доступ (50%) (рис. 1.3) [7].

Відповідаючи на питання про пріоритети безпеки на поточний рік, організації підкреслили запобігання неправильним конфігураціям хмари (20%), досягнення нормативної відповідності (19%), захист хмарних додатків (16%) і захист від зловмисного програмного забезпечення (15%).

Фахівці з безпеки шукають шляхи покращення безпеки публічних хмар. Коли запитали, які елементи керування підвищать їхню впевненість у прийнятті

хмарних служб, три елементи керування очолюють список: шифрування даних у стані спокою (54%), автоматизація відповідності (46%), а також налаштування та застосування політик безпеки (46%) [7].

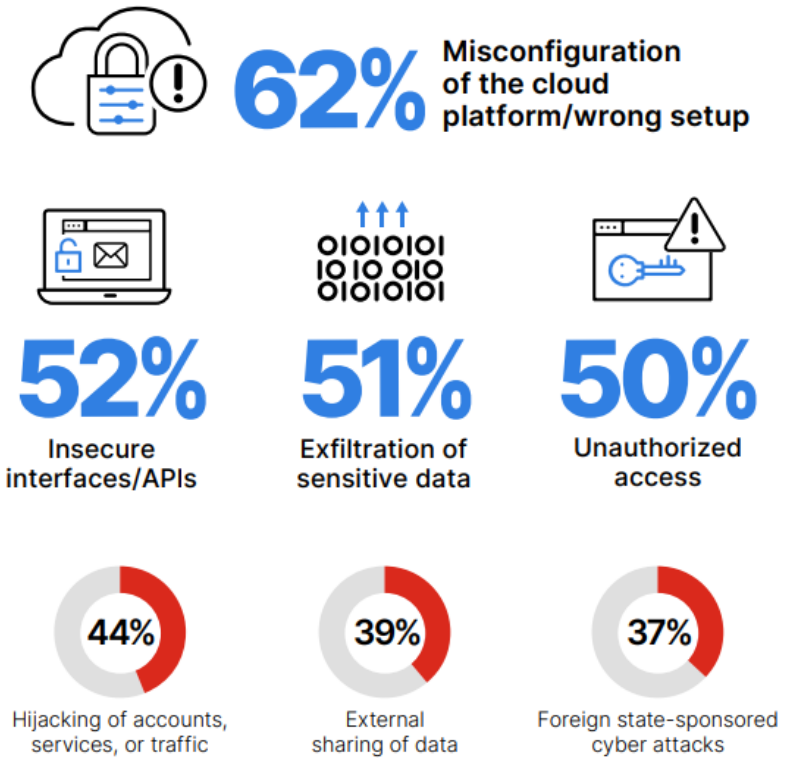

Рис. 1.3. Найбільші загрози хмарній безпеці за даними [7]

Багатохмарні середовища продовжують ускладнювати роботу та створювати проблеми з безпекою. Нестача навичок безпеки стає головною проблемою (61% порівняно з 57% минулого року), потім слідує захист даних (53%), розуміння того, як різні рішення поєднуються один з одним (51%), і втрата видимості та контролю (47) %) [7].

Організації віддають перевагу декільком критичним факторам для розгляду хмарних рішень безпеки над застарілими платформами. Найбільшими факторами є краща масштабованість (55%) і швидший час розгортання (50%), за якими йдуть економія коштів (43%) і краща видимість активності користувачів і поведінки системи (40%) [7].

1.2. Аналіз підходів до управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ

Віртуалізація швидко розвивається та стає необхідною частиною стратегій хмарної безпеки. Все більше організацій у всьому світі впроваджуватимуть інструменти віртуалізації для забезпечення своїх вимог до даних. В останні роки інфраструктура віртуальних машин була найпоширенішою потужною технологією, незважаючи на пов'язані з цим ризики, такі як атаки типу «людина посередині» та DDoS-атаки.

У міру того, як кіберзлочинці стають все більш витонченими, інструменти безпеки розвиваються одночасно з технологією віртуалізації, що дозволяє ізолювати операційну систему та підвищувати безпеку. Це зробило віртуалізацію найкращим підходом до хмарної безпеки, допомагаючи організаціям забезпечувати безпеку конфіденційної інформації [8].

Організації використовують віртуальні машини декількома способами підвищення своєї хмарної безпеки, включаючи віртуалізацію операційної системи, віртуалізацію додатків та інфраструктуру віртуальних робочих столів. У той час як останні два рішення торкаються лише невеликої частини множини вразливостей, віртуалізація операційної системи усуває проблеми безпеки у хмарі, властиві програмному забезпеченню для віртуалізації додатків та VDI [8].

Віртуалізація операційної системи дозволяє організаціям захищати критично важливу інформацію від будь-якого напряму атаки. Крім того, на відміну від інших підходів, він забезпечує їм досягнення результатів, очікуваних та необхідних від професіоналів. Завдяки цьому кінцеві користувачі додатків можуть встановлювати, працювати та отримувати доступ до ресурсів у міру потреби, без бар'єрів безпеки та не турбуючись про компрометацію конфіденційних даних.

Застосовуючи віртуалізацію у своєму хмарному середовищі організації можуть реалізувати наступні переваги безпеки [8]:

1. Гнучкість. Організації мають гнучкість для спільного використання

систем без необхідності обміну важливою інформацією або даними між системами.

2. Захист даних. Вони можуть запобігти втраті або пошкодженню важливих даних у випадках, коли система скомпрометована через зловмисні дії.

3. Захист від атак. Вони мають можливість знизити ризик множинних атак у разі розкриття, методично ізолюючи додатки та віртуальні машини.

4. Економічна ефективність. Це підвищує фізичну безпеку організацій за рахунок зниження вимог до обладнання, що призводить до меншої кількості центрів обробки даних.

5. Поліпшений контроль доступу. Системним та мережним адміністраторам пропонується більш високий рівень контролю доступу, що розділяє обов'язки та підвищує ефективність системи.

Ключовим міркуванням, яке повинні враховувати організації, є те, що їхня система має бути відповідним чином налаштована або налаштована для ефективного використання віртуалізації для забезпечення хмарної безпеки. Сучасні організації повинні захищати свої віртуальні середовища від зростаючої кількості загроз.

Деякі з ключових міркувань захисту віртуального середовища включають оновлення програмного забезпечення, дотримання передових методів налаштування та використання антивірусного програмного забезпечення. Незважаючи на те, що певний ризик загроз зберігається навіть при використанні деяких засобів захисту, для організацій важливо запровадити інструменти безпеки для відстеження змін та забезпечення безпеки пропускної спроможності.

Віртуалізація – це життєздатне рішення для організацій, які зосереджені на посиленні своєї хмарної безпеки. Щоб забезпечити надійний захист, необхідно впровадити та ретельно дотримуватися багаторівневого захисту. Організаціям необхідно виробити стратегію, краще підготуватися та зрозуміти, як вирішувати проблеми безпеки у віртуальній інфраструктурі та її компонентах. Віртуалізація має бути головним пріоритетом, а не другорядним завданням для організацій, які прагнуть посилити свою безпеку хмар [8].

Безпека віртуальної мережі є найгіршою проблемою з усіх, оскільки вона поєднує проблеми, створені традиційним хостингом і безпекою додатків, із проблемами безпеки мережі, а потім додає проблеми віртуальних ресурсів і сервісів [9].

У випадку хмарно-віртуальної безпеки для мереж найбільшою відмінністю є відображення віртуальних ресурсів, тобто структура, необхідна для підключення розміщених компонентів. Коротше кажучи, проблеми з безпекою хмарних віртуальних сервісів виникають через те, що інструменти безпеки, призначені для захисту функцій розміщеного програмного забезпечення, відрізняються від тих, що захищають фізичні пристрої.

Першим кроком у забезпеченні безпеки віртуальної машини в хмарних обчисленнях є ізоляція нових розміщених елементів. Наприклад, припустімо, що три функції, розміщені в периферійному пристрої, можна розгорнути в хмарі або як частину площини даних служби, з адресами, видимими для користувачів мережі, або як частину приватної підмережі, яка є невидимою. Якщо ви розгортаєте в хмарі, то будь-яку функцію можна атакувати, а також можливо, що ваші процеси хостингу та керування стануть видимими та вразливими. Якщо ви ізолюєте підключення до хостингу та функцій у приватній підмережі, вони захищені від зовнішнього доступу [9].

Сьогодні в контейнерному хостингу, як у центрі обробки даних, так і в хмарі, компоненти додатків розгортаються всередині приватної підмережі. У результаті відкриваються лише адреси, що представляють API, до яких користувачі мають отримати доступ. Той самий принцип потрібно застосовувати до віртуальних функцій; розкрити інтерфейси, до яких користувачі фактично підключаються, і приховати решту за допомогою захищених адрес.

Другий крок у хмарно-віртуальній безпеці – це сертифікація віртуальних функцій і функцій на відповідність вимогам безпеки, перш ніж ви дозволите їх розгортати. Зовнішні атаки є реальним ризиком у віртуальних мережах, але внутрішня атака є катастрофою. Якщо в сервіс вводиться функція з бекдорною помилкою безпеки, вона стає частиною інфраструктури сервісу та з більшою

ймовірністю матиме відкриті вектори атак на інші елементи інфраструктури [9].

Приватні підмережі можуть допомогти у вирішенні питань безпеки віртуальних машин у хмарних обчисленнях. Якщо нові компоненти можуть отримати доступ лише до інших компонентів у тому самому екземплярі служби, зменшується ризик того, що зловмисне програмне забезпечення може бути введено в нову функцію, розміщену на сервері програмного забезпечення. Так, бекдор-атака може поставити під загрозу сам сервіс, але менш імовірно, що зловмисне програмне забезпечення поширюється на інші сервіси та клієнтів [9].

Важливо наполягати на чіткому процесі управління життєвим циклом для всіх розміщених функцій і функцій, які оператори можуть перевіряти та контролювати. Якщо компанії, які постачають ваші розміщені функції або функції, належним чином перевірять свій новий код, менш імовірно, що він міститиме випадкові вразливості або навмисно введені бекдори.

Третій крок полягає в тому, щоб відокремити управління і оркестровку інфраструктурою від сервісу. API керування завжди становлять серйозний ризик, оскільки вони розроблені для контролю функцій, функцій і поведінки сервісу. Важливо захистити всі такі API, але критично важливо захистити API, які контролюють елементи інфраструктури, до яких користувачі сервісу ніколи не повинні мати доступу.

Найважливішою областю, яку слід вивчити для забезпечення безпеки віртуальних машин у хмарних обчисленнях, є специфічна для віртуальних функцій частина структури диспетчера віртуальних мережевих функцій (Virtual Network Functions Manager, VNFM), затверджена групою галузевих специфікацій ETSI NFV (Network Functions Virtualization). Цей код надається постачальником VNF, і він, ймовірно, потребуватиме доступу до API, які представляють елементи інфраструктури, а також оркестровки або інструментів розгортання. Ці елементи не потребують нічого, крім поганого дизайну, щоб відкрити шлюз до API керування інфраструктурою, що може вплинути на безпеку та стабільність функцій, що використовуються у віртуальних хмарних службах [9].

Захист VNFM означає вимогу, щоб постачальники VNF пропонували свої

архітектури, що керують підключеннями VNFM до інфраструктури або API розгортання/керування, для перегляду та можливих покращень безпеки. Важливо переконатися, що жоден користувач служби, VNF або VNFM, пов’язаний з іншими VNF або сервісами, не зможе отримати доступ до API керування інфраструктурою.

Обмежуючи доступ, ви обмежуєте ризик для безпеки. Крім того, оператори повинні вимагати, щоб доступ до API керування інфраструктурою та оркестрування з будь-якого джерела реєструвався, а будь-який доступ або зміни переглядалися, щоб запобігти витоку доступу до керування.

Четвертий і останній пункт безпеки віртуальної хмарної мережі полягає в тому, щоб віртуальні мережеві підключення не перетиналися між клієнтами або сервісами. Віртуальна мережа – це чудовий спосіб створення гнучких з’єднань із повторно розгорнутими або масштабованими функціями, але щоразу, коли змінюється віртуальна мережа, можливо, це може випадково встановити з’єднання між двома різними службами, орендарями або розгортанням функцій. Це може призвести до витоку площини даних, з’єднання між реальними мережами користувачів або витоку керування або контролю, що може дозволити одному користувачеві впливати на сервіс іншого.

Чіткі практики та політики, що регулюють віртуальне підключення, можуть зменшити ризик подібної помилки, але запобігти їй дуже важко. Це пов’язано з непрямим зв’язком між віртуальною мережею, яка з’єднує функції, і реальною мережею, яка з’єднує користувачів. Одним із засобів є використання мережевого сканера або інструменту інвентаризації для пошуку пристроїв і віртуальних пристроїв у віртуальній мережі та порівняння цього результату з очікуваною топологією сервіса. Це можна запустити як останній крок зміни віртуальної мережі [9].

1.3. Аналіз існуючих рішень щодо управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ

У сучасному динамічному середовищі потрібне нове мислення, особливо тому, що інфраструктура є більш абстрактною та менш визначеною, усе потребує веб-інтерфейсу, агенти та важкі клієнти неприйнятні, а традиційні засоби захисту більше не застосовуються [10].

