

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

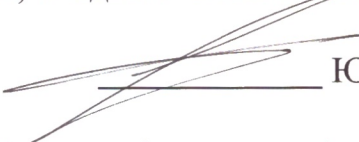
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та інструменти AWS Direct
Connect для з'єднання з хмарною IT-
інфраструктурою підприємства»

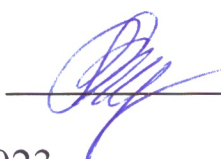
Виконав студент 2-го курсу групи КІм-22-1
спеціальності 123 «Комп'ютерна інженерія»

 Д. В. Бабіч

Керівник доцент кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук, доцент

 Ю. Б. Бродський

Рецензент професор кафедри комп'ютерної
інженерії та кібербезпеки, доктор технічних наук,
доцент

 В. В. Воротніков

Житомир – 2023

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 123 «Комп'ютерна інженерія»
Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та
кібербезпеки

 Андрій
Єфіменко

13 жовтня 2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Бабіч Дмитро Володимирович

Тема роботи: **«МЕТОДИ ТА ІНСТРУМЕНТИ AWS DIRECT
CONNECT ДЛЯ З'ЄДНАННЯ З ХМАРНОЮ ІТ-
ІНФРАСТРУКТУРОЮ»**

затверджена Наказом університету від 13 жовтня 2023 р. № 571/с

Термін здачі студентом закінченої роботи 28 грудня 2023 р.

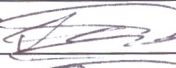
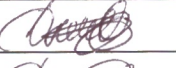
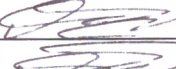
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

1. методи та інструменти, які використовуються в рамках AWS Direct Connect для інтеграції корпоративної ІТ-інфраструктури з хмарними сервісами
2. з'єднання та взаємодія між корпоративною мережею підприємства та хмарною інфраструктурою AWS через Direct Connect

Обладнання та програмне забезпечення:

1. акаунт Amazon Web Services
2. маршрутизатор Cisco CSR 1000V

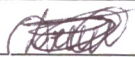
Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	А.А. Єфіменко	13.10.23 	13.10.23 
2	А.А. Єфіменко	13.10.23 	13.10.23 
3	А.А. Єфіменко	13.10.23 	13.10.23 

Студент  Д. В. Бабіч

Керівник  Ю. Б. Бродський

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	20.10.2023 – 23.10.2023	
2	Планування та розробка концепції	24.10.2023 – 27.10.2023	
3	Збір необхідної літератури та джерел. Аналіз зібраної інформації.	27.10.2023 – 30.10.2023	
4	Детальне вивчення теми першого розділу.	01.11.2023 – 07.11.2023	
5	Дослідження та аналіз для другого розділу. Написання та редагування другого розділу.	07.11.2023 – 14.11.2023	
6	Зосередження на практичних аспектах теми. Написання та редагування третього розділу.	14.11.2023 – 21.11.2023	
7	Перегляд написаного матеріалу. Внесення корективів та редагування.	21.11.2023 – 28.11.2023	
8	Написання висновків	01.12.2023 – 05.12.2023	
9	Форматування та остаточне редагування	05.12.2023 – 12.12.2023	
10	Підготовка презентації та матеріалів для захисту.	20.12.2023 – 25.12.2023	

Студент _____ Д. В. Бабіч

Керівник _____ Ю. Б. Бродський

АНОТАЦІЯ

Пояснювальна записка містить: 60 сторінок текстової частини, 41 рисунок, 2 таблиці та 25 джерел.

Метою даної роботи є проведення дослідження методів та інструментів AWS Direct Connect для забезпечення надійного та ефективного з'єднання з хмарною ІТ-інфраструктурою підприємства. В роботі детально розглядаються компоненти та конфігурація AWS Direct Connect, включаючи створення віртуальних інтерфейсів і Direct Connect Gateway, які забезпечують збільшення пропускної спроможності та підвищення безпеки передачі даних.

В теоретичній частині представлено огляд можливостей та принципів роботи AWS Direct Connect, тоді як у практичній частині демонструється покрокове налаштування служби та валідація її працездатності. Результати тестування підтверджують ефективність пропонованої архітектури у реальних умовах використання.

Ключові слова: AWS DIRECT CONNECT, ХМАРНІ РЕСУРСИ, ВІРТУАЛЬНИЙ ІНТЕРФЕЙС, КОРПОРАТИВНА ІТ-ІНФРАСТРУКТУРА, ОПТИМІЗАЦІЯ МЕРЕЖІ.

						КІМ.КР.Б – 123 – 04 – ПЗ				
Змн.	З	Арк.	Ар	№ докум.	№	Підпис	Під	Дата		
Розроб.				Бабіч Д.В.						
Керівник				Бродський Ю. Б.						
Реценз.				Єфіменко А.А.						
Н. контр. Н.				Бродський Ю. Б.						
Затверд.				Єфіменко А. А.						
Методи та інструменти AWS Direct Connect для з'єднання з хмарною ІТ-інфраструктурою підприємства							Лім.	Арк.	Аркушів	
									4	60
							ФІКТ, Гр. Кім-22-1			

ANNOTATION

The explanatory note contains: 60 pages of text, 41 figures, 2 tables and 25 sources.

The purpose of this paper is to study the methods and tools of AWS Direct Connect to ensure a reliable and efficient connection to the enterprise cloud IT infrastructure. The paper discusses in detail the components and configuration of AWS Direct Connect, including the creation of virtual interfaces and the Direct Connect Gateway, which provide increased bandwidth and enhanced data security.

The theoretical part provides an overview of AWS Direct Connect capabilities and principles, while the practical part demonstrates step-by-step configuration of the service and validation of its performance. The test results confirm the effectiveness of the proposed architecture in real-world use.

Keywords: AWS DIRECT CONNECT, CLOUD RESOURCES, VIRTUAL INTERFACE, CORPORATE IT INFRASTRUCTURE, NETWORK OPTIMISATION.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				5
Змн.	Арк.	№ докум.	Підпис	Дата		

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ AWS DIRECT CONNECT	10
1.1 Огляд концепцій Direct Connect	10
1.2 Типи віртуальних інтерфейсів (VIF).....	12
1.3 Direct Connect Gateway та Transit VIF	16
1.4 BGP Communities та Bidirectional Forwarding Detection у Direct Connect	18
1.5 Надійність та резервування. Link Aggregation Groups (LAGs) у Direct Connect	20
Висновки до першого розділу	24
РОЗДІЛ 2 РОЗРОБКА ТА ВПРОВАДЖЕННЯ АРХІТЕКТУРИ ПІДКЛЮЧЕННЯ ДО DIRECT CONNECT	25
2.1 Процедура встановлення Direct Connect	25
2.2 Побудова архітектури	26
2.3 Безпека та шифрування у AWS Direct Connect.....	28
2.4 Ціноутворення AWS Direct Connect	30
Висновки до другого розділу.....	32
РОЗДІЛ 3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ AWS DIRECT CONNECT ...	34
3.1 Заовлення з'єднання AWS Direct Connect через партнера	34
3.2 Створення Private та Public Virtual Interface (VIF):	38
3.3 Конфігурація DX Gateway та його налаштування	42
3.4 Налаштування моніторингу для Direct Connect	44

3.5 Тестування та перевірка з'єднання Direct Connect на працездатність	46
Висновки до третього розділу	48
ВИСНОВКИ.....	49
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	50
ДОДАТКИ.....	52

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

VPN – Virtual Private Network

VLAN – Virtual Local Area Network

IPsec – Internet Protocol Security

DX – Direct Connect

DX GW – Direct Connect Gateway

VGW – Virtual Private Gateway

TGW – Transit Gateway

VIF – Direct Connect

VPC – Virtual Private Cloud

BGP – Border Gateway Protocol

BFD – Bidirectional Forwarding Detection

AWS – Amazon Web Services

ASN – Autonomous System Number

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		8

ВСТУП

Актуальність теми. У сучасному цифровому світі, де хмарні технології стають основою для інновацій та ефективного управління ІТ-інфраструктурою підприємств, забезпечення надійного та швидкого з'єднання з хмарними сервісами стає актуальним завданням для багатьох організацій. AWS Direct Connect від Amazon Web Services є однією з ключових технологій, яка дозволяє підприємствам створити безпечне і продуктивне з'єднання з хмарною ІТ-інфраструктурою. Розуміння та ефективне використання методів та інструментів AWS Direct Connect стає надзвичайно важливим для підприємств, які прагнуть оптимізувати свою інфраструктуру та забезпечити безпеку та продуктивність своїх хмарних з'єднань.

Метою кваліфікаційної роботи є проведення дослідження методів та інструментів AWS Direct Connect для забезпечення надійного та ефективного з'єднання з хмарною ІТ-інфраструктурою підприємства. Робота спрямована на розуміння концептуальних основ AWS Direct Connect, аналіз безпеки, продуктивності та надійності, а також розробку практичних рекомендацій для впровадження та налаштування з'єднань.

Об'єктом дослідження є процес забезпечення надійного та ефективного з'єднання з хмарною ІТ-інфраструктурою підприємства за допомогою AWS Direct Connect. Робота охоплює аналіз технічних аспектів цього сервісу, його можливостей та переваг у контексті інтеграції хмарних ресурсів з традиційними ІТ-інфраструктурами підприємства.

Предметом дослідження є методи та інструменти AWS Direct Connect, які використовуються для створення з'єднання між корпоративною інфраструктурою підприємства та хмарними сервісами Amazon Web Services.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		9

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ AWS DIRECT CONNECT

1.1 Огляд концепцій Direct Connect

AWS Direct Connect представляє собою високоефективне фізичне з'єднання, яке надає підприємствам прямий доступ до хмарної інфраструктури AWS. Ключовим аспектом цього сервісу є його здатність надавати високу пропускну здатність та низьку затримку мережевих з'єднань, що є критично важливим для багатьох бізнес-додатків. Існує два типи підключення до AWS Direct Connect[4]:

- **Виділені підключення**, де підтримуються порти зі швидкістю 1 Гбіт/с, 10 Гбіт/с та 100 Гбіт/с. Ці підключення забезпечують високу пропускну здатність для інтенсивних додатків та великих обсягів даних.
- **У хостингових підключеннях** швидкість з'єднання варіюється від 50 Мбіт/с до 10 Гбіт/с. Ці підключення надаються через затверджених партнерів AWS Direct Connect і підходять для більш гнучких або масштабованих рішень.

З'єднання встановлюється між бізнес інфраструктурою клієнта, місцем розташування Direct Connect і відповідним регіоном AWS (наприклад, us-east-1). У секторі замовника або комунікаційного партнера знаходиться маршрутизатор клієнта або партнера, який забезпечує підключення до мережі. Місце розташування DX включає в себе необхідне обладнання, таке як DX-маршрутизатори та сервери, для реалізації мережевого з'єднання[8].

AWS орендує простір у колокейшн-центрах, які знаходяться у різних географічних регіонах по всьому світу. Ці центри надають необхідну інфраструктуру та обладнання для фізичного з'єднання мереж клієнтів AWS з їх хмарними сервісами. Цей підхід дозволяє AWS забезпечувати високу доступність та надійність з'єднань за допомогою Direct Connect, не несучи при цьому витрат та відповідальності за повне управління фізичними

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

місцями розташування. Такий варіант співпраці є ефективним для обох сторін: AWS забезпечує якісні мережеві послуги, а колокейшн-центри - надійну інфраструктуру та обслуговування.

Час налаштування для AWS Direct Connect залежить від кількох факторів, включаючи тип підключення та географічне розташування. У загальному випадку, цей процес може варіюватися від кількох днів до кількох тижнів. Для виділених підключень час налаштування зазвичай довший, оскільки вони потребують фізичного підключення в точці обслуговування AWS Direct Connect та налаштувань з боку AWS та клієнта. У випадку хостингових підключень, які надаються через партнерів AWS, час налаштування може бути коротшим, оскільки багато інфраструктурних компонентів вже передбачені на місці.

Cross-connect (наскрізне підключення) у контексті AWS Direct Connect є критично важливим компонентом, який забезпечує фізичне з'єднання між портом AWS DX маршрутизатором та клієнта. Це процес встановлення прямого мережевого з'єднання, яке здійснюється в колокейшн-центрі, де розміщено обладнання AWS DX[1].

Між портом AWS DX та маршрутизатором клієнта, можливо використовувати виключно оптоволоконні одномодові кабелі. Одномодові оптоволоконні кабелі забезпечують високу якість передачі даних на значні відстані.

Для забезпечення оптимальної роботи AWS Direct Connect, особливо при використанні одномодового оптоволокна, важливо вибирати відповідні фізичні підключення, які сумісні з потрібною швидкістю та типом з'єднання. Для 1 Гбіт/с з'єднань використовуються 1000Base-LX трансивери, які працюють на довжині хвилі 1310 нм. Для з'єднань зі швидкістю 10 Гбіт/с та 100 Гбіт/с використовуються 10GBase-LR або 10GBase-ER та 100GB-LR відповідно. Крім того, клієнтські роутери повинні підтримувати BGP та BGP MD5 аутентифікацію. Також рекомендується відключати функцію auto

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

negotiation, і параметри такі як швидкість порту та режим full duplex потрібно налаштовувати вручну[2].

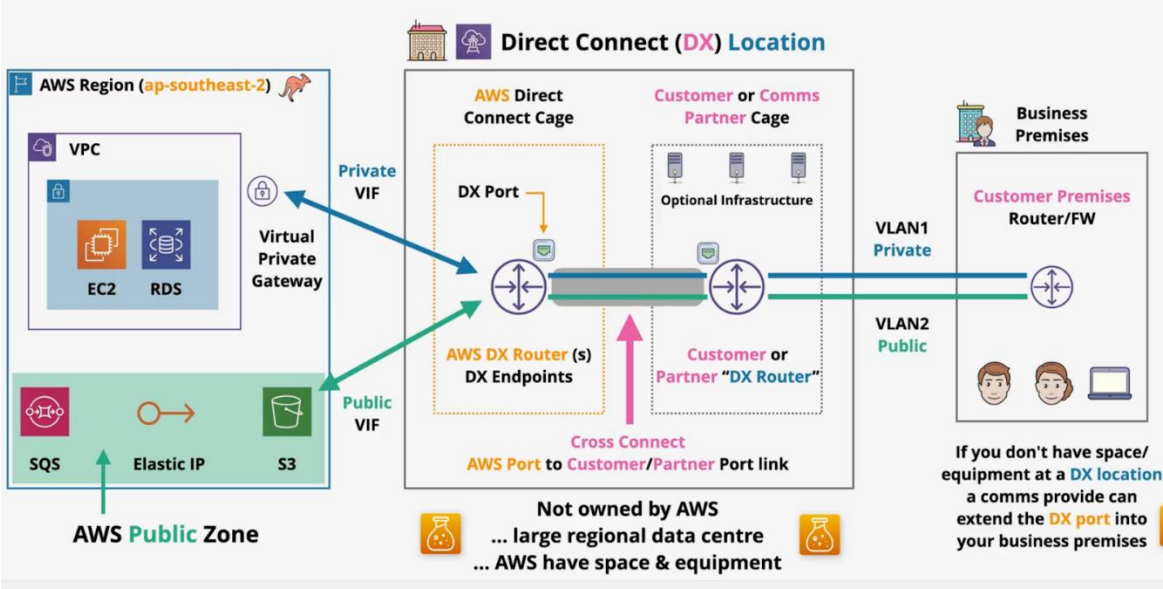


Рисунок 1.1 – Архітектура Direct Connect[2]

1.2 Типи віртуальних інтерфейсів (VIF)

AWS DX забезпечує безперебійну інтеграцію з існуючими мережевими архітектурами через інтеграцію сесій BGP та VLANs. Як основний компонент, DX створює фізичне з'єднання першого рівня, яке становить основу передачі даних. Однак, він працює на другому рівні - канальному, використовуючи переваги Ethernet-з'єднання для надання стабільного з'єднання між середовищем клієнта та AWS.

Надійність з'єднань DX полягає в їх здатності інтегрувати кілька мереж третього рівня, таких як віртуальні приватні хмари та публічні зони, через одне фізичне з'єднання. Ця інтеграція координується за допомогою віртуального інтерфейсу (VIF), конструкції, яка розширює можливості з'єднання другого рівня для підтримки кількох мереж третього рівня. VIF складається з сесії BGP підключення, спареного з VLAN, що дозволяє обмін префіксами, які спрямовують потік даних між середовищем AWS та мережею клієнта[5].

Компонент VLAN сприяє організації мережі та безпеці, ізолюючи різні мережі третього рівня за допомогою тегування 802.1Q для збереження

розподілення трафіку. Крім того, реалізація аутентифікації BGP MD5 забезпечує прийняття лише перевірених та автентифікованих передач даних, зміцнюючи цілісність обміну даними.

VIFs класифікуються на три типи, кожен з яких виконує певну мережеву функцію. Публічні віртуальні інтерфейси (Public VIFs) надають можливість підключення до сервісів AWS, які не розміщені у віртуальних приватних хмарах (VPC), або до тих, що працюють у VPC, але використовують публічну адресацію. Приватні віртуальні інтерфейси (Private VIFs) використовуються для з'єднання з приватними мережами AWS, тобто з VPCs, що використовують приватну адресацію. Транзитні віртуальні інтерфейси (Transit VIF) дозволяють інтеграцію між з'єднанням DX та Transit Gateway (TGW).

Одне з'єднання DX може мати до 50 публічних та приватних VIF або один транзитний VIF. Для хостингових з'єднань доступний тільки один VIF. Сесія BGP, яка є частиною VIF, встановлюється між маршрутизатором клієнта DX та маршрутизатором AWS DX і може бути розширена до інфраструктури клієнта. Сесії BGP аутентифіковані за допомогою MD5. VLAN/BGP сесія може бути розширена до інфраструктури клієнта відповідно до потреб за допомогою технології Q-in-Q[6].

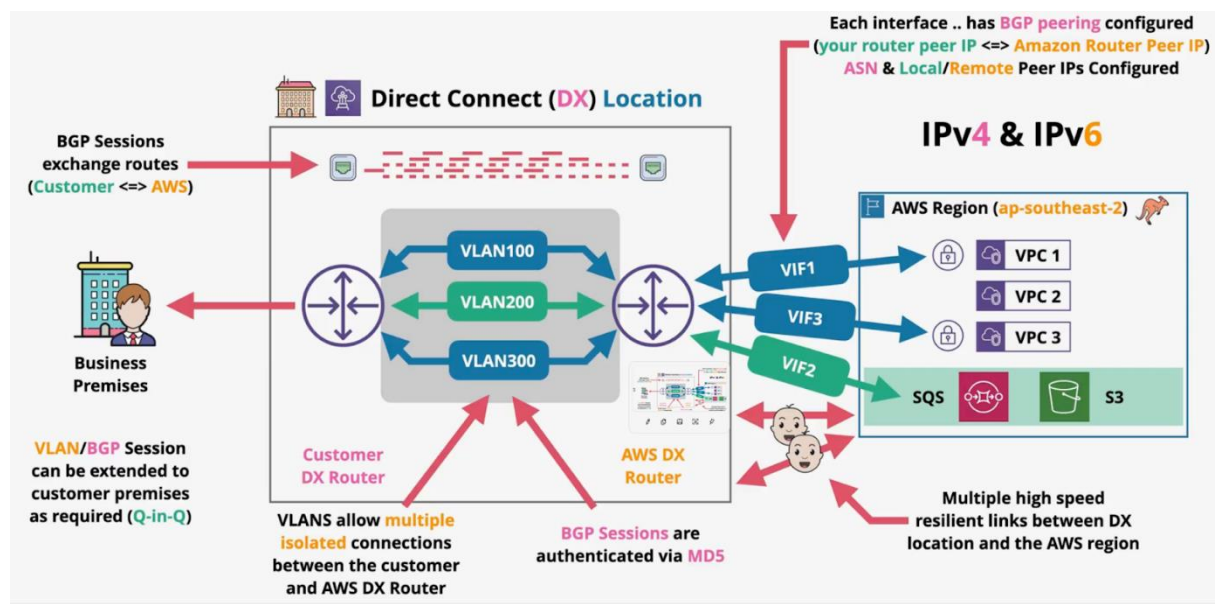


Рисунок 1.2 – Direct Connect VIFs[2]

Private VIF встановлюються в рамках з'єднання DX і традиційно використовувалися для забезпечення доступу до ресурсів одного VPC через приватні IP-адреси. Використання приватного VIF дозволяє здійснювати доступ до екземплярів EC2 у VPC за їхніми приватними IPv4-адресами. У контексті доступу до цих ресурсів за публічними IPv4-адресами, приватний VIF не підходить, оскільки VPC оперує лише приватними IP. Зазвичай приватні VIF асоціюються з віртуальними приватними шлюзами (VGW), які прив'язані до одного VPC і мають бути в тому ж регіоні, де і DX-з'єднання.

Однією з ключових особливостей приватного VIF є відсутність вбудованого шифрування трафіку, що змушує застосунки використовувати власні методи шифрування, наприклад HTTPS, для захисту даних. Приватні VIF підтримують стандартний розмір MTU 1500 або 9001 для Jumbo Frames, що може покращити ефективність передачі великих даних. Крім того, функція розповсюдження маршрутів для VGW активована за замовчуванням, що спрощує маршрутизацію між VPC та корпоративними мережами.[7]

Створення приватних віртуальних інтерфейсів (Private VIF) для AWS Direct Connect передбачає вибір з'єднання, через яке буде працювати VIF. Можна обрати за замовчуванням віртуальний приватний шлюз (VGW) або Direct Connect Gateway, в залежності від потреб. Власник інтерфейсу може бути як поточний обліковий запис, так і інший.

Для VLAN використовується стандарт 802.1Q, і конфігурація VLAN повинна відповідати налаштуванням клієнта. Автономна система BGP (BGP ASN) може бути публічною або приватною; у випадку приватного використання, номери ASN повинні лежати в діапазоні від 64512 до 65535[4].

Адреси однорангових вузлів BGP (Peer IPs) можуть бути автоматично генеровані. AWS використовує BGP Peer IPs, зазвичай з маскою підмережі /30. Користувачі можуть оголошувати за замовчуванням усі маршрути або

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		14

конкретні корпоративні префікси, але загальна кількість оголошуваних префіксів не повинна перевищувати 100.

Public VIFs використовуються для доступу до послуг, які доступні у публічній зоні AWS, включаючи такі сервіси як Amazon SNS, SQS, S3 та інші, що використовують еластичні IP-адреси. Важливо відзначити, що через Public VIF немає прямого доступу до приватних служб VPC. Тим не менш, Public VIF дозволяє доступ до всіх регіонів публічної зони через глобальну мережу AWS.

AWS оголошує через BGP всі діапазони публічних IP-адрес для користувачів, а з боку користувачів є можливість анонсувати через BGP власні публічні IP-адреси. Це забезпечує двостороннє спілкування в рамках BGP, що дозволяє обмінюватися маршрутами між користувацьким обладнанням та обладнанням AWS. Проте, варто зазначити, що публічні VIF не є транзитивними — це означає, що анонсовані префікси користувача не поширюються на інших клієнтів AWS.

Комбінація Public VIF та VPN створює шифрований і аутентифікований тунель, який дозволяє підключатися до публічних кінцевих точок AWS, таких як VGW або TGW, з низькою затримкою через DX. Цей тунель є транзит-агностичним, що означає, що користувач може використовувати DX або публічний інтернет для транзиту[20].

За допомогою VPN з публічним VIF можна створювати приватні з'єднання з VPC, навіть коли вони розташовані в інших регіонах через глобальну мережу AWS. Це забезпечує кінцевий захист (end-to-end encryption) для даних, що передаються, проте варто враховувати криптографічні накладні витрати, які можуть обмежувати швидкість передачі даних. VPN може бути використаний під час налаштування DX або як запасний варіант для DX.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		15

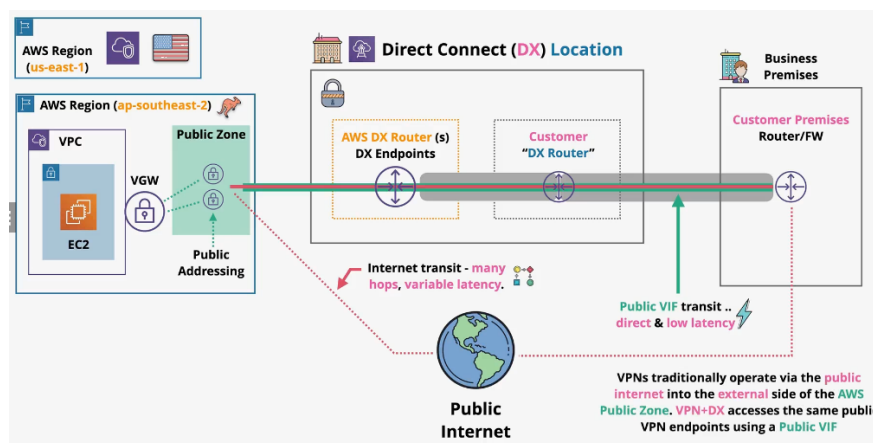


Рисунок 1.3 – Public VIF використовуючи публічні IP VGW[10]

1.3 Direct Connect Gateway та Transit VIF

Direct Connect Gateway є глобальним мережевим пристроєм, який дає можливість доступу до ресурсів AWS через AWS Direct Connect з будь-якого регіону. Використання Private VIF з DX Gateway дозволяє асоціювати ваші Virtual Private Gateways (VGW), які прикріплені до VPC, забезпечуючи глобальне підключення.

Таке підключення забезпечує обмін даними між VPC та локальними мережами користувача, а також дозволяє комунікацію між різними VPC, що знаходяться на одному Direct Connect Gateway. За допомогою одного приватного VIF можна асоціювати один Direct Connect Gateway та до десяти VGW, тобто один DX може мати до 50 приватних VIF, що еквівалентно можливості підключення до 500 VPC.

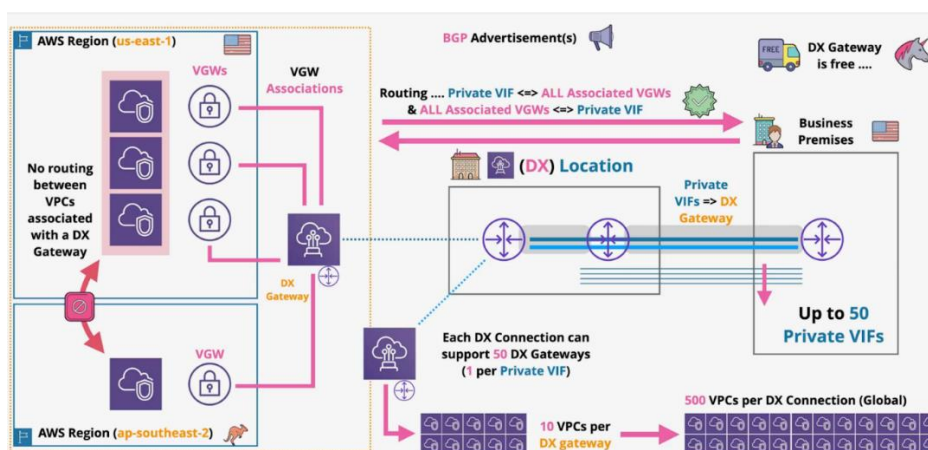


Рисунок 1.4 – Архітектура мережі з DX Gateway[11]

		Бабіч Д. В.			Арк.
		Бродський Ю. Б.			
Змн.	Арк.	№ докум.	Підпис	Дата	16

Існують різні сценарії використання DX Gateway, такі як асоціації віртуальних приватних шлюзів, де DX Gateway забезпечує доступ до VPC в різних регіонах AWS через одне з'єднання AWS DX. Також, DX Gateway можуть використовуватися між акаунтами, де різні акаунти можуть запропонувати асоціації до DX Gateway, що належить іншому акаунту.