На додаток до викликів, пов’язаних із хмарою, існують проблеми, пов’язані з динамізмом віртуалізації в хмарі [10]:

динамічне переміщення віртуальних машин (ВМ): сьогодні гіпервізори переміщують робочі навантаження на основі угоди про рівень обслуговування (SLA), політики енергоспоживання, політики стійкості та багатьох інших причин. Сучасні IT-адміністратори більше не можуть бути впевнені, де в центрі обробки даних знаходиться робоче навантаження;

розширені рівні інфраструктури для керування та захисту: залежно від типу хмарної моделі, що використовується, існує велика кількість додаткових рівнів інфраструктури, таких як шлюзи, брандмауери, маршрутизатори доступу та інші, якими потрібно одночасно керувати та захищати. час, який дозволяє авторизованим користувачам виконувати свої завдання;

кілька операційних систем і додатків на сервер: на стандартному віртуальному апаратному забезпеченні кілька робочих навантажень на фізичному сервері виконуються одночасно з кількома операційними системами та навіть з однаковими операційними системами, але на різних рівнях виправлень;

усунення фізичних кордонів між системами: у міру того, як віртуалізація зростає, робочі навантаження розміщуються в одній фізичній інфраструктурі.

відстеження програмного забезпечення та конфігурації віртуальних машин. Оскільки IT-інфраструктура стає віртуалізованою, стає дедалі складніше керувати конфігурацією програмного забезпечення, зокрема рівнями виправлень, виправленнями безпеки, аудитами безпеки тощо, не лише для гостьових операційних систем, але й для іншої віртуалізованої інфраструктури, наприклад

віртуальними розподіленими комутаторами.

Захист віртуального сервера для VMware показано на рис. 1.4.

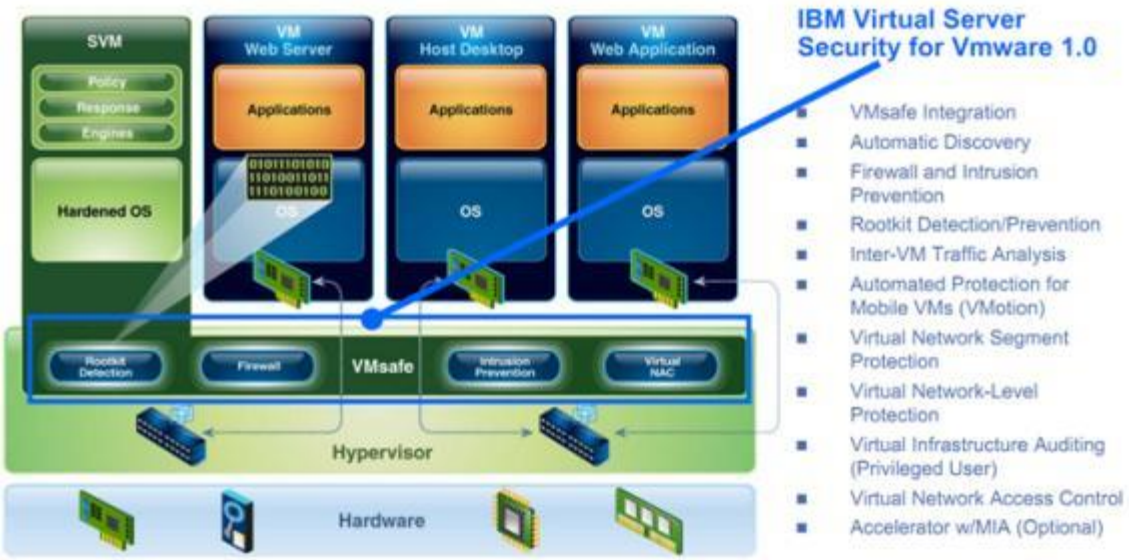

Рис. 1.4. Архітектура захисту віртуального сервера для VMware [10]

Приклад архітектури Virtual Server Protection для VMware показано на рис. 1.5.

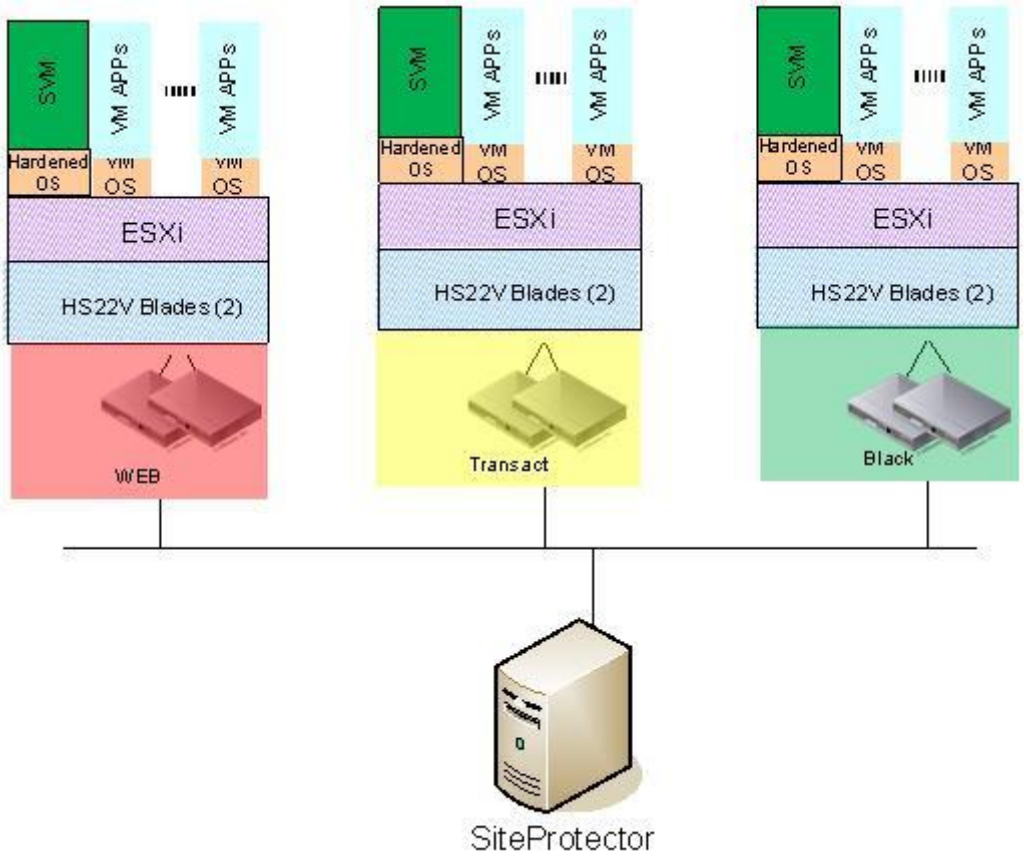

Рис. 1.5. Приклад архітектури Virtual Server Protection для VMware [10]

У прикладі на рис. 1.5 три кластери ESX знаходяться в трьох окремих мережевих зонах (WEB, Transact і Black), розділених фізично. Захист віртуального сервера для VMware розгортається на кожному хості ESX у кластері (у цьому прикладі – блейд-сервери HS22V), який відстежує всі віртуальні машини, коли вони підключаються до мережі. Усі дані про події політики SVM пересилає на пристрій SiteProtector.

Сьогодні VMware є лідером у сфері віртуалізації підприємств. Використовується багатьма підприємствами для розміщення критично важливих для бізнесу робочих навантажень, він має чудові функції та можливості за всіма напрямками, коли йдеться про керованість, масштабованість і високу доступність.

Хоча VMware vSphere пропонує чудові можливості високої доступності для ваших клієнтів і зацікавлених сторін, ви все одно повинні захистити свої дані від катастрофи. В основі будь-якого гарного плану аварійного відновлення — ефективне резервне копіювання. Коли справа доходить до захисту віртуальних машин, є найкращі методи, яких слід дотримуватися під час резервного копіювання даних [11].

Для більшості підприємств, коли йдеться про віртуальні машини (ВМ), будь-який збій програмного чи апаратного забезпечення зазвичай призводить до певного ступеня фінансових втрат у разі перерв у роботі служби. Такі дії, як детальне відновлення та повне аварійне відновлення, також можуть бути особливо корисними в конкретних випадках використання. І ви можете виконати всі ці методи відновлення даних (і багато іншого) за допомогою належного рішення для резервного копіювання віртуальної машини VMware [11].

Dell PowerProtect Data Manager забезпечує програмний захист даних, автоматичне виявлення, дедуплікацію, оперативну гнучкість, самообслуговування та управління IT для фізичних, віртуальних і хмарних середовищ [11].

PowerProtect Data Manager забезпечує стабільний захист середовищ VMware. Менеджер даних – це єдине рішення, яке забезпечує власну інтеграцію vSphere із vCenter для захисту віртуальних машин, дозволяючи адміністраторам сховищ і резервного копіювання, а також власникам віртуальних машин вибирати

політику зберігання, яка автоматично застосовуватиметься до кожної віртуальної машини під час її створення [11].

Інтеграція PowerProtect Data Manager із віртуальними машинами допомагає керувати, захищати та повторно використовувати дані віртуальних машин на підприємстві шляхом розгортання служб для виконання таких завдань [11]:

виявляти, отримувати доступ і відновлювати копії віртуальної машини без збоїв у основному та захисному сховищах без впровадження нової інфраструктури чи складності;

автоматизація ефективного створення копій;

автоматизація збереження даних, відповідність SLA, забезпечуючи збереження потрібної кількості копій у потрібному місці з належним рівнем захисту;

оптимізація операції на основі дієвої аналітики та розуміння.

Послідовне резервне копіювання VM: захоплюються всі диски віртуальної машини одночасно та створюються резервні копії даних у цільових сховищах, щоб створити узгоджену з транзакціями резервну копію. Цей параметр можна використовувати для віртуальних машин Windows і Linux, а також для гостьових операційних систем, у яких є програми, відмінні від SQL Server.

VM Direct Engine – це пристрій захисту в PowerProtect Data Manager, який дозволяє керувати та захищати активи віртуальної машини. Програмне забезпечення PowerProtect Data Manager постачається в комплекті з вбудованим механізмом VM Direct і дозволяє розгортати додаткові зовнішні механізми VM Direct [11].

VM Direct Engine розгортається в середовищі vSphere для створення резервних копій знімків віртуальної машини. VM Direct Engine покращує продуктивність і зменшує використання пропускної здатності мережі завдяки використанню дедуплікації пристроїв серії PowerProtect DD на стороні джерела.

В основному існує два типи VM Direct Engines: внутрішні та зовнішні, які схематично показано на рисунках 1.6 та 1.7 відповідно.

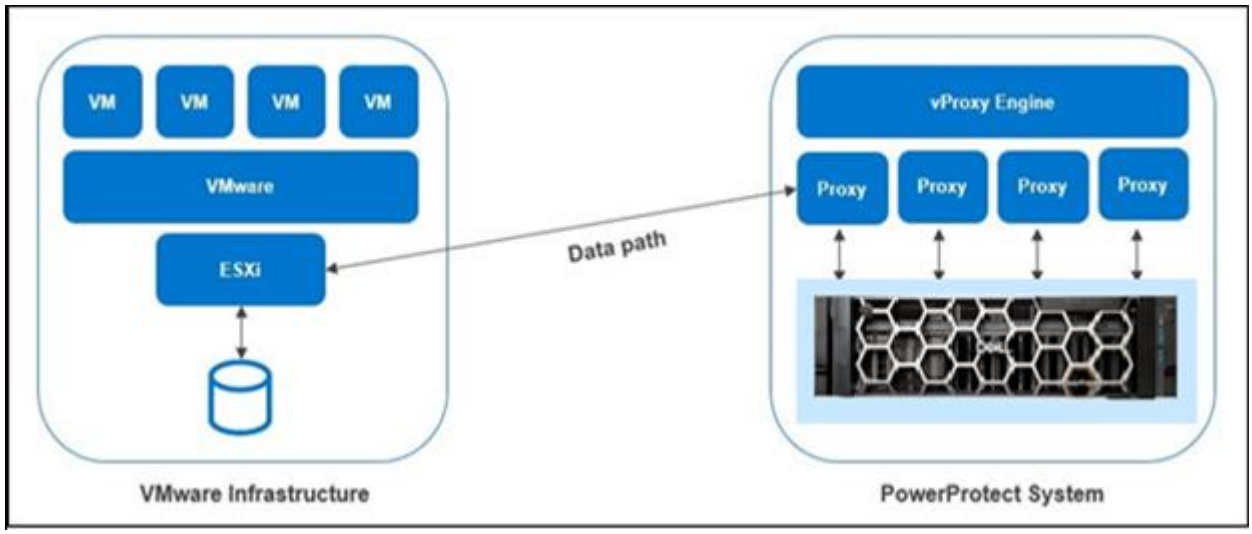

Рис. 1.6. Схема внутрішнього VM Direct Engine [11]

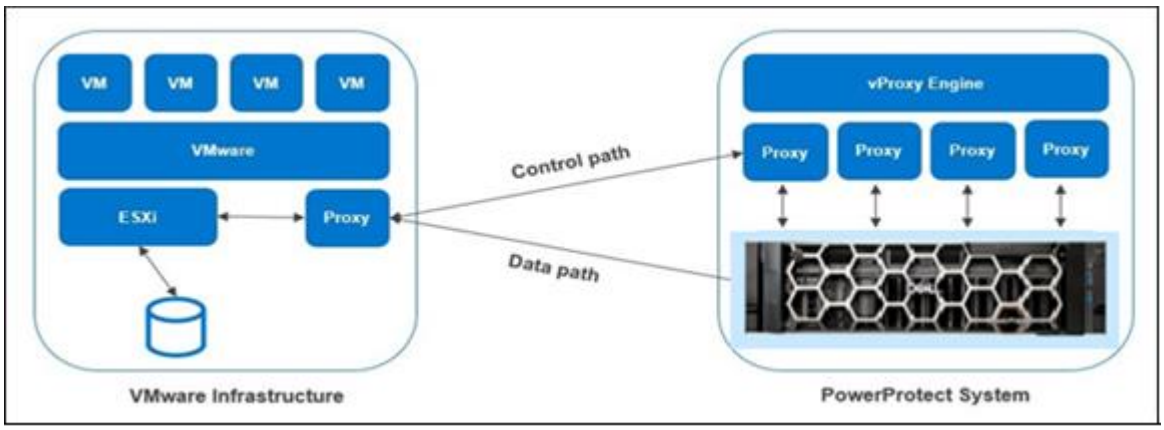

Рис. 1.7. Схема зовнішнього VM Direct Engine [11]

Залежно від версії vSphere і вибраних параметрів політики захисту віртуальної машини VM Direct може захищати віртуальні машини за допомогою традиційних миттєвих знімків VMware API for Data Protection (VADP) або за допомогою механізму захисту Transparent Snapshot Data Mover (TSDM), представленого у версії PowerProtect Data Manager19.9 [11].