DX Gateway також підтримує транзитний VIF, кожен з яких може підтримувати до трьох TGW. DX GW може бути пов'язаний або з VPC та приватними VIF, або з TGW і транзитним VIF, але не з обома одночасно.

Транзитний VIF може з'єднуватися з будь-яким TGW, але DXGW не здійснює маршрутизацію між своїми атакментами, для цього потрібно використовувати TGW peering. До кожного TGW можна приєднати до 20 DX GW. Кожен TGW підтримує 5000 приєднань та 50 пірінгів, кожен з яких, в свою чергу, дозволяє 5000 приєднань, забезпечуючи можливість створення складних мережевих архітектур.

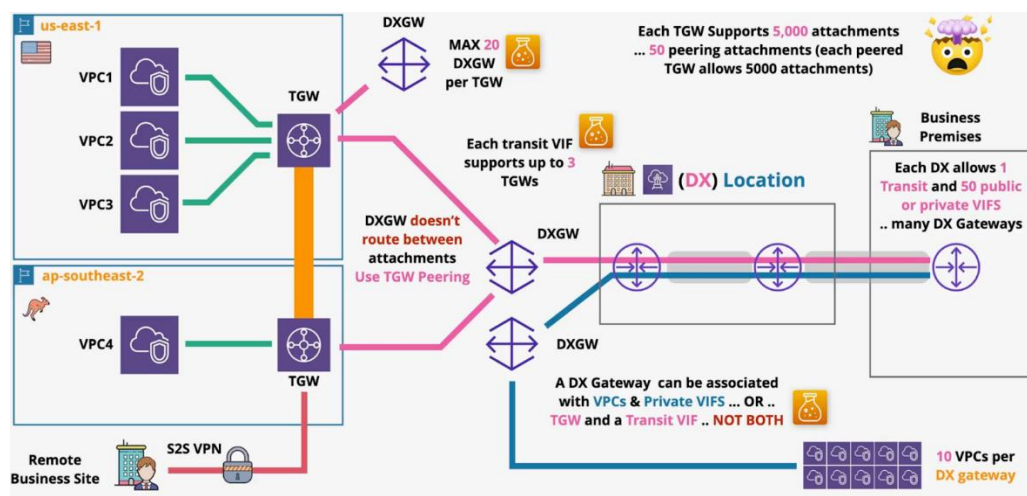


Рисунок 1.5 – Transit VIF та Gateway

DX Gateway не підтримує маршрутизацію між інтерфейсами, які приєднані до шлюза. Це означає, що, хоча індивідуальні мережі, такі як VPC1, можуть з'єднуватися з DX Gateway та обмінюватися даними з інфраструктурою підприємства, але VPC, які приєднані до даного DX Gateway не мають доступу між собою. Така обмеженість вимагає альтернативного рішення для взаємодії між мережами[4].

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

TGW дозволяє маршрутизацію між прикріпленнями DX Gateway, забезпечуючи з'єднання між офісами, що використовують DX. Така конфігурація дозволяє VPC у регіоні us-east-1 комунікувати через TGW з різними бізнес-інфраструктурами.

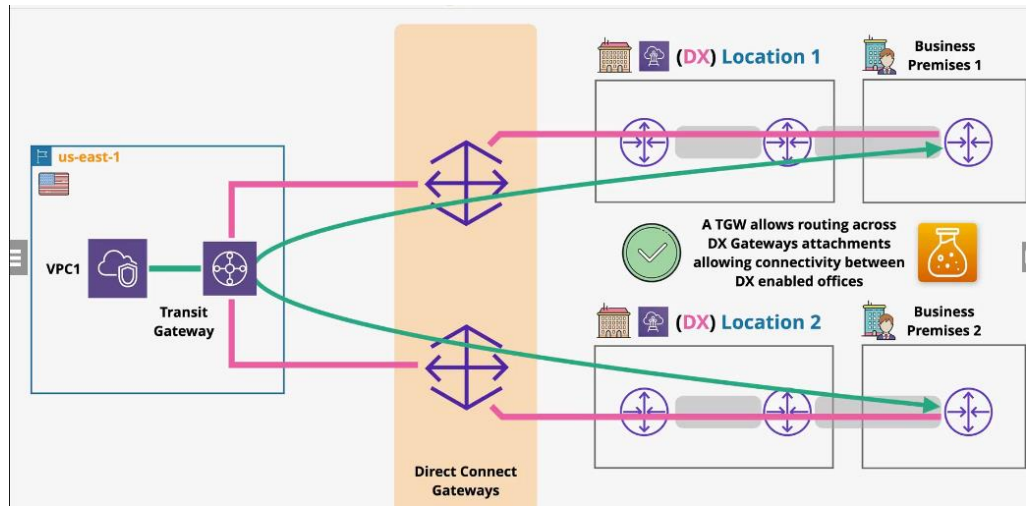


Рисунок 1.6 – Схема маршрутизації мережі з використанням AWS Direct Connect

На схемі зображено дві DX локації, які з'єднуються з віртуальним приватним хмарним середовищем (VPC1) через TGW. Транзитний шлюз дозволяє маршрутизувати трафік між шлюзами Direct Connect, забезпечуючи підключення між офісами, які використовують Direct Connect.

1.4 BGP Communities та Bidirectional Forwarding Detection у Direct Connect

Протокол Bidirectional Forwarding Detection (BFD) з AWS Direct Connect використовується для покращення часу аварійного перепідключення в мережі. Чим менший час переключення, тим краще для стабільності з'єднань. BFD працює через механізм BGP keep-alives, які налаштовані на 30-секундні інтервали. Ці сигнали дозволяють мережевому обладнанню визначати, чи активне з'єднання[3].

Є таймер затримки (hold-down timer), який починає відлік з нуля і рахує до 90 секунд. Кожен успішно отриманий keep-alive сигнал скидає цей таймер до нуля. Якщо таймер досягає 90 секунд, VIF вважається

недоступним. Такий період у 90 секунд є досить значним часом для систем автоматизації і мереж, оскільки він може вплинути на продуктивність і доступність сервісів. Використання BFD з Direct Connect допомагає зменшити потенційні простої в роботі мережі, швидко ідентифікуючи проблеми з з'єднанням та ініціюючи аварійне переключення у разі відмови[18].

Використання протоколу BFD разом із AWS DX можна значно покращити час реагування на проблему зі з'єднанням, забезпечуючи відновлення менше ніж за секунду. Інтервал реагування на проблему в BFD на AWS встановлений на 300 мілісекунд. Застосовуючи множник реагування на проблему BFD, який дорівнює числу 3 за замовчуванням, загальний час виявлення проблеми з підключенням можна скоротити до 900 мілісекунд[20].

VIFs за замовчуванням налаштовані на використання BFD, що дозволяє швидко виявляти та реагувати на проблеми з'єднання. Тим не менш, від клієнта вимагається конфігурація з його боку, включаючи налаштування BGP, для повної інтеграції з BFD. Ці налаштування забезпечують, що в разі відмови шляхи маршрутизації можуть бути швидко оновлені, щоб зменшити перерви в мережевому з'єднанні.

Наступник кроком в покращенні маршрутизації в DX є BGP Communities. BGP Communities є потужним механізмом для управління маршрутами в мережевій інфраструктурі. Це додаткові метадані у вигляді міток чи тегів, які прикріплюються до оголошених префіксів, надаючи можливість гнучкого управління політиками маршрутизації.

BGP Communities можуть бути загальновідомими та визначеними, включаючи директиви, такі як NO_EXPORT, що інструктує не оголошувати маршрут зовнішнім піринговим вузлам, та NO_ADVERTISE, яке забороняє оголошення маршруту будь-яким піринговим вузлам.

Звичайні спільноти BGP представлені 32-бітним значенням, яке розділене на два 16-бітних блоки. Ці значення зазвичай представлені у

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

формі "AS_NUMBER:OPERATOR_ASSIGNED_VALUE", де AS_NUMBER - це номер автономної системи, а OPERATOR_ASSIGNED_VALUE - це значення, призначене оператором. Наприклад, 7224:9100 або 7224:8100[24].

Оператори BGP, чи то зі сторони користувача, чи AWS, можуть вживати дій згідно із політиками, заснованими на спільнотах BGP. Це дозволяє управляти маршрутизацією на більш точному рівні, зокрема визначати, як маршрути будуть оголошуватися та прийматися у мережі.

BGP Communities використовуються для гнучкого управління маршрутизацією в рамках ASN. За допомогою BGP Communities можна контролювати "як далеко" AWS буде оголошувати маршрути користувачів. Це надає можливість адміністраторам BGP визначати правила для обробки вхідних оголошень префіксів на основі тегів спільнот BGP.

Завдяки цим тегам, адміністратори мають змогу впливати на рішення прийняття або відхилення префіксів, що приходять від зовнішніх пірів. Наприклад, вони можуть використовувати такі спільноти, як "Local Preference", для вказівки маршрутизаторам, які маршрути мають перевагу при обробці.

Ці налаштування дозволяють не лише оптимізувати мережевий трафік всередині однієї автономної системи, а й впливати на рішення інших автономних систем щодо вибору шляхів маршрутизації до вашої мережі. Окрім управління рекламуванням маршрутів, BGP Communities можуть бути використані для ряду інших цілей, зокрема для налаштування політик маршрутизації на основі географічного розташування, забезпечення безпеки та оптимізації продуктивності[25].

1.5 Надійність та резервування. Link Aggregation Groups (LAGs) у Direct Connect

Концепція LAG (Link Aggregation Group) дозволяє об'єднувати кілька фізичних з'єднань у єдине логічне з'єднання, що збільшує пропускну здатність. Наприклад, можна створити LAG із двома портами по 100 Гбіт/с

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

або з чотирма портами, кожен з яких менше 100 Гбіт/с, утворивши агрегацію до 200 Гбіт/с. Усі порти в LAG мають працювати на однаковій швидкості та бути підключеними до однієї точки. Хоча LAG забезпечує певний рівень відмовостійкості, AWS не рекламує цю функціональність як основний спосіб забезпечення високої доступності, але як засіб для захисту від збоїв окремих кабелів чи портів. Параметр "minimumLinks" визначає мінімальну кількість з'єднань, які повинні залишатися активними для роботи LAG[13].

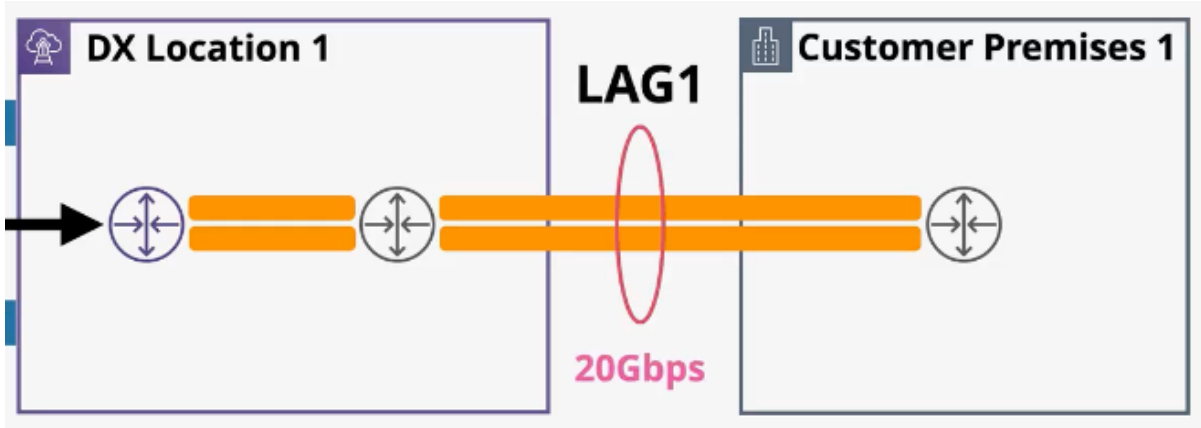


Рисунок 1.6 – Link Aggregation Group

Наявність з'єднання Direct Connect від локальної мережі до AWS не гарантує, що це з'єднання буде працювати завжди. AWS регіони мають кілька DX локацій, як правило, у великих міських центрах. Ці локації з'єднані з AWS регіонами через резервовані високошвидкісні канали. У кожній DX локації розміщений AWS DX Router, до якого підключається клієнт при купівлі DX з'єднання. Там же можна знайти маршрутизатор клієнта або провайдера. Стандартно, одне крос-підключення з'єднує порт DX із маршрутизатором клієнта або провайдера. DX також забезпечує зв'язок від DX локації до інфраструктури клієнта.

Потенційною єдиною точкою відмови є: DX локація, DX Router, крос-підключення, маршрутизатор клієнта, медіаконвертер (якщо використовується), приміщення клієнта та мережеве обладнання клієнта. За замовчуванням, DX не є відмовостійким. Це продукт, який залежить від багатьох фізичних компонентів, які можуть бути взаємозалежними. Якщо

мережеве з'єднання між AWS та локальним дата-центром є дійсно критичним, тоді вам також слід спроектувати високу доступність з'єднань Direct Connect[22].

Найпростіший приклад, коли у вас є одне з'єднання DX між AWS та локальним дата-центром. Якщо ви обмежені в коштах і немає можливості мати друге з'єднання DX, тоді, можливо, краще скористатися простішим рішенням -VPN як резервний зв'язок. Отже, якщо з'єднання DX зазнає збою, тоді трафік може йти через VPN. VPN трафік йде через інтернет, що також означає, що не можна отримати таку ж пропускну здатність і затримку через VPN. Отже, це означає більші затримки, ніж у DX, і, можливо, з'єднання не буде таким стабільним, оскільки використовує Інтернет.

Архітектура (рисунок 1.7) використовує кілька пристроїв як у місцях прямого підключення, так і в інфраструктурі підприємства замовника. Єдині точки відмови – це місце розташування DX, приміщення замовника та потенційний шлях розширення каналу зв'язку. При створенні з'єднання DX можна попросити AWS скористатися іншим маршрутизатором. І навіть якщо цього не вказати, AWS завжди спробує знайти інший пристрій AWS для побудови вашого другого з'єднання, тому що вже є відповідність між вашими з'єднаннями та пристроями AWS, які використовуються в місці розташування DX. Але знову ж таки, якщо подивитися на місце розташування Direct Connect, то воно все ще використовує тільки одну локацію.

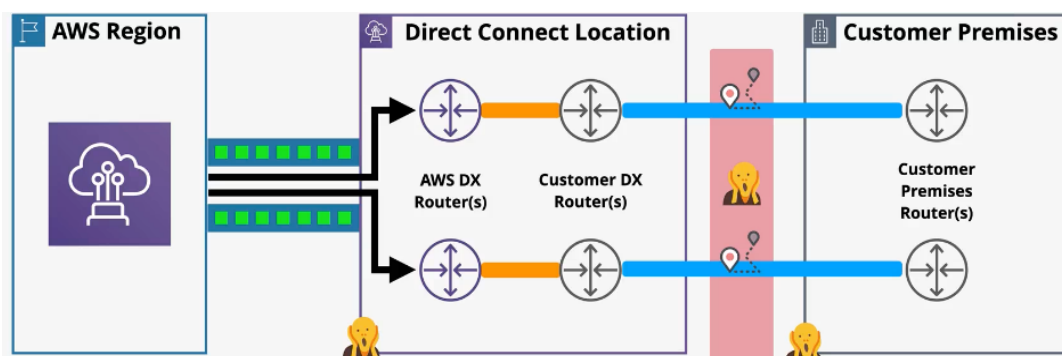


Рисунок 1.7 – Архітектурна схема підключення AWS Direct Connect з однією локацією

Щоб уникнути збоїв на рівні локацій, розглядається варіант використання двох локацій Direct Connect. Одне з'єднання розташоване в першій локації Direct Connect, а друге - у другій. Така структура краща, ніж попередня, оскільки вона може витримати відмову однієї з локацій Direct Connect, забезпечуючи вищу відмовостійкість.

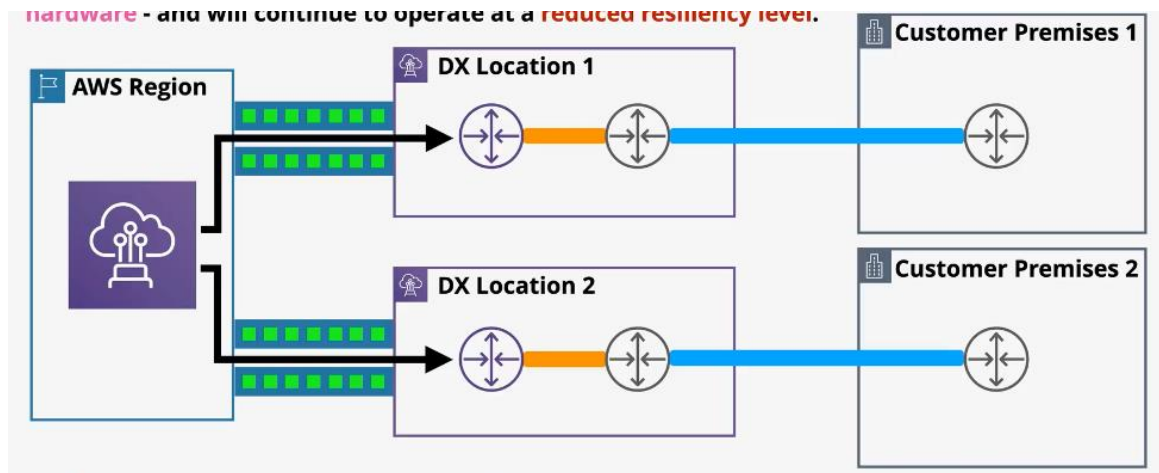


Рисунок 1.8 – Архітектурна схема підключення AWS Direct Connect з двома локаціями

У сценарії з особливо важливими робочими навантаженнями важливо мати надлишковість, включаючи дві локації Direct Connect, кожна з яких має два пристрої для завершення з'єднань Direct Connect. Це найбільш відмовостійка конфігурація, яку AWS рекомендує для критичних робочих навантажень.

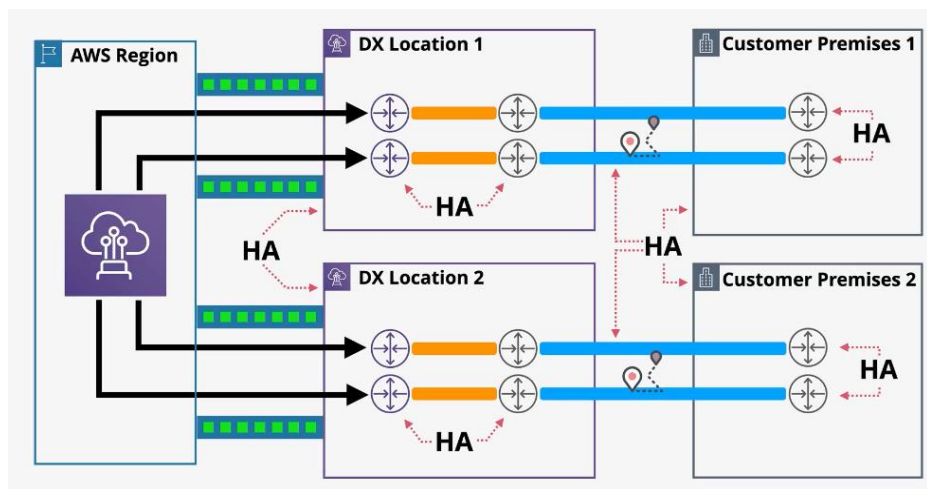


Рисунок 1.9 – Архітектурна схема підключення AWS Direct Connect з двома локаціями

На рисунку 1.9 показано, як реалізовано високу доступність (HA) у конфігурації AWS Direct Connect через дві окремі локації - DX Location 1 і DX Location 2. Це забезпечує резервування та відмовостійкість з'єднань між AWS регіоном та інфраструктурою підприємства.

Потрібно вирішити, який тип робочих навантажень наявний, чи можуть вони витримати збої мережі, який час відновлення даних очікується і які фінанси потрібні на використання кількох з'єднань DX. І слід пам'ятати, що DX не є відмовостійкою технологією, якщо ви не спроектували її відповідним чином.

Висновки до першого розділу

У цьому розділі було проведено аналіз теоретичних аспектів AWS Direct Connect, які становлять основу для подальшого дослідження та впровадження з'єднань з хмарною інфраструктурою. Досліджено ключові концепції AWS Direct Connect та отримано загальне уявлення про цей сервіс, його призначення та можливості.

Розглянуто різні типи віртуальних інтерфейсів (VIF) та їх функціональність, що дозволяє визначити відповідність конкретних вимог інфраструктури. Детально розглянуто концепції Direct Connect Gateway та Transit VIF, їхню роль у підключенні різних регіонів та мереж.

Описано використання BGP Communities та Bidirectional Forwarding Detection в AWS Direct Connect для забезпечення надійності та безпеки з'єднання. Розглянуто питання надійності, резервування та використання Link Aggregation Groups (LAGs) для підвищення доступності з'єднань.

Досліджено поняття, необхідні для подальшого проектування, реалізації та аналізу з'єднань з AWS Direct Connect. Отримані відомості будуть корисними для подальших практичних застосувань.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

РОЗДІЛ 2 РОЗРОБКА ТА ВПРОВАДЖЕННЯ АРХІТЕКТУРИ ПІДКЛЮЧЕННЯ ДО DIRECT CONNECT

2.1 Процедура встановлення Direct Connect

Процес встановлення з'єднання Direct Connect розпочинається в спеціалізованому місці, відомому як DX Location, яке оснащено обладнанням AWS, а також обладнанням клієнта чи провайдера. Це важливо підкреслити, що саме Amazon Web Services не володіє цими місцями розташування; натомість, компанія орендує необхідне простір у колокейшн-центрах. Встановлення з'єднань у таких місцях виконується виключно персоналом дата-центру, і для цього потрібна авторизація від усіх зацікавлених сторін. Ключовим елементом у процедурі авторизації є Letter of Authorization Customer Facility Access (LOA-CFA), документ, який надає офіційне дозвіл на доступ та встановлення з'єднань необхідного обладнання, що гарантує дотримання всіх процедур безпеки та протоколів управління.

Кроки підключення наступні:

1. Клієнт подає запит на підключення DX в місці розташування DX.
2. Порт DX виділяється на маршрутизаторі AWS DX.
3. Клієнт завантажує LOA-CFA (Лист дозволу та форму доступу до об'єктів клієнта).
4. Клієнт завершує запит до дата-центру на крос-підключення та надає LOA-CFA.
5. Персонал дата центру забезпечує крос-підключення від AWS маршрутизатора до обладнання клієнта або провайдера.
6. Фізичний рівень 1 тепер активний.

Перед тим, як персонал дата-центру може виконати будь-які дії, необхідно забезпечити строгий контроль доступу та відповідність усім вимогам безпеки. Це гарантує, що лише авторизований персонал має доступ до обладнання та інфраструктури.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

AWS забезпечує технічну підтримку протягом усього процесу встановлення з'єднання. Це включає консультації з клієнтами щодо оптимальної конфігурації та найкращих практик.

Такий підхід до підключення забезпечує високий рівень надійності та безпеки, що є критично важливим для бізнес-операцій, які залежать від хмарних технологій.

2.2 Побудова архітектури

Перед початком розробки архітектури необхідно визначити основні вимоги до підключення. До них відносяться пропускна здатність, затримки, вимоги до безпеки, а також потреби у високій доступності. Розуміння цих параметрів є ключовим для вибору оптимальної конфігурації.

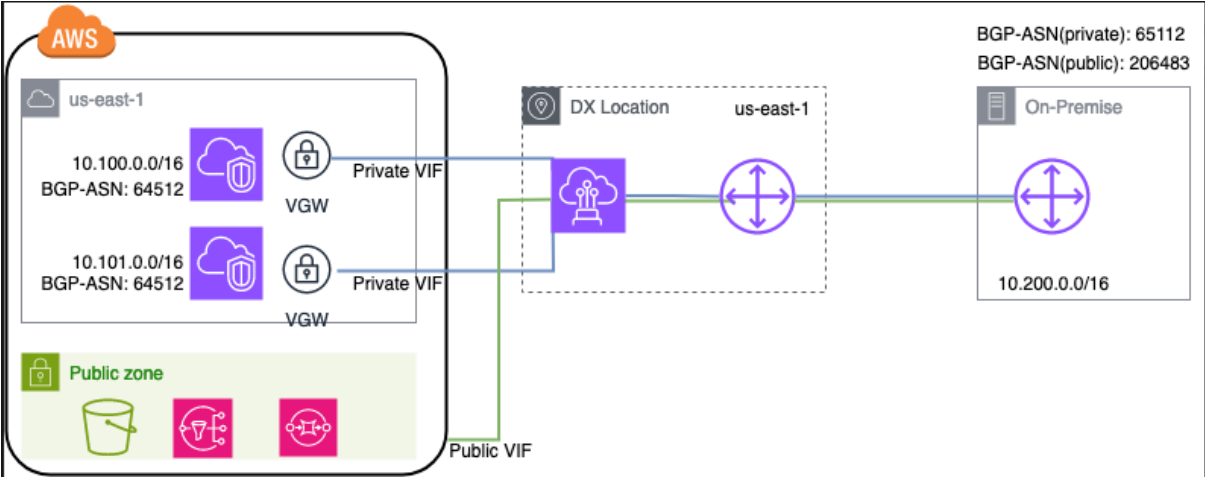


Рисунок 2.1 – Архітектура гібридного підключення з AWS Direct Connect

На діаграмі зображено, як буде використовуватися AWS DX для інтеграції локальної інфраструктури ІТ-підприємства з хмарними ресурсами у AWS регіоні us-east-1. Показано два приватних віртуальних інтерфейси, які забезпечують підключення до віртуальних приватних шлюзів (VGW) для окремих IP-діапазонів, та один публічний віртуальний інтерфейс, що підключається до публічної зони AWS. Використання автономних систем (ASN) для приватного і публічного зв'язку дозволяє налаштувати

маршрутизацію за допомогою BGP для забезпечення зв'язності між різними середовищами.

Таблиця 2.1. Схема адресацій та номер ASN для першої схеми

Region	Префікс	BGP-ASN	Тип інтерфейсу
us-east-1	10.100.0.0/16	65112	Private VIF
us-east-1	10.101.0.0/16	65112	Private VIF
Global	AWS Public IP	7244	Public VIF
On-premise	10.200.0.0/16	206483	Public VIF

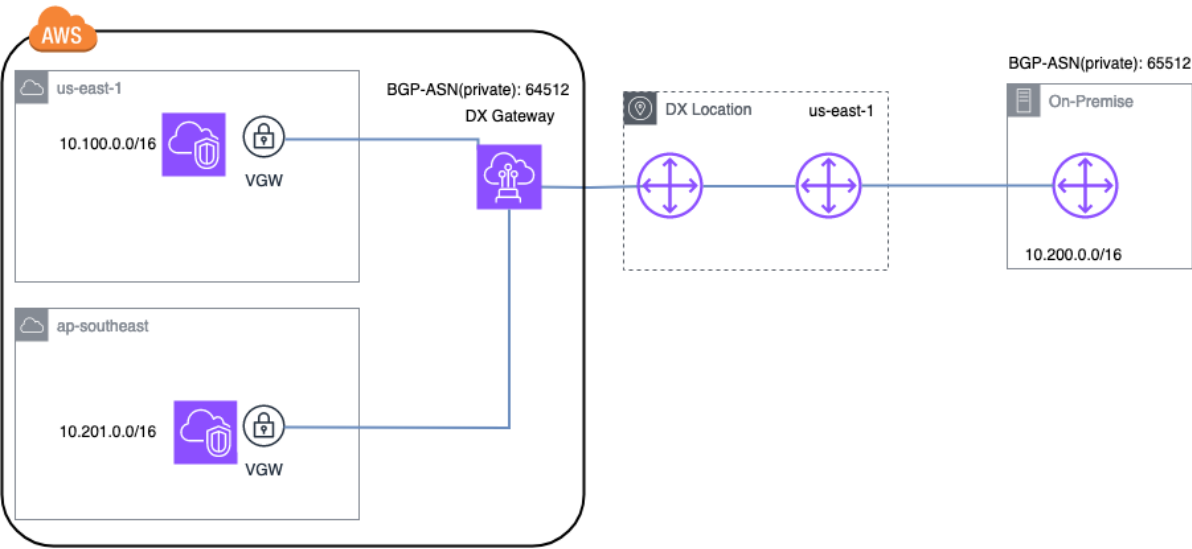


Рисунок 2.2 – Архітектура гібридного підключення з AWS Direct Connect з використанням DX Gateway

Архітектура з DX Gateway(рисунок 2.2) описує розгортання мережі з використанням AWS DX для забезпечення приватного з'єднання між корпоративною інфраструктурою та хмарними середовищами AWS у двох регіонах: us-east-1 та ap-southeast. Кожен з AWS VPC має VGW.