Зовнішній VM Direct Engine не потрібен для політик захисту віртуальних машин, які використовують механізм захисту Transparent Snapshot Data Mover (TSDM). Для цих політик достатньо вбудованого VM Direct Engine.

TSDM – це механізм захисту в PowerProtect Data Manager, розроблений для заміни механізму захисту VMware vStorage API for Data Protection (VADP) для захисту віртуальної машини від збоїв.

Після резервного копіювання віртуальних активів у рамках політики захисту віртуальної машини в інтерфейсі PowerProtect Data Manager користувачі можуть виконувати відновлення на рівні образу та файлу з резервних копій окремої чи кількох віртуальних машин, а також відновлювати окремі диски віртуальних машин (VMDK). до свого початкового місця розташування.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ В AZURE

2.1. Мережеві сервіси хмарної платформи Azure

Згідно з рейтингом ITCandor Microsoft Azure є одним із лідерів в IaaS (інфраструктура як послуга) і PaaS (платформа як послуга). Ця потужна комбінація сервісів дозволяє створювати, розгортати й керувати програмами, що забезпечує високу продуктивність. Система побудована на основі двох моделей (IaaS і PaaS), що надає більше можливостей для розробки IT-інфраструктури [1].

Особливістю Microsoft Azure є те, що цю технологію можна швидко масштабувати відповідно до вимог компанії, тому клієнт платить лише за фактичне використання платформи. Платформа Microsoft Azure ґрунтується на зростаючій глобальній мережі центрів обробки даних під керуванням Microsoft. Завдяки цьому клієнтам відкриваються можливості запуску додатків із високою продуктивністю для користувачів із різних країн [1].

Мережеві сервіси в Azure надають різноманітні мережеві можливості, які можна використовувати разом або окремо. Серед них є сервіси захисту додатків, які захищають інформаційні ресурси за допомогою як окремо, так і в комбінації цих мережевих сервісів в Azure – балансування навантаження, приватне посилання, захист від DDoS-атак, брандмауер, групи безпеки мережі, брандмауер веб-додатків, управління та захист кінцевих точок віртуальної мережі [2].

Сервіси підключення. Ресурси Azure та локальні ресурси підключаються за допомогою будь-якої з цих мережевих служб в Azure або їх комбінації: віртуальна мережа (VNet), віртуальна глобальна мережа, ExpressRoute, VPN-шлюз, NAT віртуальної мережі, Azure DNS, сервіс пірингу та Azure Bastion.

Сервіси захисту додатків. Додатки захищаються з використанням будь-якого поєднання цих мережевих сервісів в Azure: Azure Load Balancer, приватний канал, захист від атак DDoS, брандмауер, групи безпеки мережі, брандмауер веб-

додатків та кінцеві точки віртуальної мережі.

Сервіси доставки додатків. Для доставки додатків до мережі Azure використовуйте будь-яку з цих мережевих сервісів до Azure або їх комбінацію: мережі доставки вмісту (CDN), Azure Front Door Service, диспетчер трафіку, шлюз додатків, аналізатор Інтернету та Load Balancer.

Моніторинг мережі. Слідкування за мережевими ресурсами здійснюється за допомогою будь-якої з цих мережевих сервісів в Azure або їх комбінації: спостерігач за мережами, ExpressRoute Monitor, Azure Monitor або точка доступу до терміналу віртуальної мережі (TAP).

Розглянемо сервіси підключення ресурсів більш детально.

Віртуальна мережа (VNet) Azure – це стандартний будівельний блок для приватної мережі організації в Azure. Ви можете використовувати віртуальні мережі для наступних завдань [2]:

Обмін даними між ресурсами Azure. Ви можете розгорнути у віртуальній мережі віртуальні машини та кілька інших типів ресурсів Azure, такі як середовище сервісу додатків Azure, сервіс Azure Kubernetes та масштабовані набори віртуальних машин Azure.

Обмін даними між ресурсами. Віртуальні мережі можна з'єднувати одна з одною. Таким чином, ресурси в цих віртуальних мережах можуть обмінюватися даними, використовуючи піринг між цими мережами. Віртуальні мережі, які ви підключаєте, можуть знаходитися в одному або різних регіонах Azure.

Підключення до Інтернету. За замовчуванням усі віртуальні мережі можуть встановлювати вихідні підключення до Інтернету. Можна також встановити вхідне підключення до ресурсу, надавши йому загальнодоступну IP-адресу, або загальнодоступний екземпляр Load Balancer. Ви також можете використовувати загальнодоступну IP-адресу або загальнодоступний Azure Load Balancer для керування вихідними підключеннями.

Взаємодія із локальними мережами. Ви можете підключити локальні комп'ютери та мережі до віртуальної мережі за допомогою VPN-шлюзу або ExpressRoute.

ExpressRoute дозволяє перенести локальні мережі в хмару Microsoft по приватному підключенню, яке забезпечується постачальником послуг з'єднання. Це підключення закрите. Трафік не проходить через Інтернет. ExpressRoute дозволяє встановлювати підключення до хмарних служб Microsoft, таких як Microsoft Azure, Microsoft 365 та Dynamics 365 (рис. 2.1).

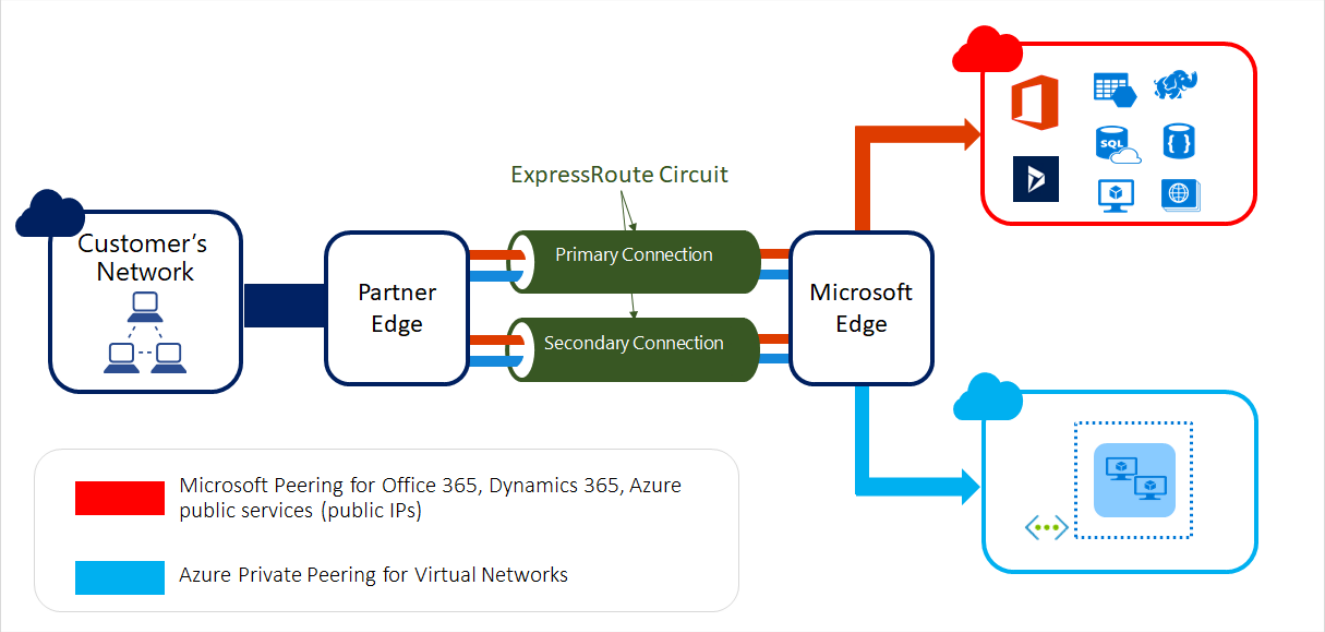

Рис. 2.1. Місце сервісу ExpressRoute [2]

VPN-шлюз допомагає створювати зашифровані підключення між віртуальними мережами або між організаціями та віртуальною мережею з локальних розташування. Існують різні конфігурації для підключень VPN-шлюзу, наприклад, "мережа – мережа", "точка – мережа" та "віртуальна мережа – віртуальна мережа". На наступній схемі показано кілька VPN-підключень типу "мережа - мережа" до однієї віртуальної мережі (рис. 2.2).

Віртуальна глобальна мережа Azure – це мережний сервіс, який забезпечує оптимізоване та автоматизоване підключення типу "гілка – гілка" через Azure. Регіони Azure служать концентраторами, до яких ви можете підключити гілки. Ви також можете використовувати магістральну мережу Azure для підключення гілок і скористатися перевагами підключення гілок до віртуальної мережі (рис. 2.3).

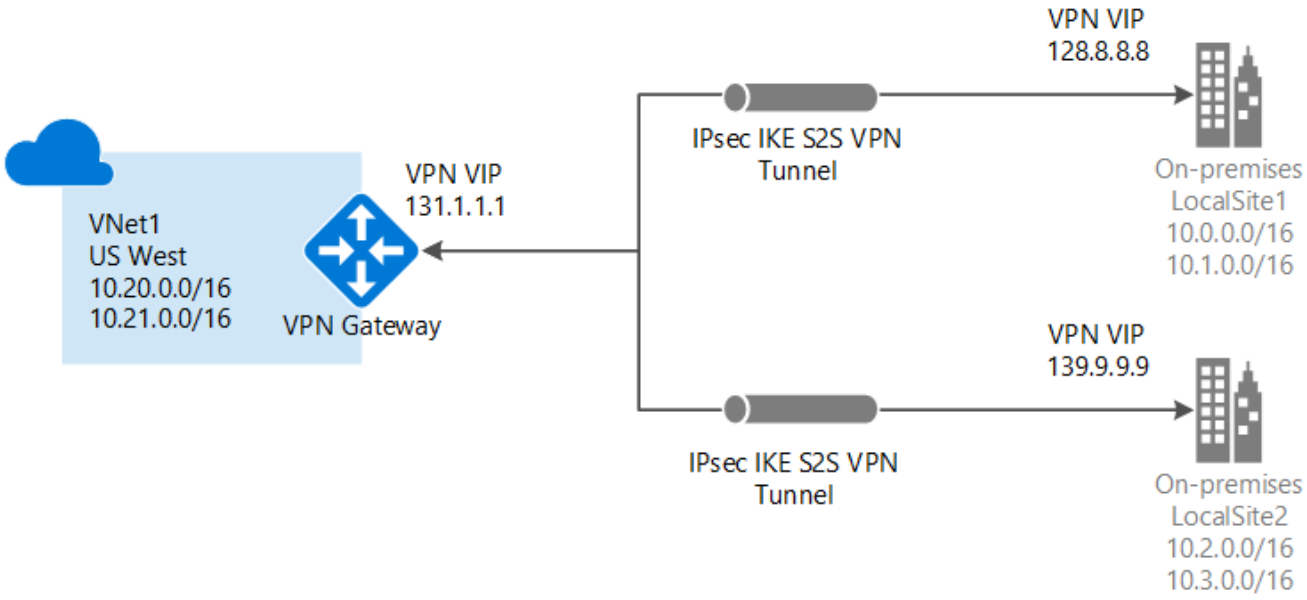

Рис. 2.2. Місце VPN-шлюзу в архітектурі мережі [2]