DX Gateway використовується як центральна точка для маршрутизації трафіку між цими VPC та корпоративною мережею. В DX Gateway призначений приватний ASN 64512 для BGP сесій з VPC, в той час як on-premise обладнання має приватний ASN 65512.

On-premise мережа має свій CIDR блок 10.200.0.0/16 і з'єднана з AWS через DX Location у регіоні us-east-1. Маршрутизація трафіку між цими мережами керується за допомогою BGP, дозволяючи обмін маршрутами та забезпечуючи необхідну зворотну сумісність із корпоративними мережевими політиками.

Опишемо необхідні дані у вигляді таблиці:

Таблиця 2.2. Схема адресацій та номер ASN для другої семи

Region	Префікс	BGP-ASN	Тип інтерфейсу
us-east-1	10.100.0.0/16	-	Private VIF
us-east-1	10.101.0.0/16	-	Private VIF
DX Gateway	-	64512	
On-premise	10.200.0.0/16	206483	Public VIF

У цьому розділі було розглянуто комплексну структуру архітектури Direct Connect для інтеграції корпоративної інфраструктури з хмарними послугами AWS. Ці зусилля сприяють створенню міцної основи для подальшої цифрової трансформації та впровадження інноваційних хмарних рішень у бізнес-операціях підприємства.

2.3 Безпека та шифрування у AWS Direct Connect

AWS Direct Connect — це приватне з'єднання між AWS і локальним дата-центром. Це означає, що від місця прямого підключення до вашого дата-центру існує виділена лінія. AWS гарантує, що порти, призначені для конкретного клієнта, належать саме цьому клієнту .

Важливо відзначити, що трафік, який передається через пряме з'єднання, за замовчуванням не шифрується, на відміну від VPN, де всі пакети зашифровані. Це означає, що якщо вам потрібне шифрування, ви повинні самостійно налаштувати його. Залежно від рівня, на якому ви хочете зашифрувати трафік, ви можете використовувати різні методи[14].

Якщо вам потрібно зашифрувати трафік на третьому рівні OSI, ви можете використовувати VPN через пряме з'єднання. Це може здатися

незвичайним, але це ефективний спосіб забезпечити безпеку. Для шифрування на другому рівні раніше не було можливостей, але тепер AWS пропонує MACSec, що дозволяє шифрувати трафік на цьому рівні. Якщо вам потрібно зашифрувати трафік на більш високому рівні, наприклад, четвертому, можна використовувати TLS для шифрування трафіку.

Важливо пам'ятати, що для шифрування третього рівня можливо налаштувати VPN через публічний VIF (Virtual Interface). Публічні IP-адреси на обох кінцях з'єднання дозволяють формувати VPN через інтернет. На стороні AWS це можна реалізувати через віртуальний приватний шлюз або транзитний шлюз, який має власні публічні IP-адреси. Таким чином, можна налаштувати IPsec-тунелі, використовуючи публічну IP-адресу VGW або транзитного шлюзу.

MACSec, як правило, працює на другому рівні і доступний тільки для виділених з'єднань. Це порівняно нова функція, і вона може не бути доступна в усіх місцях прямого підключення. MACSec використовується стандарт IEEE 802.1 і забезпечує конфіденційність даних, цілісність і автентичність походження даних. Це важливо для забезпечення безпеки з'єднання. Перешкоджає можливості зломисників перехопити та повторно передати кадри. Крім того, MACSec потрібно активувати на обох кінцях з'єднання, і на стороні AWS, і на стороні маршрутизатора клієнта.

Шифрування відбувається в кожному сегменті між двома пристроями, що гарантує безпеку даних на кожному кроці передачі. Включає 16-байтовий тег MACsec та 16-байтову суму для перевірки цілісності (Integrity Check Value, ICV).

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		29

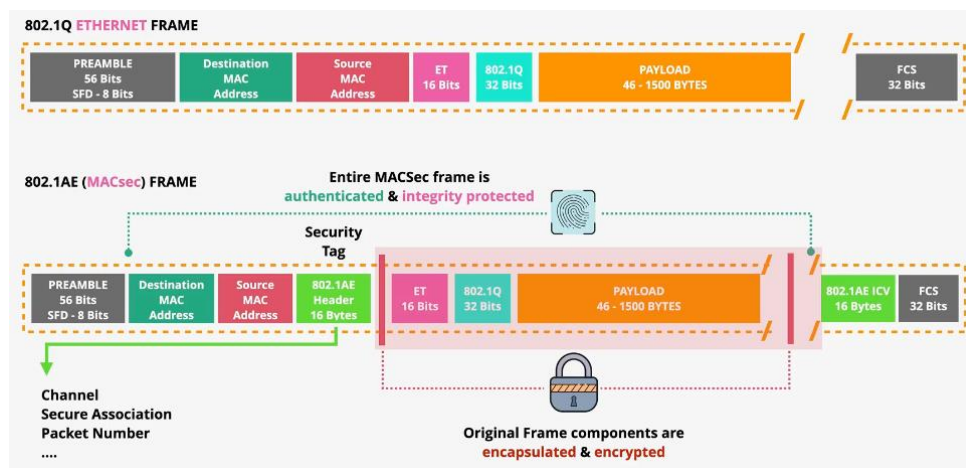


Рисунок 2.3 – Порівняння структур кадрів Ethernet та MACsec[15]

Завдяки цим характеристикам MACsec є потужним інструментом для забезпечення безпеки даних у великомасштабних мережах з високою пропускнуою здатністю, таких як терабітні мережі. Однак MACsec вимагає підтримки на обладнанні як з боку AWS, так і з боку клієнта.

Таким чином, для безпеки прямого з'єднання існує кілька варіантів шифрування трафіку. Найпоширеніший вибір — це шифрування на четвертому рівні за допомогою протоколів вищого рівня, таких як HTTPS, що використовують протокол транспортного рівня. Для шифрування на третьому або другому рівнях можна використовувати IPSec VPN або MACsec відповідно. Ці методи забезпечують додатковий рівень безпеки для трафіку, який передається через пряме з'єднання.

2.4 Ціноутворення AWS Direct Connect

В даному розділі розглянемо ключові аспекти ціноутворення AWS Direct Connect, які часто сприймаються як складні через включення численних компонентів та можливість використання декількох облікових записів. Розглянемо детально структуру витрат, щоб ясно визначити, які витрати несуть користувачі при використанні цієї послуги.

Плата погодинно за використання порта. Залежить від пропускнуої здатності з'єднання Direct Connect. Ця плата стягується незалежно від того, чи використовується з'єднання, і залежить від швидкості з'єднання (1 Гбіт/с чи 10 Гбіт/с). Вартість може варіюватися в залежності від того, чи є

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

з'єднання виділеним або розміщеним на хостингу. Відображає вартість передачі даних із AWS до локальної мережі або точки Direct Connect [21].

Важливо, що за передачу даних на вхід плата не стягується. У випадку виділених з'єднань, плата за порт-годину є фіксованою і застосовується, як тільки з'єднання стає доступним. Вартість залежить від пропускну здатності та регіону розташування AWS Direct Connect. Відповідальність за оплату за порт-годину лежить на обліковому записі, що запитав з'єднання. Це стосується як виділених, так і хостингових з'єднань[22].

Port hours: Dedicated Connections

Port hour pricing for dedicated connections is consistent across all AWS Direct Connect locations globally, except in Japan. The table below lists the port hour price by dedicated connection capacity selected.

Capacity	Port hour rate (Excluding Japan)	Port hour rate in Japan
1 Gbps	\$0.30/hour	\$0.285/hour
10 Gbps	\$2.25/hour	\$2.142/hour
100 Gbps	\$22.50/hour	\$22.50/hour

Рисунок 2.4 – Ціна за порт погодинно для dedicated з'єднань

За передачу даних на вхід не стягується плата. Вартість передачі даних назовні залежить від регіону джерела AWS. Наприклад, тариф за передачу даних з регіону, що не є Вірджинією, до Лас-Вегаса становить \$0.02 за гігабайт. Зазвичай, плата за передачу даних назовні покладається на обліковий запис, якому належить ресурс, що відправляє трафік.

To Direct Connect Location in: ↓↓↓↓	Data transfer from AWS Region or Local Zone											
	United States*	Canada	Europe	Asia Pacific (Tokyo, Osaka)	Asia Pacific (Seoul, Singapore, Hong Kong, Bangkok)	Asia Pacific (Indonesia)	Asia Pacific (Manila)	Asia Pacific (India)	South America (Sao Paulo, Mexico)	Asia Pacific (Australia, Auckland)	Middle East (Bahrain, Israel, UAE)	Africa (Cape Town, Lagos)
	United States	\$0.0200	\$0.0200	\$0.0282	\$0.0900	\$0.0900	\$0.1062	\$0.1062	\$0.0850	\$0.1500	\$0.1300	\$0.1100
	Canada	\$0.0200	\$0.0200	\$0.0300	\$0.0900	\$0.0900	\$0.1062	\$0.1062	\$0.0850	\$0.1500	\$0.1300	\$0.1100
	Europe	\$0.0200	\$0.0300	\$0.0200	\$0.0600	\$0.0900	\$0.1062	\$0.1062	\$0.0850	\$0.1107	\$0.1300	\$0.1000
	Japan	\$0.0491	\$0.0500	\$0.0600	\$0.0410	\$0.0420	\$0.0547	\$0.0547	\$0.1132	\$0.1700	\$0.1132	\$0.1500
	Hong Kong SAR, Malaysia, S. Korea, Singapore & Taiwan, Bangkok	\$0.0491	\$0.0500	\$0.0600	\$0.0410	\$0.0410	\$0.0594	\$0.0594	\$0.1000	\$0.1700	\$0.1107	\$0.1500

Рисунок 2.5 – Вартість на передачу від AWS Direct Connect

При залученні кількох облікових записів AWS, важливо розуміти, хто відповідає за які витрати. Наприклад, якщо з'єднання належить одному

акаунту, а VIF — іншому, витрати за порт-годину оплачує власник з'єднання, тоді як витрати за передачу даних назовні залежать від власника ресурсу, який генерує трафік.

Важливо розуміти, що плата за порт-годину застосовується незалежно від того, чи активно використовується з'єднання. Оплата за порт-годину припиняється тільки після видалення з'єднання з облікового запису AWS. У випадку з хостинговими з'єднаннями, потрібно звернутися до партнера Direct Connect для відключення з'єднання для припинення виставлення рахунків.

Висновки до другого розділу

У цьому розділі було розглянуто ключові аспекти встановлення та використання AWS DX. Процес встановлення DX, який описано у підрозділі 2.1, підкреслює його простоту та ефективність у забезпеченні безперервного з'єднання між користувацькою інфраструктурою та хмарними послугами AWS.

У підрозділі 2.2 розглянуто створення архітектури для підключення, що є фундаментальним для оптимізації продуктивності та забезпечення масштабованості системи. Цей аспект особливо важливий для бізнесів, які прагнуть до розширення своїх мережевих можливостей з мінімальними затримками.

Безпека та шифрування, обговорені у підрозділі 2.3, відіграють критичну роль у захисті даних. DX забезпечує високий рівень безпеки, оскільки транзит даних відбувається через приватне з'єднання, мінімізуючи ризики, пов'язані з публічним Інтернетом.

Нарешті, у підрозділі 2.4 було розглянуто ціноутворення AWS DX. Важливо зазначити, що ціни залежать від використання та обраного типу з'єднання, що дозволяє користувачам оптимізувати витрати залежно від їх потреб.

Загалом, даний розділ забезпечує необхідних кроків для розробки та впровадження ефективної та безпечної архітектури підключення за

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		32

допомогою AWS DX. Ці знання є надзвичайно важливим для організацій, що бажають інтегрувати свої операції з хмарними послугами AWS, забезпечуючи при цьому високу продуктивність, безпеку та ефективність витрат.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		33

РОЗДІЛ 3 ПРАКТИЧНЕ ЗАСТОСУВАННЯ AWS DIRECT CONNECT

3.1 Заовлення з'єднання AWS Direct Connect через партнера

На веб-порталі партнера вибрано необхідний тип з'єднання для підключення. У цьому конкретному випадку, обрано сервіс AWS Direct Connect із налаштуванням одиночного з'єднання:

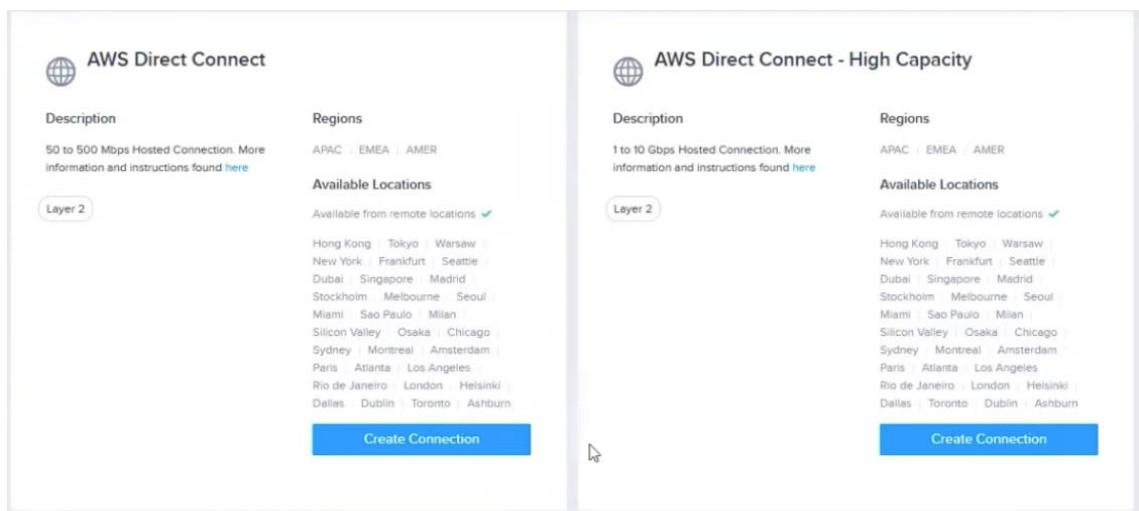


Рисунок 3.1 – Вибір типу підключення Direct Connect

На зображенні (рисунок 3.2) показано послідовність дій для підключення, починаючи з отримання інформації про акаунт Amazon у консолі управління AWS, створення з'єднання через Equinix Fabric, і завершуючи прийняттям з'єднання у консолі управління AWS або на панелі керування Equinix Fabric:

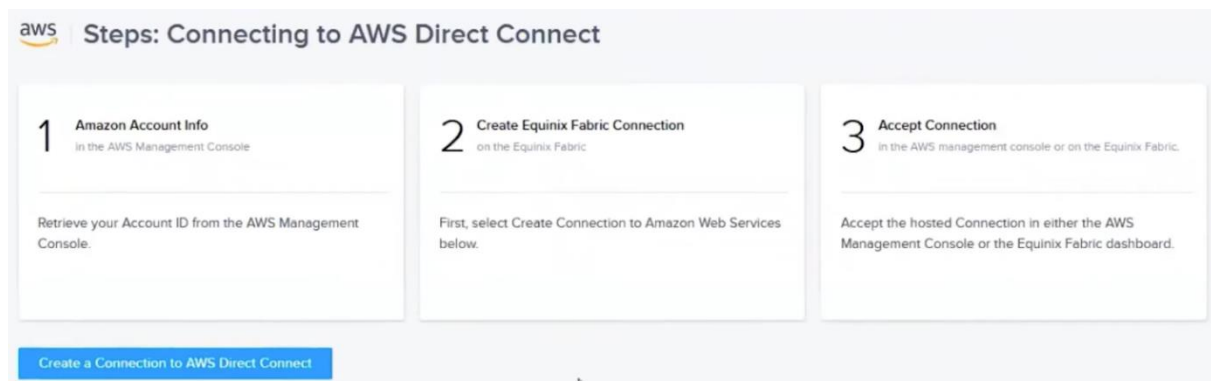


Рисунок 3.2 – Кроки підключення

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		34

Обрано порт та віртуальний пристрій Cisco. Знімок екрану демонструє інтерфейс користувача для замовлення AWS Direct Connect, де користувач вибирає локацію 'Chicago', тип віртуального пристрою та тип з'єднання 'Single Connection':

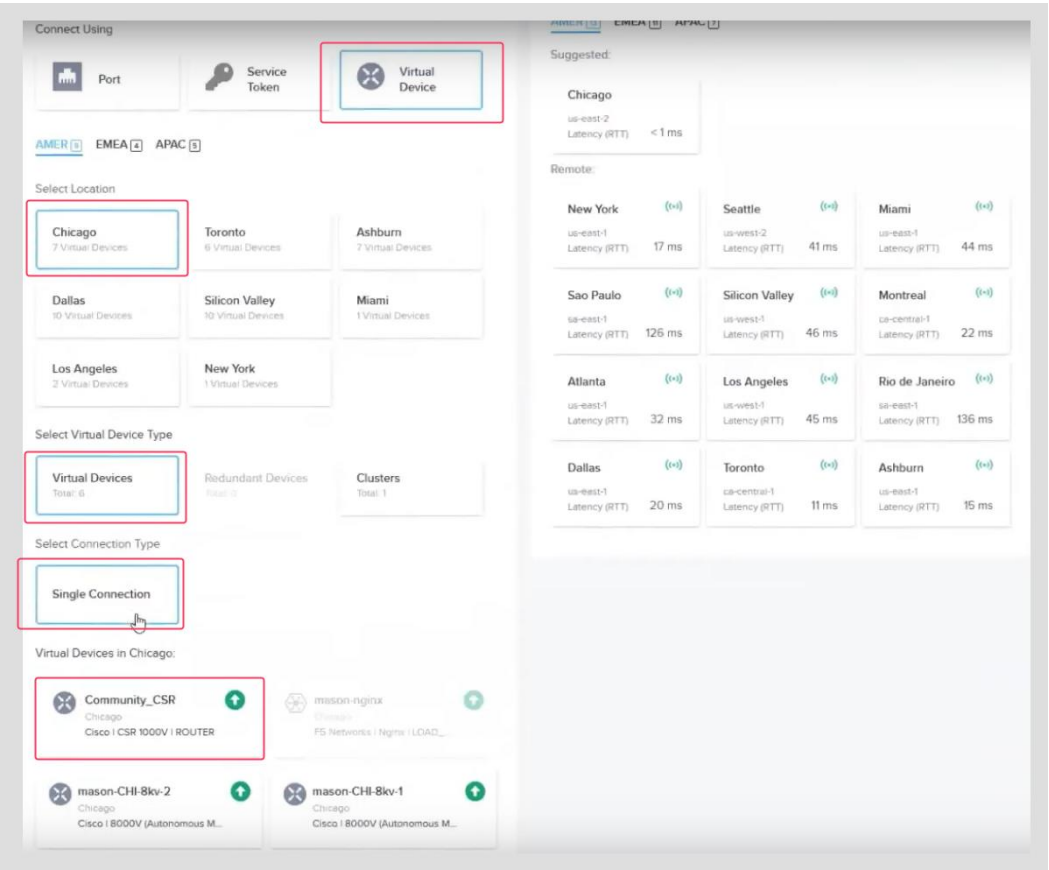


Рисунок 3.3 – Вибір параметрів підключення

Наступним кроком потрібно дати назву з'єднанню та вказати ID акаунту в якому планується створити з'єднання:

Connection Information

Virtual Connection Name:

Comm

AWS ACCOUNT ID

Рисунок 3.4 – Заповнення параметрів для створення з'єднання

Необхідно обрати відповідну швидкість з'єднання DX:

Connection Speed	
Billing Tier Up to 50 Mbps	50 Mbps Monthly Charge 75.00 USD Speed Selected
Billing Tier Up to 200 Mbps	100 Mbps Monthly Charge 100.00 USD Select Bandwidth
Billing Tier Up to 200 Mbps	200 Mbps Monthly Charge 100.00 USD Select Bandwidth
Billing Tier Up to 500 Mbps	300 Mbps Monthly Charge 150.00 USD Select Bandwidth

Рисунок 3.5 – Швидкість з'єднання

Кінцевий етап оформлення замовлення AWS DX, де вказані деталі підключення, включно з іменем з'єднання, швидкістю та вартістю. Користувач може перевірити всю інформацію, внести потрібні зміни, а потім підтвердити та оплатити замовлення:

Review [Open a Support Case](#)

Preview

Community_CSR Chicago — Speed 50 Mbps Latency (RTT) < 1 ms — AWS Amazon Web Services Chicago

Connection Summary	
Connection Name	Community_AWS
Virtual Device Name	Community_CSR
Speed	50 Mbps
Billing Tier	Up to 50 Mbps
Purchase Order Number	-
AWS ACCOUNT ID	██████████
Average last month latency	< 1 ms
Interface Name	GigabitEthernet5

Pricing Overview

Connection Monthly Charge **75.00 USD**

Additional taxes and/or fees may apply, depending on the Metro. Billing will begin when the Connection is provisioned.

[Design Summary](#)

Notifications 1 Recipient(s)

Enter email address(es) that will receive notifications about this Connection.

██████████

[Add Another Email](#)

[Previous](#) [Submit Order](#)

Рисунок 3.6 – Підтвердження замовлення

Після цього, протягом деякого часу в AWS Management Console з'явиться повідомлення, що DX Connection перебуває в стані замовлення.

Це означає, що з'єднання наразі обробляється та буде активовано після завершення всіх налаштувань."

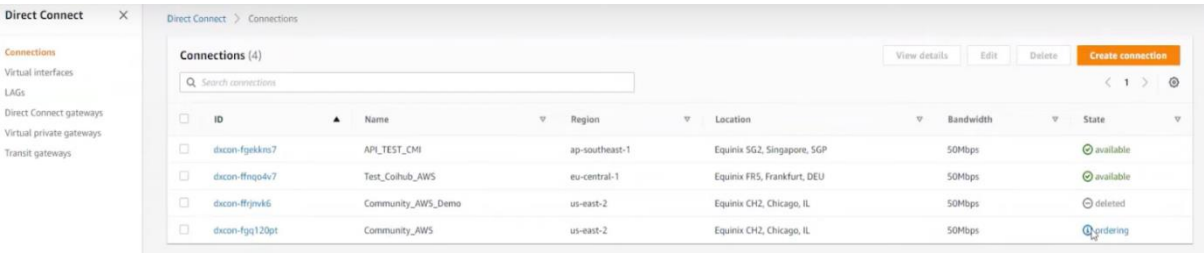


Рисунок 3.7 – AWS Management Console

Потрібно підтвердити з'єднання Direct Connect за допомогою CLI чи AWS Management Console:

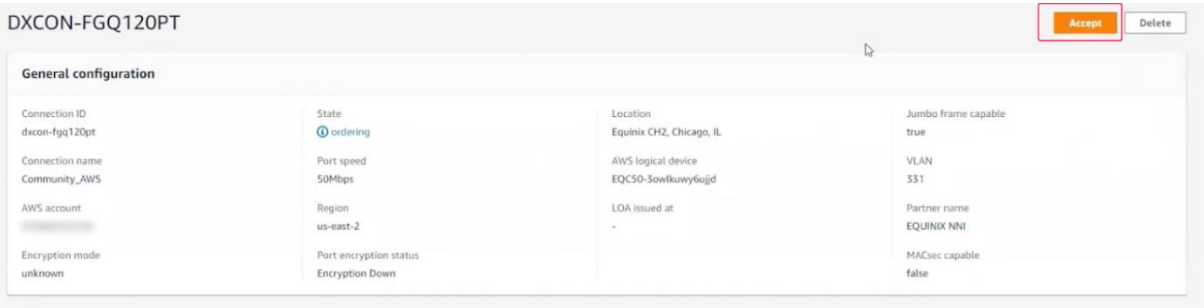


Рисунок 3.8 – Прийняття з'єднання

Після чого інтерфейс у AWS Management Console із деталями з'єднання, переходить в стан доступний. Це означає, що з'єднання успішно налаштовано і готове до використання у вказаній локації та з обраною швидкістю порту:

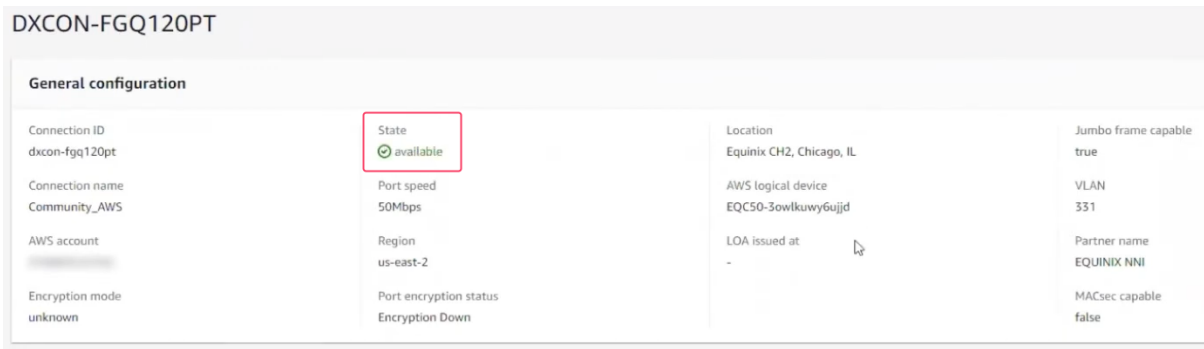


Рисунок 3.9 – Конфігурація DX з'єднання

Після активації фізичного з'єднання, можна приступити до створення віртуальних інтерфейсів, які дозволять ізолювати та керувати трафіком даних між корпоративними дата-центрами та ресурсами AWS.

3.2 Створення Private та Public Virtual Interface (VIF):

Під час створення Private Virtual Interface (Private VIF) для AWS Direct Connect, необхідно вказати наступні параметри:

- Тип з'єднання. Вибір між з'єднанням AWS DX або Link Aggregation Group (LAG).
- Тип VIF. Вказати, що це Private VIF.
- Назва VIF. Будь-яка назва за вашим вибором.
- Власник VIF. Ваш AWS акаунт або інший AWS акаунт, якщо це розміщений VIF (hosted VIF).
- Тип шлюзу:
 - a. Віртуальний приватний шлюз (Virtual Private Gateway)
 - b. Direct Connect Gateway
- Унікальний ID VLAN, який не дублюється на тому ж DX з'єднанні (в діапазоні 1-4094).
- BGP Peer IP адреси:
 - a. Для Public VIF (IPv4): Вказати публічні IP адреси, які ви використовуєте для сесії BGP.
 - b. Для Private VIF (IPv4): Вказати приватні IP адреси в діапазоні 169.254.0.0/16, які ви використовуєте для сесії BGP.
- BGP тип адрес. Вибір між IPv4 або IPv6. Amazon автоматично виділяє /125 IPv6 CIDR, користувач не може вказати свої власні IPv6 адреси.
- BGP ASN:
 - a. Публічний ASN: Має належати клієнту та бути присвоєним IANA (Internet Assigned Numbers Authority).
 - b. Приватний ASN: Може бути встановлений клієнтом та має бути в діапазоні від 64512 до 65534 (16-бітний) або від 1 до 2147483647 (32-бітний).
- BGP MD5 аутентифікаційний ключ:

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

а. Якщо клієнт не надасть ключ, AWS автоматично згенерує аутентифікаційний ключ для BGP сесії.