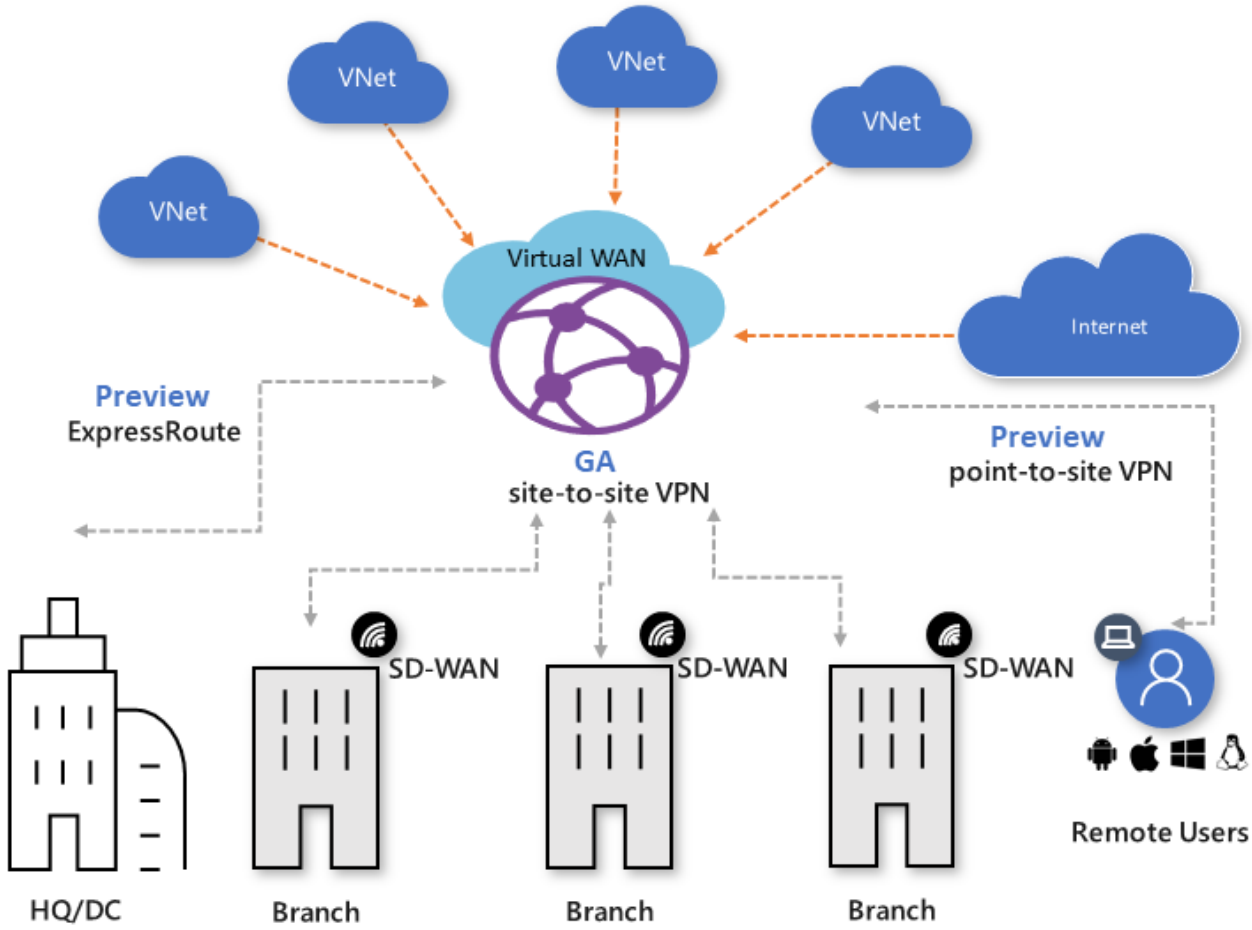

Рис. 2.3. Віртуальна глобальна мережа Azure [2]

Віртуальна глобальна мережа Azure (рис. 2.3) об'єднує безліч сервісів підключення до хмари Azure, таких як VPN типу "мережа – мережа", ExpressRoute та користувальницьке VPN-підключення типу "точка – мережа", в один інтерфейс операцій. Підключення до віртуальних мереж Azure встановлюється за допомогою підключення до віртуальної мережі (рис. 2.3).

Azure DNS є сервісом розміщення доменів DNS, яка здійснює дозвіл імен на базі інфраструктури Microsoft Azure. Розміщуючи домени в Azure, ви можете керувати своїми записами DNS за допомогою тих самих облікових даних, API та інструментів та оплачувати використання, як і інші служби Azure.

Azure Bastion – це повністю керований платформою сервіс PaaS, який створюється у віртуальній мережі. Він забезпечує безпечне та безперебійне підключення RDP або SSH до віртуальних машин безпосередньо на порталі Azure за протоколом TLS. При підключенні за допомогою Azure Bastion до віртуальних машин не потрібні загальнодоступні IP-адреси.

Шлюз NAT віртуальної мережі: NAT (перетворення мережевих адрес) віртуальної мережі полегшує можливість вихідного Інтернет-підключення для віртуальних мереж (рис. 2.4).

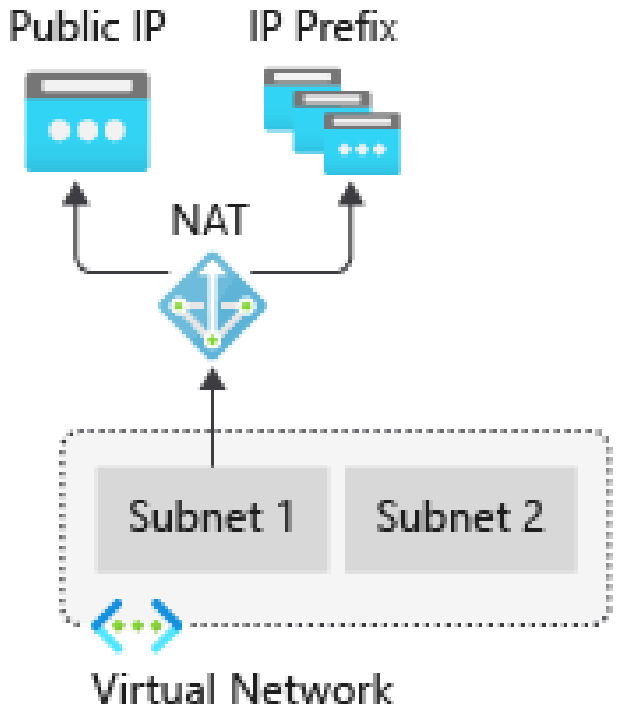

Рис. 2.4. Шлюз NAT віртуальної мережі [2]

При налаштуванні NAT у підмережі всі вихідні підключення використовують вказані статичні загальнодоступні IP-адреси. Вихідне підключення можливе без підсистеми балансування навантаження або загальнодоступних IP-адрес шляхом прямого підключення до віртуальних машин.

Сервіс пірінгу Azure розширює можливості клієнтів щодо підключення до хмарних служб (Microsoft), таких як Microsoft 365, Dynamics 365, SaaS (програмне забезпечення як послуга), Azure та будь-яких служб Microsoft, які працюють через загальнодоступний Інтернет.

2.2. Призначення та основні функції віртуальної мережі Azure

Віртуальна мережа (VNet) Azure – це стандартний будівельний блок для приватної мережі організації в Azure. Віртуальна мережа дозволяє ресурсам Azure різних типів (наприклад, віртуальним машинам Azure) обмінюватися даними один з одним через локальні мережі та через Інтернет. Віртуальна мережа схожа на традиційну мережу, з якою ви будете працювати у власному центрі обробки даних, але пропонує додаткові можливості інфраструктури Azure, наприклад масштабування, доступність та ізоляція [4].

Навіщо використовувати віртуальну мережу Azure? Віртуальна мережа Azure дозволяє ресурсам Azure безпечно взаємодіяти один з одним, з Інтернетом та локальними мережами. За допомогою віртуальної мережі можна реалізувати такі основні сценарії, як взаємодія ресурсів Azure з Інтернетом, обмін даними між ресурсами Azure, взаємодія з локальними ресурсами, фільтрація мережного трафіку, маршрутизація мережного трафіку та інтеграція із службами Azure.

Обмін даними через Інтернет. За замовчуванням усі віртуальні мережі можуть встановлювати вихідні підключення до Інтернету. Можна також встановити вхідне підключення до ресурсу, надавши йому загальнодоступну IP-адресу, або загальнодоступний екземпляр Load Balancer. Загальнодоступну IP-адресу або загальнодоступну підсистему балансування навантаження також можна використовувати для керування вихідними з'єднаннями [4].

При використанні лише внутрішнього екземпляра Load Balancer (цін. категорія "Стандартний") вихідні підключення будуть недоступними, доки ви не налаштуєте для вихідних підключень використання загальнодоступної IP-адреси рівня екземпляра або загальнодоступного екземпляра Load Balancer.

Обмін даними між ресурсами Azure. Безпечний обмін даними між ресурсами забезпечується одним із наступних способів [4]:

через віртуальну мережу. Ви можете розгорнути у віртуальній мережі віртуальні машини та кілька інших типів ресурсів Azure, наприклад середовища Служби додатків Azure, Службу Azure Kubernetes та Масштабовані набори віртуальних машин Azure. Повний список ресурсів Azure, які можна розгорнути у віртуальній мережі, див. у статті Інтеграція віртуальної мережі для служб Azure;

через кінцеву точку служби для віртуальної мережі. Розширіть діапазон приватних IP-адрес та можливості ідентифікації своєї віртуальної мережі до ресурсів служби Azure (наприклад, облікові записи служби сховища Azure та Бази даних SQL Azure), використовуючи пряме підключення. Кінцеві точки служб дозволяють захищати критично важливі ресурси служб Azure у межах вашої віртуальної мережі. Для отримання додаткових відомостей див . розділ Кінцеві точки служб віртуальної мережі;

базовий піринговий зв'язок між віртуальними мережами. Віртуальні мережі можна підключати між собою. Таким чином, ресурси у цих віртуальних мережах можуть обмінюватися даними, використовуючи піринговий зв'язок між цими мережами. Віртуальні мережі, які ви підключаєте, можуть знаходитися в одному або різних регіонах Azure.

Обмін даними через локальні ресурси. Локальні комп'ютери та мережі можна підключити до віртуальної мережі за допомогою будь-якого з наступних способів [4]:

віртуальна приватна мережа (VPN) типу "точка - мережа". Встановлюється між віртуальною мережею та окремим комп'ютером у вашій мережі. Необхідно налаштувати підключення для кожного комп'ютера, який потрібно підключити до віртуальної мережі. Цей тип підключення ідеально підходить для новачків, які не

вміють працювати в Azure, або для розробників, тому що при використанні існуючу мережу майже не потрібно змінювати. Обмін даними між комп'ютером та віртуальною мережею здійснюється через Інтернет за допомогою зашифрованого тунелю;

VPN-підключення "мережа - мережа". Встановлюється між локальним VPN-пристроєм та VPN-шлюзом Azure, розгорнутим у віртуальній мережі. Використовуючи такий тип з'єднання, авторизовані локальні ресурси можуть отримати доступ до віртуальної мережі. Обмін даними між локальним VPN-пристроєм та VPN-шлюзом Azure здійснюється через Інтернет за допомогою зашифрованого тунелю;

Azure ExpressRoute. Встановлюється між вашою мережею та Azure через учасник ExpressRoute. Це підключення закрите. Трафік не проходить через Інтернет.

Фільтрування мережного трафіку. Мережевий трафік між підмережами можна фільтрувати такими способами [4]:

групи безпеки мережі. Групи безпеки мережі та програми можуть містити декілька правил безпеки щодо вхідного та вихідного трафіку, що дозволяє фільтрувати його за вихідною та кінцевою IP-адресою, портом та протоколом;

віртуальні мережеві модулі. Віртуальний мережевий модуль є віртуальною машиною, яка виконує мережеву функцію (наприклад, брандмауер, оптимізація WAN та ін.).

Маршрутизація мережевого трафіку. За промовчанням Azure маршрутизує трафік між підмережами, підключеними віртуальними мережами, локальними мережами та Інтернетом. Щоб перевизначити маршрути за промовчанням, що створюються в Azure, використовуйте такі варіанти [4]:

таблиці маршрутів. Ви можете створити таблиці користувача з маршрутами, які визначають напрямок передачі трафіку для кожної підмережі;

маршрути протоколу BGP. При підключенні віртуальної мережі до локальної мережі за допомогою VPN-шлюзу або ExpressRoute Azure можна розповсюдити локальні маршрути BGP у віртуальних мережах.

Інтеграція віртуальної мережі для служб Azure. Інтеграція служб Azure з віртуальною мережею Azure забезпечує закритий доступ до служби з віртуальних машин або обчислювальних ресурсів у віртуальній мережі. Сервіси Azure можна інтегрувати з віртуальною мережею такими способами [4]:

розгортання виділених екземплярів служби у віртуальній мережі. У цьому випадку закритий доступ до цих служб зможе здійснюватися у віртуальній мережі та з локальних мереж;

використання приватного каналу для приватного доступу до конкретного екземпляра сервісу з віртуальної мережі та локальних мереж.

Ви також можете отримати доступ до сервісу за допомогою загальнодоступних кінцевих точок, розширивши віртуальну мережу за допомогою додавання сервісу за допомогою кінцевих точок сервісу. Кінцеві точки сервісу дозволяють захистити ресурси сервісу у віртуальній мережі.

Обмеження віртуальної мережі Azure. Існують певні обмеження на кількість ресурсів Azure, які можна розгорнути. Для більшості обмежень мережі Azure встановлено максимальні значення.

Віртуальні мережі та зони доступності. Віртуальні мережі та підмережі охоплюють усі зони доступності в регіоні. Їх не потрібно розділяти за зонами доступності для розміщення зональних ресурсів. Наприклад, якщо ви налаштували зональну віртуальну машину, то при виборі зони доступності для віртуальної машини вам не доведеться брати до уваги віртуальну мережу. Це стосується інших зональних ресурсів.

2.3. Призначення та архітектура сервісу Azure Bastion

Azure Bastion – це сервіс, який дозволяє підключатися до віртуальної машини за допомогою браузера та порталу Azure або через рідний клієнт SSH або RDP, уже встановлений на локальному комп’ютері. Сервіс Azure Bastion – це повністю керований платформою сервіс PaaS, який застосовується у корпоративній віртуальній мережі. Він забезпечує безпечне та безперебійне

підключення RDP/SSH до корпоративних віртуальних машин безпосередньо з порталу Azure через протокол TLS [3].