Створення приватного віртуального інтерфейсу, призначеного для з'єднання з Amazon VPC:

Virtual interface type

Type

☒ Private

A private virtual interface should be used to access an Amazon VPC using private IP addresses.

☐ Public

A public virtual interface can access all AWS public services using public IP addresses.

☐ Transit

A transit virtual interface is a VLAN that transports traffic from a Direct Connect gateway to one or more transit gateways.

Private virtual interface settings

Virtual interface name

A name to help you identify the new virtual interface.

babich-kim221-VIF

Name must contain no more than 100 characters. Valid characters are a-z, 0-9, and hyphens (-).

Connection

The physical connection on which the new virtual interface will be provisioned.

Sovereign-House-Six-Degrees

Virtual interface owner

The account that will own the virtual interface.

☒ My AWS account

☐ Another AWS account

Gateway type

Gateway type for this virtual interface.

☐ Direct Connect Gateway - recommended

Allows connections to multiple VPCs and Regions.

☒ Virtual Private Gateway

Allows connections to a single VPC in the same Region.

Virtual private gateway

A virtual private gateway attached to a VPC you wish to connect to.

platform-vgw

Virtual Local Area Network (VLAN)

The Virtual Local Area Network number for the new virtual interface.

2798

Valid ranges are 1 - 4094

BGP ASN

The Border Gateway Protocol (BGP) Autonomous System Number (ASN) of your on-premises router for the new virtual interface.

65100

Valid ranges are 1 - 2147483647.

Additional settings

Cancel

Create virtual interface

Рисунок 3.10 – Створення Private VIF в AWS Management console

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				39
Змн.	Арк.	№ докум.	Підпис	Дата		

Налаштування IP-адресації для віртуального інтерфейсу AWS:

▼ Additional settings

Address family - *optional*

Determines whether the virtual interface is created with an IPv4 or IPv6 peering.

☒ IPv4

☐ IPv6

Your router peer ip - *optional*

The BGP peer IP configured on your endpoint.

172.16.3.1/30

Amazon router peer IP - *optional*

The BGP peer IP configured on the AWS endpoint.

172.16.3.2/30

BGP authentication key - *optional*

The password that will be used to authenticate the BGP session.

my-secret-password

Рисунок 3.11 – Налаштування IP-адресації на Private VIF

Конфігурація маршрутизатора на IT-підприємстві для AWS Direct Connect з підтримкою BFD:

```
no ip redirect
bfd slow-timers 10000

conf t
int gi0/0/1.1300
bfd interval 300 min_rs 300 multiplier 3
description "Direct Connect to Amazon VPC"
encapsulation dot1q 2798
ip address 172.16.3.1 255.255.255.252

router bgp 65100
neighbor 172.16.3.2 remote-as 64512
neighbor 172.16.3.2 fall-over bfd
neighbor 172.16.3.2 password aQ434rsd45fafdsa
network 0.0.0.0
```

Рисунок 3.12 – Налаштування маршрутизатора підприємства

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				40
Змн.	Арк.	№ докум.	Підпис	Дата		

Згодом, після успішного налаштування та обміну префіксами Private VIF переходить в стан «доступний»:

ID	Name	Region	Connection ID	VLAN	Type	State
dvif-8py75m	connection-prod	ap-east-1	dccon-fg5m896r	2798	private	available

Рисунок 3.13 – Private VIF в AWS Management Console

Для налаштування Public VIF потрібно додатково вказати які префікси повинні оголошуватися до Amazon:

Your router peer ip
The BGP peer IP configured on your endpoint.

10.0.0.1/30

Amazon router peer IP
The BGP peer IP configured on the AWS endpoint.

10.0.0.2/30

Prefixes you want to advertise
The list of IP prefix CIDRs that you want to advertise to Amazon over this virtual interface, including the peer IPs.

192.0.20.0/28
192.0.2.28/30

Specify up to 100 prefixes, each separated with a comma. Or, put each prefix on separate lines.

Рисунок 3.14 – Private VIF в AWS Management Console

AWS перевіряє право власності на ці IP-префікси. Трафік повинен бути призначеним для публічних префіксів AWS. Транзитивна маршрутизація між з'єднаннями не підтримується. AWS також виконує фільтрацію вхідних пакетів, тобто приймає трафік тільки з анонсованих префіксів. Щодо вихідних політик публічного Wi-Fi, вони визначають, яким шляхом піде трафік з AWS до маршрутизатора клієнта, особливо коли існує кілька з'єднань Direct Connect. Пріоритет має найдовший відповідний префікс. Крім того, AWS також анонсує всі локальні та віддалені префікси регіонів у on-premise мережу.

Створений Public VIF:

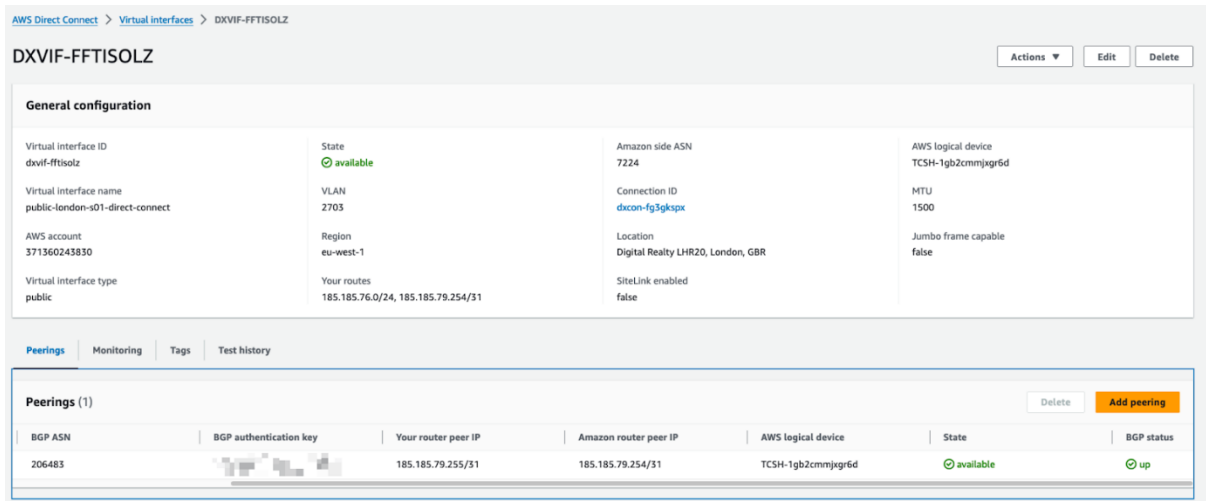


Рисунок 3.15 – Public VIF в AWS Management Console

3.3 Конфігурація DX Gateway та його налаштування

Створення нового шлюзу Direct Connect, який дозволяє забезпечити з'єднання з віртуальними приватними хмарами в різних регіонах AWS:

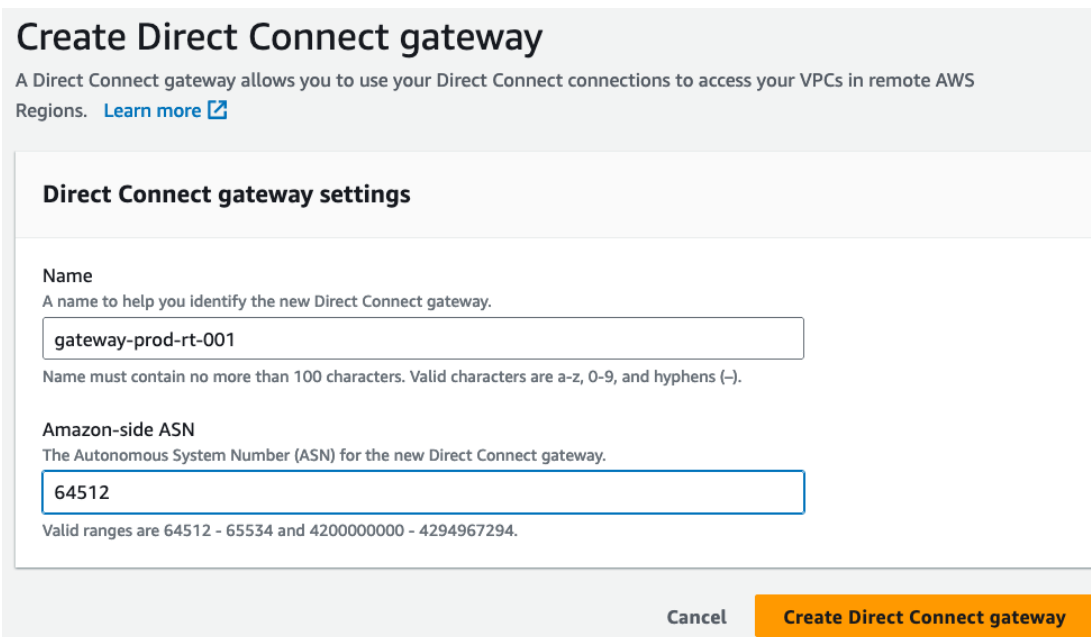


Рисунок 3.16 – Створення DX Gateway

Створений DX Gateway:



Рисунок 3.17 – Створення DX Gateway

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

Інтерфейс асоціації шлюзу в AWS, де користувач може вибрати вже наявний шлюз для асоціації з новим шлюзом Direct Connect. Також надається можливість обрати дозволені префікси IP-адрес, які можуть бути оголошені через Direct Connect шлюз, забезпечуючи контрольований доступ до ресурсів on-premises мережі:

Associate gateway

Association settings

Gateways
The gateway you want to associate with the new Direct Connect gateway.

My gateway ▼

You can only associate gateways of the same type to a Direct Connect gateway. Transit gateways and virtual private gateways attached to a VPC are available for selection.

Allowed prefixes - optional
List of prefixes you want to be allowed to be advertised to the on-premises network through the Direct Connect gateway.

192.0.20.0/28
192.0.2.28/30

Specify up to 200 prefixes, each prefix separated by a comma. Or, put each prefix on separate lines.

Cancel Associate gateway

Рисунок 3.18 – Асоціація DX GW з відповідними шлюзами

На зображенні (рисунок 3.19) представлено секцію 'Gateway associations' в AWS Management Console, яка показує два шлюзи, асоційовані з різними AWS регіонами. Кожен запис включає ідентифікатор шлюзу, регіон, AWS обліковий запис, дозволені префікси IP-адрес, та їх поточний стан, що підтверджує їх асоціацію та готовність до використання.

Virtual interface attachments

Gateway associations

Gateway associations (2)

Search gateway associations

Edit

Disassociate

Associate gateway

☐	ID	Region	AWS account	Allowed prefixes	State
☐	vgw-019b53439ccdb9aee	ap-southeast-1	371	103.73.187.0/26, 103.73.187.128/26, 103.7...	associated
☐	vgw-0ce082c2cad8a2077	ap-southeast-2	371	103.73.186.0/26, 103.73.186.128/26, 103.7...	associated

Рисунок 3.19 – Gateway associations в AWS Management Console

Розділ 'Virtual interface attachments' в AWS Management Console, де відображено два віртуальні інтерфейси, що були приєднані до DX GW. Кожен інтерфейс має унікальний ID, регіон розташування, ідентифікатор AWS облікового запису, а також стан, що вказує на їх успішне приєднання:

Virtual interface attachments					
Virtual interface attachments (2)		Search virtual interface attachments			
☐	ID	Region	AWS account	State	
☐	dxvif-ffgq2g16	ap-southeast-1	3713	attached	
☐	dxvif-ffpyj75m	ap-east-1	371	attached	

Рисунок 3.20 – Virtual interface attachments в AWS Management Console

3.4 Налаштування моніторингу для Direct Connect

Amazon CloudWatch є інтегрованим рішенням для моніторингу сервісів, що працюють на Amazon Web Services, та дозволяє користувачам отримувати і аналізувати ключові метрики в реальному часі. Для сервісу AWS Direct Connect, CloudWatch надає можливість стежити за станом з'єднання та його продуктивністю, що є критично важливим для підтримання безперебійності бізнес-процесів.

Метрики CloudWatch для Direct Connect дають змогу контролювати наступне::

- ConnectionState: 1 означає, що з'єднання активне, а 0 - що воно відключене.
- Параметри трафіку: є метрики для вихідного та вхідного трафіку (Egress та Ingress).
- Помилки: метрики, що вказують на кількість помилок на стороні обладнання AWS.
- Рівень сигналу: LightLevelTx та LightLevelRx для перевірки здоров'я оптичного зв'язку.
- Шифрування: якщо включено MACSec, можна відслідковувати стан шифрування з'єднання.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				44
Змн.	Арк.	№ докум.	Підпис	Дата		

Використовуючи ці метрики, можна встановити сповіщення в CloudWatch для реагування на зміни стану з'єднання та інші важливі параметри, що допоможе швидко реагувати на проблеми та оптимізувати продуктивність.

Metric

Edit

Graph

This alarm will trigger when the blue line goes below the red line for 1 datapoints within 5 minutes.

No unit

2

1

0

08:00

09:00

10:00

ConnectionState

Namespace

AWS/DX

Metric name

ConnectionState

ConnectionId

dxcon-fgcitu5j

Statistic

Average

Period

5 minutes

Conditions

Threshold type

Static

Use a value as a threshold

Anomaly detection

Use a band as a threshold

Whenever ConnectionState is...

Define the alarm condition.

Greater

> threshold

Greater/Equal

>= threshold

Lower/Equal

<= threshold

Lower

< threshold

than...

Define the threshold value.

1

Must be a number

Рисунок 3.21 – Створення сповіщення для відстеження стану з'єднання

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				45
Змн.	Арк.	№ докум.	Підпис	Дата		

3.5 Тестування та перевірка з'єднання Direct Connect на працездатність

Перевірка статусу 'available' з'єднань через AWS Management Console:

Connections (6)

Search connections

View details

Edit

Delete

☐	ID	Name	Region	Location	Bandwidth	State
☐	dxcon-fg5m896r		ap-east-1	Equinix HK1, Tsuen Wan, N.T., Hong ...	50Mbps	available
☐	dxcon-fg9auzn1x		ap-southeast-1	iAdvantage MEGA-i, Hong Kong, HK...	50Mbps	available
☐	dxcon-fg3gkspk		eu-west-1	Digital Realty LHR20, London, GBR	1Gbps	available
☐	dxcon-fgt5tk1u		eu-west-1	Equinix LDS, Slough, GBR	1Gbps	available
☐	dxcon-fgctusj		us-east-1	165 Halsey Street, Newark, NJ	300Mbps	available
☐	dxcon-fh7g9wgh		us-east-1	165 Halsey Street, Newark, NJ	300Mbps	available

Рисунок 3.22 – Вкладка Connections в AWS Management Console

Перевірка статусу 'available' віртуальних інтерфейсів через AWS Management Console:

Virtual interfaces (10)

Search virtual interfaces

View details

Edit

Delete

Actions

Create virtual interface

☐	ID	Name	Region	Connection ID	VLAN	Type	State
☐	devif-ffpj75m		ap-east-1	dxcon-fg5m896r	2798	private	available
☐	devif-ffgq2g16		ap-southeast-1	dxcon-fg9auzn1x	2797	private	available
☐	devif-fg35nqqs		eu-west-1	dxcon-fgt5tk1u	2701	private	available
☐	devif-fh9q0kk3		eu-west-1	dxcon-fgt5tk1u	2700	private	available
☐	devif-fftisolz		eu-west-1	dxcon-fg3gkspk	2703	public	available
☐	devif-fg2rx23d		eu-west-1	dxcon-fg3gkspk	2500	private	available
☐	devif-fg271yzh		eu-west-1	dxcon-fgt5tk1u	2702	public	available
☐	devif-fh4mtrkc		eu-west-1	dxcon-fgt5tk1u	2001	private	available
☐	devif-fhkaamr		us-east-1	dxcon-fgctusj	1000	public	available
☐	devif-fggw5gkt		us-east-1	dxcon-fh7g9wgh	1002	private	available

Рисунок 3.23 – Вкладка Virtual Interfaces в AWS Management Console

Вивід команди перегляду BGP маршрутів на маршрутизаторі підприємства:

```
LAB-SW-1# show ip bgp neighbors 169.254.249.5 received-routes vrf amandeeep

Peer 169.254.249.5 routes for address family IPv4 Unicast:
BGP table version is 6, local router ID is 10.200.0.200
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: i - IGP, e - EGP, ? - incomplete, l - multipath

  Network          Next Hop          Metric      LocPrf      Weight Path
* > e10.100.0.0/16  169.254.249.5              0 64512 i
```

Рисунок 3.24 – Вивід команди show ip bgp neighbors

Вивід команди перегляду BGP маршрутів, які оголошуються в AWS VPC:

```
LAB-SW-1# show ip bgp neighbors 169.254.249.5 advertised-routes vrf amandeep

Peer 169.254.249.5 routes for address family IPv4 Unicast:
BGP table version is 6, local router ID is 10.200.0.200
Status: s-suppressed, x-deleted, S-stale, d-dampened, h-history, *-valid, >-best
Path type: i-internal, e-external, c-confed, l-local, a-aggregate, r-redist
Origin codes: i - IGP, e - EGP, ? - incomplete, l - multipath

  Network          Next Hop          Metric    LocPrf    Weight Path
*>10.200.0.200/32   0.0.0.0           100       32768    i
*>169.254.249.4/30 0.0.0.0           100       32768    i
LAB-SW-1#
```

Рисунок 3.25 – Вивід команди show ip bgp neighbors

Активація автоматичного поширення маршрутів у клієнтській VPC з on-premise середовища через віртуальний приватний шлюз:

Routes	Subnet associations	Edge associations	Route propagation	Tags
Route Propagation (1)				
Find virtual private gateway				
Virtual Private Gateway				Propagation
vgw-019b53439ccdb9aee / prod-apse1-rt				Yes

Рисунок 3.26 – Route Propagation налаштування

Перегляд активних маршрутів у таблиці маршрутизації VPC, із зазначенням статусу та інформацією про поширення маршрутів.

Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (7)				
Filter routes				
Destination	Target	Status	Propagated	
0.0.0.0/0	vgw-0cc368908d0104423	Active	Yes	
5.180.190.176/28	local	Active	No	
5.180.190.208/28	local	Active	No	
10.0.0.0/8	vgw-0cc368908d0104423	Active	Yes	
10.204.0.0/16	local	Active	No	
38.105.217.176/28	local	Active	No	
38.105.217.208/28	local	Active	No	

Рисунок 3.27 – Таблиця маршрутизації з увімкненим Route Propagation налаштуванням

Завершення процесу перевірки працездатності AWS Direct Connect включає перевірку стану з'єднання через AWS Management Console, встановлення та моніторинг CloudWatch алармів для ключових метрик, та перегляд таблиць маршрутизації для забезпечення коректного маршрутизування трафіку між on-premise інфраструктурою та AWS. Це

гарантує, що з'єднання активне, дані безперебійно передаються, і можливі інциденти будуть швидко виявлені та вирішені.

Висновки до третього розділу

У розділі 3 було розглянуто практичне застосування AWS Direct Connect, що охоплює ключові етапи від замовлення з'єднання до його тестування. Зокрема, було висвітлено процес замовлення з'єднання через партнера, який включає вибір та налаштування Private та Public Virtual Interfaces для забезпечення безпечного і надійного з'єднання між корпоративною інфраструктурою та хмарними сервісами AWS.

Описано створення та конфігурацію DX Gateway, яка є важливою для управління трафіком і забезпечення його ефективного розподілу. Налаштування моніторингу через CloudWatch дозволяє відстежувати стан з'єднання та оперативно реагувати на будь-які зміни. Завершальний етап тестування та перевірки підтверджує працездатність з'єднання Direct Connect та його готовність до використання в продуктивному середовищі.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		48

ВИСНОВКИ

Було детально розглянуто ключові аспекти Direct Connect, включаючи віртуальні інтерфейси, Direct Connect Gateway, та важливість безпеки і надійності з'єднань. Проаналізовано ключові аспекти Direct Connect для розуміння його компонентів та функціональності.

Спроектовано архітектурне рішення підключення, з орієнтацією на безпеку, шифрування та оптимізацію витрат. Зосереджено увагу на розробці архітектури підключення. Було висвітлено критичні аспекти безпеки, шифрування, та економічні чинники, що впливають на вибір та реалізацію рішень.

Запропоновано практичні рекомендації та стратегії для ефективного використання AWS Direct Connect. Покращено взаємодію між корпоративними дата-центрами та хмарою AWS.

Оптимізовано процеси моніторингу та управління з'єднаннями для забезпечення стабільної та надійної роботи.

Підвищено ефективність хмарних рішень через оптимізацію взаємодії з AWS Direct Connect, надаючи цінний внесок у сферу хмарних обчислень та управління даними. Завдяки детальному аналізу, проектуванню, та практичному застосуванню, дана робота значно підвищує ефективність та оптимізацію взаємодії між корпоративними дата-центрами та хмарними сервісами AWS.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		49

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. AWS Direct Connect User Guide. Amazon Web Services, Inc. 120 p.
2. Networking to AWS: Best Practices and Design Patterns. AWS Whitepapers, Amazon Web Services, Inc. 90 p.
3. Hybrid Cloud Network Architecture: Implementing AWS Direct Connect". AWS Whitepapers, Amazon Web Services, Inc. 70 p.
4. Morris, K. AWS Networking Deep Dive: Elastic Load Balancing (ELB). Udemy Course.
5. Jackson, B. "Architecting for the Cloud: AWS Best Practices". AWS Whitepapers, Amazon Web Services, Inc. 82 p.
6. Rhoton, J. "Cloud Computing Explained: Implementation Handbook for Enterprises". Recursive Press, 2017. 350 p.
7. Adams, K. "AWS Certified Advanced Networking Official Study Guide: Specialty Exam". John Wiley & Sons, 2018. 550 p.
8. Golden, B. "Amazon Web Services for Dummies". For Dummies, 2019. 450 p.
9. Sbarski, P. "Serverless Architectures on AWS". Manning Publications, 2017. 320 p.
10. Wittig, M. & Wittig, A. "Amazon Web Services in Action". Manning Publications, 2015. 424 p.
11. Chapman, M. & Barrett, J. "AWS for Administrators for Dummies". For Dummies, 2017. 384 p.
12. AWS Certified Solutions Architect Official Study Guide: Associate Exam. John Wiley & Sons, 2017. 504 p.
13. Cole, M. & Palmer, A. "Practical AWS Networking". Packt Publishing, 2018. 246 p.
14. "Building a Scalable and Secure Multi-VPC AWS Network Infrastructure". AWS Whitepapers, Amazon Web Services, Inc. 130 p.
15. Vazquez, R. & Chapman, M. "AWS Networking Cookbook". Packt Publishing, 2017. 368 p.

		Бабіч Д. В.			<i>КІМ.КР.Б – 123 – 04 – ПЗ</i>	Арк.
		Бродський Ю. Б.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

16. AWS: Security Best Practices on AWS. AWS Whitepapers, Amazon Web Services, Inc. 65 p.
17. Alapati, S. "AWS Identity and Access Management (IAM) User Guide". Amazon Web Services, Inc. 250 p.
18. Turnbull, J. "The Art of Monitoring". James Turnbull, 2016. 600 p.
19. Implementing Network Security on AWS". AWS Whitepapers, Amazon Web Services, Inc. 95 p.
20. Sanjar, G. "AWS System Administration: Best Practices for Sysadmins in the Amazon Cloud". O'Reilly Media, Inc., 2018. 400 p.
21. AWS Direct Connect Billing and Pricing. Amazon Web Services, Inc. 20 p.
22. Brown, E. "AWS Disaster Recovery". Whitepaper, Amazon Web Services, Inc., 2016. 150 p.
23. Uchenna, C. "AWS Networking Fundamentals". Kindle Edition, 2019. 300 p.
24. Performance Tuning for AWS". Amazon Web Services, Inc. 200 p.
25. AWS Best Practices for DDoS Resiliency". AWS Whitepapers, Amazon Web Services, Inc. 75 p.

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

ДОДАТКИ

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Додаток А – Конфігураційний файл маршрутизатора ІТ-підприємства

Current configuration: 2115 bytes

```
interface GigabitEthernet0/1
! channel-group 1 mode passive (In case of a LAG connection)
no ip address

interface GigabitEthernet0/1.1300
! interface port-channel 1.1300 (In case of a LAG connection)
description "Direct Connect to your Amazon VPC or AWS Cloud"
encapsulation dot1Q 1300
ip address 198.1.2.1 255.255.255.252

router bgp 9000
address-family ipv4
neighbor 198.1.2.2 remote-as 64512
neighbor 198.1.2.2 password hellow-world
network 0.0.0.0
exit
```

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		53

Додаток В – Інфраструктура як код з використанням CloudFormation

AWS::TemplateFormatVersion: '2010-09-09'

Description: AWS Direct Connect with Public and Private VIFs and DX Gateway

Resources:

MyDirectConnect:

Type: 'AWS::DirectConnect::Connection'

Properties:

Bandwidth: '1Gbps'

Location: 'EqDC2'

ConnectionName: 'MyDXConnection'

MyPublicVIF:

Type: 'AWS::DirectConnect::VirtualInterface'

Properties:

ConnectionId: !Ref MyDirectConnect

VirtualInterfaceType: 'public'

VirtualInterfaceName: 'MyPublicVIF'

ASN: 12345

RouterPeerIP: '203.0.113.1'

AmazonAddress: '203.0.113.2'

AddressFamily: 'ipv4'

RouteFilterPrefixes:

- Cidr: '0.0.0.0/0'

MyPrivateVIF:

Type: 'AWS::DirectConnect::VirtualInterface'

Properties:

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		54

ConnectionId: !Ref MyDirectConnect
VirtualInterfaceType: 'private'
VirtualInterfaceName: 'MyPrivateVIF'
ASN: 12345
RouterPeerIP: '192.0.2.1'
AmazonAddress: '192.0.2.2'
AddressFamily: 'ipv4'
VirtualGatewayId: 'vgw-xxxxxxx'

MyDirectConnectGateway:

Type: 'AWS::DirectConnect::DirectConnectGateway'
Properties:
DirectConnectGatewayName: 'MyDXGateway'
AmazonSideASN: 64512

MyGatewayAssociation:

Type: 'AWS::DirectConnect::GatewayAssociation'
Properties:
DirectConnectGatewayId: !Ref MyDirectConnectGateway
AddAllowedPrefixesToDirectConnectGateway:
- Cidr: '10.0.0.0/16'
VirtualGatewayId: 'vgw-xxxxxxx'

Outputs:

DirectConnectId:
Description: The Direct Connect ID
Value: !Ref MyDirectConnect

		Бабіч Д. В.			КІМ.КР.Б – 123 – 04 – ПЗ	Арк.
		Бродський Ю. Б.				
Змн.	Арк.	№ докум.	Підпис	Дата		55

PublicVIFId:

Description: The Public Virtual Interface ID

Value: !Ref MyPublicVIF

PrivateVIFId:

Description: The Private Virtual Interface ID

Value: !Ref MyPrivateVIF

DirectConnectGatewayId:

Description: The Direct Connect Gateway ID

Value: !Ref MyDirectConnectGateway