У разі підключення через Azure Bastion, віртуальним машинам не потрібна загальнодоступна IP-адреса, агент або спеціальне клієнтське програмне забезпечення. Bastion забезпечує безпечне підключення RDP і SSH до всіх віртуальних машин у віртуальній мережі, в якій він наданий. Використання Azure Bastion захищає віртуальні машини від доступу портів RDP/SSH до зовнішнього світу, водночас забезпечуючи безпечний доступ за допомогою RDP/SSH [3]. Місце сервісу Azure Bastion в архітектурі Azure показано на рис. 2.5.

Ключовими перевагами застосування Azure Bastion є [3]:

отримання доступу до сеансу RDP і SSH безпосередньо на порталі Azure, використовуючи безперебійний досвід одним натисканням миші;

Azure Bastion використовує веб-клієнт на основі HTML5, який автоматично транслюється на локальний пристрій. Сеанс RDP/SSH здійснюється через TLS на порту 443. Це дозволяє трафіку безпечніше проходити через брандмауери;

Azure Bastion відкриває підключення RDP/SSH до корпоративної віртуальної машини Azure за допомогою приватної IP-адреси віртуальної машини. При цьому не потрібна публічна IP-адреса на корпоративній віртуальній машині;

не потрібно застосовувати будь-які керуванням групами безпеки мережі NSG до підмережі Azure Bastion. Оскільки Azure Bastion підключається до корпоративних віртуальних машин через приватну IP-адресу, можна налаштувати свої NSG, щоб дозволити RDP/SSH лише з Azure Bastion. Це усуває клопоти з керування NSG кожного разу, коли потрібно безпечно підключитися до віртуальних машин;

Azure Bastion – це повністю керована платформа PaaS від Azure, яка внутрішньо захищена для забезпечення безпечного з’єднання RDP/SSH;

корпоративні віртуальні машини захищені від сканування портів зловмисниками та користувачами, оскільки не потрібно підключати віртуальні машини до Інтернету;

Azure Bastion розташований на периметрі корпоративної віртуальної

мережі, тож не потрібно турбуватися про захист кожної віртуальної машини у корпоративній віртуальній мережі;

платформа Azure захищає від експлойтів нульового дня, підтримуючи Azure Bastion надійним і завжди оновленим.

Azure Bastion розгортається у віртуальній мережі та підтримує піринг віртуальної мережі. Зокрема, Azure Bastion керує підключенням RDP/SSH до віртуальних машин, створених у локальних або однорангових віртуальних мережах (рис. 2.5).

RDP і SSH є одними з основних засобів, за допомогою яких можна підключитися до робочих навантажень, що виконуються в Azure. Розкривати порти RDP/SSH через Інтернет небажано та розглядається як значна поверхня загрози.

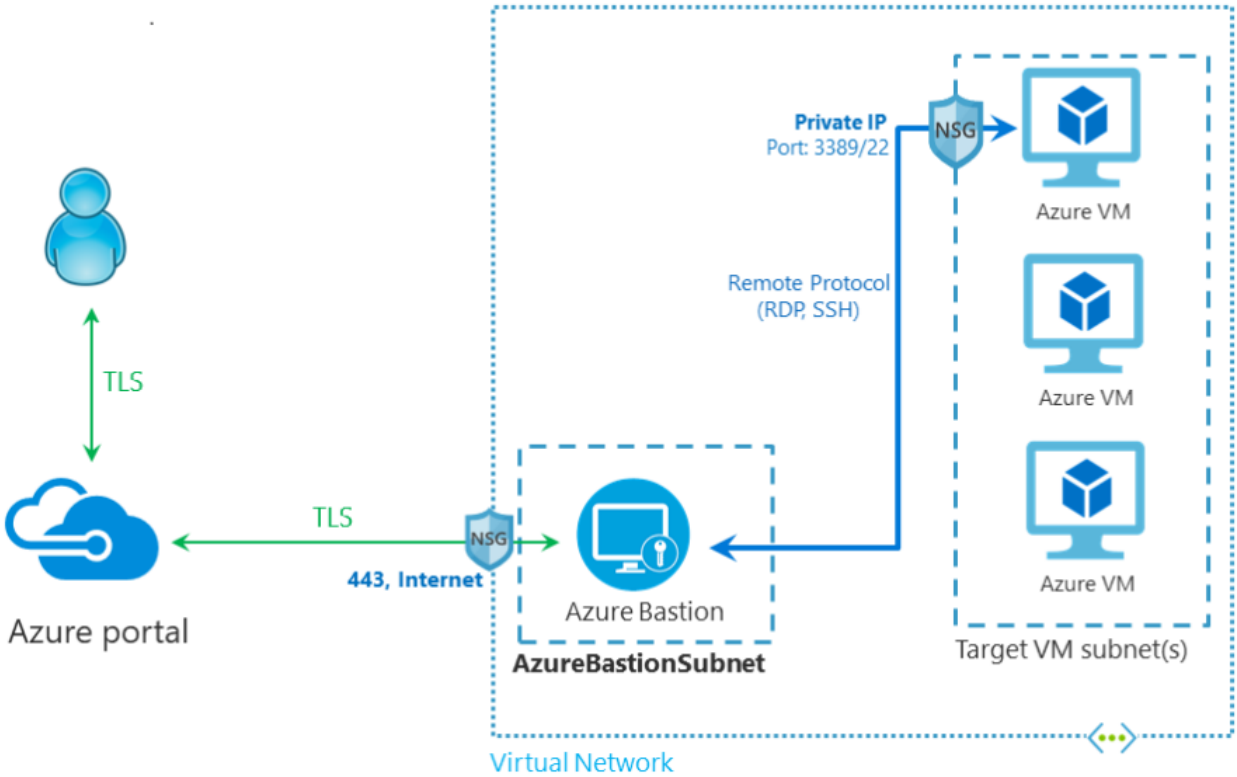

Рис. 2.5. Місце сервісу Azure Bastion в архітектурі [3]

Це часто відбувається через вразливість протоколу. Щоб стримати цю поверхню загрози, можна розгорнути хости-Azure Bastionи (також відомі як стрибкові сервери) на загальнодоступній стороні корпоративної периметральної мережі. Хост-сервери Bastion розроблені та налаштовані таким чином, щоб

протистояти атакам. Сервери Bastion також забезпечують підключення RDP і SSH до робочих навантажень, що знаходяться за Bastion, а також далі всередині мережі [3].

Основу архітектури розгортання Azure Bastion складають [3]:

хост Bastion розгортається у віртуальній мережі, яка містить підмережу AzureBastionSubnet із мінімальним префіксом /26;

користувачі підключаються до порталу Azure за допомогою будь-якого браузера HTML5;

користувачі вибирають віртуальну машину для підключення;

сеанс RDP/SSH відкривається в браузері;

віртуальній машині Azure не потрібна публічна IP-адреса.

Azure Bastion підтримує масштабування вузла вручну. Можна налаштувати кількість базових екземплярів (одиниць масштабування) для керування числом паралельних підключень RDP та SSH, які може підтримувати Azure Bastion. Збільшення кількості базових екземплярів дозволяє Azure Bastion керувати великою кількістю одночасних сеансів. Зменшення кількості екземплярів зменшує кількість сеансів, що одночасно підтримуються. Azure Bastion підтримує до 50 базових екземплярів. Ця функція доступна лише для номера SKU Azure Bastiony Azure рівня "Стандартний".

Примірник – це оптимізована віртуальна машина Azure, яка створюється при налаштуванні Azure Bastion. Він повністю управляється Azure та виконує всі процеси, необхідні для Azure Bastion. Примірник також називається одиницею масштабування. Підключення до віртуальних машин клієнта здійснюється через екземпляр Azure Bastion. При налаштуванні Azure Bastion за допомогою номера SKU "Базовий" створюються два екземпляри. При використанні номера SKU "Стандартний" можна вказати кількість екземплярів. Цей процес називається масштабуванням вузла.

Кожен екземпляр може підтримувати 25 одночасних підключень за протоколом RDP та 50 одночасних підключень за протоколом SSH для середніх робочих навантажень. Кількість підключень для екземплярів залежить від того,

які дії ви виконуєте при підключенні до клієнтської віртуальної машини. Наприклад, якщо виконуються будь-які процеси, що інтенсивно використовують дані, для обробки екземпляра створюється більша навантаження. Після перевищення кількості паралельних сеансів потрібна додаткова одиниця масштабування (примірник).

Примірники створюються в AzureBastionSubnet. Щоб забезпечити масштабування вузла, AzureBastionSubnet повинен дорівнювати /26 або більше. При використанні меншої підмережі кількість екземплярів, які можна створити, обмежена.

Отже, Azure Bastion – це сервіс, який дозволяє захищено підключатися до віртуальної машини за допомогою браузера та порталу Azure або через рідний клієнт SSH або RDP, уже встановлений на локальному комп’ютері.

Таким чином, Azure Bastion надає можливості безпечного застосування віртуальних машин організації, що зменшує різного роду збитки бізнесу у разі здійснення на нього різних кібератак.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ДОСТУПОМ КОРИСТУВАЧІВ ДО ВІРТУАЛЬНИХ МАШИН ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

3.1. Порядок розгортання Azure Bastion з налаштуванням по замовчанню

Розглянемо порядок розгортання рішення Azure Bastion з параметрами за замовчанням у віртуальній мережі за допомогою порталу Azure. Після розгортання Azure Bastion можна встановити SSH- або RDP-підключення до віртуальних машин у віртуальній мережі через Azure Bastion за допомогою приватної IP-адреси віртуальної машини. При підключенні до віртуальної машини їй не потрібна загальнодоступна IP-адреса, клієнтське програмне забезпечення, агент або спеціальна конфігурація. Azure Bastion – це служба PaaS, яка підтримується для вас, а не вузол-Azure Bastion, який ви встановлюєте на одну зі своїх віртуальних машин та підтримуєте самостійно [5].

Наведені нижче кроки дозволять розгорнути Azure Bastion із ресурсу віртуальної машини за допомогою порталу Azure. При розгортанні за замовчуванням параметри підбираються на основі тієї віртуальної мережі, в якій буде розгорнутий Azure Bastion. Після розгортання Azure Bastion ви підключаєтеся до віртуальної машини за протоколом RDP або SSH, використовуючи приватну IP-адресу віртуальної машини. Якщо загальнодоступна IP-адреса на віртуальній машині не потрібна для інших цілей, її можна видалити.

Треба відмітити, що є й інший варіант розгортання: Azure Bastion можна розгорнути з ресурсу віртуальної мережі. Дії будуть майже такими ж, але шлях починається від ресурсу віртуальної мережі, а не віртуальної машини [5].

Віртуальна машина у віртуальній мережі. При розгортанні Azure Bastion з використанням значень за замовчуванням значення витягуються з віртуальної мережі, де знаходиться віртуальна машина. Ця віртуальна машина не стає

частиною самого розгортання Azure Bastion, але ви підключитеся до неї пізніше в цій вправі [5].

Якщо у вас немає віртуальної машини у віртуальній мережі, створіть її за допомогою короткого посібника зі створення віртуальної машини Windows або короткого посібника зі створення віртуальної машини Linux [5].

Якщо у вас є віртуальна мережа, не забудьте вибрати її на вкладці *Мережа* при створенні віртуальної машини. Якщо у вас немає віртуальної мережі, її можна створити одночасно з віртуальною машиною.

Необхідні ролі на віртуальній машині [5]:

роль читача на віртуальній машині;

роль читача на мережевому адаптері з приватною IP-адресою для віртуальної машини.

Необхідні вхідні порти віртуальної машини [5]:

3389 для віртуальних машин Windows;

22 для віртуальних машин Linux.

Використання Azure Bastion Azure з приватними зонами DNS зараз не підтримується. Перш ніж почати, переконайтеся, що віртуальна мережа, в якій планується розгорнути ресурс Azure Bastion, не пов'язана з приватною зоною DNS.

Таблиця 3.1

Базові значення для віртуальної мережі та віртуальної машини

ім'я ;	Значення
Віртуальна машина	TestVM
Група ресурсів	TestRG1
Регіон	Східна частина США
Віртуальна мережа	VNet1
Простір адрес	10.1.0.0/16
підмережі;	Зовнішній інтерфейс: 10.1.0.0/24

Приведемо приклади значень налаштувань.

При створенні цієї конфігурації ви можете застосувати наведені у табл. 3.1 приклади значень або замінити їх на власні.

Значення для Azure Bastion:

При розгортанні з параметрів віртуальної машини для Azure Bastion автоматично налаштовуються стандартні значення, отримані з віртуальної мережі. Вони наведені у табл. 3.2.

Таблиця 3.2

Базові значення для віртуальної мережі та віртуальної машини

Ім'я	Значення за замовчуванням
AzureBastionSubnet	Ця підмережа створюється у віртуальній мережі як /26
номер SKU	Basic
Ім'я	На основі імені віртуальної мережі.
Ім'я загальнодоступної IP-адреси	На основі імені віртуальної мережі.

Розгортання Azure Bastion

При створенні Azure Bastion за допомогою параметрів за замовчанням параметри налаштовуються для вас. Не можна змінити значення або вказати додаткові значення для розгортання за замовчанням. Після завершення розгортання ви можете перейти на сторінку конфігурації вузла-Azure Bastion, щоб вибрати додаткові параметри та компоненти. Наприклад, номер SKU за замовчанням – *Базовий*. Пізніше можна змінити його на *Стандартний*, щоб отримати доступ до додаткових функцій.

1. Увійдіть на портал Azure .

2. На порталі перейдіть до віртуальної машини, до якої необхідно підключитися. Значення з віртуальної мережі, де знаходиться ця віртуальна машина, будуть використовуватися для створення розгортання Azure Bastion.

3. На домашній сторінці віртуальної машини в розділі *Операції* в меню зліва виберіть *Azure Bastion*. Коли відкриється сторінка *Azure Bastion*, буде перевірено, чи достатньо доступного адресного простору для створення *AzureBastionSubnet*. Якщо його недостатньо, ви побачите параметри, які дозволяють додати до

віртуальної мережі додатковий адресний простір для задоволення цієї вимоги.

4. На сторінці *Azure Bastion* можна переглянути деякі значення, які будуть використовуватися при створенні вузла-Azure Bastion для віртуальної мережі. Натисніть кнопку *Розгорнути Azure Bastion*, щоб розгорнути Azure Bastion за промовчанням.

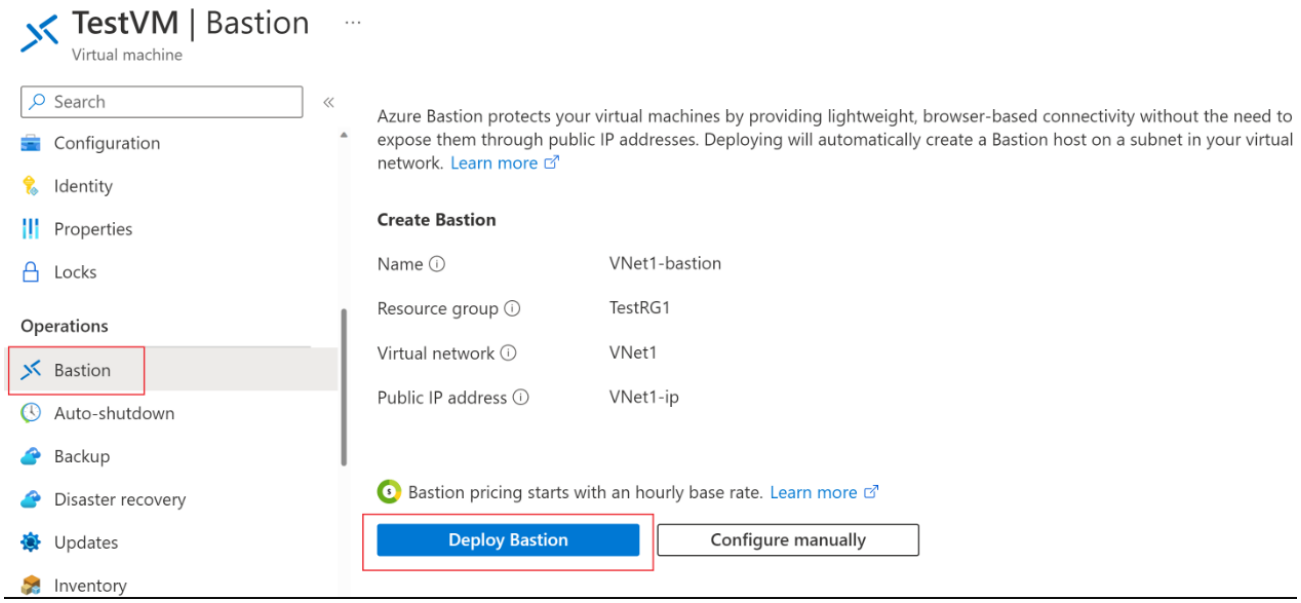

Рис. 3.1. Сторінка Azure Bastion

5. Розпочнеться розгортання Azure Bastion. Це може тривати близько 10 хвилин.

Підключення до віртуальної машини

Після завершення розгортання Azure Bastion екран зміниться на сторінку Підключення (рис. 3.2).

1. Введіть облікові дані для автентифікації. Потім натисніть Connect (Підключитися).

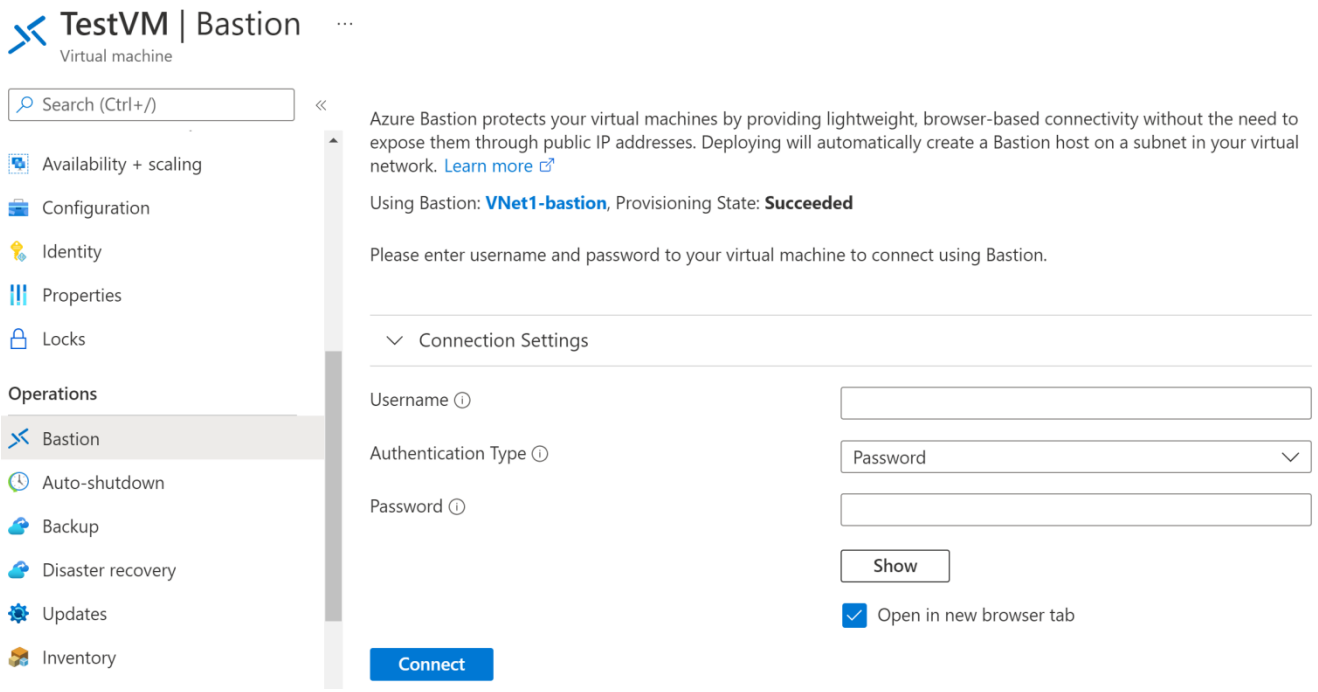

Рис. 3.2. Сторінка Підключення

2. Підключення до цієї віртуальної машини через Azure Bastion відкриватиметься безпосередньо на порталі Azure (через HTML5) з використанням порту 443 та сервісу Azure Bastion. Коли з'явиться запит на дозвіл буфера обміну, виберіть *Дозволити*. Це дозволить використовувати стрілки віддаленого буфера обміну в лівій частині екрана.

При підключенні робочого стола віртуальної машини може виглядати інакше, ніж на знімку екрана з прикладу.

Поєднання клавіш у режимі підключення до віртуальної машини можуть працювати не так, як на локальному комп'ютері. Наприклад, при підключенні до віртуальної машини Windows із клієнта Windows поєднанню клавіш CTRL+ALT+DELETE на локальному комп'ютері еквівалентні клавіші CTRL+ALT+END. Щоб зробити те саме з комп'ютера Mac у режимі підключення до віртуальної машини Windows, використовуйте клавіші FN + CTRL + ALT + BACKSPACE.

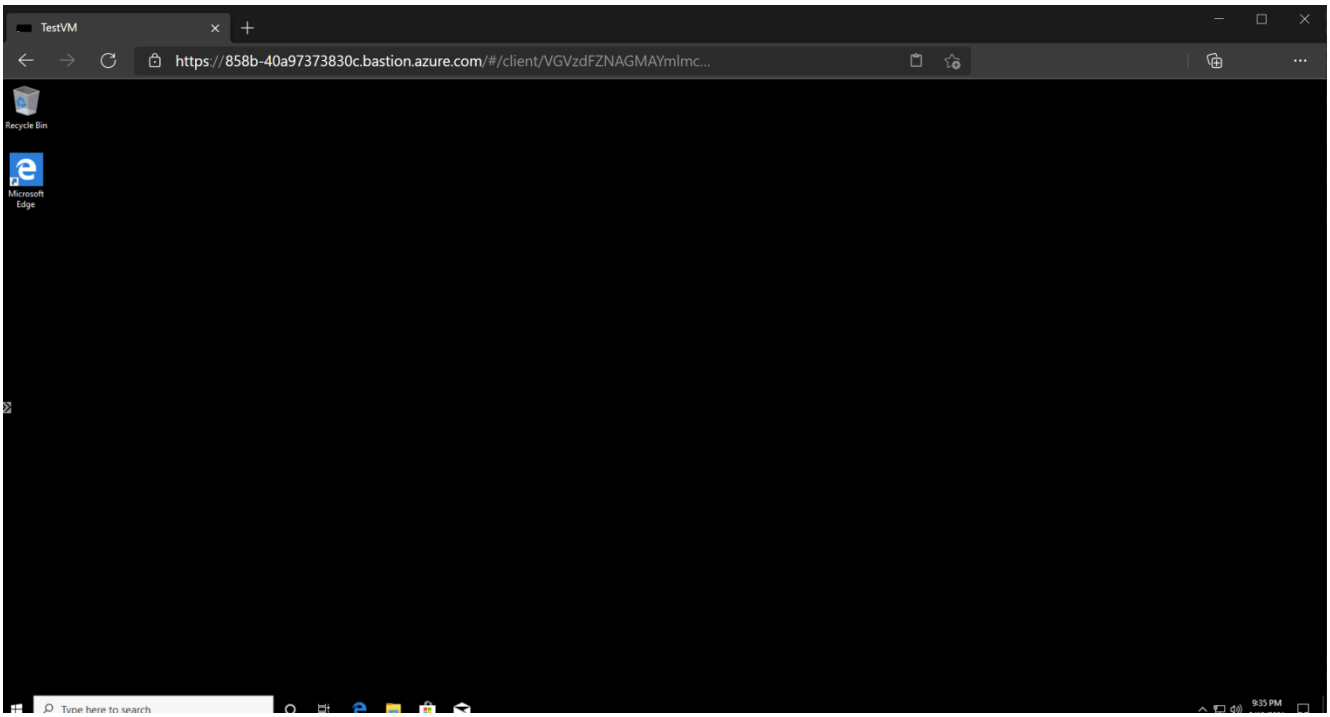

Рис. 3.3. Режим підключення до віртуальної машини

Включення аудіовиходу

Ви можете увімкнути віддалений аудіовиход для віртуальної машини. На одних віртуальних машинах цей параметр увімкнено автоматично, на інших – вам потрібно включити параметри аудіо вручну. Параметри можна змінити на віртуальній машині. У розгортанні Azure Bastion не потрібно налаштовувати спеціальні параметри конфігурації для включення віддаленого аудіовиходу.

Аудіовиход використовує пропускну здатність підключення до Інтернету.

Щоб увімкнути віддалений аудіовихід на віртуальній машині Windows, зробіть таке:

1. Після підключення до віртуальної машини в нижньому правому куті панелі інструментів ви побачите кнопку налаштування звуку.

2. Клацніть правою кнопкою миші та виберіть *Звуки*.

3. З'явиться спливаюче вікно із запитом на увімкнення сервісу Windows Audio. Виберіть *Так*. Ви можете налаштувати додаткові параметри звуку у вікні *Звук*.

4. Щоб перевірити виведення звуку, наведіть вказівник миші на кнопку налаштування звуку на панелі інструментів.

Видалення загальнодоступної IP-адреси віртуальної машини

При підключенні до віртуальної машини за допомогою Azure Bastion Azure для віртуальної машини не потрібна загальнодоступна IP-адреса. Якщо ви не використовуєте загальнодоступну IP-адресу для інших цілей, ви можете відв'язати її від віртуальної машини. Щоб скасувати зв'язок загальнодоступної IP-адреси з віртуальною машиною, зробіть таке.

1. Перейдіть до віртуальної машини та виберіть *Мережі*. Виберіть *Загальнодоступну IP-адресу карти*, щоб відкрити сторінку загальнодоступної IP-адреси.

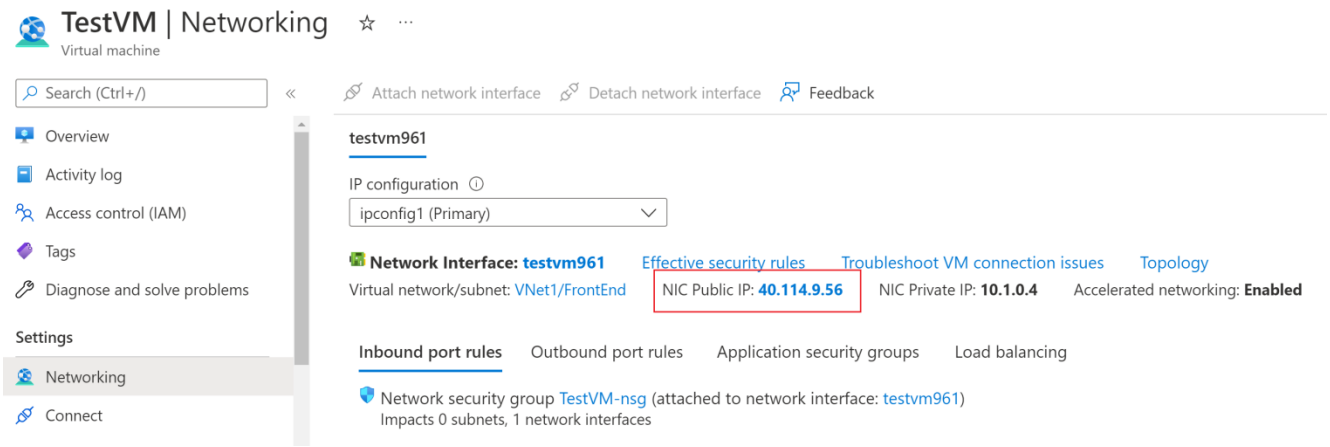

Рис. 3.4. Сторінка Мережі

2. На сторінці *Загальнодоступна IP-адреса* ви побачите мережний інтерфейс віртуальної машини в розділі *Пов'язані* в нижньому правому кутку сторінки. Натисніть кнопку *Скасувати зв'язок* у верхній частині сторінки.

3. Виберіть *Так*, щоб скасувати зв'язок IP-адреси з інтерфейсом мережі. Коли ви скасуєте зв'язок загальнодоступної IP-адреси з інтерфейсом віртуальної машини, ви побачите, що вона зникла з розділу *Пов'язані*.

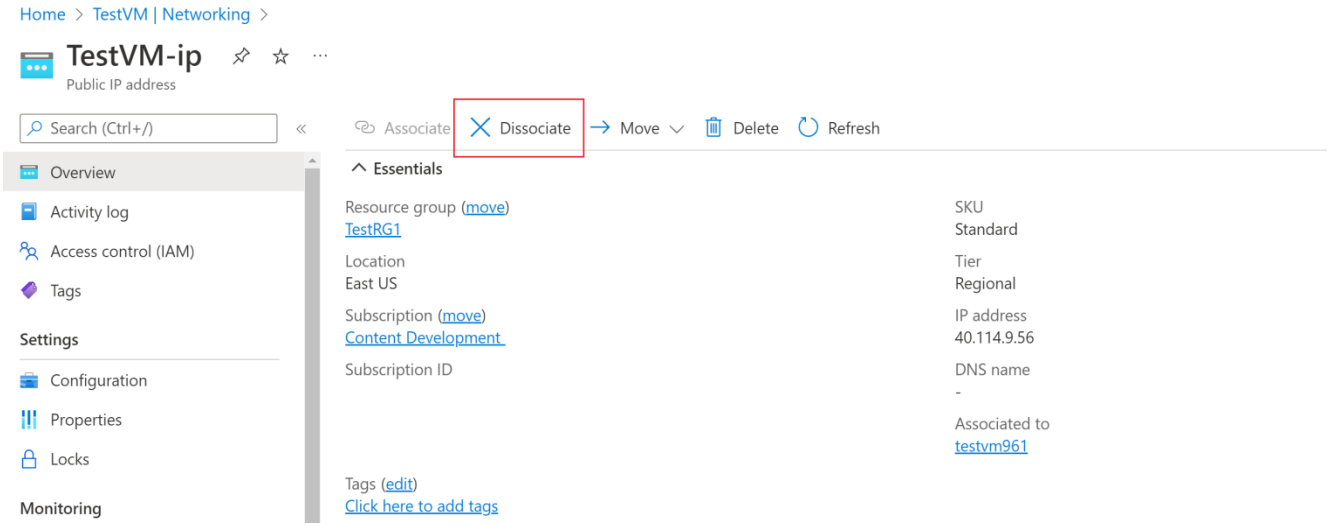

Рис. 3.5. Сторінка Пов'язані

4. Після скасування зв'язку з IP-адресою можна видалити ресурс загальнодоступної IP-адреси. На сторінці *Загальнодоступна IP-адреса віртуальної машини* виберіть *Видалити*.

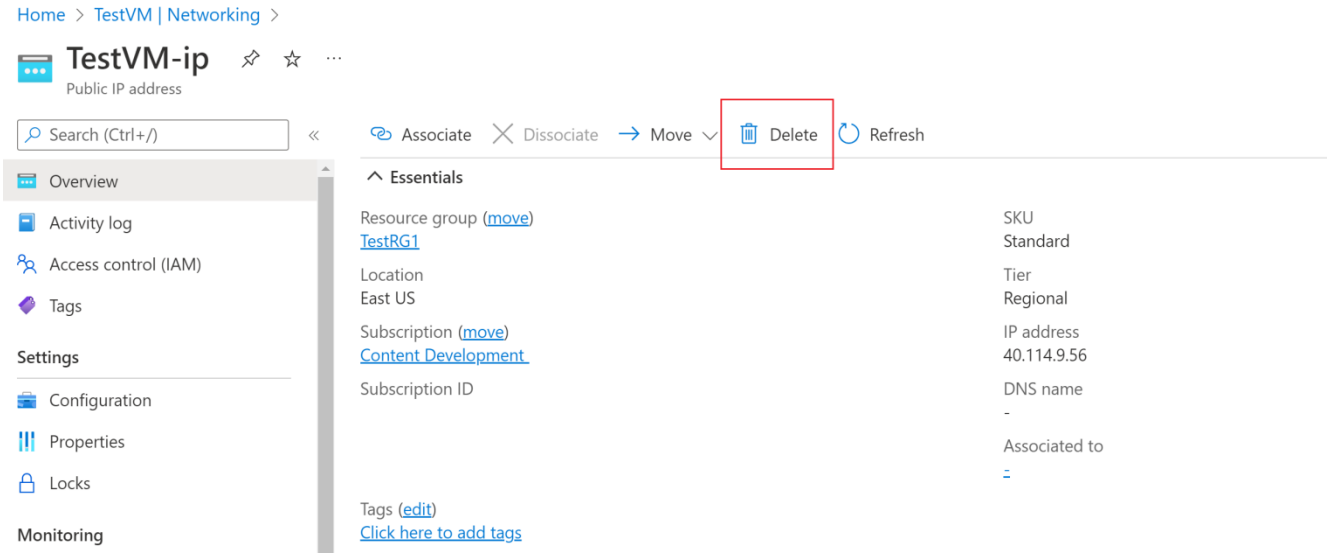

Рис. 3.6. Вкладка Видалити

5. Натисніть *Так*, щоб видалити загальнодоступну IP-адресу.

Очищення ресурсів

Після завершення роботи з віртуальною мережею і віртуальними машинами видаліть групу ресурсів і всі ресурси, що містяться в ній.

1. Введіть назву групи ресурсів у полі *Пошук* у верхній частині порталу та виберіть її в результатах пошуку.

2. Виберіть *Видалити групу ресурсів*.

3. У полі *TYPE THE RESOURCE GROUP NAME* (Введіть ім'я групи ресурсів) введіть ім'я та виберіть *Видалити*.

Таким чином, ми розглянули, як розгорнути Azure Bastion для віртуальної мережі та безпечно підключитися до віртуальної машини через нього. Потім можна налаштувати додаткові функції та працювати з підключеннями до віртуальних машин.

3.2. Порядок організації віддаленої роботи з використанням мережевих сервісів Azure

Розглянемо, як використовувати мережні сервісу Azure, мережу Microsoft та партнерську екосистему Azure для віддаленої роботи та усунення проблем із мережею. Розглянемо можливості, які організації можуть використовувати для організації віддаленого доступу користувачів або доповнення до існуючих рішень для збільшення їх пропускної спроможності в періоди пікового навантаження.

Архітекторам мереж доводиться вирішувати такі проблеми [6]:

справлятися з інтенсивнішим використанням мережі;

забезпечувати надійне підключення для більшої кількості співробітників та клієнтів компанії;

надавати підключення до віддалених точок по всьому світу.

Не у всіх мережах виникають затори через масове підключення віддалених співробітників. Зокрема, це стосується приватних глобальних мереж та основних корпоративних мереж. Вузькі місця зазвичай виникають лише в домашніх широкосмугових мережах та VPN-шлюзах корпоративних локальних мереж [6].

Планувальники мереж можуть впоратися з проблемою вузьких місць і контролювати навантаження мережі за рахунок інтелектуального перенаправлення та розподілу навантаження і якщо пам'ятатимуть, що різні типи

трафіку потребують різних пріоритетів мережевої обробки. Наприклад, при дистанційній консультації у лікаря дуже важливо передавати трафік у реальному часі, а затримки та тремтіння неприпустимі. Разом з тим, при реплікації того ж трафіку між сховищами затримки несуттєві. Перший трафік необхідно спрямовувати найоптимальнішим мережевим маршрутом з вищою якістю обслуговування; а для другого трафіку можна вибрати маршрут із неоптимальними параметрами [6].

Тому, еластичність та високий рівень доступності – основні характеристики мережі Azure. В Azure передбачена стійкість до раптових змін рівня використання ресурсів, що дозволяє успішно впоратися з періодами пікового завантаження.

Крім того, корпорація Microsoft оперує однією з найбільших мереж у світі. Мережа Microsoft розрахована на високу доступність і здатна витримувати різноманітні збої: від неполадок з одним мережевим елементом до відмови всього регіону.

Мережа Microsoft розроблена відповідно до вимог та підтримує оптимальну продуктивність при передачі різних типів мережевого трафіку, включаючи чутливий до затримок мультимедійний трафік Skype та Teams, CDN, аналізу великих даних у реальному часі, сервісу сховища Azure, Bing та Xbox. Щоб забезпечити оптимальну продуктивність для різних типів трафіку, мережа Microsoft притягує весь трафік, що передається через її ресурси, якомога ближче до його джерела [6].

Наведені нижче мережеві функції Azure дозволяють використовувати можливості притягування трафіку в глобальній мережі Microsoft і тим самим підвищити ефективність роботи клієнтів у мережі. Притягнення трафіку до мережі Microsoft допомагає максимально швидко вивантажувати трафік з першої та останньої ділянок мережі, де можуть виникати затори в періоди пікового навантаження [6].

Організація віддаленої роботи працівників

VPN-шлюз Azure підтримує VPN-підключення типу "точка - мережа" (P2S) та "мережа - мережа" (S2S). За допомогою VPN-шлюзу Azure можна

масштабувати підключення співробітників для безпечного доступу до розгорнутих ресурсів Azure та локальних ресурсів.

У разі використання протоколу SSTP (Secure Sockets Tunneling Protocol) підтримується не більше 128 одночасних підключень. Щоб отримати більше підключень, ми рекомендуємо перейти на OpenVPN або IKEv2.

Для доступу до ресурсів, розгорнутих в Azure, віддалені розробники можуть використовувати замість VPN-підключення рішення Azure Bastion, щоб отримати безпечний доступ до оболонки (RDP або SSH), для якої не потрібно мати загальнодоступні IP-адреси на віртуальних машинах.

Для агрегації великомасштабного VPN-підключення, щоб підтримати будь-які підключення між ресурсами в різних локальних розташуваннях по всьому світу і в різних регіональних віртуальних мережах із зіркоподібною топологією, а також оптимізувати використання кількох домашніх широкосмугових мереж, можна застосувати Віртуальну глобальну мережу Azure.

Щоб підтримати віддалених співробітників, можна також розгорнути інфраструктуру віртуальних робочих столів (VDI), розміщену у віртуальній мережі Azure та захищену за допомогою Брандмауера Azure. Віртуальний робочий стіл Azure (AVD) – це служба віртуалізації для комп'ютерів та програм на основі Azure. За допомогою Віртуального робочого столу Azure можна організувати масштабоване та гнучке середовище в рамках підписки Azure, не запускаючи додаткових серверів шлюзу. Ви несете одноосібну відповідальність за віртуальні машини AVD у своїй віртуальній мережі.

Azure має в своєму розпорядженні велику екосистему партнерів. Мережеві віртуальні пристрої на базі Azure від наших партнерів також допомагають масштабувати підключення VPN.

Розширені можливості підключення працівників для доступу до глобально розподілених ресурсів

Наступні сервіси Azure допоможуть співробітникам отримати доступ до ваших глобально розподілених ресурсів. Ресурси можуть знаходитися в будь-якому регіоні Azure, локальних мережах або навіть в інших загальнодоступних

або приватних хмарах.

Піринг між віртуальними мережами Azure. Якщо ви розгортаєте ресурси в кількох регіонах Azure та (або) агрегуєте підключення віддалених співробітників, які використовують кілька віртуальних мереж, ви можете встановити підключення між кількома віртуальними мережами Azure за допомогою піринг.

Рішення на основі Azure VPN. Віддаленим співробітникам, підключеним до Azure через VPN-підключення P2S або S2S, можна надати доступ до локальних мереж, налаштувавши VPN-підключення S2S між локальними мережами та VPN-шлюзом Azure.

ExpressRoute. Приватний пірінг ExpressRoute дозволяє забезпечити приватне підключення між розгорнутими службами Azure та локальною інфраструктурою чи інфраструктурою центру спільного розміщення. ExpressRoute також надає доступ до загальнодоступних кінцевих точок мережі Microsoft з вашої локальної мережі через пірінг Microsoft. Підключення ExpressRoute не проходять через загальнодоступний Інтернет. Вони забезпечують більш безпечне, надійне та швидкісне підключення, ніж звичайні підключення через Інтернет, при меншій кількості затримок, які простіше прогнозувати.

Якщо ви звернетесь до постачальника мережі, який входить до нашої екосистеми партнерів ExpressRouteВи зможете швидше забезпечити підключення з великою пропускною здатністю до мережі Microsoft. ExpressRoute Direct дозволяє безпосередньо підключити вашу локальну мережу до магістралі Microsoft. ExpressRoute Direct пропонує подвійні канали з пропускною здатністю 10 Гбіт/с або 100 Гбіт/с.

Віртуальна глобальна мережа Azure забезпечує ефективну взаємодію між вашими підключеннями VPN і каналами ExpressRoute. Як вже згадувалося, Віртуальна глобальна мережа Azure також підтримує будь-які підключення між ресурсами в різних локальних розташуваннях по всьому світу та в різних регіональних мережах із зіркоподібною топологією.

Масштабування підключень клієнтів до зовнішніх ресурсів

У ті моменти, коли в мережу заходить більше людей, трафік багатьох

корпоративних веб-сайтів зростає. Шлюз додатків Azure допомагає керувати цим підвищеним зовнішнім робочим навантаженням.

Підтримка трафіку в декількох хмарах від Microsoft

Корпорація Microsoft надає глобальні можливості підключення до служб, розгорнутих в інших загальнодоступних хмарах. Для цього можна використовувати віртуальну глобальну мережу Azure, VPN або ExpressRoute. Щоб розширити можливості підключення Azure до інших хмар, можна налаштувати VPN-підключення S2S між двома хмарами. Підключення Azure до інших загальнодоступних хмар можна також організувати за допомогою ExpressRoute. Хмара Oracle Cloud належить до екосистеми партнерів ExpressRoute. Ви можете налаштувати пряму взаємодію між Azure та інфраструктурою Oracle Cloud. Більшість постачальників послуг, що належать до екосистеми партнерів ExpressRoute, також пропонують приватне підключення до інших загальнодоступних хмар. За допомогою їх можна встановити через ExpressRoute приватне підключення між службами, розгорнутими в Azure, та іншими хмарами.

Azure Bastion відіграє ключову роль у підтримці сценаріїв віддаленої роботи, дозволяючи користувачам підключення до Інтернету для доступу до віртуальних машин Azure. Зокрема, ця служба дозволяє IT-адміністраторам керувати програмами, що працюють в Azure, у будь-який час та з будь-якої точки світу.

Безпечний доступ до віртуальних машин

Зокрема, Azure Bastion забезпечує безпечне та зручне підключення за протоколом RDP або SSH до віртуальних машин у віртуальній мережі Azure безпосередньо на порталі Azure без використання загальнодоступної IP-адреси.

Azure Bastion розгортається для кожної віртуальної мережі окремо. Це означає, що компанії можуть налаштувати один екземпляр сервісу Azure Bastion та керувати ним, щоб швидко забезпечити підтримку віддаленого доступу користувачів до віртуальних машин у віртуальній мережі Azure.

3.3. Рекомендації щодо застосування технології управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ

Зруйнована віртуальна інфраструктура створює ризики для будь-якого бізнесу. І це може значно вплинути на те, як швидко ви зможете отримати свої дані та відновити роботу після атаки.

Сьогодні багато компаній використовують віртуалізовану інфраструктуру для більш простого зберігання даних. Це тому, що цей підхід перевершує фізичні рішення завдяки підвищеній гнучкості, простому забезпеченню та доступній ціні. Однак ця модель також вимагає комплексного підходу до безпеки.

Існує набагато більший ризик втрати даних, оскільки багато інструментів і практик для фізичного захисту даних майже марні у віртуальному середовищі. Віртуальні загрози бувають різними, тому потрібно думати не тільки про традиційний захист периметра.

Отже, якщо ви використовуєте віртуалізовану інфраструктуру для зберігання даних необхідно дотримуватися наступних порад.

Не залишайте віртуалізовану інфраструктуру напризволяще. Безпека віртуалізації має вирішальне значення для стратегії безпеки кожного бізнесу. Зрештою, зараз ми живемо у світі віртуалізованих середовищ і маємо застосовувати безпеку на всіх його рівнях.

Треба вживати заходів захисту від зовнішніх атак, які складають реальну загрозу для віртуалізованої інфраструктури. Якщо хакери проникнуть у ваше програмне забезпечення для керування хостом або сервером, вони зможуть легко отримати доступ до інших важливих частин вашої системи. Вони можуть створити нового користувача, призначити права адміністратора, а потім використати ці повноваження, щоб отримати або знищити конфіденційні дані вашої компанії.

Необхідно керувати обміном файлами та копіюванням. Спільне використання хоста та віртуальної машини зазвичай має бути вимкнено. Те саме

стосується копіювання елементів між консоллю віддаленого керування та віртуальною машиною. Ви можете налаштувати параметри за замовчуванням, налаштувавши хост-систему ESXi, але ця дія не рекомендована. Оскільки, якщо хакер отримає доступ до вашої консолі керування, він зможе скопіювати дані за межі вашого віртуального середовища або встановити зловмисне програмне забезпечення у вашу віртуальну машину.

Необхідно вживати заходів протидії шкідливому програмному забезпеченню. Віртуальні машини схильні до багатьох атак, серед яких програми-вимагачі є одними з найпопулярніших. З цієї причини вкрай важливо регулярно створювати резервні копії даних вашого веб-сайту та зберігати їх поза сайтом у місці, де вони не можуть бути зашифровані хакерами. Якщо ви не зробите резервні копії, ви можете опинитися в ситуації, коли хакери можуть вимагати у вас гроші, щоб розшифрувати ваші дані.

Відновити віртуальну машину досить складно, навіть якщо ви регулярно виконуєте резервне копіювання. Тому вам потрібно навчати членів вашої команди знижувати ризик отримання програм-вимагачів та інших вірусів.

Необхідно займатися питаннями оптимізації безпеки віртуалізованої інфраструктури. Віртуальне розростання часто асоціюється зі зростанням віртуальних середовищ. Ця концепція просто означає, що чим більше ви розширюєте, тим більшою є потреба у захисті ваших віртуальних машин. Однак кількість машин може перерости вашу здатність це робити.

Щоб керувати своїм віртуальним розростанням, необхідно:

постійно створюйте інвентаризацію всіх своїх машин;

налаштуйте спостережні пункти з моніторингом у кількох місцях;

відстежуйте IP-адреси, які мають доступ до ваших віртуальних машин;

не використовуйте оператори надання бази даних для надання привілеїв іншим користувачам:

зберігайте резервні копії як на сайті, так і поза ним;

регулярно оцінюйте своє віртуальне середовище та визначайте, які машини вам потрібні, а які – непотрібні;

майте центральний журнал ваших систем і реєструйте всі дії обладнання;

створіть графік технічного обслуговування виправлень для всіх машин, щоб підтримувати їх у актуальному стані.

Необхідно приділяти ретельну увагу налаштуванням віртуальної конфігурації. Якщо ви використовуєте віртуальні сервери, ви ризикуєте серйозними дефектами конфігурації. Ось чому важливо переконатися, що початкові налаштування не загрожують безпеці. Це включає непотрібні порти, непотрібні служби та подібні вразливості. Інакше всі ваші віртуальні машини успадкують однакові проблеми.

Правда полягає в тому, що багато компаній мають погані конфігурації віртуальної мережі. Ви можете уникнути того, щоб бути одним із них, переконавшись, що всі віртуальні програми, які викликають хост (і навпаки), мають правильну сегментацію. Це включає бази даних і всі веб-сервіси.

Варто також зазначити, що більшість платформ віртуалізації пропонують лише три параметри безпеки комутатора: підроблені передачі, зміни MAC-адреси та безладний режим. Немає захисту для віртуальних систем, які підключаються до інших областей мережі.

Отже, обов’язково досліджуйте кожну платформу віртуалізації, яка дозволяє такий тип зв’язку, включаючи всі витоки пам’яті, функції копіювання та вставлення та драйвери пристроїв. Ви також можете налаштувати активи моніторингу системи, щоб стежити за цими шляхами.

Необхідно належним чином захистити всі частини вашої інфраструктури. Це включає його фізичні компоненти (комутатори, хости, фізичне сховище, маршрутизатори), а також віртуальні та гостьові системи. Не забувайте також про всі свої хмарні системи.

Що стосується захисту різних частин інфраструктури, необхідно зробити:

установіть останню версію прошивки для своїх хостів. Віртуалізована інфраструктура повинна мати найновіші виправлення безпеки. Тому оновлюйте всі інструменти VMware. Ваші активні мережеві елементи, такі як маршрутизатори, комутатори та балансувальники навантаження, мають

використовувати останню версію мікропрограми;

виправляйте всі операційні системи з автоматичними оновленнями. Заплануйте встановлення виправлень у неробочий час і включіть автоматичні перезавантаження. У всіх віртуалізованих середовищах має бути встановлене (і регулярно оновлюватися) надійне програмне забезпечення для захисту від зловмисного програмного забезпечення та антивірусне програмне забезпечення.

Необхідно розробити та мати надійний резервний план. Належне аварійне відновлення і плани резервного копіювання мають вирішальне значення для того, щоб ваш бізнес міг продовжувати роботу після атаки. Це тому, що як ваші фізичні, так і віртуальні компоненти можуть однаково постраждати від збитків, завданих хакерськими атаками тощо.

Також обов’язково створіть резервні копії віртуальних машин і фізичних серверів. На щастя, ви можете створити резервну копію своїх фізичних систем, які працюють на Windows або Linux, а також віртуальних машин, які працюють на будь-якій ОС.

Таким чином, дотримання фахівцями з кібербезпеки цих основних рекомендацій забезпечить безпеку віртуальних машин організації в хмарі.

ВИСНОВКИ

В роботі досліджено проблему управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ, визначено його мету та завдання.

Мережеві сервіси в Azure надають різноманітні мережеві можливості, які можна використовувати разом або окремо. Серед них є сервіси захисту додатків, які захищають інформаційні ресурси за допомогою як окремо, так і в комбінації цих мережевих сервісів в Azure – балансування навантаження, приватне посилання, захист від DDoS-атак, брандмауер, групи безпеки мережі, брандмауер веб-додатків, управління та захист кінцевих точок віртуальної мережі.

Проведено аналіз існуючих технологій управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ. Досліджено методи та засоби управління доступом користувачів до віртуальних машин організації в Azure. Визначено призначення, основні функції та склад рішення управління доступом користувачів до віртуальних машин організації в Azure.

Azure Bastion – це сервіс, який дозволяє підключатися до віртуальної машини за допомогою браузера та порталу Azure або через рідний клієнт SSH або RDP, уже встановлений на локальному комп’ютері. Сервіс Azure Bastion – це повністю керований платформою сервіс PaaS, який застосовується у корпоративній віртуальній мережі. Він забезпечує безпечне та безперебійне підключення RDP/SSH до корпоративних віртуальних машин безпосередньо з порталу Azure за допомогою протоколу TLS.

На основі досліджень проведених в роботі розглянуто порядок розгортання сервісу Azure Bastion з налаштуваннями по замовчанню, а також порядок організації віддаленої роботи з використанням мережевих сервісів Azure.

Розроблено рекомендації фахівцям з кібербезпеки щодо управління доступом користувачів до віртуальних машин організації при застосуванні

хмарних платформ.

Таким чином, правильна реалізація управління доступом користувачів до віртуальних машин організації при застосуванні хмарних платформ має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Microsoft Azure. UCloud. [Електронний ресурс] – Режим доступу: https://ucloud.ua/service/microsoft-azure/.

2. Azure networking services overview. Microsoft. Article, 27/07/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/networking/fundamentals/networking-overview.

3. What is Azure Bastion? Microsoft. Article, 21/09/2022. [Електронний ресурс] – Режим доступу: [https://learn.microsoft.com/en-gb/azure/bastion/bastion-overview.

4. What is Azure Virtual Network? Article 27/10/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/ru-ru/azure/virtual-network/virtual-networks-overview.

5. Quickstart: Deploy Azure Bastion with default settings. Article 10/09/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/ru-ru/azure/bastion/quickstart-host-portal.

6. Working remotely using Azure networking services. 23/06/2022. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/networking/working-remotely-support?toc=%2Fazure%2Fbastion%2Ftoc.json.

7. Cloud Security Report 2022 – Fortinet. [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-cloud-security.pdf.

8. Pratyaksha Rawal. Virtualization Gains Popularity as a Viable Solution for Enhancing Cloud Security. September 7, 2020. [Електронний ресурс] – Режим доступу: https://cloudlytics.com/virtualization-gains-popularity-as-a-viable-solution-for-enhancing-cloud-security/.

9. Tom Nolle. 4 steps to ensure virtual machine security in cloud computing. [Електронний ресурс] – Режим доступу:

https://www.techtarget.com/searchsecurity/tip/4-steps-to-ensure-virtual-machine-security-in-cloud-computing.

10. Manav Gupta. Securing virtual machines in the cloud. IBM. [Електронний ресурс] – Режим доступу: https://www.ibm.com/blogs/cloud-computing/2012/01/12/securing-virtual-machines-in-the-cloud/.

11. Chetan Padhy. Data Protection for Virtualized Environments: Made Simpler with PowerProtect Data Manager. August 11th, 2022 [Електронний ресурс] – Режим доступу: https://infohub.delltechnologies.com/p/data-protection-for-virtualized-environments-made-simpler-with-powerprotect-data-manager/.

12. Бойко Максим Миколайович. Технологія забезпечення безпечного доступу користувачів до віртуальних машин Azure. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 9-11. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)